O‘zbekiston Respublikasi
Raqamli texnologiyalar vazirligi

Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari
universiteti

O‘zbekiston Respublikasi
Ta’lim va ilm-fan vazirligi



“CYBERCRYPTUZ”

Respublika ilmiy-texnik konferensiyasi

Toshkent, 23-oktabr, 2026-yil

MA’RUZALAR TO‘PLAMI

TOSHKENT 2026

O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

O‘zbekiston Respublikasi Ta’lim va ilm-fan vazirligi

“CYBERCRYPTUZ”

Respublika ilmiy- texnik konferensiyasi
Toshkent, 23-oktabr, 2026-yil

MA’RUZALAR TO‘PLAMI

TOSHKENT 2026

KONFERENSIYA TASHKILIY QO‘MITASINING
T A R K I B I:

1.	MAXKAMOV B.SH.	Rais, rektor
2.	YAXSHIBAYEV D.S.	Yoshlar masalalari va ma’naviy-ma’rifiy ishlar bo‘yicha birinchi prorektor
3.	TO‘RAYEV SH.SH.	Ilmiy ishlar va innovatsiyalar bo‘yicha prorektor
4.	TASHEV K.A.	O‘quv ishlari bo‘yicha prorektor
5.	SULTANOV DJ.B.	Transformatsiya va xalqaro strategik rivojlantirish bo‘yicha prorektori
6.	TOSHMATOV S.Z.	Moliya-iqtisod ishlari bo‘yicha prorektor
7.	NASRULLAYEV N.B.	Kiberxavfsizlik fakulteti dekani
8.	HAYDAROV E.D.	Axborot xavfsizligi kafedrasi mudiri
9.	XUDOYKULOV Z.T.	Kriptologiya kafedrasi mudiri
10.	ALLANOV O.M.	Kiberxavfsizlik va kriminalistika kafedrasi mudiri
11.	MAXMUDJANOV S.U.	Sun’iy intellekt va innovatsion ekotizimni rivojlantirish bo‘limi boshlig‘i
12.	AMIROV A.A.	Bosh hisobchi
13.	JO‘RAYEV D.A.	Raqamli infratuzilmani rivojlantirish markazi boshlig‘i
14.	JOLDASOV SH.B.	O‘quv media markazi direktori

DASTURIY QO‘MITA TARKIBI:

1.	GANIYEV S.K.	Axborot xavfsizligi kafedrasi professori, t.f.d.
2.	G‘ULOMOV SH.R.	Ta’lim sifatini ta’minlash bo‘limi boshlig‘i, DSc, professor.
3.	BOYQUZIYEV I.M.	Kiberxavfsizlik va kriminalistika kafedrasi dotsenti, DSc
4.	GANIYEV A.A.	Axborot xavfsizligi kafedrasi dotsenti, t.f.n.
5.	KUCHKAROV T.A.	Axborot xavfsizligi kafedrasi dotsenti, t.f.n.
6.	SAMAROV H.Q.	Axborot xavfsizligi kafedrasi dotsenti, t.f.n.
7.	IMAMALIYEV A.T.	Kriptologiya kafedrasi dotsenti, PhD

1-SHO‘BA.
KIBERXAVFSIZLIKNING ZAMONAVIY MUAMMOLARI

MASHINALI O‘QITISH ALGORITMLARI ASOSIDA FISHING HUJUMLARINI ANIQLASH USULINI ISHLAB CHIQISH VA TAHLIL QILISH

Esanov O.O., Sobirova Sh.E.
Sharof Rashidov nomidagi Samarqand davlat universiteti

Annotatsiya: Mazkur tadqiqotda mashinali o‘qitish algoritmlari asosida fishing hujumlarini aniqlash usuli ishlab chiqildi va uning samaradorligi tahlil qilindi. Fishing hamda haqiqiy HTML sahifalaridan olingan ma’lumotlar to‘plamiga dastlabki ishlov berish, tozalash, normalizatsiya va cross-validation usullari qo‘llanildi. Aniqlash uchun Logistik regressiya, Qarorlar daraxti, Random Forest, XGBoost va Naive Bayes algoritmlaridan foydalanildi; samaradorlik Accuracy, Precision, Recall, F1-score, ROC-AUC va Confusion Matrix ko‘rsatkichlari asosida baholandi. Natijalar mashinali o‘qitish algoritmlarining fishing hujumlarini yuqori aniqlik bilan aniqlash imkoniyatiga ega ekanligini ko‘rsatdi va bu tadqiqot ishonchli usul ishlab chiqishda amaliy ahamiyatga ega.

Kalit so‘zlar: fishing hujumlari, kiberxavfsizlik, mashinali o‘qitish, klassifikatsiya, Logistik regressiya, KNN, Qarorlar daraxti, Naive Bayes, Random Forest, XGBoost, fishing aniqlash.

Аннотация: В данном исследовании разработан метод обнаружения фишинговых атак на основе алгоритмов машинного обучения, включающий предварительную обработку, очистку, нормализацию и кросс-валидацию данных. Использовались алгоритмы Logistik regressiya, Qarorlar daraxti, Random Forest, XGBoost и Naive Bayes; эффективность моделей оценивалась по Accuracy, Precision, Recall, F1-score, ROC-AUC и Confusion Matrix. Результаты показали высокую точность обнаружения фишинговых атак и практическую значимость разработанного метода.

Ключевые слова: фишинговые атаки, кибербезопасность, машинное обучение, классификация, Logistik regressiya, KNN, Qarorlar daraxti, Naive Bayes, Random Forest, XGBoost, обнаружение фишинга.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberxavfsizlikka tahdid soluvchi hujumlar soni ham ortib bormoqda. Ayniqsa, fishing hujumlari foydalanuvchilarning login-parollari, bank ma’lumotlari va boshqa maxfiy axborotlarini qo‘lga kiritishga qaratilgan eng xavfli ijtimoiy muhandislik hujumlaridan biri hisoblanadi. Anti-Fishing Working Group (APWG) ma’lumotlariga ko‘ra, 2025-yilning birinchi choragida dunyo bo‘yicha 1 003 924 ta fishing hujumi qayd etilgan bo‘lib, bu so‘nggi yillardagi eng yuqori ko‘rsatkichlardan biri hisoblanadi. Moliyaviy va onlayn to‘lov tizimlariga qaratilgan hujumlar barcha fishing hodisalarining 30,9 % qismini tashkil etgan. 2026-yil birinchi chorak hisobotida esa 971 181 ta fishing hujumi aniqlanganligi qayd etilgan bo‘lib, telekommunikatsiya, SaaS va veb-pochta xizmatlari asosiy nishonga aylangan [1].

Verizon kompaniyasining 2025-yilgi Data Breach Investigations Report (DBIR) hisobotiga ko‘ra, 22 mingdan ortiq xavfsizlik hodisasi va 12 195 ta tasdiqlangan ma’lumot sizib chiqish holati tahlil qilingan bo‘lib, hisob ma’lumotlarini o‘g‘irlash bilan bog‘liq hujumlar barcha buzilishlarning 22 % ini, Yevropa, Yaqin Sharq va Afrika hududlaridagi buzilishlarning 19 % ida

fishing hujumlari ishtirok etganini ko‘rsatgan [2] - bu fishing hujumlari hanuzgacha global kiberxavfsizlik muammosi ekanligini tasdiqlaydi.

Fishing hujumlarini aniqlashda qora ro‘yxatlar (blacklist), qoidalar va imzolar asosida ishlovchi an’anaviy himoya vositalari keng qo‘llaniladi. Biroq hujumchilarning yangi domenlar yaratishi va URL yashirish usullaridan foydalanishi sababli bu usullar zamonaviy tahdidlarni yetarli samaradorlikda aniqlay olmaydi. Shu sababli mashinali o‘qitishga qiziqish ortmoqda - bunday algoritmlar katta hajmdagi ma’lumotlardan yashirin bog‘lanishlarni aniqlash va avval uchramagan hujumlarni ham belgilar asosida klassifikatsiya qilish imkoniyatiga ega. Ilmiy tadqiqotlarda Random Forest, XGBoost, Qarorlar daraxti kabi algoritmlar fishing aniqlashda 96–97 % gacha aniqlik ko‘rsatgani qayd etilgan [4, 5, 7].

Ushbu tadqiqotning maqsadi fishing hujumlarini aniqlash uchun mashinali o‘qitish algoritmlariga asoslangan model ishlab chiqish hamda Logistik regressiya, Qarorlar daraxti, Random Forest, XGBoost va Naive Bayes samaradorligini qiyosiy tahlil qilishdan iborat. Ma’lumotlar to‘plamiga dastlabki ishlov berish, normalizatsiya va kross-validatsiya qo‘llanildi; samaradorlik Accuracy, Precision, Recall, F1-score, ROC-AUC va xatoliklar matritsasi asosida baholandi.

Tadqiqotning asosiy vazifalari quyidagilardan iborat:

– fishing hujumlarini aniqlash uchun ma’lumotlar to‘plamini tahlil qilish;
– ma’lumotlarni oldindan qayta ishlash va model uchun tayyorlash;
– mashinali o‘qitish algoritmlarini o‘qitish va sinovdan o‘tkazish;
– modellar samaradorligini turli baholash mezonlari asosida taqqoslash;
– eng samarali modelni aniqlash va uning amaliy qo‘llash imkoniyatlarini baholash.

Adabiyotlar tahlili

So‘nggi yillarda fishing hujumlarini aniqlashda mashinali o‘qitish algoritmlaridan foydalanishga bag‘ishlangan tadqiqotlar soni sezilarli ortdi - buning sababi an’anaviy qora ro‘yxat va signatura asosidagi usullarning yangi fishing saytlarni aniqlashdagi samaradorligi pasayib borayotganidir. Sahingoz va boshqalar [4] URL xususiyatlariga asoslangan yondashuvni, Rao va Pais [5] esa qaror daraxti algoritmini taklif qilgan. Adabiyotlar tahlili fishingni aniqlashda eng ko‘p qo‘llaniladigan algoritmlar Logistik regressiya, KNN, Qarorlar daraxti, Random Forest, SVM va XGBoost ekanligini ko‘rsatadi; ularning sifati ma’lumotlar to‘plami, xususiyatlar va giperparametrlarga bog‘liq.

Logistik regressiya sodda, natijalari izohlanishi oson va hisoblash xarajati past, biroq chiziqli bo‘lmagan bog‘lanishlarda samaradorligi pasayadi. KNN oddiy bo‘lsa-da, katta ma’lumotlarda hisoblash murakkabligi ortadi va shovqinga sezgir. Qarorlar daraxti murakkab bog‘lanishlarni aniqlaydi va vizual tahlili qulay, ammo chuqurligi nazorat qilinmasa overfitting yuzaga keladi. Random Forest, XGBoost va Deep Learning yuqori aniqlik bersa-da, resurs talabi yuqori; amaliy tizimlarda tezkorlik va tushuntiriluvchanlik muhim.

Mazkur tadqiqotning yangiligi shundan iboratki, fishing va haqiqiy HTML sahifalari datasetida besh algoritmning samaradorligi yagona eksperimental muhitda qiyosiy tahlil qilinadi hamda Accuracy, Precision, Recall, F1-score va ROC-AUC asosida eng samarali model aniqlanadi.

Tadqiqot metodologiyasi

Tadqiqotda fishing va haqiqiy veb-sahifalarga oid belgilarni o‘z ichiga olgan ma’lumotlar to‘plamidan foydalanildi. Dataset jami 11 054 ta yozuv va 32 ustundan tashkil topgan bo‘lib, shundan 31 tasi mustaqil belgilar (features), 1 tasi sinf belgisi (class). Belgilar veb-sahifalarning

URL manzili, domen xususiyatlari va HTML tuzilmasiga oid tavsiflardan iborat bo‘lib, fishing va haqiqiy sahifalarni ajratishda muhim ahamiyatga ega. Modellarni o‘qitishda barcha 31 belgi mustaqil o‘zgaruvchi, class ustuni esa bog‘liq o‘zgaruvchi sifatida ajratib olindi:

$$X = Dataset - Class$$

$$Y = Class$$

bu yerda, X - modelga uzatiladigan belgilar to‘plami, Y esa bashorat qilinadigan sinf qiymatini bildiradi.

Dataset tuzilmasi df.info() funksiyasi yordamida tekshirildi, df.isnull().sum() orqali bo‘sh qiymatlar nazorat qilindi - yo‘qolgan (NULL) qiymatlar aniqlanmadi, shu sababli qo‘shimcha tozalash talab etilmadi. df.describe() funksiyasi yordamida sonli belgilar bo‘yicha statistik tavsiflar o‘rganilib, ma’lumotlarning model yaratish uchun yaroqli ekanligi tasdiqlandi.

Ma’lumotlar train_test_split() funksiyasi yordamida Training set - 80 %, Test set - 20 % nisbatida, random_state = 42 parametri bilan ajratildi:

1-jadval

To‘plam	O‘lcham
X_train	8843 × 31
X_test	2211 × 31
y_train	8843
y_test	2211

Datasetdagi barcha belgilar bir xil diapazonda taqdim etilganligi sababli qo‘shimcha normalizatsiya yoki standartlashtirish talab etilmadi.

Modelning barqarorligini baholash maqsadida 5 qatlamli kross-validatsiya (5-Fold Cross Validation) qo‘llanildi. Random Forest modeli uchun olingan aniqlik ko‘rsatkichlari: 0.9787; 0.9760; 0.9747; 0.9570; 0.9566 bo‘lib, o‘rtacha aniqlik *96.86 %*ni tashkil etdi. Bu qiymat test to‘plamida olingan 96.97 % natijaga juda yaqin bo‘lgani sababli modelda sezilarli overfitting kuzatilmadi - Random Forest modeli turli ma’lumotlar bo‘linishlarida ham barqaror ishlashini ko‘rsatdi.

Mashinali o‘qitish modeli

Tadqiqotda Logistik regressiya, K-Nearest Neighbors (KNN), Qarorlar daraxti, Naive Bayes va Random Forest algoritmlaridan foydalanildi. Har bir modelning ishlash prinsipi va matematik asoslari quyida keltirilgan.

Logistik regressiya. Ikkilik klassifikatsiya masalalarida keng qo‘llaniladigan statistik model. Sigmoid funksiyasi yordamida natijani 0 va 1 oralig‘idagi ehtimolga o‘tkazadi:

$$P(Y = 1) = 1 / (1 + e^{-z}) \quad (1)$$

$$z = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n \quad (2)$$

bu yerda, x_i - belgilar qiymati, β_i - model koeffitsiyentlari. Algoritm sodda tuzilishi, tez ishlashi va natijalarni tushuntirish imkoniyati bilan ajralib turadi.

K-Nearest Neighbors (KNN). Yangi obyektni unga eng yaqin qo‘shni obyektlar sinfiga qarab tasniflaydi, masofa Evklid formulasi bilan hisoblanadi:

$$d(x, y) = \sqrt{\Sigma_{i=1}^{n} (x_i - y_i)^2} \quad (3)$$

Model yangi namunani eng yaqin k ta qo‘shnining ko‘pchilik ovoziga qarab klassifikatsiya qiladi. Algoritm sodda, biroq ma’lumotlar hajmi ortishi bilan hisoblash xarajatlari ham ortadi.

Qarorlar daraxti. Ma’lumotlarni ketma-ket shartlar asosida bo‘lish orqali klassifikatsiya qiladi; belgi tanlashda Gini indeksi qo‘llaniladi:

$$Gini = 1 - \Sigma_{i=1}^{n} p_i^2 \quad (4)$$

bu yerda, p_i - i-sinf ehtimoli. Gini qiymati qanchalik kichik bo‘lsa, tugundagi ma’lumotlar shunchalik bir jinsli hisoblanadi. Daraxt chuqurligining ortishi overfitting holatiga olib kelishi mumkin.

Naive Bayes. Bayes teoremasiga asoslangan ehtimollik modeli bo‘lib, belgilarni o‘zaro mustaqil deb faraz qiladi:

$$P(C|X) = [P(X|C) \cdot P(C)] / P(X) \quad (5)$$

bu yerda, P(C|X) - obyektning C sinfga tegishli bo‘lish ehtimoli, P(X|C) - belgilar kuzatilganda C sinf ehtimoli, P(C) - sinfning dastlabki ehtimoli, P(X) - belgilar ehtimoli. Algoritm hisoblash tezligi yuqori va katta hajmdagi ma’lumotlarda samarali, biroq belgilar orasidagi kuchli bog‘liqlik aniqlikni pasaytirishi mumkin.

Random Forest. Ansambl o‘qitish usuliga asoslangan bo‘lib, bir nechta qaror daraxti natijasini birlashtirib yakuniy qarorni qabul qiladi:

$$\hat{y} = mode(T_1, T_2, ..., T_n) \quad (6)$$

bu yerda, T_1, T_2, …, T_n - alohida daraxtlar natijalari, $\hat{y}$ - yakuniy bashorat. Random Forest overfitting muammosini kamaytiradi hamda klassifikatsiya aniqligini oshiradi, shu sababli fishing aniqlashda eng samarali algoritmlardan biri sifatida qayd etilgan [7].

Eksperimental natijalar

Modellar klassifikatsiya vazifasida sinovdan o‘tkazildi, baholash mezoni sifatida Accuracy, Precision, Recall va F1-score ishlatildi.

2-jadval

Modellarni klassifikatsiya vazifasida sinovdan o‘tkazish natijalari

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Logistik regressiya	93.17	93.19	93.17	93.16
KNN	60.24	60.08	60.24	60.14
Qarorlar daraxti	95.79	95.79	95.79	95.79
Naive Bayes	88.47	89.31	88.47	88.51
Random Forest	96.97	96.97	96.97	96.97
Optimized Random Forest	97.01	97.00	97.00	97.00

Yuqoridagi jadval natijalaridan ko‘rinib turibdiki, eng yuqori aniqlik Optimized Random Forest modelida (97.01 %) kuzatildi. Random Forest 96.97 %, Qarorlar daraxti 95.79 %, Logistik regressiya 93.17 %, Naive Bayes 88.47 % natija ko‘rsatdi. Eng past natija KNN algoritmida 60.24 %. Har bir model uchun to‘g‘ri/xato tasniflash sonlari 2-jadvalda keltirilgan:

3-jadval

Modellarni klassifikatsiya vazifasida sinovdan o‘tkazish natijalari

Model	To‘g‘ri: Haqiqiy	Xato: Fishing deb	Xato: Haqiqiy deb	To‘g‘ri: Fishing
Logistik regressiya	884	92	59	1176
KNN	516	460	419	816
Qarorlar daraxti	928	48	45	1190
Naive Bayes	918	58	197	1038
Random Forest	940	36	31	1204

Natijalar Random Forest modelining eng kam xatolikka ega ekanligini ko‘rsatadi (jami 67/2251); KNN algoritmida esa xato klassifikatsiyalar soni (879/2211) boshqa modellarga nisbatan ancha yuqori bo‘ldi.

Natijalar tahlili

Eng yuqori aniqlik Random Forest modelida kuzatildi: dastlabki model 96.97 %, optimallashtirilgandan so‘ng 97.01 % ga yetdi - buning sababi ansambl o‘qitish usulida bir nechta daraxt natijasining birlashtirilishi bo‘lib, bu xatolarni kamaytiradi va umumlashtirish qobiliyatini oshiradi. Qarorlar daraxti (95.79 %) ham yuqori natija berdi, biroq bitta daraxtga asoslangani sababli pastroq qoldi. Logistik regressiya (93.17 %) chiziqli bog‘lanishlarni yaxshi aniqladi; Naive Bayes’da (88.47 %) belgilar mustaqilligi farazi natijani pasaytirdi. KNN (60.24 %) eng past natijani ko‘rsatdi. Bu mazkur datasetda yetarli samaradorlik bermaganini bildiradi.

Logistik regressiya va Naive Bayes sodda tuzilishi sababli tez ishlaydi; KNN esa har bir namuna uchun masofa hisoblagani sababli xarajati yuqori. Random Forest ko‘plab daraxt yaratsada, yuqori aniqligi buni oqlaydi. Kross-validatsiya natijasi (96.86 %) test natijasiga (96.97 %) yaqin bo‘lgani uchun sezilarli overfitting aniqlanmadi. feature_importances_ orqali eng katta ta’sir ko‘rsatuvchi 10 ta belgi aniqlanib, grafik tasvirlandi. Umuman olganda, natijalar Random Forest modelining eng samarali yechim ekanligini ko‘rsatdi.

Xulosa

Ushbu tadqiqotda fishing hujumlarini aniqlash uchun Logistik regressiya, KNN, Qarorlar daraxti, Naive Bayes va Random Forest algoritmlari qo‘llanildi hamda samaradorligi taqqoslandi. Random Forest modeli 97.01 % aniqlik bilan eng yuqori natijani ko‘rsatib, eng samarali model sifatida tanlandi. Natijalar mashinali o‘qitish usullarining fishing hujumlarini aniqlash samaradorligini sezilarli oshirishini tasdiqladi; model axborot xavfsizligi tizimlari, veb-brauzerlar va elektron pochta xizmatlarida qo‘llanilishi mumkin. Kelgusida datasetni kengaytirish, chuqur o‘qitish usullaridan foydalanish hamda real vaqt tizimlariga joriy etish rejalashtirilmoqda.

Foydalanilgan adabiyotlar

1. APWG. Fishing Activity Trends Report. Anti-Fishing Working Group, 2024.
2. Verizon. 2024 Data Breach Investigations Report (DBIR). Verizon Enterprise, 2024.
3. Aldwairi M., Alsaadi I. Detecting Fishing Websites Using ML Techniques. IJACSA, 2017.
4. Sahingoz O.K. et al. ML Based Fishing Detection from URLs. Expert Systems with Applications, 117, 2019, pp. 345–357.
5. Rao R.S., Pais A.R. Detection of Fishing Websites Using Qarorlar daraxti Algorithm. Procedia Computer Science, 45, 2015, pp. 537–546.
6. Breiman L. Random Forests. Machine Learning, 45(1), 2001, pp. 5–32.
7. Quinlan J.R. Induction of Qarorlar daraxtis. Machine Learning, 1(1), 1986, pp. 81–106.
8. Hosmer D.W., Lemeshow S., Sturdivant R.X. Applied Logistik regressiya. John Wiley & Sons, 2013.
9. Géron A. Hands-On ML with Scikit-Learn, Keras and TensorFlow. O‘Reilly Media, 2022.
10. UCI ML Repository. Fishing Websites Dataset. University of California, Irvine.

TARMOQ XAVFSIZLIGINI TA’MINLASH UCHUN TRAFIKDAGI PAKETLARNI FILTRLASH USULLARI

Tashev S.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada paketlarni filtrlash texnologiyalari keng ko‘lamda ko‘rib chiqilgan. Paketlarni filtrlash texnologiyasi tarmoq xavfsizligini oshirish va tarmoqqa kiruvchi zararli yoki istalmagan trafikni kamaytirish maqsadida qo‘llaniladi. Shuningdek, maqolada paketlarni filtrlash texnologiyasining afzalliklari va kamchiliklari tahlil qilingan. Filtrlashning asosiy afzalliklari sifatida tarmoq resurslarining samarali ishlatilishi va tashqi tahdidlardan himoyalanish qayd etilgan hamda maqolada paketlarni filtrlash bo‘yicha muhim strategiyalar ham batafsil yoritilgan, jumladan statik, dinamik va fragmentlangan paketlarni filtrlash usullari o‘rganilgan. Bundan tashqari maqolada paketlarni filtrlash spetsifikatsiyasini yaxshilash, barcha sarlavha maydonlariga kirish imkoniyatini kengaytirish hamda filtrlash qoidalarini soddalashtirish strategiyalari taklif etilgan.

Kalit so‘zlar: Tarmoq xavfsizligi, tarmoqlararo ekran, paketlarni filtrlash, marshrutlash jadvali, paketlarni filtrlashning ilovalari

Аннотация: В данной статье всесторонне рассматриваются технологии фильтрации пакетов. Технология фильтрации пакетов применяется для повышения уровня сетевой безопасности и сокращения объёма вредоносного или нежелательного трафика, поступающего в сеть. Кроме того, в статье анализируются преимущества и недостатки данной технологии. К основным преимуществам фильтрации относятся эффективное использование сетевых ресурсов и защита от внешних угроз. В статье также подробно рассматриваются ключевые стратегии фильтрации пакетов, включая методы статической, динамической фильтрации и фильтрации фрагментированных пакетов. Помимо этого, предлагаются стратегии совершенствования спецификации фильтрации пакетов, расширения возможностей доступа ко всем полям заголовка пакета и упрощения правил фильтрации.

Ключевые слова: сетевая безопасность, межсетевой экран, фильтрация пакетов, таблица маршрутизации, приложения для фильтрации пакетов.

Kirish

Internetning tez o‘sishi butun dunyo bo‘ylab millionlab kompyuterlarni bog‘ladi, tashqi dunyo bilan aloqa o‘rnatish uchun kompaniyalar internetga ulanishi kerak. Shaxsiy tarmoq bo‘lgan Intranet deb nomlanuvchi alohida tashkilotlarning shaxsiy tarmoqlari umumiy tarmoqqa, ya’ni Internetga ulangan bo‘lishi kerak. Tashkilotlarning shaxsiy ma’lumotlari xavfsizligini ta’minlash uchun alohida tarmoqlar umumiy foydalanishdan himoyalangan bo‘lishi kerak. Paketli filtrlashni amalga oshirish odatda arzon. Ammo shuni tushunish kerakki, paketli filtrlash qurilmasi dastur yoki proksi-server tarmoqlararo ekran bilan bir xil darajadagi xavfsizlikni ta’minlamaydi. Eng sodda IP tarmoqlaridan tashqari barchasi IP quyi tarmoqlaridan iborat va marshrutizatorlarni o‘z ichiga oladi.

Paket filtrlashni ishlash jarayoni

Barcha paketli filtrlar bir xil umumiy rejimda ishlaydi. TCP/IP protokoli stekining tarmoq sathi va transport sathida ishlagan holda, har bir paket protokollar stekiga kirayotganda tekshiriladi. Quyidagi ma’lumotlar uchun tarmoq va transport sarlavhalari diqqat bilan tekshiriladi.

– protokol (IP sarlavhasi, tarmoq sathi) – IP sarlavhasida 9-bayt (bayt soni noldan boshlanishini unutmang) paketning protokolini aniqlaydi. Ko‘pgina filtr qurilmalari TCP, UPD va ICMP o‘rtasida farqlash qobiliyatiga ega.

– manba manzili (IP sarlavhasi, tarmoq sathi) - bu paketni yaratgan xostning 32 bitli IP manzilidir.

– maqsad manzili (IP sarlavhasi, tarmoq sathi) - bu paket uchun mo‘ljallangan xostning 32 bitli IP manzilidir.

– manba porti (TCP yoki UDP sarlavhasi, transport sathi) - TCP yoki UDP tarmoq ulanishining har bir uchi portga ulangan. TCP portlari alohida va UDP portlaridan farq qiladi. 1024 dan past raqamlangan portlar ajratilgan - ular maxsus belgilangan foydalanishga ega. 1024 (shu jumladan) dan yuqori raqamlangan portlar efemer portlar deb nomlanadi. Ular sotuvchining xohishiga ko‘ra ishlatilishi mumkin. "Mashhur" portlar ro‘yxati uchun RFP1700 ga qarang. Manba porti psevdo-tasodifiy tayinlangan efemer port raqamidir. Shunday qilib, manba portida filtrlash ko‘pincha unchalik foydali emas.

– maqsad porti (TCP yoki UDP sarlavhasi, transport sathi) - Belgilangan port raqami paket yuborilgan portni bildiradi. Belgilangan hostdagi har bir xizmat portni tinglaydi. Filtrlanishi mumkin bo‘lgan ba’zi taniqli portlar: 20/TCP va 21/TCP - ftp ulanish/ma’lumotlar, 23/TCP - telnet, 80/TCP - http va 53/TCP - DNS zonasi uzatish.

– ulanish holati (TCP sarlavhasi, transport sathi) – Ulanish holati paketning tarmoq seansining birinchi paketi ekanligini ko‘rsatadi. TCP sarlavhasidagi ACK biti “false” yoki birinchi paket bo‘lsa, sessiya 0 ga o‘rnatiladi. ACK biti “false” yoki 0 ga o‘rnatilgan har qanday paketlarni rad etish yoki o‘chirish orqali xostga ulanish o‘rnatishga ruxsat berish juda oddiy.

– Paketlarni filtrlash paketlarning sarlavhasi ma’lumotlarini tahlil qilish va paketni tushirish yoki yo‘naltirish to‘g‘risida qaror qabul qilishni o‘z ichiga oladi. Qaror bir nechta parametrlarga asoslanishi mumkin. Paketlarni filtrlash ilovalari ma’murga qaror qabul qilishda rioya qilinishi kerak bo‘lgan qoidalarni belgilashga imkon beradi. Administrator tomonidan belgilangan qoidalar kiruvchi yoki chiquvchi paketlarga asoslanishi mumkin. Kiruvchi va chiquvchi paketlarga asoslangan qoidalarni belgilash qobiliyati administratorga filtrlash sxemasida yo‘riqnoma ko‘rinishini sezilarli darajada nazorat qilish imkonini beradi va ikkitadan ortiq interfeyslardan iborat marshrutizatorlarda filtrlashga yordam beradi. Tashqi dunyodan kelgan tajovuzkorlar ichki manba manzillarini soxtalashtirishi va ichki xostdan ekanligini da’vo qilishi mumkin, bu sodir bo‘lmasligiga ishonch hosil qilish uchun administrator paketlar qayerdan kelgan interfeysni bilishi orqali manbani bilishi kerak. Ichki manba manzillarini soxtalashtiradigan barcha paketlarni tashlab yuborish mumkin.

Paketlarni filtrlash strategiyasi

Paketli filtrlashning asosiy afzalliklari - kiruvchi paketli trafikni kamaytirish va tarmoq manbalaridan zararli va istalmagan foydalanishdan himoya qilish hisoblanadi [1]. Paket filtrlashni amalga oshirish uchun bir nechta strategiyalardan foydalanish mumkin. Ulardan ba’zilari quyidagilar:

Marshrutlash jadvali yechimlari

Ushbu sxemada paketni yo‘naltirish yoki tashlab yuborish qarori marshrutlash jadvalini qidirishga asoslanadi. Marshrutlash jadvali yozuvlari paketlar qaysi manzillarga yo‘naltirilishi mumkinligi va qaysi biriga yo‘naltirilmasligini hal qiladi. Ushbu yechim statik marshrutlardan foydalanilganda yordam beradi. RIP kabi marshrutlash protokollari qo‘llaniladi, ammo ular

xavfsiz emas. Routerlar RIP ma’lumotlarini qaysi manbalardan qabul qilishni tanlashlari mumkin, bu tasodifiy taqdim etilgan noto‘g‘ri ma’lumotlarning oldini olishda yordam beradi.

Kirish va chiqishni filtrlash

Ushbu sxemada filtrlash tarmoqning tashqi interfeysida kirish va chiqish yo‘nalishlarida amalga oshiriladi. Buning yordamida tarmoqdagi ichki marshrutlashni sekinlashtirmasdan tarmoq xavfsizligiga erishiladi [2].

Manba manzilini filtrlash

Ushbu sxemada ichki tarmoq ulanishlari bitta autentifikatsiya sxemasiga va tashqi tarmoqqa ulanishlar boshqasiga ega bo‘ladi. Ichki ulanishlar tashkilotdagi ichki manzillar maydoni bilan bog‘lanishlarni tashkil qiladi. Agar tashqi interfeysga filtr qo‘llanilsa, u ichkaridan, lekin aslida tashqi ulanishdan bo‘lgan paketlarni rad etadi, ya’ni manba va maqsad manzillari ichki manzil maydonida bo‘ladi, lekin paket tarmoq tashqarisidan keladi.

Protokol portini filtrlash

Ushbu sxemada tashqi tarmoqdan kirish mumkin bo‘lgan xizmatlarni cheklovchi filtrni qo‘llash orqali tashqi tarmoqdan qaysi maqsad portlari to‘plamiga kirish mumkinligini aniqlash uchun maqsad port tekshiriladi [4]. Masalan, SMTP, nntp, ftp-ma’lumotlar, ftp, barmoq, telnet, login va qobiq kabi TCP xizmatlarining har qandayiga tashqi tarmoqlarga kirish taqiqlanishi mumkin.

Kengaytirilgan filtrlash strategiyalari

Border Manager 3.7 da Novell kabi tijorat sotuvchilari tomonidan qo‘llaniladigan ba’zi boshqa strategiyalar statik paketlarni filtrlash va TCP ACK bit filtrlash, dinamik paketlarni filtrlash va parchalangan paketlarni filtrlash kabi kengaytirilgan xususiyatlardir.

Statik paketlarni filtrlash

Statik filtrlashda ichki tarmoqlar, ya’ni intranet va tashqi tarmoq, ya’ni internet o‘rtasidagi chegarani kesib o‘tgan har bir paket tekshiriladi. Statik paket filtri protokol identifikatori, manba va manzil IP manzillari va port raqamlari, kiruvchi va chiquvchi paketlar uchun yo‘riqnoma interfeysi kabi parametrlarni aniqlash uchun har bir paketning sarlavhasi ma’lumotlarini tekshiradi.

Ushbu parametrlar tekshiriladi, so‘ngra paketni jo‘natish yoki o‘chirish to‘g‘risidagi qaror kirish va chiqish qoidalarining belgilangan to‘plamiga muvofiq amalga oshiriladi.

TCP ACK bit filtrlash

TCP ACK bit filtrlashda tarmoqqa faqat TCP ACK bit o‘rnatilgan paketlarga ruxsat beriladi. TCP ACK filtrlash barcha tashqi xostlarni autentifikatsiyasiz ichki xostlarga TCP ulanishini boshlashiga yo‘l qo‘ymaydi.

Dinamik paketlarni filtrlash

Dinamik paketli filtrlashda, shuningdek, statistik paket filtrlash sifatida ham tanilgan, o‘tishga ruxsat bergan chiquvchi paketlarni kuzatib boradi va faqat mos keladigan paketlarni qaytarishga imkon beradi. Qaytish filtri har safar paket umumiy tarmoqqa uzatilganda javob paketiga ruxsat berish uchun dinamik ravishda yaratiladi. Bu sxema ham kamroq ulanishni, ham ulanishga yo‘naltirilgan protokollarni qo‘llab-quvvatlaydi.

Fragmentli paketlarni filtrlash

Paketlar fragmentlar deb ataladigan kichik bo‘laklarga bo‘lingan, birinchi bo‘lakda to‘liq sarlavha ma’lumotlari mavjud, avval faqat birinchi paket tushib ketgan, chunki sarlavha ma’lumotlarisiz quyidagi paketlarni qayta yig‘ib bo‘lmaydi, ammo bu keyingi paketlar tarmoqni to‘ldirish uchun ishlatilishi mumkin. Bunga yo‘l qo‘ymaslik uchun tarmoqli kengligini sarflagan

holda, filtrlash birinchi paketni, shuningdek, bir xil manba va maqsad manzillari va interfeyslariga ega bo‘lgan barcha keyingi paketlarni o‘chirib tashlaydi.

Joriy paketlarni filtrlash muammolari

Paketni filtrlash umumiy tarmoq xavfsizligini yaxshilash vositasi bo‘lishi mumkin. Bu imkoniyatni taklif qiluvchi IP-routerlar soni ortib bormoqda. Agar ma’murlar undan to‘g‘ri foydalansalar, paketlarni filtrlash juda xavfsiz va foydali vosita bo‘lishi mumkin. Hozirgi vaqtda paketli filtrlash xavfsizlik devorini xavfsiz va samarali qilish uchun loyihalash va amalga oshirishda bir qator qiyinchiliklar yuzaga keladi [5].

Quyida hal qilinishi kerak bo‘lgan ba’zi muammolar keltirilgan:

– Noto‘g‘ri tasniflash: Paket filtri manba IP manzili soxtalashtirilganda paketni noto‘g‘ri tasniflashi mumkin. Manba portiga asoslangan filtrlash shunga o‘xshash muammoga duch keladi, masalan, manba mashinasi ushbu portda shubhali mijoz yoki serverni ishga tushirishi mumkin.

– O‘zgaruvchan sarlavha uzunligi: Variantlar maydoni IP paket sarlavhasi uzunligini o‘zgaruvchan qiladi. Shunday qilib, yuqori darajadagi protokol ma’lumotlarini topish qiyin bo‘lishi mumkin, masalan, TCP/UDP sarlavhalari, ofsetga asoslangan naqshlarni moslashtirishning oddiy usullaridan foydalanganda.

– Fragmentli paket: Paket parchalanganda, ba’zi paket filtrlari boshqa bo‘laklar qabul qiluvchi uchun foydasiz bo‘ladi, deb hisoblab, birinchi fragmentni tashlab qo‘yadi. Biroq, bu erda xatarlar paydo bo‘ladi, xakerlar tizimni aldash yo‘llarini topishlari mumkin. Biroq, bu paketlarni filtrlash jarayonini sezilarli darajada murakkablashtirishi mumkin.

– Oldindan belgilangan sarlavha maydonlari: Bu moslashuvchanlikka qattiq ta’sir qiladi. Agar ma’mur qaror qabul qilishda qaysi sarlavha maydonlaridan foydalanishni aniq belgilamasa, kerakli xavfsizlik siyosatini samarali amalga oshirib bo‘lmaydi. Masalan, TCP "SYN" bayrog‘i o‘rnatilgan paketlarni bloklashni xohlashingiz mumkin, ammo paket filtri ushbu maydonni filtr spetsifikatsiyasi uchun ishlatishga ruxsat bermasligi mumkin [3].

Joriy paketlarni filtrlash muammolari uchun mumkin bo‘lgan yechimlar:

1) Filtr spetsifikatsiyasining sintaksisini yaxshilash
2) Filtrlash me’zonlari sifatida barcha tegishli sarlavha maydonlarini ochish
3) Chiquvchi filtrlarga ham, kiruvchi filtrlarga ham ruxsat berish
4) Filtrlarni ishlab chiqish, sinovdan o‘tkazish va monitoring qilish vositalarini soddalashtirish

Paket filtrlarining afzalliklari:

– Ushbu tarmoqlararoekranlari arzon, ular tarmoq ishlashiga ozgina ta’sir qiladi.
– Ular mijoz kompyuterlarini har qanday maxsus tarzda sozlashni talab qilmaydi.
– Ilova mustaqilligi
– Masshtablilik
– Paketni filtrlash tez, moslashuvchan va shaffof (mijoz tomonidan o‘zgartirishlar kiritish talab qilinmaydi).
– Ular paketlarni juda tez tezlikda qayta ishlashlari mumkin.
– Ular 3-sath paketlari va 4-sath segment sarlavhalaridagi ko‘pgina sohalarda osongina mos kelishi mumkin, bu esa xavfsizlik siyosatini amalga oshirishda katta moslashuvchanlikni ta’minlaydi.

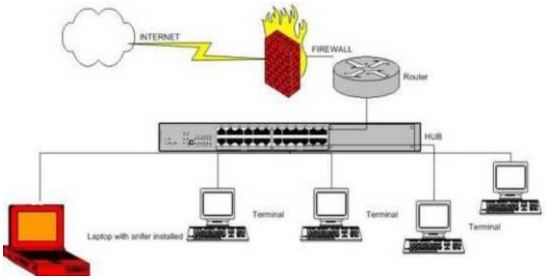
Paket filtrlarining kamchiliklari:

Ular o‘z-o‘zidan juda xavfsiz deb hisoblanmaydi, chunki ular amaliy sath protokollarini tushunmaydilar. Ular paketlar bo‘yicha tarkibga asoslangan qarorlar qabul qila olmaydi. Ular

manbasiz va ulanish holatini saqlamaydi. Ular, shuningdek, juda kam yoki umuman ro‘yxatga olish qobiliyatiga ega, bu esa tarmoq hujum ostida ekanligini aniqlashni qiyinlashtiradi. Taqdim etish va rad etish qoidalarini sinovdan o‘tkazish ham qiyin, bu tarmoqni zaif yoki noto‘g‘ri sozlangan qoldirishi mumkin [5].

Paketlarni filtrlashning ilovalari

Paket filtrlash qurilmasi tarmoqdagi birinchi mudofaa chizig‘i bo‘lishi mumkin va ma’lum turdagi paketlarni himoyalangan tarmoqqa kirishini bloklash uchun ishlatiladi. Bu kirish filtri sifatida tanilgan. Garchi mustahkam xavfsizlik devori bo‘lmasa-da, u proksi yoki dastur xavfsizlik devoridagi yukni kamaytirish uchun ishlatilishi mumkin. Quyidagi diagramma paket filtri va proksi-server yoki dastur xavfsizlik devoridan foydalanishning oddiy misolini ko‘rsatadi.



1-rasm. Paketlarni filtrlashning tarmoqlararo ekrani

Xulosa

Xulosa qilib shuni ta’kidlash mumkinki mazkur maqolada paketlarni filtrlash texnologiyalarining tarmoq xavfsizligini ta’minlashdagi roli, uning afzalliklari va kamchiliklari tahlili keltirilgan. Paketlarni filtrlashning ijobiy jihatlari sifatida resurslardan samarali foydalanish va tashqi xavflardan himoyalanish qayd etilgan, statik, dinamik va fragmentlangan paketlarni filtrlash usullari ham tahlil qilingan. Shuningdek, tarmoq xavfsizligini oshirishda imkon beruvchi paketlarni filtrlash qoidalarini soddalashtirish va spetsifikatsiyasini yaxshilash bo‘yicha takliflar ishlab chiqilgan.

Foydalanilgan adabiyotlar

1. Gulomov Sh.R. Tarmoqdagi zararli trafik turlari va ularni aniqlash. Multidisciplinary Scientific Journal. December, Issue 24 | 2023, -B.424-432

2. SN Tashev, AG Ganiev The Role of “Imagination” in the Process of “Creative Thinking” Developing Students'“Imagination” and “Creative Thinking” Skills in Teaching Physics. Annals of the Romanian Society for Cell Biology, 2021/3/6, 633-642

3. SN Tashev THE ROLE OF “IMAGINATION” IN THE PROCESS OF “CREATIVE THINKING”, DEVELOPING STUDENTS’ “IMAGINATION” AND “CREATIVE THINKING” SKILLS IN TEACHING PHYSICS PSYCHOLOGY AND EDUCATION, 3569-3575

4. Y.B. Karamatovich, T.S. Norboboevich, N.I. Ibrohimovich. Verification of the pocket filtering based on method of verification on the model. 2019 International Conference on Information Science and Communications Technologies (ICISCT)

5. J. Ning et al., “Pine: Enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment,” in Proc. Eur. Symp. Res. Comput. Secur., 2020, pp. 3–22

AXBOROT XAVFSIZLIGI MONITORINGI TIZIMIDA XABARLARNI KO‘P DARAJALI SAQLASH VA KORRELYATSIYALASH MEXANIZMI

Gafurov Sh.R.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada elektron hukumat tizimidagi axborot xavfsizligi monitoringi tizimida to‘planadigan xabarlarni ko‘p darajali saqlash va ularning hayotiy siklini boshqarish yondashuvi hamda axborot xavfsizligiga tegishli ma’lumotlarni korrelyatsiyalash mexanizmi ko‘rib chiqiladi. Mexanizm kontekstli, tuzilmaviy, funksional va xatti-harakatlar tahlilini tizimlararo korrelyatsiya va biznes tahlili bilan to‘ldiradi. Taklif etilgan yondashuv ma’lumotlar bazasi so‘rovlarini qayta ishlash vaqtini qisqartirish, noto‘g‘ri pozitivlar sonini kamaytirish va mavjud infratuzilmadan foydalangan holda hujumlarni aniqlash aniqligini oshirishga xizmat qiladi.

Kalit so‘zlar: elektron hukumat tizimi, axborot xavfsizligi monitoringi, axborot xavfsizligi xabari, korrelyatsiya, ma’lumotlarni saqlashning hayotiy sikli, kontekstli tahlil, noto‘g‘ri pozitiv.

Аннотация. В статье рассматриваются подход к многоуровневому хранению сообщений, накапливаемых системой мониторинга информационной безопасности электронного правительства, и управлению их жизненным циклом, а также механизм корреляции данных, относящихся к информационной безопасности. Механизм дополняет контекстный, структурный, функциональный и поведенческий анализ межсистемной корреляцией и бизнес-анализом. Предложенный подход позволяет сократить время обработки запросов к базе данных, уменьшить число ложных срабатываний и повысить точность обнаружения атак с использованием существующей инфраструктуры.

Ключевые слова: система электронного правительства, мониторинг информационной безопасности, сообщение информационной безопасности, корреляция, жизненный цикл хранения данных, контекстный анализ, ложное срабатывание.

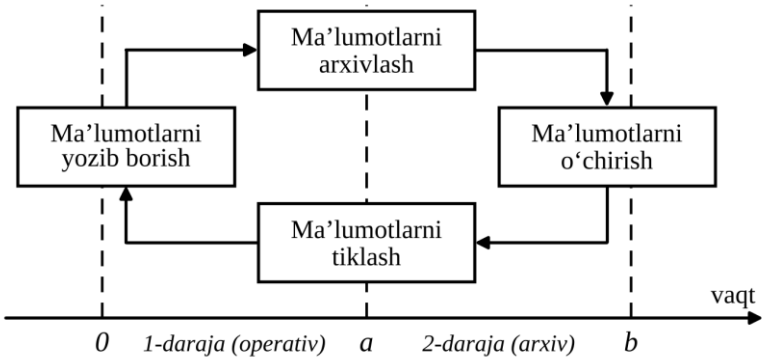
Kirish

Elektron hukumat tizimida axborot xavfsizligi monitoringi tizimi milliy segmentdagi veb-resurslarning himoya vositalaridan keladigan xabarlarni to‘playdi, normallashtiradi va ma’lumotlar bazasida saqlaydi. Xabar manbalari soni yuzlab bo‘lishi va ularning har biri soniyasiga o‘nlab xabar yaratishi mumkinligi sababli ma’lumotlar bazasi tez kattalashadi. Xabarlar soni ortishi bilan so‘rovlarni qayta ishlashga ketadigan vaqt va resurslar ko‘payadi, zamonaviy hujumlar esa juda tez sodir bo‘ladi va xabarlarni o‘z vaqtida tahlil qilishni talab etadi [1, 2]. Ikkinchi muammo – monitoring tizimi ishlashi davomida noto‘g‘ri pozitivlar va haqiqiy hujumlarning o‘tkazib yuborilishi (birinchi va ikkinchi tur xatoliklar) yuzaga kelishi. Hodisaning har qanday noto‘g‘ri identifikatsiyasi tashkilot uchun istalmagan oqibatlarga olib keladi. Ushbu ishda bu ikki muammoni birgalikda hal etishga qaratilgan yondashuv – xabarlarni ko‘p darajali saqlash va ularni kengaytirilgan korrelyatsiyalash mexanizmi bayon etiladi.

Asosiy qism

Monitoring tizimining arxitekturasida xabarlar 1-modulda yaratiladi, 2-modulda to‘planadi va normallashtiriladi, 3-modulda saqlanadi. Taklifga ko‘ra, 3-modulga ierarxiya kiritiladi va 2-moduldan olingan ma’lumotlarni saqlashning hayotiy sikli boshqariladi. Tushunish oson bo‘lishi

uchun yondashuv ikki darajali sxemada ko‘rsatilgan (1-rasm), darajalar soni esa elektron hukumat tizimining qamrovidan kelib chiqib belgilanadi.



1-rasm. Ma’lumotlarni saqlash jarayonining hayotiy siklini boshqarish

Birinchi darajada joriy ma’lumotlar saqlanadi. Ularning saqlanish muddati 3-modulda qayd etilgan vaqtdan boshlab *a* oydan oshmaydi; *a* qiymati samaradorlik talablari va tizimning ma’lumotlarni saqlash siyosati bilan belgilanadi va odatda 1 oydan 3 oygacha bo‘ladi. Birinchi darajadagi ma’lumotlar operativ ish uchun ishlatiladi. *a* oy o‘tgach, ma’lumotlar ikkinchi darajaga – arxivga o‘tkaziladi. Saqlanish muddati *b* oydan oshgan ma’lumotlar ikkinchi darajadan o‘chiriladi; *b* tashkilot qoidalari va saqlash siyosati bilan belgilanadi va odatda 36 oydan 120 oygacha bo‘ladi. Xavfsizlik ma’muri bu vaqt oraliqlarini istalgan paytda o‘zgartirishi mumkin. Hayotiy siklni boshqarish uchun to‘rtta tartib amalga oshiriladi: ma’lumotlarni identifikatsiya qilish, birinchi darajadan ikkinchi darajaga arxivlash, ikkinchi darajadan birinchi darajaga qayta tiklash va o‘chirish.

Bunday tashkil etish quyidagi afzalliklarni beradi:

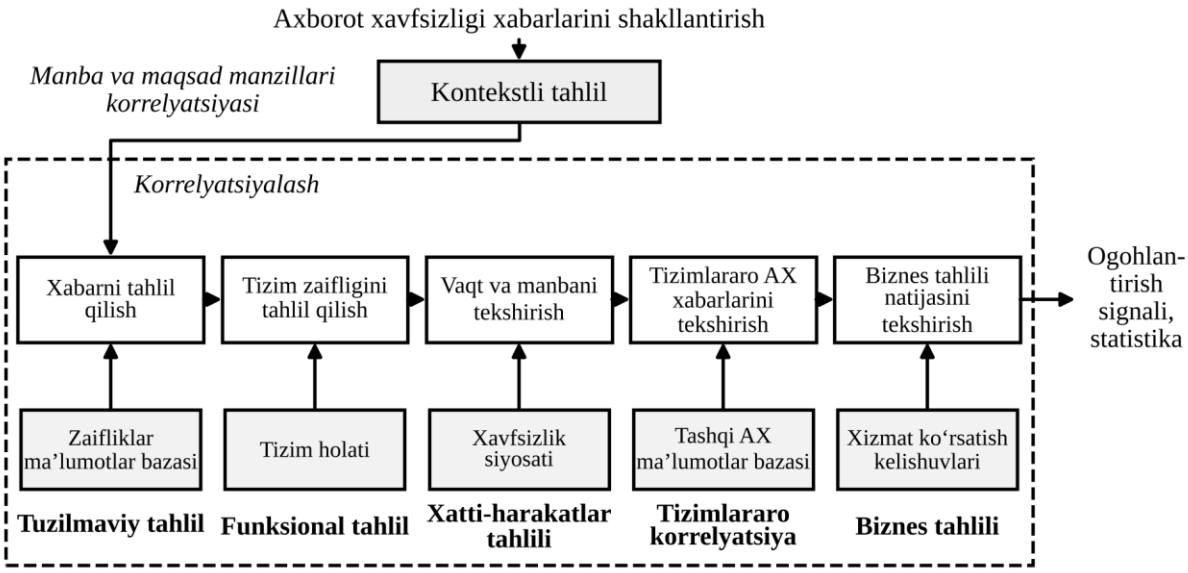
– birinchi darajada ma’lumotlar kamroq bo‘lgani sababli ma’lumotlar bazasi so‘rovlarini qayta ishlash vaqti qisqaradi;

– muhim ma’lumotlar arzonroq saqlash vositalariga arxivlanadi va me’yoriy hujjatlar talablariga muvofiqlik ta’minlanadi;

– ma’lumotlarning hayotiy sikl davomidagi aylanishi avtomatlashtiriladi.

Saqlash ierarxiyasi kiritilgach, monitoring tizimida qo‘llaniladigan tahlil turlarini korrelyatsiyaning ikki qo‘shimcha turi bilan to‘ldirish mumkin bo‘ladi. Birinchisi – axborot xavfsizligi xabarlarini boshqaruv tizimi bilan, ya’ni elektron hukumat tizimiga integratsiya qilingan tizimlarning me’yoriy hujjatlari bazasi bilan bog‘lash. Bugungi kunda ayrim funksiyalarni ixtisoslashgan uchinchi tomon tashkilotiga (autsorsingga) berish keng tarqalgan bo‘lib, funksiya bilan birga axborot xavfsizligi risklari ham o‘tkaziladi. Shu sababli olingan xabarlarning tashkilot tuzgan shartnomalar va kelishuvlar qoidalariga muvofiqligi tahlil qilinadi. Ikkinchisi – turli tizimlarning monitoring tizimlari o‘rtasida xabarlarni korrelyatsiyalash. Texnik jihatdan har ikki tur tuzilmaviy tahlil kabi maxsus tahlil modullari yordamida amalga oshiriladi.

Korrelyatsiyalash mexanizmida tahlil tartibi muhim ahamiyatga ega, chunki har bir tahlil turi monitoring tizimi unga yetarli ma’lumot to‘plagandagina bajariladi (2-rasm). Avval kontekstli tahlil o‘tkaziladi: u xabarlarni qabul qilish va qayta ishlash bosqichida, manba va maqsad manzillari asosida amalga oshiriladi. So‘ng ketma-ket tuzilmaviy, funksional va xatti-harakatlar tahlili bajariladi; ular mos ravishda zaifliklar ma’lumotlar bazasiga, tizim holati haqidagi ma’lumotlarga va xavfsizlik siyosatiga tayanadi. Keyin tizimlararo korrelyatsiya tashqi axborot xavfsizligi ma’lumotlar bazasi bo‘yicha tekshiriladi. Oxirida yuqori darajadagi biznes tahlili o‘tkazilib, hodisaning elektron hukumat tizimiga qanday ta’sir qilishi haqida xulosa chiqariladi.



2-rasm. Axborot xavfsizligiga tegishli ma'lumotlarni korrelyatsiyalash mexanizmi

Elektron hukumat tizimida xizmatlar internetda joylashgan veb-ilovalar orqali ko‘rsatiladi, ularga qonuniy foydalanuvchilar ham, hujumchilar ham murojaat qilishi mumkin. Asosiy xavfsizlik mexanizmlari – foydalanuvchi autentifikatsiyasi, ma'lumotlarni shifrlash va tarmoqlararo ekran – parametrlarni manipulyatsiya qilish, saytlararo skriptlar va kod kiritish kabi hujumlarga qarshi aksariyat hollarda yetarli emas [3–5]. Hujumlarni aniqlash aniqligini oshirish usuli sifatida monitoring tizimi tarkibida umumiy ma'lumotlar bazasidan foydalanish va turli tizimlar o‘rtasida xabarlarni korrelyatsiyalash taklif etiladi [6]. Ma'lumot almashinuvi ikki usulda tashkil etilishi mumkin:

– yopiq usul – almashinuvda cheklangan sondagi tizimlar qatnashadi va har bir monitoring tizimi qolgan barcha tizimlar bilan bevosita ma'lumot almashadi; bu usul elektron hukumat tizimining monitoring tizimlari yoki bir xil faoliyat turidagi tashkilotlar uchun mos keladi;

– ochiq usul – yagona ma'lumotlar bazasi elektron hukumat tizimiga ulangan barcha tashkilotlar foydalanishi mumkin bo‘lgan serverda joylashtiriladi va har bir monitoring tizimi faoliyati davomida to‘plagan IP-manzillar haqidagi ma'lumotlarni unga yuboradi.

Har ikki holda ham almashinuv xavfsiz protokol (SSH, HTTPS) orqali amalga oshirilishi, monitoring tizimlari autentifikatsiyadan o‘tkazilishi va ularning ma'lumotlar bazasiga kirishi nazorat qilinishi shart. Tizimlararo korrelyatsiya natijasida biror tizimda mahalliy darajada tahdid aniqlansa, monitoring tizimi shu tahdid bilan bog‘liq hujumchi identifikatorini aniqlash imkonini beradi. Monitoring tizimi muayyan hodisaga tegishli barcha xabarlar to‘plamini baholab, to‘g‘ri nazorat qarorini qabul qilishi, masalan, tarmoqlararo ekranga hujumni bloklovchi buyruqlarni yuborishi mumkin [7].

Yondashuvning muhim xususiyati shundaki, u yangi infratuzilma talab qilmaydi: xabarlar bazasi, boshqaruv tizimining me'yoriy bazasi va axborot xavfsizligi tizimlari o‘rtasidagi aloqa mavjud monitoring tizimi doirasida tashkil etiladi. Bu axborot xavfsizligi uchun yagona infratuzilmani saqlash hisobiga xarajatlarni kamaytiradi, boshqa tizimlar bilan integratsiya mexanizmini takomillashtiradi va elektron hukumat tizimining axborot xavfsizligini har tomonlama tahlil qilish uchun asos yaratadi.

Xulosa

Axborot xavfsizligi monitoringi tizimida xabarlarni ko‘p darajali saqlash operativ ma’lumotlar hajmini cheklaydi va so‘rovlarni qayta ishlashni tezlashtiradi, arxiv darajasi esa me’yoriy talablarga muvofiqlikni ta’minlaydi. Kontekstli, tuzilmaviy, funksional va xatti-harakatlar tahlilini tizimlararo korrelyatsiya hamda biznes tahlili bilan to‘ldiruvchi mexanizm xabarlarni boshqaruv tizimi talablari – shartnomalar va kelishuvlar qoidalari – bilan bog‘lash va shu asosda qaror qabul qilish imkonini beradi. Natijada tashqi tahdidlarni tahlil qilishda noto‘g‘ri pozitivlar soni kamayadi va elektron hukumat tizimining axborot xavfsizligi ta’minlanganlik ko‘rsatkichi yaxshilanadi. Korrelyatsiya va kontekstli tahlil elektron hukumat tizimini monitoring qilish dasturiy vositasida [8] qo‘llanilgan.

Foydalanilgan adabiyotlar

1 Zou Z., Yin J., Fan S., Zhang X. Research on Network Security Event Correlation Analysis Method Based on Knowledge Graph // 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). Chongqing, China, 2024. P. 772–776.

2 Huang X., Zhao J., Shang Z., Wang C., Liu X., Li J. A Correlation Analysis-Based Security Event Processing System for Power Networks // 2022 2nd International Conference on Electrical Engineering and Control Science (IC2ECS). Nanjing, China, 2022. P. 298–301.

3 Seid E., Popov O., Blix F. Towards Security Attack Event Monitoring for Cyber Physical-Systems // ICISSP. 2023. P. 722–732.

4 Seid E., Popov O., Blix F. Evaluation of Asfalia, a Security Attack Event Monitoring Framework // Procedia Computer Science. 2024. Vol. 237. P. 793–802.

5 Seid E., Popov O., Blix F. Security Attack Behavioural Pattern Analysis for Critical Service Providers // Journal of Cybersecurity and Privacy. 2024. Vol. 4, No. 1. P. 55–75.

6 Kholidy H.A. Autonomous mitigation of cyber risks in the Cyber–Physical Systems // Future Generation Computer Systems. 2021. Vol. 115. P. 171–187.

7 Akbarzadeh A., Katsikas S.K. Dependency-based security risk assessment for cyber-physical systems // International Journal of Information Security. 2023. Vol. 22, No. 3. P. 563–578.

8 Gafurov Sh.R., Botirov F.B. Axborot xavfsizligi talablari bo‘yicha elektron hukumat tizimini monitoring qilish dasturi. EHM uchun dasturga guvohnoma № DGU 37522. Toshkent, 08.05.2024.

ELEKTRON HUKUMAT TIZIMINI MONITORING QILISH DASTURIY VOSITASINI AMALDAGI ANALOGLAR BILAN QIYOSIY SINASH NATIJALARI

Gafurov Sh.R.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada axborot xavfsizligi talablari bo‘yicha elektron hukumat tizimini monitoring qilish uchun ishlab chiqilgan dasturiy vositani amaldagi oltita monitoring vositasi bilan qiyosiy sinash natijalari keltiriladi. Sinovda jami 24310 ta hodisa – uzilishlar, deface, tarmoq hujumlari, veb-hujumlar, insidentlar va oddiy hodisalar – qamrab olingan. Ishlab chiqilgan dasturiy vosita 22849 ta hodisani aniqlagan, bu eng yaqin analogga nisbatan 0,70 foiz yuqori; hodisalarni aniqlashga ketgan umumiy vaqt esa 5 daqiqaga kam.

Kalit so‘zlar: elektron hukumat tizimi, axborot xavfsizligi monitoringi, dasturiy vosita, qiyosiy sinov, tarmoq hujumi, insident, aniqlash vaqti.

Аннотация. В статье приводятся результаты сравнительного испытания программного средства, разработанного для мониторинга системы электронного правительства по требованиям информационной безопасности, с шестью существующими средствами мониторинга. Испытание охватывало 24310 событий: сбои соединения, дефейс, сетевые атаки, веб-атаки, инциденты и обычные события. Разработанное программное средство выявило 22849 событий, что на 0,70 % выше, чем у ближайшего аналога, а суммарное время обнаружения событий оказалось на 5 минут меньше.

Ключевые слова: система электронного правительства, мониторинг информационной безопасности, программное средство, сравнительное испытание, сетевая атака, инцидент, время обнаружения.

Kirish

Elektron hukumat tizimiga ulangan tashkilotlarning veb-ilovalarida ruxsat etilmagan harakat aniqlanganda tegishli tizim ma’muriga ogohlantirishning o‘z vaqtida yetib borishi muammoni tez va sifatli bartaraf etishning birinchi qadamidir. Tahdid, hujum va insidentlar qancha erta aniqlansa, ulardan himoyalanish shuncha oson, ko‘riladigan zarar esa shuncha kam bo‘ladi. Monitoring tizimlariga qo‘yiladigan talablar O‘z DSt ISO/IEC 27004:2022 standartida belgilangan [1], bunday tizimlarni qurish masalalari qator ishlarda o‘rganilgan [2–4]. Muallif tomonidan ma’lumotlar oqimida axborot xavfsizligining buzilishini aniqlash usuli, birlashtirilgan baholash va moslashuvchan konfiguratsiya blokini nazoratlash algoritmlari asosida ikkita dasturiy vosita ishlab chiqilgan [5, 6]. Ushbu ishning maqsadi – dasturiy vositani amalda qo‘llanilayotgan monitoring vositalari bilan bir xil sharoitda solishtirish natijalarini bayon etishdir.

Asosiy qism

Dasturiy vosita elektron hukumat tizimiga ulangan, milliy segmentda joylashgan davlat va nodavlat tashkilotlarining veb-saytlarini real vaqt rejimida monitoring qiladi: veb-saytning asosiy sahifasidagi o‘zgarishlarni va veb-saytning ishlamayotganini aniqlaydi, aniqlangan hodisa haqida operatorni ogohlantiradi. Uning modullari EAGLE EYE monitoring dasturiy kompleksiga integratsiya qilingan, natijalar kompleksning boshqaruv panelida vizuallashtiriladi. Dasturiy vosita Linux operatsion tizimida ishlaydi; 4 yadroli protsessor, 16 Gb operativ xotira va 100 Gb hajmli disk talab qilinadi. Texnik talablar bajarilmasa, hujumlarni aniqlashda ortiqcha yuklanishlar yuzaga keladi va dasturiy vosita imkoniyatlaridan to‘liq foydalanilmaydi.

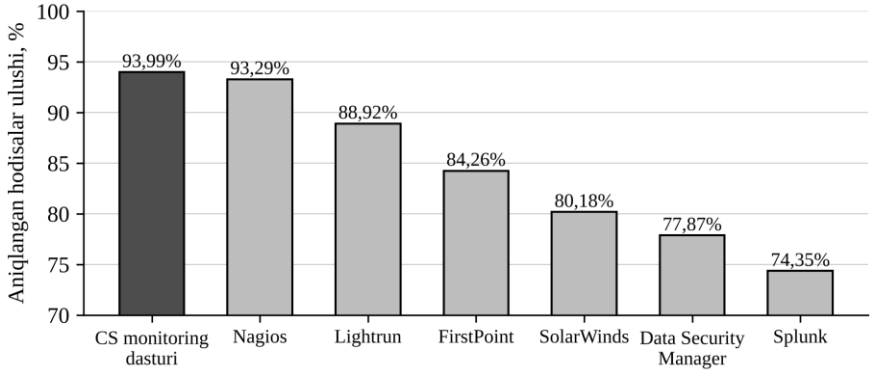
Qiyosiy sinovda ishlab chiqilgan «CS monitoring dasturi» bilan birga SolarWinds, Data Security Manager, Splunk, Lightrun, FirstPoint va Nagios vositalari qatnashdi. Barcha vositalar bir xil hodisalar to‘plamida sinaldi: 1050 ta uzilish (ulanishdagi xatolik), 4 ta deface, 440 ta tarmoq hujumi, 81 ta veb-hujum, 1512 ta insident va 21223 ta oddiy hodisa – jami 24310 ta. Tarmoq hujumlari tarkibiga DDoS (85 ta), XSS (65), SQL inyeksiya (61), brute force (43), virus va zararli dasturlar yordamidagi hujumlar (41), fishing (28), razvedka (25), nolinchi kun hujumi (19), eksploytdan foydalanishga urinish (18), seansni o‘g‘irlash (16), spufing (13), MITM (11), DNS spufing (9) va URL interpretatsiyasi (6) hujumlari kirdi. Har bir vosita uchun aniqlangan hodisalar soni va ularni aniqlashga ketgan vaqt qayd etildi (1- va 2-jadvallar).

1-jadval

Dasturiy vositalar tomonidan aniqlangan hodisalar soni

Dasturiy vosita	Uzilish	Deface	Tarmoq hujumi	Veb-hujum	Insident	Oddiy hodisa	Jami	Ulushi, %
Sodir etilgan hodisalar	1050	4	440	81	1512	21223	24310	100
CS monitoring dasturi	1026	4	440	78	1365	19936	22849	93,99
Nagios	1024	4	440	75	1301	19836	22680	93,29
Lightrun	906	3	347	62	1284	19014	21616	88,92
FirstPoint	931	4	347	64	1154	17983	20483	84,26
SolarWinds	992	4	352	65	1026	17053	19492	80,18
Data Security Manager	801	1	359	65	1245	16459	18930	77,87
Splunk	846	2	386	72	1302	15467	18075	74,35

Ishlab chiqilgan dasturiy vosita 24310 ta hodisadan 22849 tasini (93,99 foiz) aniqladi. Eng yaqin natijani Nagios ko‘rsatdi – 22680 ta (93,29 foiz), ya’ni ishlab chiqilgan vosita 169 ta ko‘p hodisani aniqladi, farq 0,70 foizni tashkil etadi. Qolgan vositalarning ko‘rsatkichi 74,35 foizdan (Splunk) 88,92 foizgacha (Lightrun) bo‘ldi (1-rasm).



1-rasm. Dasturiy vositalar tomonidan aniqlangan hodisalar ulushi

Hodisa turlari kesimida ham ishlab chiqilgan vosita barcha toifalarda eng yuqori yoki unga teng natijaga erishdi. 440 ta tarmoq hujumining barchasini faqat ikki vosita – ishlab chiqilgan dastur va Nagios – aniqladi, qolganlarida bu ko‘rsatkich 347–386 ta. Veb-hujumlarning 81 tadan 78 tasi (Nagios – 75, qolganlari – 62–72), insidentlarning 1512 tadan 1365 tasi (Splunk – 1302,

Nagios – 1301) aniqlandi. To‘rtta deface hodisasining barchasini ishlab chiqilgan dastur, SolarWinds, FirstPoint va Nagios qayd etdi.

2-jadval

Hodisalarni aniqlash vaqtining davomiyligi, min

Dasturiy vosita	Uzilish	Deface	Tarmoq hujumi	Veb-hujum	Insident	Oddiy hodisa	Jami
CS monitoring dasturi	3	1	15	6	28	45	98
Nagios	3	1	18	6	28	47	103
Lightrun	3	1	19	23	37	56	139
FirstPoint	3	1	18	19	41	58	140
SolarWinds	7	3	26	17	35	54	142
Data Security Manager	3	1	29	6	36	59	134
Splunk	3	1	31	17	41	57	150

Aniqlash vaqti bo‘yicha ham ishlab chiqilgan vosita ustunlikka ega: barcha toifalar bo‘yicha jami 98 daqiqa, Nagiosda – 103 daqiqa, ya’ni 5 daqiqaga kam; qolgan vositalarda bu ko‘rsatkich 134–150 daqiqa. Farq ayniqsa tarmoq hujumlarida seziladi: ular 15 daqiqada aniqlangan, boshqa vositalarda esa 18–31 daqiqa talab qilingan. Bu natija monitoring tizimida birlashtirilgan baholash va moslashuvchan konfiguratsiya blokini nazoratlash qo‘llanilishi bilan izohlanadi: himoya vositalarining sozlamalari xavf darajasiga moslashtiriladi, yakuniy qaror esa bitta birlashtirilgan baho asosida qabul qilinadi.

Dasturiy vosita «Kiberxavfsizlik markazi» davlat unitar korxonasi, «UZINFOCOM» MChJ va Raqamli hukumat loyihalarini boshqarish markazining korporativ tarmoqlarida tajribaviy sinovdan o‘tkazilgan va tarmoqlararo ekran, IDS/IPS, DLP, ruxsatlarni boshqarish hamda zaxira nusxa olish tizimlari bilan integratsiya qilingan. Aniqlangan hodisalar sinflarga ajratilib, tizim ma’muriga hisobot shaklida taqdim etiladi, ruxsat etilmagan harakatlar haqida esa ma’mur onlayn (monitoring tizimidagi profil orqali) va oflayn (SMS-xabar orqali) rejimlarda xabardor qilinadi.

Sinovlarda dasturiy vositaning sifat ko‘rsatkichlari ham baholandi. Ma’lumotlar oqimida aniqlangan buzilishlarni tahlil qilish asosida buzilishning hujumga aylanishi mumkinligi yoki tizimdagi texnik xatolik ekanligi farqlanadi va shunga mos qaror qabul qilinadi. Hodisalarni ularning sodir bo‘lish muhitiga qarab korrelyatsiya va kontekstli tahlil qilish hodisalarning keyingi holatini prognozlash imkonini beradi. Dasturiy vosita hodisalarning qayd yozuvlarini yuritadi va tizimdagi barcha hodisalarning amalga oshish ketma-ketligini jamlagan hisobotni shakllantiradi.

Xulosa

Qiyosiy sinov natijalariga ko‘ra, ishlab chiqilgan dasturiy vosita 24310 ta hodisadan 22849 tasini aniqlab, eng yaqin analog – Nagios (22680 ta) – ga nisbatan 0,70 foiz yuqori aniqlikni ko‘rsatdi va hodisalarni aniqlashga ketadigan vaqtni 5 daqiqaga qisqartirdi. Dasturiy vositani yanada takomillashtirish uchun texnik talablarni monitoring qamroviga qarab kamaytirish, qaror qabul qilish moduliga sun’iy intellekt algoritmlarini kiritish hamda Windows operatsion tizimi va mobil platformalar uchun versiyalarni ishlab chiqish rejalashtirilgan.

Foydalanilgan adabiyotlar

1 O‘z DSt ISO/IEC 27004:2022 (ISO/IEC 27004:2016, IDT). Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini boshqarish. Monitoring, o‘lchash, tahlil qilish va baholash.

2 Duan X., Zhou Y., Guan J. Exploration on Heterogeneous Network Security Monitoring Algorithm Based on Big Data Intelligent Information Technology // 2023 IEEE 15th International Conference on Computational Intelligence and Communication Networks (CICN). Bangkok, Thailand, 2023. P. 154–158.

3 Yang C., Tan Y., Zhang J., Chen X., Li S., Li P. Information System Information Security Hidden Danger Monitoring Tool // 2023 Panda Forum on Power and Energy (PandaFPE). Chengdu, China, 2023. P. 414–420.

4 Nasrullayev N.B. Axborot xavfsizligi monitoringi tizimi ishlashining samaradorligini oshirish usullari va algoritmlari: texnika fanlari bo‘yicha falsafa doktori (PhD) dissertatsiyasi avtoreferati. Toshkent, 2019. 46 b.

5 Gafurov Sh.R., Botirov F.B. Axborot xavfsizligi talablari bo‘yicha elektron hukumat tizimini monitoring qilish dasturi. EHM uchun dasturga guvohnoma № DGU 37522. Toshkent, 08.05.2024.

6 Gafurov Sh.R., Botirov F.B. CS monitoring dasturi. EHM uchun dasturga guvohnoma № DGU 37520. Toshkent, 08.05.2024.

“.UZ” DOMENIDAGI TAHDIDLARNI QAROR QABUL QILISH DARAXTIGA ASOSLANGAN TAYANCH VEKTORLAR USULI YORDAMIDA ANIQLASH

Gafurov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada internet tarmog‘ining milliy segmenti – “.uz” domenida joylashgan veb-ilovalar va resurslarga bo‘ladigan tahdidlar hamda hujumlarni aniqlash uchun tayanch vektorlar usulini qaror qabul qilish daraxti bilan birlashtirish yondashuvi ko‘rib chiqiladi. Daraxtning tuzilishi sinf namunalarining markazlari orasidagi masofa va sinflardagi namunalar soni asosida quriladi, har bir tugunda ikki sinfli tayanch vektorlar klassifikatori joylashadi. Yondashuv namunalar bazasida tegishli belgiga ega bo‘lmagan tahdidlarni ham sinflarga ajratish imkonini beradi.

Kalit so‘zlar: milliy segment, “.uz” domeni, tahdidlarni aniqlash, tayanch vektorlar usuli, qaror qabul qilish daraxti, ko‘p sinfli tasniflash, hujumlarni aniqlash tizimi.

Аннотация. В статье рассматривается подход к обнаружению угроз и атак на веб-приложения и ресурсы, размещённые в национальном сегменте сети Интернет – домене «.uz», основанный на объединении метода опорных векторов с деревом принятия решений. Структура дерева строится на основе расстояния между центрами образцов классов и числа образцов в классах, а в каждом узле размещается двухклассовый классификатор опорных векторов. Подход позволяет относить к классам и те угрозы, для которых в базе образцов отсутствует соответствующий признак.

Ключевые слова: национальный сегмент, домен «.uz», обнаружение угроз, метод опорных векторов, дерево принятия решений, многоклассовая классификация, система обнаружения атак.

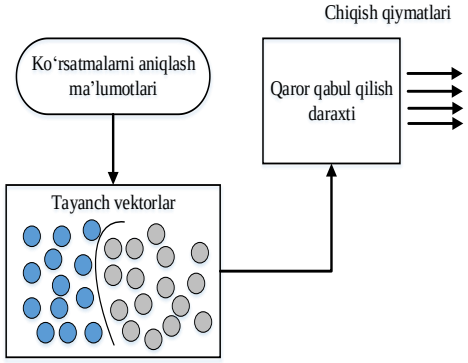
Kirish

Internet tarmog‘idagi veb-sahifalar va resurslar soni ortib borishi bilan milliy segment xavfsizligini ta’minlash masalasi ham dolzarblashmoqda. Mavjud xavfsizlik texnologiyalari asosan ma’lumotlarni shifrlash va ruxsatsiz kirishni nazoratlashga qaratilgan, biroq ular to‘liq xavfsizlikni ta’minlay olmaydi. Milliy segmentda qo‘llaniladigan hujumlarni aniqlash tizimlari (IDS/IPS) funksionalligiga ko‘ra suiiste’mollik detektorlari va anomaliya detektorlariga bo‘linadi: birinchisi avval aniqlangan tahdid namunalari (belgilari) bilan solishtirishga, ikkinchisi oddiy foydalanish xatti-harakatlarini saqlash va audit ma’lumotlarini tahlil qilishga asoslanadi [1]. Har ikki holatda ham tizim real vaqtda hujumlarni tasniflashi va tasnifga ko‘ra himoya mexanizmini ishga tushirishi kerak. Muallifning avvalgi ishida milliy segmentdagi tahdidlarni tayanch vektorlar usuli (SVM) yordamida aniqlash taklif etilgan [2]. Tayanch vektorlar dastlab ikkilik tasniflash uchun ishlab chiqilgan, amaliyotda esa hodisalarni bir nechta sinfga ajratish talab etiladi. Ushbu ishda shu muammoni hal etuvchi – tayanch vektorlarni qaror qabul qilish daraxti bilan birlashtiruvchi usul bayon etiladi.

Asosiy qism

Milliy segmentdagi hodisalar besh sinfga ajratiladi: oddiy (normal) hodisa va to‘rt turdagi hujum – DoS (katta hajmdagi trafik generatsiyasi orqali xizmat ko‘rsatishdan voz kechishga majburlash), U2R (ro‘yxatdan o‘tgan foydalanuvchining ma’mur imtiyozini egallashi), R2L (masofadagi ro‘yxatdan o‘tmagan foydalanuvchining tarmoqdagi kompyuterga ruxsat olishi) va

Probe (maxfiy axborotni olish maqsadida portlarni skanerlash). Ko‘p sinfli tayanch vektorlarni qurishning klassik usullari – “bittasi qolganlariga qarshi” (OVR), “bittasi bittasiga qarshi” (OVO) va yo‘naltirilgan asiklik graf (DAG) – ma’lum kamchiliklarga ega: OVR usulida o‘qitish va sinov bosqichlari sekin kechadi, OVO usulida k ta sinf uchun $k(k-1)/2$ ta klassifikator quriladi va sinflar soni ortganda usul sekinlashadi [3, 4]. Shu sababli tayanch vektorlarni qaror qabul qilish daraxti asosida tashkil etish taklif etiladi (1-rasm). Turli modellarni birlashtirish alohida modelning cheklovlarini kamaytiradi va yakka modelga nisbatan yaxshiroq samaradorlikni ta’minlaydi [5, 6].



1-rasm. Tahdidlar va hujumlarni aniqlash tizimining qaror qabul qilish daraxtiga asoslangan moduli

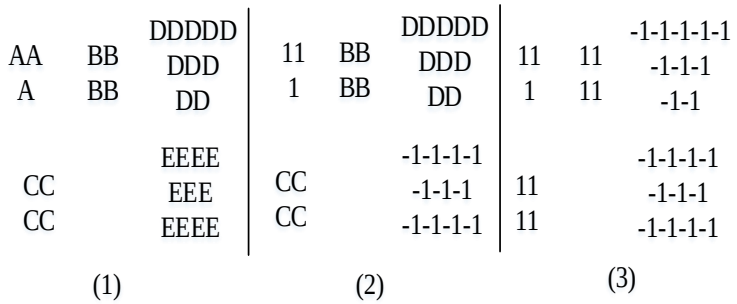
Birinchi bosqichda ma’lumotlarni “normal” va “hujum”ga ajratuvchi ikkilik qaror daraxti shakllantiriladi, keyingi bosqichlarda jarayon to‘rt turdagi hujum uchun takrorlanadi. Daraxt modeli ikki sinfli tayanch vektorlar ketma-ketligidan iborat bo‘lib, uning tuzilishi ikki sinf namunalari orasidagi masofa va har bir sinfdagi namunalar soni bilan belgilanadi. i-sinf namunalarining markaziy nuqtasi quyidagicha hisoblanadi:

$$c_i = \frac{\sum_{m=1}^{n_i} x_m^i}{n_i} \quad (1)$$

bu yerda n_i – i-sinfdagi namunalar soni, $i = 1, 2, \ldots, k$. Ikki sinf markazlari orasidagi Evklid masofasi $Ed_{ij} = \|c_i - c_j\|$ ga teng. Sinflarning o‘zaro ajralganligi namunalarning o‘z markazi atrofida tarqalishini hisobga oluvchi masofa bilan baholanadi:

$$d_{ij} = \frac{Ed_{ij}}{\gamma_i + \gamma_j}, \quad \gamma_i = \frac{\sum_{m=1}^{n_i} \|x_m^i - c_i\|}{n_i} \quad (2)$$

Barcha sinf juftliklari uchun masofalar hisoblanib, orasidagi masofa eng katta bo‘lgan juftlik topiladi. Besh sinf {A, B, C, D, E} misolida (2-rasm) eng katta masofa A va E sinflari orasida bo‘lsin: A sinf “1”, E sinf “−1” deb belgilanadi. Qolgan sinflar shu ikki sinfgacha bo‘lgan masofalarni solishtirish orqali taqsimlanadi: $d_{BA} < d_{BE}$ va $d_{CA} < d_{CE}$ bo‘lgani uchun B va C “1” sinfga, $d_{DA} > d_{DE}$ bo‘lgani uchun D “−1” sinfga o‘tkaziladi.

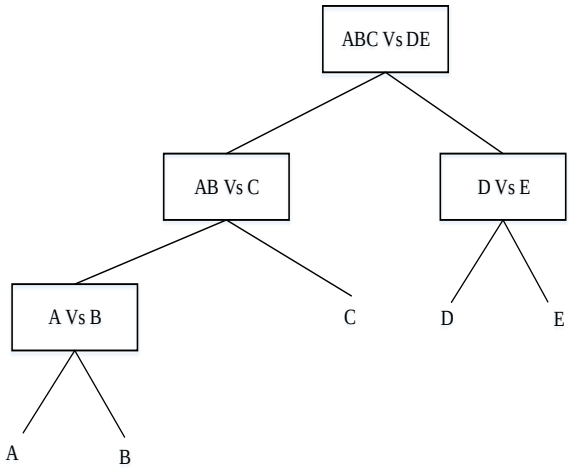


2-rasm. Beshta sinf namunasini ikkita sinfga ajratish mexanizmi

Hosil bo‘lgan ikki guruhning muvozanati quyidagi parametr bilan nazorat qilinadi:

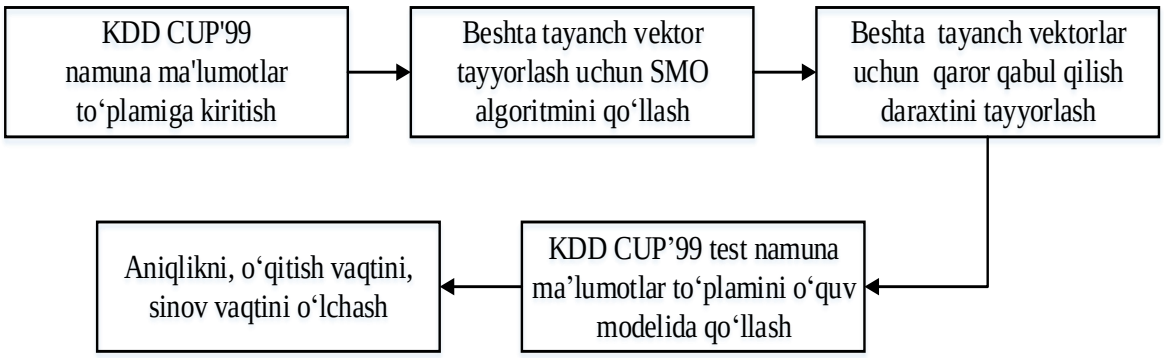
$$\mu = \frac{min(n_1, n_{-1})}{max(n_1, n_{-1})} \quad (3)$$

bu yerda n_1 va n_{-1} – “1” va «−1» sinflaridagi namunalar soni. Biror sinfni boshqa guruhga o‘tkazish haqidagi taxmin faqat yangi hisoblangan μ′ qiymati μ dan katta bo‘lsagina qabul qilinadi, aks holda bekor qilinadi; jarayon μ ortmay qolguncha takrorlanadi. Natijada beshta sinf {A, B, C} va {D, E} kichik to‘plamlariga bo‘linadi va bu birinchi klassifikatorni beradi. So‘ng har bir kichik to‘plamda bitta element qolguncha bo‘lish rekursiv davom ettiriladi va mos klassifikatorlar quriladi (3-rasm). Noma’lum namunani sinash daraxtning birinchi tugunidan boshlanadi va daraxt bo‘ylab davom etadi; oxirgi tugun namunaning natijaviy sinfini beradi [7].



3-rasm. Beshta guruhga tasniflash uchun qaror qabul qilish daraxti

Tayanch vektorlar katta hajmdagi namunalarda sekin, kichik hajmdagi namunalarda esa juda tez ishlaydi. Hujum belgilarining hajmi kichik bo‘lgani sababli usul hujumlarni aniqlashda samarali; katta hajmdagi namunalar bilan ishlash zarur bo‘lganda SMO (Sequential Minimal Optimization) algoritmi qo‘llaniladi [8]. Taklif etilgan usul algoritmi besh qadamdan iborat (4-rasm): KDD CUP’99 hujum namunalari ma’lumotlar to‘plamiga kiritiladi [9]; beshta tayanch vektorni tayyorlash uchun SMO algoritmi qo‘llaniladi; ular uchun qaror qabul qilish daraxti quriladi; test namunalari to‘plami o‘quv modelida qo‘llaniladi; aniqlik, o‘qitish vaqti va sinov vaqti o‘lchanadi.



4-rasm. Sinov qadamlari ketma-ketligi

Usul «Internet tarmog‘ining milliy segmentida tahdidlarni aniqlash dasturi»da amalga oshirilgan [10]. KDD CUP’99 va CERT r5.2 to‘plamlaridan olingan 30000 ta namunadan iborat nazorat tanlanmasida dasturiy vosita tahdid va hujumlarning 96,5 foizini aniqlagan, 2,8 foizi aniqlanmagan, xatolik 0,7 foizni tashkil etgan. «Kiberxavfsizlik markazi» DUKning korporativ tarmog‘ida 65081 ta hodisa tahlil qilinib, ulardan 28154 tasi tahdid ekanligi aniqlangan: 11469 tasi ichki, 12056 tasi tashqi, 4326 tasi strukturalangan va 303 tasi strukturalanmagan tahdidlar. Xatolik

ko‘rsatkichi bo‘yicha dasturiy vosita Cisco NGIPS ga nisbatan taxminan 1,7 marta, Suricata ga nisbatan taxminan 1,3 marta yaxshiroq natija ko‘rsatgan [11].

Xulosa

Tayanch vektorlarni qaror qabul qilish daraxti bilan birlashtirish ko‘p sinfli tasniflash masalasini ikki sinfli klassifikatorlar ketma-ketligiga keltiradi. Daraxt tuzilishi sinf markazlari orasidagi masofa va guruhlar muvozanati asosida avtomatik quriladi. Usul “.uz” domenidagi tahdid va hujumlarning tanlanma belgilari mavjud bo‘lmagan holatlarda ham namuna ma’lumotlar to‘plamini o‘quv tanlanma modeliga kiritish va tasodifiy hodisalarni tahdidlar hamda oddiy hodisalar sinflariga ajratish imkonini beradi. Usul asosida ishlab chiqilgan dasturiy vosita nazorat tanlanmasida 96,5 foiz aniqlikni ko‘rsatdi.

Foydalanilgan adabiyotlar

1 Kumavat K.S., Gomes J. Survey of Detection Techniques for DDoS Attacks // 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). London, United Kingdom, 2022. P. 657–663.

2 Gafurov A.A. On the Internet Method of Identifying Threats Using SVM // Eurasian Research Bulletin. 2024. Vol. 35. P. 22–28.

3 Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A survey of network-based intrusion detection data sets // Computers & Security. 2019. Vol. 86. P. 147–167.

4 Wankhede S., Kshirsagar D. DoS Attack Detection Using Machine Learning and Neural Network // 2018 Fourth International Conference on Computing Communication Control and Automation. 2018.

5 Taghavinejad S.M., Taghavinejad M., Shahmiri L., Zavvar M., Zavvar M.H. Intrusion Detection in IoT-Based Smart Grid Using Hybrid Decision Tree // 2020 6th International Conference on Web Research (ICWR). Tehran, Iran, 2020. P. 152–156.

6 Gunduz M.Z., Das R. Cyber-security on smart grid: Threats and potential solutions // Computer Networks. 2020. P. 107094.

7 Mahdavinejad M.S., Rezvan M., Barekatain M., Adibi P., Barnaghi P., Sheth A.P. Machine learning for Internet of Things data analysis: A survey // Digital Communications and Networks. 2018. Vol. 4, No. 3. P. 161–175.

8 Kousar H., Mulla M.M., Shettar P., Narayan D.G. Detection of DDoS Attacks in Software Defined Network using Decision Tree // 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT). Bhopal, India, 2021. P. 783–788.

9 KDD Cup 1999 Data. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

10 Gafurov A.A., Botirov F.B. Internet tarmog‘ining milliy segmentida tahdidlarni aniqlash dasturi. EHM uchun dasturga guvohnoma № DGU 37519. Toshkent, 08.05.2024.

11 Xamdamov R.X., Gafurov A.A. Milliy segmentda tahdidlarni va hujumlarni aniqlash usullarining samaradorligini baholash // Цифровые технологии и искусственный интеллект: настоящее и будущее: сборник докладов Международной научно-практической конференции. Ташкент, 2025. С. 222–227.

MILLIY SEGMENTDA TAHDID VA HUJUMLAR HAQIDAGI OGOHLANTIRISHLARNI KORRELYATSIYALASH JARAYONINING KONSEPTUAL MODELI

Gafurov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada internet tarmog‘ining milliy segmentida joylashgan veb-resurslarni himoyalashda hujumlarni aniqlash tizimlari yaratadigan ogohlantirishlarni korrelyatsiyalash jarayonining konseptual modeli ko‘rib chiqiladi. Model hodisalarni boshqarishning uch blokidan iborat: ogohlantirishlarni yig‘ish, ularni agregatlash va verifikatsiyalash hamda yuqori darajali ogohlantirishlar moduli. Tahdidlar va hujumlar soni orasidagi bog‘lanish tanlanma kovariatsiya yordamida baholanadi. Model yolg‘on ogohlantirishlar sonini kamaytirish va ko‘p bosqichli hujumlarni aniqlash imkonini beradi.

Kalit so‘zlar: milliy segment, “.uz” domeni, ogohlantirishlar korrelyatsiyasi, konseptual model, kovariatsiya, meta-ogohlantirish, yolg‘on ogohlantirish, hujumlarni aniqlash tizimi.

Аннотация. В статье рассматривается концептуальная модель процесса корреляции оповещений, формируемых системами обнаружения атак при защите веб-ресурсов, размещённых в национальном сегменте сети Интернет. Модель состоит из трёх блоков управления событиями: модуля сбора оповещений, модуля их агрегирования и верификации и модуля оповещений высокого уровня. Связь между числом угроз и атак оценивается с помощью выборочной ковариации. Модель позволяет сократить число ложных оповещений и выявлять многоэтапные атаки.

Ключевые слова: национальный сегмент, домен «.uz», корреляция оповещений, концептуальная модель, ковариация, мета-оповещение, ложное оповещение, система обнаружения атак.

Kirish

Milliy segmentdagi veb-resurslarga hujum yoki ruxsat etilmagan kirish amalga oshirilganda hujumchi qayd fayllarida (loglarda) iz qoldirmasdan harakat qila olmaydi, hujumlarni aniqlash tizimlari esa shubhali harakatlar haqida tizim ma’muriga ogohlantirish yuboradi. Biroq ogohlantirishlar soni juda ko‘p bo‘lgani sababli haqiqiy buzilishlar ular orasida yo‘qolib ketadi va axborot xavfsizligi riski ortadi. Mutaxassislar vaqtining katta qismini qayd ma’lumotlari bazalarini boshqarishga sarflaydi, insidentlarni o‘rganish va hujumlarga reaksiya ko‘rsatish esa ikkinchi o‘ringa tushib qoladi. Ogohlantirishlar sonini kamaytirish uchun ma’murlar aniqlash chegarasini ko‘taradi, lekin bu aniqlashning umumiy darajasini pasaytirishi mumkin [1]. Shu sababli “.uz” domenida quyi darajada ishlaydigan aniqlash tizimlaridan keluvchi axborotni korrelyatsiyalash talab etiladi. Ushbu ishda milliy segmentda korrelyatsiya jarayonining takomillashtirilgan konseptual modeli bayon etiladi.

Asosiy qism

Milliy segmentda korrelyatsiya jarayoni deganda ikkita tasodifiy miqdor – tahdid T va hujum H – ning bir-biriga aloqadorligi tushuniladi. Tahdid va hujum bir-biriga umuman bog‘liq bo‘lmasligi ham mumkin; bunday bog‘lanishlar yolg‘on korrelyatsiya sifatida belgilanadi. Ikki o‘zgaruvchi orasidagi bog‘lanish o‘lchami sifatida n ta kuzatuv bo‘yicha tanlanma kovariatsiya qo‘llaniladi:

$$cov(T,H) = \frac{1}{n}\sum_{i=1}^{n}(T_i - \overline{T})(H_i - \overline{H}) \quad (1)$$

Hisoblash uchun milliy segment himoya tizimida aniqlangan tahdid va hujumlarning kunlik dinamikasi olindi. Kuzatuvlar 24.07.2024 dan 30.07.2024 gacha, har kuni sutkaning ixtiyoriy tanlangan bir soatlik oralig‘ida o‘tkazildi (1-jadval).

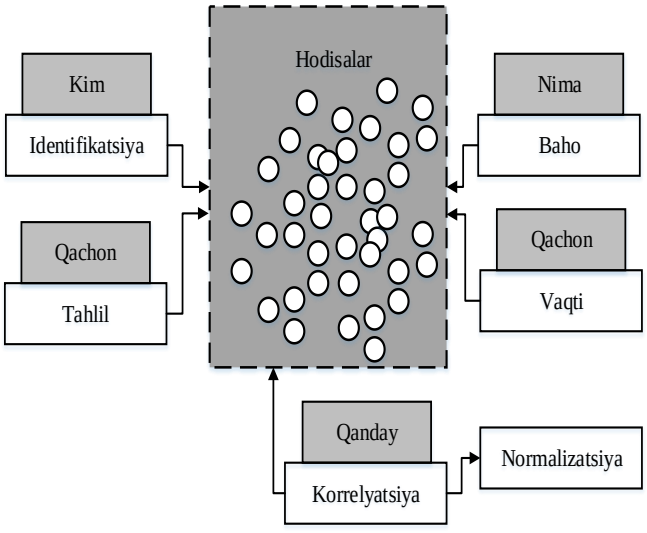
1-jadval

Milliy segmentda sodir bo‘lgan tahdidlar va hujumlar dinamikasi

№	Kuzatish sanasi	Tahdidlar, T	Hujumlar, H	T − T o‘rt.	H − H o‘rt.	Ko‘paytma
1	24.07.2024	3	1	0,429	−0,571	−0,245
2	25.07.2024	2	2	−0,571	0,429	−0,245
3	26.07.2024	3	1	0,429	−0,571	−0,245
4	27.07.2024	4	3	1,429	1,429	2,041
5	28.07.2024	3	1	0,429	−0,571	−0,245
6	29.07.2024	2	2	−0,571	0,429	−0,245
7	30.07.2024	1	1	−1,571	−0,571	0,898
	Yig‘indi	18	11	–	–	1,714
	O‘rtachasi	2,571	1,571	–	–	0,245

Yetti kunda 18 ta tahdid va 11 ta hujum qayd etilgan, tanlanma kovariatsiya 0,245 ga teng. Kovariatsiyaning musbatligi kuzatilgan davrda tahdidlar va hujumlar soni bir yo‘nalishda o‘zgarganini bildiradi, ammo har bir tahdid hujumga aylanmaydi. Demak, har bir ogohlantirishga alohida javob berish o‘rniga ularni o‘zaro bog‘lab tahlil qilish zarur.

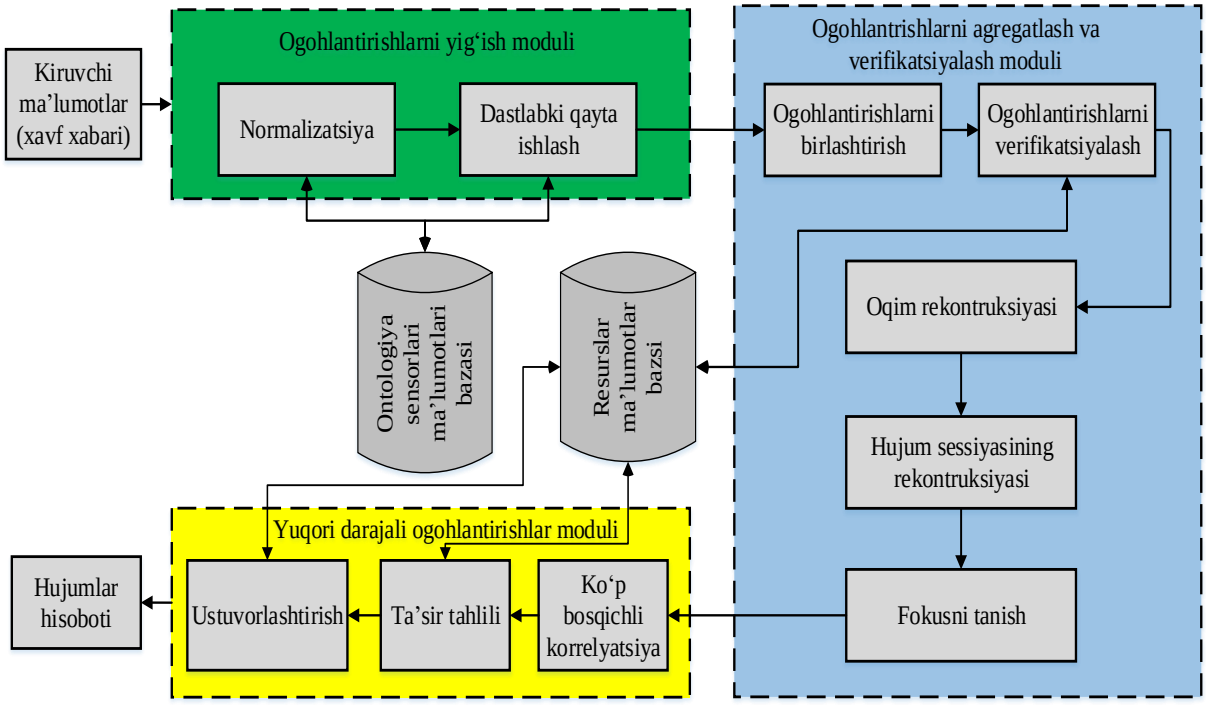
Ogohlantirishlarni korrelyatsiyalash usullarini uch guruhga ajratish mumkin: ogohlantirish atributlari (manba IP-manzili, port va boshqalar) orasidagi o‘xshashlikka asoslangan usullar [2]; hujumning ma’lum ssenariylariga asoslangan usullar (ular ssenariylarni oldindan ko‘rsatishni talab qiladi va faqat ma’lum hujumlarni aniqlaydi); alohida hujumlarning oqibatlari va dastlabki shartlariga asoslangan usullar. Korrelyatsiya vositalari uchun kiruvchi ma’lumotlar hujumlarni aniqlash va bartaraf etish tizimlari, tarmoqlararo ekranlar, veb-server jurnallari kabi turli manbalardan to‘planadi (1-rasm).



1-rasm. Ogohlantirishlar korrelyatsiyasi

Bir nechta manbadan kelgan ogohlantirishlarni korrelyatsiyalash ikki ustunlikni beradi. Birinchidan, bir xil xavf xabarlari birlashtirilib, ortiqcha ogohlantirishlar bartaraf etiladi: IDS/IPS tizimlarida skanerlash kabi hodisalarning takrorlanishi ko‘p miqdorda ortiqcha ogohlantirish hosil qiladi. Ikkinchidan, ko‘p bosqichli hujumlar aniqlanadi: bunday hujumning har bir qadami alohida ogohlantirish yaratadi va ularni faqat o‘zaro aloqalarni tahlil qilish orqali yagona hujum sifatida ko‘rish mumkin.

Shulardan kelib chiqib, milliy segmentda korrelyatsiya jarayonining konseptual modeli hodisalar boshqaruvining uch blokidan iborat etib taklif etiladi (2-rasm). Ogohlantirishlarni yig‘ish moduli xavf xabari sensorlaridan kelgan ma’lumotlarni normalizatsiya qiladi va dastlabki qayta ishlaydi; bunda manba yoki maqsad atributi bo‘sh bo‘lgan xabarlarga eng mos qiymatlar beriladi. Agregatlash va verifikatsiyalash moduli ogohlantirishlarni birlashtiradi va tekshiradi, oqimni hamda hujum sessiyasini rekonstruksiya qiladi, hujum fokusini aniqlaydi. Yuqori darajali ogohlantirishlar moduli ko‘p bosqichli korrelyatsiyani, ta’sir tahlilini va ustuvorlashtirishni bajarib, hujumlar hisobotini shakllantiradi. Modullar ontologiya va sensorlar ma’lumotlar bazasi hamda resurslar ma’lumotlar bazasiga tayanadi.



2-rasm. Milliy segmentdagi korrelyatsiya jarayonining konseptual modeli

Modelning komponentalari turli muhit va vaqt doirasida ishlaydi: ba’zilari qisqa vaqt oynasida bitta serverda yaratilgan ogohlantirishlarni, boshqalari bir necha soat davom etadigan va turli hostlarni qamraydigan hujum ssenariylarini korrelyatsiyalaydi. Bitta komponenta korrelyatsiyalagan ogohlantirishlar keyingi komponentaning kiruvchi ma’lumotlari bo‘lib xizmat qiladi; ayrim komponentalar parallel yoki bir necha marta qo‘llanilishi mumkin. Korrelyatsiya hujumga oid axborotni yo‘qotmasdan bajarilishi shart, buning uchun ikki toifadagi operatsiyadan foydalaniladi: bir nechta bog‘liq ogohlantirishni bitta meta-ogohlantirishga birlashtirish hamda yolg‘on va mavjud bo‘lmagan signallarni aniqlab, jarayondan chiqarish [3].

Model asosida ishlab chiqilgan dasturiy vosita [4] “UZINFOCOM” MChJning milliy segmentda joylashgan veb-resurslarida sinovdan o‘tkazilgan. Xalqaro internet segmentidan yo‘naltirilgan 608 ta DDoS hujumining 98,5 foizi, ya’ni taqriban 599 tasi aniqlangan. Tizimning yolg‘on ishga tushish holatlari 0,7 foizni tashkil etgan, bu boshqa tizimlarga nisbatan 1,1–1,6

marta yaxshi ko‘rsatkichdir. Yolg‘on ishga tushishlarni kamaytirish mexanizmining o‘zi muallifning alohida ishida bayon etilgan [5]. Sinov natijalariga ko‘ra, barcha tahdidlar ham hujumga aylanmasligini hisobga olish himoya talab etilmaydigan tahdidlardan ortiqcha himoyalanishga ketadigan xarajatlarni tejash imkonini beradi.

Xulosa

Milliy segmentda korrelyatsiya jarayonining takomillashtirilgan konseptual modeli ogohlantirishlarni yig‘ish, agregatlash va verifikatsiyalash hamda yuqori darajali ogohlantirishlar modullaridan iborat. Model yolg‘on ogohlantirishlar sonini kamaytiradi va bitta komponenta korrelyatsiyalagan ogohlantirishlardan keyingi komponentaning kiruvchi ma’lumotlari sifatida foydalanish imkonini beradi. Model asosidagi dasturiy vosita amaliy sinovda 608 ta DDoS hujumining 98,5 foizini aniqladi, yolg‘on ishga tushishlar ulushi 0,7 foizni tashkil etdi.

Foydalanilgan adabiyotlar

1. Kumavat K.S., Gomes J. Survey of Detection Techniques for DDoS Attacks // 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM). London, United Kingdom, 2022. P. 657–663.

2. Ambore B., Gupta A.D., Rafi S.M., Yadav S., Joshi K., Sivakumar R.D. A Conceptual Investigation on the Image Processing using Artificial Intelligence and Tensor Flow Models through Correlation Analysis // 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). Greater Noida, India, 2022. P. 278–282.

3. Mukhopadhyay D., Singal G., Ahuja N. DLSDN: Deep Learning for DDoS attack detection in Software Defined Networking // 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence). 2021.

4. Gafurov A.A., Botirov F.B. Internet tarmog‘ining milliy segmentida tahdidlarni bartaraf etish dasturi. EHM uchun dasturga guvohnoma № DGU 37518. Toshkent, 08.05.2024.

5. Botirov F.B., Haydarov E.D., Gafurov A.A. A mechanism to reduce system false starts in attack detection // Science and Education in Karakalpakstan. 2024. №3/2(43). P. 461–463.

MUHIM AXBOROT INFRATUZILMALARI OBYEKTLARINING KIBER-FIZIK TIZIM SIFATIDAGI ARXITEKTURAVIY XUSUSIYATLARI VA KIBERXAVFSIZLIK TAHDIDLARINING TASNIFI

Xudoykulov Z.T., Imamaliyev A.T.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda muhim axborot infratuzilmalari (MAI) obyektlarining kiber-fizik tizim sifatidagi arxitekturaviy xususiyatlari va kiberxavfsizlik tahdidlari tadqiq etiladi. MAI obyektlarida IT va operatsion texnologiyalarning (OT) integratsiyalashuvi natijasida kiber va fizik jarayonlar o‘rtasidagi bog‘liqlik kuchayib bormoqda. Ishda MAI obyektining ko‘p qatlamli arxitekturasi tavsiflanib, asosiy kiberxavfsizlik tahdidlari tasniflangan. Taklif etilgan yondashuv MAI obyektlarida dinamik kiberxavfni baholash va Zero Trust asosida adaptiv foydalanishni boshqarish mexanizmlarini ishlab chiqish uchun nazariy asos yaratadi.

Kalit so‘zlar: muhim axborot infratuzilmasi, kiber-fizik tizim, kiberxavfsizlik, OT, IT, SCADA, ICS, kiberxavf, kiberhujum, Zero Trust.

Аннотация. В тезисе исследуются архитектурные особенности объектов критической информационной инфраструктуры (КИИ) как киберфизических систем и классификация угроз кибербезопасности. Интеграция информационных технологий и операционных технологий (ОТ) в объектах КИИ усиливает взаимосвязь между кибернетическими и физическими процессами. В работе рассматривается многоуровневая архитектура объекта КИИ и классифицируются основные угрозы кибербезопасности. Предложенный подход формирует теоретическую основу для оценки динамического киберриска и разработки механизмов адаптивного управления доступом на основе концепции Zero Trust.

Ключевые слова: критическая информационная инфраструктура, киберфизическая система, кибербезопасность, OT, IT, SCADA, ICS, киберриск, кибератака, Zero Trust.

Kirish

Raqamli texnologiyalarning jadal rivojlanishi natijasida energetika, transport, moliya, telekommunikatsiya, sog‘liqni saqlash, suv ta’minoti va ishlab chiqarish kabi strategik sohalarning faoliyati axborot-kommunikatsiya texnologiyalariga tobora ko‘proq bog‘lanmoqda. Mazkur tizimlarning ishlashidagi uzilishlar nafaqat axborot resurslarining yo‘qolishiga, balki real fizik jarayonlarning buzilishi, iqtisodiy zarar va xizmatlarning to‘xtashiga olib kelishi mumkin [1,4].

Muhim axborot infratuzilmasi obyektlarining o‘ziga xos jihati shundaki, ularda axborot texnologiyalari (IT) va operatsion texnologiyalar (OT) birgalikda ishlaydi. NIST tomonidan berilgan OT xavfsizligi bo‘yicha tavsiyalarda OT fizik muhit bilan bevosita o‘zaro ta’sirlashuvchi va fizik jarayonlarni monitoring hamda boshqarishga xizmat qiluvchi tizimlar majmuasi sifatida ko‘rib chiqiladi [1].

IT tizimlari asosan ma’lumotlarni qayta ishlash, saqlash va uzatishga yo‘naltirilgan bo‘lsa, OT tizimlari fizik jarayonlarni monitoring qilish va boshqarish bilan bog‘liq. Masalan, elektr energetikasi obyektida serverlar, ma’lumotlar bazalari va korporativ tarmoq IT muhitini tashkil etsa, PLC(Programmable Logic Controller), RTU(Remote Terminal Unit), SCADA(Supervisory

Control and Data Acquisition), sensorlar va aktuatorlar OT muhitining asosiy elementlari hisoblanadi.

Natijada MAI obyektlarida kiber muhitdagi o‘zgarishlar fizik jarayonlarga, fizik jarayonlardagi o‘zgarishlar esa axborot tizimlariga ta’sir ko‘rsatishi mumkin. Aynan ushbu ikki tomonlama bog‘liqlik MAI obyektlarini kiber-fizik tizim sifatida tadqiq etish zaruratini yuzaga keltiradi [2, 3].

MAI obyektlarining kiber-fizik tizim sifatidagi arxitekturasi

Kiber-fizik tizim (Cyber-Physical System - CPS) fizik jarayonlar va ularni kuzatish, boshqarish hamda tahlil qilishga xizmat qiluvchi hisoblash va kommunikatsiya komponentlarining integratsiyalashgan majmuasi hisoblanadi [2, 3].

CPS xavfsizligi bo‘yicha tadqiqotlarda fizik jarayonlar, hisoblash vositalari va kommunikatsiya infratuzilmasining o‘zaro bog‘liqligi asosiy xususiyatlardan biri sifatida ko‘rsatiladi [2].

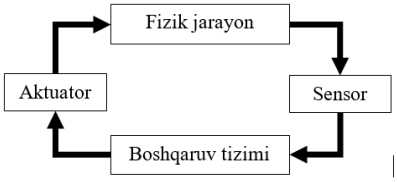
MAI obyektini umumlashtirilgan holda quyidagi asosiy qatlamlardan tashkil topgan kiber-fizik arxitektura sifatida ifodalash mumkin:

1. fizik qatlam;
2. qurilmalar va boshqaruv qatlami;
3. tarmoq va kommunikatsiya qatlami;
4. axborot va hisoblash qatlami;
5. monitoring va boshqaruv qatlami.

1. Fizik qatlam. Fizik qatlam MAI obyektida bevosita real jarayonlarni amalga oshiruvchi qurilmalar va texnologik uskunalarni o‘z ichiga oladi. Energetika obyektlarida generatorlar, transformatorlar va elektr uzatish qurilmalari, transport tizimlarida svetoforlar, temir yo‘l qurilmalari va transport vositalari, ishlab chiqarishda esa stanoklar, robotlashtirilgan qurilmalar va texnologik agregatlar ushbu qatlamga tegishli [1, 3].

Sensorlar fizik muhitdan harorat, bosim, kuchlanish, tok, tezlik yoki oqim kabi parametrlarni o‘lchaydi. Aktuatorlar esa boshqaruv tizimidan kelgan buyruqlar asosida fizik jarayonga ta’sir ko‘rsatadi [2].

Shunday qilib, MAI obyektida quyidagi ko‘rinishda yopiq boshqaruv sikli hosil bo‘ladi:



1-rasm. MAI obyektida yopiq boshqaruv sikli

2. Qurilmalar va boshqaruv qatlami. Ushbu qatlam fizik jarayonlardan ma’lumotlarni yig‘ish va ularni boshqarish uchun foydalaniladigan PLC, RTU, IED, kontrollerlar va boshqa qurilmalarni o‘z ichiga oladi [1].

PLC sensorlardan kelayotgan ma’lumotlarni qabul qiladi, oldindan belgilangan algoritm asosida qayta ishlaydi va aktuatorlarga boshqaruv signalini yuboradi. ICS xavfsizligi bo‘yicha tadqiqotlarda bunday boshqaruv komponentlarining buzilishi fizik jarayonlarga bevosita ta’sir ko‘rsatishi mumkinligi ta’kidlanadi [4].

3. Tarmoq va kommunikatsiya qatlami. Tarmoq qatlami MAI obyektining turli komponentlari o‘rtasida ma’lumot almashinuvini ta’minlaydi. Bunda Ethernet, IP, TCP/UDP, Modbus TCP, DNP3, IEC 60870-5-104 va OPC UA kabi texnologiyalar va protokollardan foydalanilishi mumkin [1].

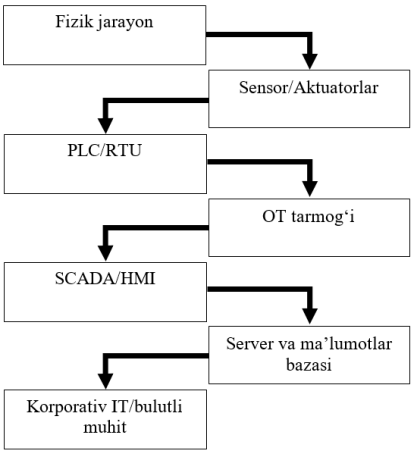
Zamonaviy OT tizimlarining korporativ IT tarmoqlari va masofaviy boshqaruv infratuzilmalari bilan integratsiyalashuvi operatsion samaradorlikni oshiradi, biroq bir vaqtning o‘zida hujum yuzasini ham kengaytirishi mumkin [1, 4].

4. Axborot va hisoblash qatlami. Mazkur qatlam serverlar, ma’lumotlar bazalari, ishchi stansiyalar, tarixiy ma’lumotlarni saqlash tizimlari va boshqa hisoblash resurslarini o‘z ichiga oladi. SCADA serverlari texnologik jarayonlarni monitoring qilish va boshqarishda, Historian tizimlari esa texnologik parametrlarning tarixiy qiymatlarini saqlashda foydalaniladi [1].

Ushbu komponentlarning buzilishi ma’lumotlarning maxfiyligi, yaxlitligi yoki mavjudligiga salbiy ta’sir ko‘rsatishi mumkin. ICS muhitida esa axborot tizimiga qilingan hujum oxir-oqibat fizik jarayonga ta’sir ko‘rsatishi ehtimoli mavjud [4].

5. Monitoring va boshqaruv qatlami. Yuqori darajadagi qatlamda operatorlarning ishchi stansiyalari, HMI, SCADA tizimlari, monitoring va tahlil vositalari joylashadi. Operator HMI orqali fizik jarayonning joriy holatini kuzatadi va zarur hollarda boshqaruv buyruqlarini shakllantiradi [1].

Shu sababli MAI obyektining umumlashtirilgan arxitekturasini 2-rasmda ifodalash mumkin.



2-rasm. MAI obyektining umumlashtirilgan arxitekturasi

MAI obyektlariga tahdidlarning tasnifi

MAI obyektlarining kiberxavfsizligini ta’minlash uchun mavjud tahdidlarni tizimli ravishda tasniflash talab etiladi. NIST OT xavfsizligi bo‘yicha qo‘llanmasida OT muhitiga xos bo‘lgan xavfsizlik tahdidlarini hisobga olish zarurligi ta’kidlanadi [1].

1-jadval

MAI obyektlariga asosiy kiberxavfsizlik tahdidlarining tasnifi

Tahdid turi	Asosiy ko‘rinishlari	Ta’sir
Tarmoq tahdidlari	DoS/DDoS, MITM, spoofing, sniffing	Aloqa buzilishi, ma’lumotlarning o‘zgartirilishi
Zararli dasturlar	Ransomware, trojan, worm, spyware	Tizimning ishdan chiqishi, ma’lumotlarning yo‘qolishi
Identifikatsiya tahdidlari	Brute-force, phishing, credential theft	Hisob yozuvining egallanishi
Ichki tahdidlar	Imtiyozni suiiste’mol qilish, xatolar	Ma’lumot yoki boshqaruvning buzilishi
Ma’lumot tahdidlari	O‘zgartirish, yo‘qotish, soxtalashtirish	Qarorlarning noto‘g‘ri qabul qilinishi

Qurilma tahdidlari	PLC/RTU konfiguratsiyasini o‘zgartirish	Fizik jarayonning noto‘g‘ri boshqarilishi
OT tahdidlari	SCADA/HMI zaifliklaridan foydalanish	Texnologik jarayonning buzilishi
Fizik tahdidlar	Qurilmaga jismoniy kirish, sabotaj	Uskunaning ishdan chiqishi
Ta’minot zanjiri tahdidlari	Uchinchi tomon dasturi yoki qurilmasi orqali hujum	Tizimga noqonuniy kirish
Masofaviy ulanish tahdidlari	VPN, RDP va boshqa servislarni suiiste’mol qilish	Ichki tarmoqqa noqonuniy kirish

Tahdidlarni maxfiylik, yaxlitlik va mavjudlik mezonlari bo‘yicha ham guruhlash mumkin. Biroq MAI obyektlari uchun ushbu uchta klassik xavfsizlik xususiyatiga qo‘shimcha ravishda fizik xavfsizlik, inson xavfsizligi va texnologik jarayonning uzluksizligi ham alohida e’tiborga olinishi lozim [1, 4].

Maxfiylikka qarshi tahdidlar. Bunday tahdidlar axborotning ruxsatsiz olinishi bilan bog‘liq. Masalan, trafikni tinglash, ma’lumotlar bazasiga noqonuniy kirish yoki maxfiy ma’lumotlarni o‘g‘irlash.

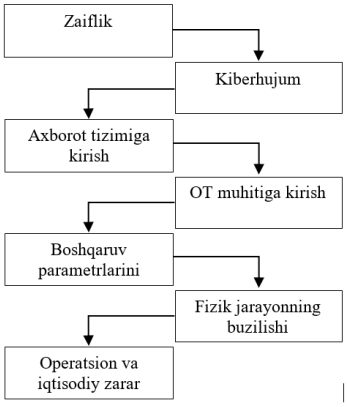
Yaxlitlikka qarshi tahdidlar. Ushbu tahdidlar ma’lumotlarning noqonuniy o‘zgartirilishiga qaratiladi. MAI uchun yaxlitlik ayniqsa muhim, chunki noto‘g‘ri texnologik parametr fizik jarayonni noto‘g‘ri boshqarishga olib kelishi mumkin [1,4].

Mavjudlikka qarshi tahdidlar. DoS/DDoS, ransomware yoki tarmoq qurilmalarini ishdan chiqarish kabi hujumlar tizimning mavjudligini buzishi mumkin [1].

Fizik jarayonga qarshi tahdidlar. MAI obyektlarida eng muhim jihatlardan biri - kiberhujumning fizik oqibatga aylanishidir. Masalan, PLC konfiguratsiyasining noqonuniy o‘zgartirilishi boshqaruv algoritmining buzilishiga va natijada fizik qurilmaning noto‘g‘ri ishlashiga olib kelishi mumkin [2, 4].

Tahdidlarning kiber-fizik jarayonlarga o‘zaro ta’siri

MAI obyektlarida kiberhujumning amalga oshirilish bosqichini 3-rasmdagi ko‘rinishda ifodalash mumkin.



3-rasm. MAI obyektlarida kiberhujumning amalga oshirilish bosqichi

CPS xavfsizligi bo‘yicha tadqiqotlarda kiber muhitdagi zaifliklardan foydalanish orqali fizik jarayonlarga ta’sir ko‘rsatish imkoniyati tizimning muhim xavfsizlik muammolaridan biri sifatida qaraladi [2]. Masalan, hujumchi korporativ tarmoqdagi foydalanuvchi hisob yozuvini qo‘lga kiritgandan so‘ng ichki tarmoqqa kirishi, OT segmentiga o‘tishi va SCADA yoki PLC komponentlariga ta’sir ko‘rsatishga urinishi mumkin [1, 4]. Shu sababli MAI obyektlarida

xavfsizlikni faqat alohida qurilmani himoyalash darajasida tashkil etish yetarli emas. Butun kiber-fizik tizim bo‘ylab xavflarni hisobga olish talab etiladi.

MAI xavfsizligini ta’minlashga zamonaviy yondashuv

MAI obyektlarining murakkab va dinamik tabiati xavfsizlikni statik qoidalar asosida emas, balki kontekst va real vaqt holatini hisobga olgan holda tashkil etishni talab qiladi.

Zero Trust Architecture yondashuvida foydalanuvchi yoki qurilmaga faqat tarmoqning ichki qismida joylashgani sababli avtomatik ravishda ishonch bildirilmaydi. Kirish qarori foydalanuvchi, qurilma, resurs va muhit haqidagi tegishli ma’lumotlarni hisobga olgan holda shakllantiriladi [5].

MAI obyektlarida quyidagi omillarni hisobga olish maqsadga muvofiq: foydalanuvchining identifikatsiyasi; qurilmaning ishonchlilik holati; foydalanuvchining odatiy xatti-harakati; tarmoqdagi joriy faollik; resursning muhimlik darajasi; aniqlangan zaifliklar; joriy kiberxavf darajasi; kirish vaqti va konteksti; avvalgi faoliyat tarixi.

Mazkur omillar asosida subyekt yoki qurilmaning dinamik xavfsizlik profili shakllantirilishi mumkin. Bu esa MAI obyektlarida dinamik riskga asoslangan foydalanishni boshqarish mexanizmlarini ishlab chiqish uchun asos bo‘lib xizmat qiladi.

Xulosa

Tadqiqot natijasida muhim axborot infratuzilmalari obyektlarini kiber-fizik tizim sifatida ko‘rib chiqish ularning xavfsizlik xususiyatlarini yanada to‘liq ifodalash imkonini berishi aniqlandi. MAI obyektlari fizik qurilmalar, sensorlar, aktuatorlar, PLC va RTU kabi boshqaruv qurilmalari, OT va IT tarmoqlari, SCADA/HMI tizimlari, serverlar hamda ma’lumotlarni qayta ishlash vositalarining o‘zaro bog‘langan majmuasidan tashkil topadi.

Mazkur arxitekturadagi o‘zaro bog‘liqlik kiberxavfsizlik tahdidlarining fizik jarayonlarga ta’sir ko‘rsatish imkoniyatini oshiradi. Shu sababli tahdidlarni faqat maxfiylik, yaxlitlik va mavjudlik nuqtayi nazaridan emas, balki ularning fizik jarayonlar, texnologik xavfsizlik va xizmatlarning uzluksizligiga ta’siri nuqtayi nazaridan ham baholash zarur.

MAI obyektlarining arxitekturaviy xususiyatlari va tahdidlar tasnifi keyingi bosqichda dinamik kiberxavfni baholash, foydalanuvchi va qurilmalarning xulq-atvor profilini shakllantirish hamda Zero Trust tamoyiliga asoslangan dinamik riskga bog‘liq foydalanishni boshqarish mexanizmlarini ishlab chiqish uchun nazariy asos yaratadi.

Foydalanilgan adabiyotlar

1. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, T. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3, 2023. DOI: 10.6028/NIST.SP.800-82r3.

2. Humayed, A., Lin, J., Li, F., Luo, B. Cyber-Physical Systems Security-A Survey. IEEE Internet of Things Journal, 2017, Vol. 4, No. 6, pp. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.

3. Lee, E. A. Cyber Physical Systems: Design Challenges. 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, 2008. DOI: 10.1109/ISORC.2008.25.

4. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., Jones, K. A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 2015, Vol. 9, pp. 52–80. DOI: 10.1016/j.ijcip.2015.02.002.

5. Rose, S., Borchert, O., Mitchell, S., Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207, 2020. DOI: 10.6028/NIST.SP.800-207.

RAQAMLASHGAN QO‘RIQLASH TIZIMLARINING KIBERBARDOSHLIGINI TA’MINLASH MUAMMOLARI

Xudoykulov Z.T., Imamaliyev A.T.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada global raqamlashtirish sharoitida raqamlashgan qo‘riqlash tizimlarining (IP-kameralar, kirish nazorati va IoT sensorlari) kiberbardoshligini ta’minlash muammolari tahlil qilingan. Tizimlarning ochiq tarmoqlarga ulanishi natijasida yuzaga keladigan asosiy kibertahdidlar, jumladan, autentifikatsiyaning buzilishi, ma’lumotlarni soxtalashtirish (video spoofing), DoS/DDoS hujumlari hamda dasturiy ta’minotdagi “backdoor” va IoT zaifliklari o‘rganib chiqilgan. Maqolada ushbu tahdidlarning jismoniy va funksional xavfsizlikka ta’siri baholanib, tizimlar kiberbardoshligini oshirish bo‘yicha muhandislik-texnik va tashkiliy choralar, xususan, Zero Trust modeli, ko‘p faktorli autentifikatsiya (MFA), end-to-end shifrlash (TLS 1.3, SRTP) va tarmoq segmentatsiyasi kabi zamonaviy himoya mexanizmlari taklif etilgan.

Kalit so‘zlar: raqamlashgan qo‘riqlash tizimlari, kiberbardoshlik, kibertahdidlar, IoT zaifliklari, video spoofing, DDoS hujumlari, Zero Trust modeli, ma’lumotlarni shifrlash, tarmoq segmentatsiyasi.

Аннотация. В данной статье анализируются проблемы обеспечения киберустойчивости цифровых систем охраны (IP-камеры, системы контроля доступа и IoT-датчики) в условиях глобальной цифровизации. Исследуются основные киберугрозы, возникающие при подключении этих систем к открытым информационным сетям, включая нарушение аутентификации, подмену данных (видео-спуфинг), DoS/DDoS-атаки, программные «бэкдоры» и уязвимости устройств интернета вещей (IoT). В работе оценивается влияние данных угроз на физическую и функциональную безопасность охраняемых объектов, а также предлагаются инженерно-технические и организационные рекомендации по повышению их киберзащищенности, такие как внедрение модели Zero Trust, многофакторной аутентификации (MFA), сквозного шифрования (TLS 1.3, SRTP) и сегментации сети.

Ключевые слова: цифровые системы охраны, киберустойчивость, киберугрозы, уязвимости IoT, видео-спуфинг, DDoS-атаки, модель Zero Trust, шифрование данных, сегментация сети.

Kirish

Bugungi kunda global raqamlashtirish jarayonlari barcha sohalar qatori xavfsizlik va qo‘riqlash faoliyatini ham tubdan transformatsiya qilmoqda. An’anaviy muhandislik-texnik vositalarning intellektual tizimlar, narsalar interneti (IoT) va sun’iy intellekt texnologiyalari bilan integratsiyalashuvi ob’ektlar xavfsizligini ta’minlashda yangi imkoniyatlar ochmoqda. Biroq, tizimlarning ochiq axborot tarmoqlariga ulanishi va raqamlashishi ularni an’anaviy jismoniy tahdidlar bilan bir qatorda, kiberhujumlar nishoniga ham aylantirmoqda. Raqamlashgan qo‘riqlash tizimlariga nisbatan amalga oshiriladigan kiberhujumlar nafaqat maxfiy ma’lumotlarning sizib chiqishiga, balki strategik ahamiyatga ega ob’ektlar boshqaruvining yo‘qotilishiga va jiddiy moddiy-ma’naviy zararlarga olib kelishi mumkin. Shu sababli, zamonaviy qo‘riqlash tizimlarining kiber-barqarorligini ta’minlash, ulardagi zaif nuqtalarni aniqlash va himoya mexanizmlarini takomillashtirish masalasi sohadagi eng ustuvor muammolardan biri hisoblanadi.

Ushbu maqolaning maqsadi raqamlashgan qo‘riqlash tizimlariga nisbatan yuzaga kelayotgan kiber-tahdidlarni tahlil qilish hamda tizimlarning kiber-barqarorligini oshirish bo‘yicha muhandislik-texnik va tashkiliy tavsiyalarni ishlab chiqishdan iborat. Ushbu maqolada quyidagi muammolar o‘rganib chiqiladi va ularni oldini olish choralari taklif etiladi: Audentifikatsiya tizimlarini buzilishi; Ma’lumotlar almashtirilishi; DoS/DDoS hujumlari; Dasturiy ta’minotdagi “Backdoor”lar; IoT tizimlaridagi zaifliklar;

Ma’lumki, autentifikatsiya tizimini buzulishi raqamlashgan qo‘riqlash tizimlarida eng xavfli kibertahdidlardan biri hisoblanadi. Bunday tahdidlar oqibatida quyidagilar yuzaga kelishi mumkin [1; 5-b]:

– fizik xavfsizlik tizimi buziladi. O‘g‘rilik, sabotaj, terror hujumlari yashirincha amalga oshirilishi mumkin.

– maxfiy axborot sizdiriladi. Video tasvirlar, kirish jurnallari, biometrik ma’lumotlar o‘g‘irlanadi.

– tizim ish faoliyati to‘xtaydi. Monitoring qilib bo‘lmaydi, signalizatsiya ishlamaydi.

– moliyaviy zarar. Jarimalar, mijozlar ishonchsizligi yuzaga keladi.

Ushbu oqibatlar yuzaga kelmasligi uchun quyidagi choralar qo‘llaniladi:

– Default parollarni majburiy o‘zgartirish.

– Parollar siyosati va MFA (Multi-Factor Authentication)ni qo‘llash.

– Eng kam vakolat tamoili.

– Parol menejerlari va monitoring. Parollar sizishini tekshirish (Have I Been Pwned integratsiyasi).

– Zero Trust modeli. Har bir kirishni doimiy tekshirish talab etiladi.

– Tarmoq segmentatsiyasi. Qo‘riqlash tizimlari alohida VLANda, internetdan izolyatsiyalangan bo‘lishi kerak.

– Doimiy monitoring va SIEM. Noqonuniy kirishga urinishlarni aniqlash (masalan, 5 daqiqada 100 ta login urinish).

– Dasturiy ta’minot (Firmware) va ularni yangilash. dasturiy ta'minotdagi xatoliklarni tuzatish, xavfsizlik zaifliklarini yopish va funksionallikni yangilash jarayonini inson aralashuvisiz amalga oshirish (Avtomatik patching). Lekin test jarayonidan o‘tkazilgandan keyin.

Ma’lumotlarni almashtirish (Spoofing yoki video feed spoofing / injection) raqamlashtirilgan qo‘riqlash tizimlarida (CCTV, IP-kameralar, videokuzatuv tizimlari) eng xavfli kibertahdidlardan biri bo‘lib, ular oqibatida quyidagilar yuzaga keladi [2; 14-b]: Fizik tahdid yashiriladi. O‘g‘rilik, sabotaj sodir bo‘ladi, lekin monitoringda "tinch" holat ko‘rsatiladi. Dalillar yo‘qoladi. Keyinroq bo‘ladigan tekshiruvda video arxiv ma’lumotlari soxta bo‘lib chiqadi. Ishonchsizlik. Tizimga bo‘lgan ishonch darajasi pasayadi, tizim xavfsizligi obro‘sizlanadi ("false sense of security").

Ushbu muammolarni oldini olish uchun quyidagi choralar qo‘llaniladi:

Tarmoqni segmentlash va himoyalash. Kameralarni alohida VLANda saqlash, firewall va IPS orqali MitM ni bloklash.

Tasdiqlash va shifrlash. RTSP o‘rniga RTSP over TLS (port 554 → 443), SRTP shifrlash, foydalanuvchilarni sertifikatlar orqali autentifikatlash.

Anomaliyani aniqlash. AI asosidagi monitoring (Nozomi, Claroty, Armis) orqali tasvir oqimida o‘zgarishlar (statik sahna uzoq davom etsa, yorug‘lik o‘zgarmasa) aniqlanadi.

Elektr tarmog'i chastotasi (Electrical Network Frequency - ENF) tekshiruvi. Elektr tarmog‘i chastotasini tasvirga “shtamp” qilib qo‘yish. Soxta video ENF ni to‘g‘ri ko‘rsatmaydi [3; 19-b].

Dasturiy ta’minot himoyasi. Signed firmware, secure boot dasturlari avtomatik yangilash.

Hayotiylik va yaxlitlik tekshiruvi. Har bir kadrda metadata (timestamp, hash) qo‘shish, uzatish zanjirini saqlash.

“Kiberxavfsizlik to‘g‘risida”gi Qonun talablariga ko‘ra, muhim ob’ektlarda monitoring va attestatsiya majburiy, video oqimini shifrlash va anomaliya aniqlashni qo‘shish kerak.

DoS/DDoS hujumlar (Denial of Service / Distributed Denial of Service) raqamlashtirilgan qo‘riqlash tizimlarida eng keng tarqalgan va jiddiy tahdidlardan biri bo‘lib, Bunday tahdidlar oqibatida quyidagilar yuzaga kelishi mumkin [4; 13-b]: Monitoring va signalizatsiya tizimi ishdan chiqadi. Real vaqt rejimida tasvir yo‘qoladi va ogohlantirish tizimi ishlamaydi. Fizik xavfsizlik buziladi. Hujumchi “tinch” tasvirni ishlatib, ob’ektga kirishi mumkin. Tizimni tiklash qiyin bo‘ladi. DDoS davom etsa, server yoki NVR (Network Video Recorder) qayta ishga tushishi uzoq vaqt talab qiladi. Moliyaviy zarari va obro‘sizlanish. Ob’ekt zarar ko‘rsa, jarimalar, mijozlar ishonchsizligi yuzaga keladi.

Dasturiy ta’minotdagi “backdoor”lar (software vulnerabilities, default passwords va outdated firmware) raqamlashtirilgan qo‘riqlash tizimlarida (IP-kameralar, sensorlar/datchiklar, kirish nazorati kontrollerlari) eng keng tarqalgan va eng oson ekspluatatsiya qilinadigan zaiflik bo‘lib, ular oqibatida quyidagilar yuzaga keladi [5; 11-b]:

Kirish huquqini olish. Buzg‘unchi administrator vakolatini olib, kameralarni o‘chirish, tasvirlarni buzish yoki eshiklarni ochish imkoniyatiga ega bo‘lishi mumkin. Botnetga qo‘shilish. Qurilmalar DDoS hujumlarida ishlatiladigan “zombi”ga aylantiriladi, bu esa monitoring tizimini to‘xtatishiga olib keladi. Fizik tahdid. Monitoring yo‘qoladi, signalizatsiya tizimi ishlamaydi, ob’ekt himoyasiz qoladi. Ma’lumot sizishi. Video arxivlari, kirish jurnallari o‘g‘irlanadi.

IoT zaifligi. IoT qurilmalari ko‘p holatlarda kuchli shifrlash tizimiga ega bo‘lmaydi. Bu esa raqamlashtirilgan qo‘riqlash tizimlarida (IP-kameralar, kirish nazorati sensorlari, IoT datchiklari, smart qulflar va boshqalar) jiddiy va keng tarqalgan muammolardan biri bo‘lib, bular natijasida quyidagi oqibatlar yuzaga keladi [6; 20-b]:

- ma’lumotlar sizishi. Video tasvirlar, kirish loglari, biometrik ma’lumotlar o‘g‘irlanadi.
- MITM va spoofing hujumlari. Tasvir buziladi yoki soxtalashtiriladi.
- Botnet va DDoS hujumlari. Zaif himoyalangan qurilmalar botga aylantiriladi.
- fizik tahdid. Monitoring tizimi buzilgani uchun ob’ekt himoyasiz qoladi.

Ushbu muammoni oldini olish uchun quyidagi choralari qo‘llaniladi:

– Nuqtadan nuqtagacha shifrlash. TLS 1.3, SRTP (video uchun), MQTT over TLS protokollaridan foydalanish.

– Xavfsizlik protokollari. HTTP o‘rniga HTTPS, RTSP o‘rniga RTSP over TLS, Telnet o‘rniga SSH protokollarini qo‘llash.

– Sertifikat asosidagi autentifikatsiya. Qurilmalarga unikal sertifikatlar berish (mTLS).

– Dasturiy ta’minot va protokollarni yangilash. Dasturiy ta’minotni avtomatik yangilash, protokol versiyalarini yangilash.

– Tarmoq himoyasi. VPN tunnel, segmentlash (VLAN), firewall orqali IoT ni izolyatsiyalash.

– Standartlardan foydalanish. IEC 62443, ISO 27001, ETSI EN 303 645 (IoT baseline security).

– Qonun talablariga rioya qilish. Shifrlangan aloqa, monitoring, attestatsiya bo‘yicha qonun talablariga rioya qilish. Xodimlarni o‘qitish, vendorlar o‘rtasida shifrlashni talab qilish.

Xulosa

Raqamlashtirish sharoitida qo‘riqlash faoliyatini muhandislik-texnik modernizatsiyalash jarayonida kibertahdidlar va zaifliklar keskin oshmoqda. Raqamlashtirilgan qo‘riqlash tizimlari (IP-kameralar, kirish nazorati, IoT sensorlari, integratsiyalashgan PSIM tizimlari) IoT texnologiyalari, bulutli hisoblash va real vaqt monitoringiga asoslangan bo‘lsada, ularning kiberbardoshligini ta’minlashda quyidagi asosiy muammolar mavjud:

– autentifikatsiya tizimining buzilishi (default/zaif parollar, credential stuffing, privilege escalation) orqali administrator huquqini qo‘lga kiritish va tizimni nazorat qilishi;

– ma’lumotlarni almashtirish (video spoofing/injection) - real tasvirni oldindan yozilgan “tinch” video bilan almashtirish (MitM yoki firmware buzilishi orqali).

– DoS/DDoS hujumlar - server yoki NVR ni to‘xtatish, monitoring va signalizatsiya tizimlarini ishdan (Mirai turidagi botnetlar orqali);

– dasturiy ta’minotdagi backdoorlar - standart parollar o‘zgartirilmasligi va firmware yangilanmasligi (Mirai, CVE zaifliklari);

– IoT zaifligi – zaif shifrlash tizimlari, xavfsiz bo‘lmagan protokollar (HTTP, RTSP, Telnet) orqali ma’lumotlar sirqib chiqishi va yashirin tinglash (Eavesdropping).

Ushbu tahdidlar oqibatida fizik xavfsizlik buziladi, monitoring tizimlari ishdan chiqadi, eshiklar masofadan ochiladi, tasvirlar buziladi, ob’ekt himoyasiz qoladi.

Kiberbardoshlikni ta’minlash uchun quyidagi choralarni qo‘llash tavsiya etiladi:

– Zero Trust modelidan, MFA va kuchli autentifikatsiya mexanizmlaridan foydalanish.

– tarmoqni segmentlash, nuqtadan nuqtaga (end-to-end) shifrlash (TLS 1.3, SRTP).

– dasturiy ta’minotni (firmware) avtomatik yangilab borish, anomaliyalarni aniqlash (AI monitoring orqali).

– IEC 62443 (OT/IoT uchun), ISO 27001 (ISMS) kabi standartlarga rioya qilish.

Foydalanilgan adabiyotlar

1. Roberts D. K. Security camera video authentication //Proceedings of 2002 IEEE 10th Digital Signal Processing Workshop, 2002 and the 2nd Signal Processing Education Workshop. – IEEE, 2002. – C. 125-130.

2. Peri D., Wool A. STOP! Camera spoofing via the in-vehicle IP network //2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2025. – C. 296-310.

3. Nagothu D. et al. Detecting malicious false frame injection attacks on surveillance systems at the edge using electrical network frequency signals //Sensors. – 2019. – T. 19. – №. 11. – C. 2424.

4. Koga K. et al. A proposal of an extended method of IP trace-back for distributed denial of service attacks using a dynamic marking scheme //Electronics and Communications in Japan. – 2011. – T. 94. – №. 12. – C. 29-44.

5. Wu Y. et al. Your firmware has arrived: A study of firmware update vulnerabilities //33rd USENIX Security Symposium (USENIX Security 24). – 2024. – C. 5627-5644.

6. Butun I., Österberg P., Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures //IEEE Communications Surveys & Tutorials. – 2019. – T. 22. – №. 1. – C. 616-644.

AN’ANAVIY VA ATRIBUTLARGA ASOSLANGAN FOYDALANISHNI BOSHQARISH MODELLARI

Xudoykulov Z.T., Imamaliyev A.T.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda axborot tizimlarida foydalanishni boshqarishning an’anaviy modellari hamda atributlarga asoslangan foydalanishni boshqarish (Attribute-Based Access Control - ABAC) modeli tahlil qilinadi. Foydalanishni boshqarish axborot xavfsizligining muhim tarkibiy qismi bo‘lib, axborot resurslariga kim, qaysi shartlarda va qanday amallarni bajarishi mumkinligini belgilaydi. An’anaviy yondashuvlarda foydalanish huquqlari asosan subyekt, obyekt, rol yoki xavfsizlik darajasi kabi oldindan belgilangan parametrlar asosida aniqlansa, ABAC modelida subyekt, obyekt, amal va muhitga oid atributlar asosida foydalanish qarori shakllantiriladi. Tezisda DAC, MAC va RBAC modellarining asosiy xususiyatlari, ularning afzalliklari va cheklovlari hamda ABAC modelining dinamik va kontekstga bog‘liq muhitlarda qo‘llanilish imkoniyatlari ko‘rib chiqiladi.

Kalit so‘zlar: axborot xavfsizligi, foydalanishni boshqarish, DAC, MAC, RBAC, ABAC, atribut, subyekt, obyekt, rol, siyosat, kontekst, xavfsizlik.

Аннотация. В данной тезисе анализируются традиционные модели управления доступом в информационных системах, а также модель управления доступом на основе атрибутов (Attribute-Based Access Control - ABAC). Управление доступом является важнейшим компонентом информационной безопасности и определяет, кто, при каких условиях и какие действия может выполнять с информационными ресурсами. В традиционных подходах права доступа определяются преимущественно на основе заранее заданных параметров, таких как субъект, объект, роль или уровень безопасности, тогда как в модели ABAC решение о предоставлении доступа формируется на основе атрибутов субъекта, объекта, действия и среды. В тезисе рассматриваются основные характеристики моделей DAC, MAC и RBAC, их преимущества и ограничения, а также возможности применения модели ABAC в динамических и контекстно-зависимых средах.

Ключевые слова: информационная безопасность, управление доступом, DAC, MAC, RBAC, ABAC, атрибут, субъект, объект, роль, политика, контекст, безопасность.

Kirish

Axborot tizimlarida ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashda foydalanishni boshqarish muhim ahamiyatga ega. Foydalanishni boshqarish mexanizmlari foydalanuvchilar va boshqa subyektlarning tizim resurslariga murojaatini nazorat qiladi hamda ularga ruxsat etilgan amallarni belgilaydi.

An’anaviy foydalanishni boshqarish yondashuvlari orasida Discretionary Access Control (DAC), Mandatory Access Control (MAC) va Role-Based Access Control (RBAC) modellari keng qo‘llaniladi. Ayniqsa, RBAC modelida ruxsatlarni foydalanuvchilarga bevosita emas, balki ular bajaradigan rollar orqali biriktirish katta axborot tizimlarida foydalanish huquqlarini boshqarishni soddalashtiradi [3].

Biroq zamonaviy korporativ tarmoqlar, bulutli hisoblash, mobil qurilmalar, IoT va taqsimlangan axborot tizimlarining rivojlanishi natijasida foydalanish qarorini faqat foydalanuvchining identifikatori yoki roli asosida qabul qilish har doim ham yetarli bo‘lmaydi.

Bunday tizimlarda foydalanuvchining roli bilan bir qatorda uning qurilmasi, joylashuvi, foydalanish vaqti, resursning turi, qurilmaning xavfsizlik holati va boshqa kontekstual omillarni ham hisobga olish talab qilinadi [1, 4].

Foydalanishni boshqarishning an’anaviy modellari

An’anaviy foydalanishni boshqarish modellarida ruxsat berish jarayoni oldindan belgilangan qoidalar va xavfsizlik siyosatlari asosida amalga oshiriladi. Ularning eng muhimlari DAC, MAC va RBAC modellaridir.

DAC modeli. Foydalanishni boshqarishning diskretsion modeli bo‘lib, unda obyekt egasi ushbu obyektga boshqa subyektlarning murojaat qilish huquqlarini belgilashi mumkin.

DAC modelida har bir obyektga nisbatan bajarilishi mumkin bo‘lgan amallar, odatda, ACL (Access Control List) orqali ifodalanadi. Masalan, *Hisobot.xlsx* fayliga nisbatan turli foydalanuvchilarga o‘qish, yozish yoki o‘chirish huquqlari berilishi mumkin.

DAC modelining asosiy afzalligi uning nisbatan sodda va moslashuvchanligidir. Shu bilan birga, foydalanuvchilar va obyektlar soni ortishi bilan ruxsatlarni boshqarish murakkablashadi. Bundan tashqari, obyekt egasining ruxsatlarni boshqa subyektlarga berish imkoniyati markazlashtirilgan xavfsizlik nazoratini murakkablashtirishi mumkin.

MAC (Mandatory Access Control) modeli - mandatliy foydalanishni boshqarish modeli bo‘lib, unda foydalanish huquqlari markazlashtirilgan xavfsizlik siyosati asosida belgilanadi. MAC yondashuvida subyektlar va obyektlarga xavfsizlik darajalari yoki teglar (yoriqlar) biriktiriladi.

Masalan, axborot resurslari quyidagi darajalarga ajratilishi mumkin: Public; Confidential; Secret; Top Secret.

Subyektning xavfsizlik darajasi va obyektning xavfsizlik yorlig‘i o‘zaro taqqoslanib, foydalanishga ruxsat berish yoki rad etish to‘g‘risida qaror qabul qilinadi.

MAC modelining muhim xususiyati shundaki, oddiy foydalanuvchi xavfsizlik siyosatini o‘z xohishiga ko‘ra o‘zgartira olmaydi. Shu sababli ushbu model qat’iy xavfsizlik talablari mavjud bo‘lgan muhitlarda qo‘llanilishi mumkin.

RBAC modelida foydalanish huquqlari foydalanuvchiga bevosita emas, balki uning *roliga* biriktiriladi. Bunda umumiy mantiq:

Foydalanuvchi → Rol → Ruxsat ko‘rinishida ifodalanadi.

RBAC modelining asosiy g‘oyasi Sandhu va boshqalar tomonidan ishlab chiqilgan klassik RBAC modellarida batafsil tavsiflangan bo‘lib, ruxsatlarni rollar orqali boshqarish yirik tizimlarda xavfsizlik ma’muriyatini soddalashtirishi ko‘rsatilgan [3].

Masalan, universitet axborot tizimida quyidagi rollar mavjud bo‘lishi mumkin: Talaba; O‘qituvchi; Kafedra mudiri; Administrator.

O‘qituvchi roliga talabalar ma’lumotlarini ko‘rish, baholarni kiritish va o‘quv materiallarini joylashtirish huquqlari biriktirilishi mumkin.

RBAC modelining afzalligi - tashkilotdagi ko‘p sonli foydalanuvchilar uchun ruxsatlarni markazlashtirilgan holda boshqarish imkoniyatidir. Biroq murakkab va dinamik sharoitlarda faqat rollardan foydalanish ortiqcha rollarning ko‘payishiga olib kelishi mumkin.

An’anaviy modellarning cheklovlari

An’anaviy modellar turli vazifalarni samarali hal qilsa-da, zamonaviy dinamik axborot tizimlarida ayrim cheklovlarga ega. Masalan, RBAC modelida foydalanuvchiga Administrator roli biriktirilgan bo‘lsa, ushbu rolga tegishli ruxsatlar odatda foydalanuvchining joriy joylashuvi, qurilmasining xavfsizlik holati yoki foydalanish vaqtiga bevosita bog‘lanmaydi.

Boshqa tomondan, zamonaviy tizimlarda quyidagi kabi shartlarni hisobga olish zarur bo‘lishi mumkin: foydalanuvchining identifikatori; lavozimi yoki roli; qurilmaning turi; qurilmaning xavfsizlik holati; IP-manzil; geografik joylashuv; foydalanish vaqti; resursning maxfiylik darajasi; bajarilayotgan amal; joriy xavfsizlik holati.

Bunday ko‘p omilli siyosatlarni ifodalash uchun atributlarga asoslangan yondashuvdan foydalanish mumkin [1, 2].

Atributlarga asoslangan foydalanishni boshqarish

ABAC (Attribute-Based Access Control) modeli - foydalanishga ruxsat berish yoki rad etish qarorini subyekt, obyekt, bajarilayotgan amal va muhitga tegishli atributlarni baholash orqali shakllantiruvchi modeldir [1].

NIST SP 800-162 hujjatida ABAC foydalanishni boshqarish metodologiyasi sifatida tavsiflanib, avtorizatsiya qarori subyekt, obyekt, so‘ralayotgan amal va zarur hollarda muhit shartlariga tegishli atributlarning siyosat va qoidalar bilan taqqoslanishi asosida aniqlanishi ko‘rsatilgan [1].

ABAC modelida asosiy atributlar to‘rtta guruhga ajratilishi mumkin [1, 2]:

Subyekt atributlari - foydalanuvchi yoki xizmat haqidagi ma’lumotlar;

Obyekt atributlari - himoyalanayotgan resurs haqidagi ma’lumotlar;

Amal atributlari - bajarilishi so‘ralayotgan amallar;

Muhit atributlari - foydalanish sodir bo‘layotgan sharoitlar.

Masalan, subyekt quyidagi atributlarga ega bo‘lishi mumkin:

role = teacher

department = cybersecurity

clearance = confidential

Obyekt atributlari:

type = student_record

classification = confidential

Amal atributlari:

action = read

Muhit atributlari:

location = university

time = working_hours

device_status = trusted

Shunda foydalanish siyosati quyidagicha ifodalanishi mumkin:

IF role = teacher

AND department = cybersecurity

AND device_status = trusted

AND location = university

AND time = working_hours

THEN Permit.

Bu yerda qaror faqat foydalanuvchining roliga emas, balki bir nechta atributlarning birgalikdagi qiymatiga asoslanadi.

ABACning moslashuvchanligi uning asosiy afzalliklaridan biri bo‘lib, u dinamik va taqsimlangan muhitlarda murakkab foydalanish siyosatlarini ifodalash imkonini beradi [2, 5].

ABAC modelining asosiy komponentlari. ABAC arxitekturasida foydalanish qarorini shakllantirishda bir nechta funksional komponentlardan foydalanish mumkin.

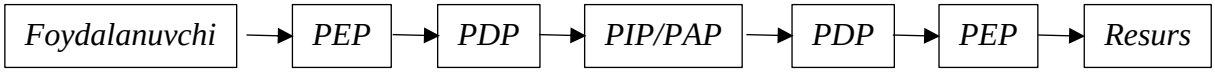
Policy Administration Point (PAP) - foydalanish siyosatlarini yaratish va boshqarish uchun xizmat qiladi.

Policy Information Point (PIP) - qaror qabul qilish uchun zarur bo‘lgan atributlarni tegishli manbalardan taqdim etadi.

Policy Decision Point (PDP) - atributlar va xavfsizlik siyosatlarini tahlil qilib, foydalanishga ruxsat berish yoki rad etish to‘g‘risida qaror chiqaradi.

Policy Enforcement Point (PEP) - PDP tomonidan shakllantirilgan qarorni amalda bajaradi.

ABACni joriy etish va siyosat qoidalarini boshqarish masalalari Hu va boshqalar tomonidan alohida tadqiq qilingan bo‘lib, ABACning moslashuvchanligi bilan bir qatorda siyosatlarni to‘g‘ri shakllantirish va boshqarish zarurligi ta’kidlangan [5].



1-rasm. Jarayonni umumiy ko‘rinish sxemasi

Foydalanuvchi resursga murojaat qilganda, PEP so‘rovni PDPga yuboradi. PDP zarur atributlarni PIP orqali oladi va tegishli siyosatlarni tekshiradi. Natijada Permit yoki Deny qarori shakllantiriladi.

RBAC va ABAC modellarining taqqoslanishi

RBAC va ABAC modellarining asosiy farqi foydalanish qarorini shakllantirishda foydalaniladigan ma’lumotlar tarkibida namoyon bo‘ladi.

1-jadval.

RBAC va ABAC modellarining asosiy farqi

Mezoni	RBAC	ABAC
Asosiy parametr	Rol	Atributlar
Qaror asoslari	Foydalanuvchi roli	Subyekt, obyekt, amal va muhit atributlari
Kontekstni hisobga olish	Cheklangan	Keng
Dinamiklik	Nisbatan cheklangan	Yuqori
Vaqtni hisobga olish	Qo‘shimcha mexanizm talab qilishi mumkin	Siyosat atributi sifatida berilishi mumkin
Joylashuvni hisobga olish	Cheklangan	Mumkin
Qurilma holatini hisobga olish	Cheklangan	Mumkin
Siyosatning moslashuvchanligi	Rolga bog‘liq	Atributlarga bog‘liq
Katta tizimlarda boshqarish	Samarali	Moslashuvchan, lekin siyosatlarni boshqarish murakkab bo‘lishi mumkin

RBAC modeli ruxsatlarni rollar asosida markazlashtirish orqali boshqarishni soddalashtiradi [3]. ABAC esa foydalanish qarorini ko‘proq kontekstual parametrlar asosida shakllantirish imkonini beradi [1, 2].

Shu sababli bu ikki modelni bir-birining mutlaq muqobili sifatida emas, balki muayyan axborot tizimining talablariga qarab qo‘llaniladigan yondashuvlar sifatida ko‘rib chiqish mumkin.

ABAC modelining zamonaviy axborot tizimlaridagi qo‘llanilishi

Bulutli hisoblash, IoT, mobil qurilmalar va taqsimlangan axborot tizimlarining rivojlanishi foydalanishni boshqarishning dinamik bo‘lishini talab qilmoqda. ABAC modeli aynan shunday muhitlarda turli atributlarni foydalanish siyosatiga kiritish imkonini beradi [2, 5].

Masalan, muhim axborot infratuzilmasining SCADA tizimida operatorga muayyan boshqaruv amalini bajarishga faqat quyidagi shartlarda ruxsat berilishi mumkin:

- operator tegishli rolga ega;
- operator ishonchli qurilmadan foydalanmoqda;
- qurilmaning xavfsizlik holati talabga javob beradi;
- operator korporativ tarmoqdan ulangan;
- murojaat ish vaqtida amalga oshirilmoqda;
- so‘ralayotgan resurs operatorning vakolat doirasiga kiradi.

Bunday shartlarning barchasini bitta foydalanish siyosatida ifodalash ABAC modelining asosiy imkoniyatlaridan biridir.

Bundan tashqari, Zero Trust Architecture konsepsiyasida resurslarga kirishda foydalanuvchi va qurilmaning ishonchliligini alohida baholash, resursga kirishni doimiy ravishda nazorat qilish va tarmoq joylashuviga avtomatik ishonmaslik tamoyillari ilgari suriladi. Bu yondashuv atributlar va kontekstga asoslangan foydalanishni boshqarish mexanizmlari bilan uyg‘unlashtirilishi mumkin.

Xulosa

Foydalanishni boshqarish axborot xavfsizligining fundamental mexanizmlaridan biri hisoblanadi. DAC, MAC va RBAC kabi an’anaviy modellar turli axborot tizimlarida foydalanish huquqlarini boshqarish uchun muhim nazariy va amaliy asosni shakllantirgan [3].

RBAC modeli foydalanuvchilarni rollar orqali boshqarish yordamida ruxsatlarni ma’muriy jihatdan soddalashtirsa, ABAC modeli subyekt, obyekt, amal va muhit atributlarini hisobga olgan holda yanada moslashuvchan siyosatlarni shakllantirish imkonini beradi [1, 2].

Zamonaviy taqsimlangan, bulutli, IoT va muhim axborot infratuzilmalari uchun foydalanish qarorini faqat foydalanuvchining roli asosida shakllantirish yetarli bo‘lmasligi mumkin. Shu sababli atributlar, kontekst va xavfsizlik holatini hisobga oluvchi yondashuvlar muhim ahamiyat kasb etmoqda.

ABAC modelining yana bir muhim xususiyati - uni RBAC bilan birgalikda qo‘llash imkoniyatidir. Bunday gibrid yondashuvda dastlab foydalanuvchining roli aniqlanib, keyinchalik uning qo‘shimcha atributlari, qurilmasi, joylashuvi, vaqti va boshqa kontekstual parametrlar asosida yakuniy foydalanish qarori shakllantirilishi mumkin [1, 5]. Bu esa zamonaviy axborot tizimlarida foydalanishni boshqarishning moslashuvchanligini oshirish imkonini beradi.

Foydalanilgan adabiyotlar

1. Hu V. C., Ferraiolo D., Kuhn D., Schnitzer A., Sandlin K., Miller R., Scarfone K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162.

2. Hu V., Kuhn D. R., Ferraiolo D., Voas J. Attribute-Based Access Control. Computer, 2015, Vol. 48, No. 2, pp. 85-88. DOI: 10.1109/MC.2015.33.

3. Sandhu R. S., Coyne E. J., Feinstein H. L., Youman C. E. Role-Based Access Control Models. IEEE Computer, 1996, Vol. 29, No. 2, pp. 38-47. DOI: 10.1109/2.485845.

4. Sandhu R., Samarati P. Access Control: Principle and Practice. IEEE Communications Magazine, 1994, Vol. 32, No. 9, pp. 40-48.

5. Hu V. C., Ferraiolo D., Kuhn D. R., Kacker R. N., Lei Y. Implementing and Managing Policy Rules in Attribute Based Access Control. Proceedings of the 2015 IEEE 16th International Conference on Information Reuse and Integration (IRI), 2015, pp. 518-525. DOI: 10.1109/IRI.2015.98.

AI MODELLARIGA UYUSHTIRILADIGAN HUJUMLAR VA ULARNI OLDINI OLISH CHORALARI

Bozorov S.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda AI modellariga qarshi hujumlarning oltita guruhi - adversarial misollar, ma’lumotlarni zaharlash va backdoor, model extraction, membership inference va ma’lumot ekstraksiyasi, prompt injection va jailbreak hamda RAG bilim bazasini zaharlash - 2020–2025-yillardagi nufuzli nashrlar va NIST, OWASP hujjatlari asosida mezonli tahlil qilingan. Hujumlar tahdid modeli va hujum qilinadigan qatlam bo‘yicha tizimlashtirilib, himoya choralarining samaradorligi va cheklovlari qiyoslangan. Tahlil natijasida birorta chora barcha qatlamlarni qoplamasligi, qatlamli himoya va adaptiv baholash zarurligi asoslangan.

Kalit so‘zlar: adversarial machine learning, data poisoning, backdoor, model extraction, membership inference, prompt injection, RAG xavfsizligi.

Аннотация. В тезисе на основе ведущих публикаций 2020–2025 гг. и документов NIST и OWASP проведён критериальный анализ шести групп атак на модели ИИ: состязательных примеров, отравления данных и бэкдоров, извлечения модели, атак вывода членства и извлечения обучающих данных, внедрения промптов и джейлбрейков, а также отравления базы знаний RAG. Атаки систематизированы по модели угроз и атакуемому уровню, сопоставлены эффективность и ограничения мер защиты. Показано, что ни одна мера не охватывает все уровни, что обосновывает необходимость многоуровневой защиты и адаптивной оценки.

Ключевые слова: состязательное машинное обучение, отравление данных, бэкдор, извлечение модели, атака вывода членства, внедрение промптов, безопасность RAG.

Kirish

AI modellari kiberxavfsizlik, moliya, sog‘liqni saqlash va davlat xizmatlarida qaror qabul qilish jarayoniga integratsiyalashgani sari ular hujum nishoniga aylanmoqda. An’anaviy dasturiy ta’minotdan farqli ravishda model xulq-atvori o‘qitish ma’lumotlaridan o‘rganilgan parametrlar bilan belgilanadi, natijasi ehtimollik xarakteriga ega, katta til modellarida (LLM) esa buyruq va ma’lumot yagona tabiiy til kanali orqali uzatiladi. NIST hisobotida AI tizimlariga qarshi hujumlar hayotiy sikl bosqichi, hujumchining maqsadi (mavjudlik, yaxlitlik, maxfiylik), imkoniyatlari va bilim darajasi bo‘yicha tasniflangan; generativ AI uchun ta’minot zanjiri, bevosita va bilvosita prompt injection hamda AI agentlari xavfsizligi alohida ajratilgan [1]. OWASP Top 10 for LLM Applications 2025 ro‘yxatida prompt injection (LLM01) birinchi o‘rinda turadi, ta’minot zanjiri (LLM03), ma’lumot va modelni zaharlash (LLM04), ortiqcha vakolat (LLM06) hamda vektor va embedding zaifliklari (LLM08) ham asosiy xavflar qatoriga kiritilgan [2].

Muammo shundaki, bunday hujumlar kod sathidagi zaifliklarni tuzatish bilan bartaraf etilmaydi, mavjud himoya choralari esa ko‘pincha bitta hujum turiga yo‘naltirilgan. Tadqiqot maqsadi - AI modellariga qarshi asosiy hujumlarni tahdid modeli va hujum qatlami bo‘yicha tizimlashtirish hamda himoya choralarining samaradorligi va cheklovlarini tekshirilgan natijalar asosida qiyoslash. Vazifalar: hujum turlarini tanlash va tasniflash; har bir guruh bo‘yicha miqdoriy dalillarni aniqlash; himoya choralarini qatlamlar bo‘yicha moslashtirish.

Tadqiqot usuli

Tadqiqotda adabiyotlarni mezonli tahlil qilish usuli qo‘llanilgan; tajriba o‘tkazilmagan va yangi algoritm taklif etilmagan. Manbalar uchta mezon asosida tanlangan: (1) taqrizdan o‘tgan nufuzli konferensiya (IEEE S&P, USENIX Security, ICML, NeurIPS, ACM AISec) yoki rasmiy tashkilot (NIST, OWASP) nashri ekanligi; (2) hujum yoki himoya samaradorligini ko‘rsatuvchi miqdoriy natija mavjudligi; (3) hayotiy siklning muayyan qatlamiga bevosita aloqadorligi. Preprintlar faqat taqrizdan o‘tgan muqobil topilmagan hollarda, maqomi ko‘rsatilgan holda ishlatilgan. Hujumlar hujumchi imkoniyati (ma’lumot manbasiga ta’sir, faqat so‘rov yuborish, kontent joylash), hujum qatlami, oqibat va himoya chorasi bo‘yicha qiyoslangan. Manbadagi natijalar havola bilan, tahliliy xulosalar esa “tahlil natijasiga ko‘ra” iborasi bilan berilgan.

Asosiy qism

Hujumlarni tanlash mezoni - hayotiy siklning to‘rt qatlamini (ma’lumot va ta’minot zanjiri, model, inferensiya API, LLM ilova) qoplash va har bir guruh uchun miqdoriy dalil mavjudligi. AI modellariga qarshi asosiy hujumlarning qiyosiy tavsifi 1-jadvalda, ularning qatlamlar bo‘yicha joylashuvi va himoya choralari bilan bog‘liqligi 1-rasmda keltirilgan.

Adversarial misollar (evasion). Hujumchi inferensiya bosqichida kirish ma’lumotiga kichik, maqsadli o‘zgartirish kiritib noto‘g‘ri natijaga erishadi; oq qutida gradientdan, qora qutida so‘rovlardan foydalaniladi. AutoAttack ansambli 50 dan ortiq himoyalangan modelga qo‘llanganda bittasidan tashqari barcha holatlarda mualliflar e’lon qilganidan past robust aniqlik olingan, farq ko‘pincha 10 foizdan oshgan [3]. Bu natija himoya samaradorligi adaptiv hujumlar bilan tekshirilmasa oshirib baholanishini ko‘rsatadi.

Ma’lumotlarni zaharlash va backdoor. Hujum o‘qitish bosqichiga va ta’minot zanjiriga yo‘naltiriladi. Muddati o‘tgan domenlarni sotib olishga asoslangan split-view hujumi LAION-400M yoki COYO-700M datasetlarining 0,01 foizini 60 AQSh dollariga zaharlash imkonini bergan, jami 10 ta ommabop veb-dataset zaif bo‘lgan; Wikipedia snapshotlariga qaratilgan frontrunning hujumi esa qisqa vaqt oralig‘idagi tahrirlardan foydalanadi [4]. Zaharlangan namunalar backdoor joylash kanali bo‘lishi mumkin: preprint maqomidagi tadqiqotda trigger bilan faollashadigan xulq-atvor supervised fine-tuning, RL va adversarial o‘qitishdan keyin ham saqlangani, adversarial o‘qitish esa modelga triggerni yaxshiroq tanishni o‘rgatishi qayd etilgan [5].

Model extraction. Hujumchi faqat ochiq API orqali so‘rov yuborib, modelning funksional xususiyatlari yoki parametrlarini tiklaydi. Odatiy API kirishi bilan 20 AQSh dollaridan kam xarajat evaziga OpenAI Ada va Babbage modellarining embedding projeksiya matritsasi to‘liq tiklangan, yashirin o‘lchamlari 1024 va 2048 ekani tasdiqlangan; gpt-3.5-turbo uchun to‘liq matritsani tiklash xarajati 2000 dollardan kam deb baholangan [6].

Membership inference va ma’lumot ekstraksiyasi. Bu hujumlar modelning o‘qitish ma’lumotlarini yodlab qolishidan foydalanadi. GPT-2 dan faqat so‘rovlar orqali yuzlab so‘zma-so‘z ketma-ketliklar, jumladan ism, telefon raqami va e-mail manzillari ajratib olingan; ular o‘qitish to‘plamida bittagina hujjatda uchragan, kattaroq modellar esa zaifroq bo‘lgan [7]. Membership inference hujumlarini o‘rtacha aniqlik bilan emas, past FPR (≤0,1%) rejimidagi TPR bilan baholash taklif qilingan; LiRA hujumi bu rejimda avvalgi usullardan 10 barobar kuchliroq bo‘lgan [8].

Prompt injection, jailbreak va RAG zaharlash. Bilvosita prompt injectionda zararli ko‘rsatma model keyinchalik o‘qiydigan veb-sahifa yoki hujjatga joylanadi; hujum GPT-4

asosidagi Bing Chat, kod yozish yordamchilari va sintetik ilovalarda namoyish etilib, ma’lumot o‘g‘irlash, o‘z-o‘zidan tarqaluvchi hujum va axborot manbalarini ifloslantirish xavflari ko‘rsatilgan [9]. Ochiq Vicuna modellarida optimallashtirilgan universal jailbreak suffikslari yopiq modellarga ko‘chib, GPT-3.5 va GPT-4 da 84 foizgacha, PaLM-2 da 66 foiz muvaffaqiyatga erishgan (preprint) [10]. RAG tizimlarida millionlab matndan iborat bilim bazasiga har bir maqsadli savol uchun beshta zararli matn joylash taxminan 90% hujum muvaffaqiyatini bergan, baholangan himoyalar esa yetarli bo‘lmagan [11]. Vositalardan foydalanadigan agentlar uchun AgentDojo benchmarkida (97 vazifa, 629 xavfsizlik testi) LLMlar hujumsiz sharoitda vazifalarning 66 foizidan kamini bajargan, mavjud hujumlar eng yaxshi agentlarga nisbatan 25 foizdan kam holatda muvaffaqiyatli bo‘lgan [12].

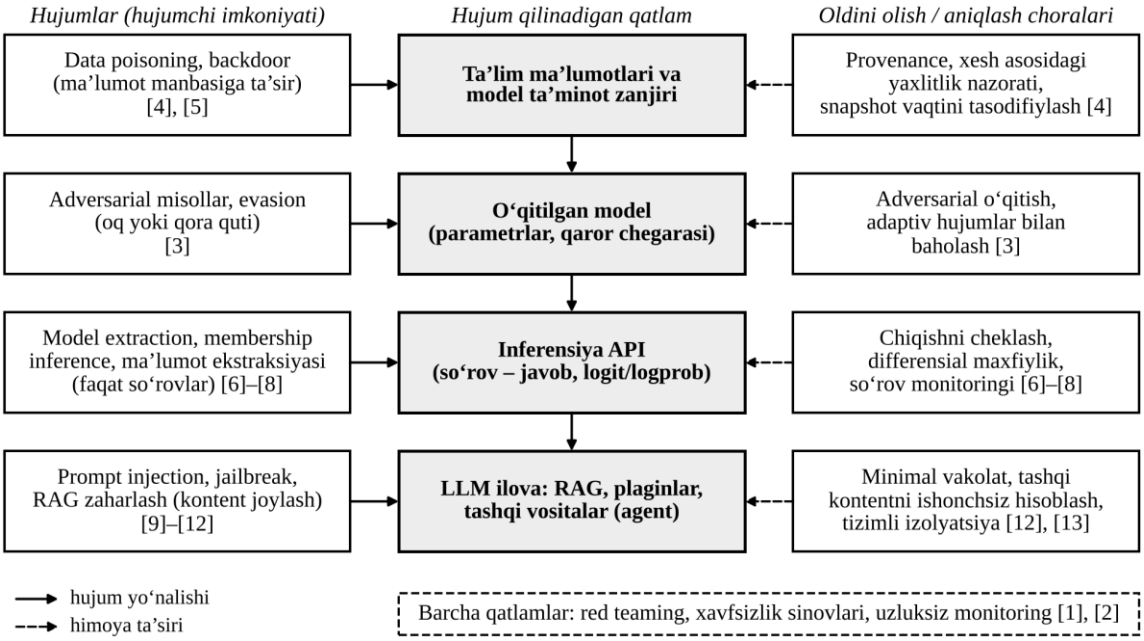
1-jadval

AI modellariga qarshi asosiy hujumlarning qiyosiy tavsifi

Hujum turi	Maqsad yoki zaiflik	Oqibat	Oldini olish / aniqlash	Cheklov
Adversarial misollar	Qaror chegarasining kichik o‘zgarishga sezgirligi	Noto‘g‘ri tasniflash	Adversarial o‘qitish, adaptiv baholash	Robustlik ko‘pincha oshirib baholanadi
Data poisoning, backdoor	Tekshirilmagan veb-dataset, trigger	Yashirin zararli xulq-atvor	Xesh orqali yaxlitlik, provenance, snapshot vaqtini tasodifiylash	Xavfsizlik o‘qitishi backdoorni olib tashlamasligi mumkin
Model extraction	API dagi logit/logprob ochiqligi	Intellektual mulk va arxitektura sizishi	Chiqishni cheklash, so‘rov monitoringi	API funksionalligi bilan murosa
Membership inference, ekstraksiya	Ma’lumotlarni yodlab qolish	Shaxsga doir ma’lumot sizishi	Differensial maxfiylik, ma’lumotni saralash, past FPR auditi	Model aniqligining pasayishi
Prompt injection, jailbreak	Buyruq va ma’lumot ajratilmagan	Himoyani chetlash, vositalarni suiiste’mol qilish	Minimal vakolat, tizimli izolyatsiya	To‘liq yechim noma’lum, foydalilik pasayadi
RAG zaharlash	Bilim bazasiga matn joylash	Maqsadli noto‘g‘ri javob	Manba ishonchliligini nazorat qilish	Baholangan himoyalar yetarli emas

1-jadval tahlili shuni ko‘rsatadiki, hujumlar zarur bo‘lgan hujumchi imkoniyati bo‘yicha keskin farqlanadi: zaharlash ma’lumot manbasiga ta’sir qilishni talab etsa [4], extraction va membership inference uchun faqat so‘rov yuborish [6]–[8], bilvosita prompt injection va RAG zaharlash uchun esa model o‘qiydigan kontentga matn joylash yetarli [9], [11]. Tahlil natijasiga ko‘ra, hujum uchun talab qilinadigan kirish darajasi qanchalik past bo‘lsa, himoya shunchalik

tizim arxitekturasi darajasida qurilishi kerak, chunki bunday hujumlarda hujumchini kirish nuqtasida cheklash imkoni kam.



1-rasm. Hujum va himoya choralarining qatlamli sxemasi

1-rasmda yuqori qatlamdagi buzilish (masalan, zaharlangan ma'lumot) quyi qatlamlarga meros bo'lib o'tadi [4], [5], LLM ilova qatlami esa tashqi kontent va vositalar orqali eng keng hujum yuzasiga ega [9], [11], [12]. Himoya choralari ham qatlamga xos: birorta chora barcha hujum guruhlarini qoplamaydi, shu sababli red teaming va uzluksiz monitoring barcha qatlamlarni qamrab oluvchi umumiy nazorat sifatida ko'rsatilgan [1], [2].

Himoya choralarining samaradorligi va cheklovlari

Ma'lumotlar qatlamida datasetlar kelib chiqishini nazorat qilish va kriptografik xesh asosidagi yaxlitlik tekshiruvi split-view zaharlashni to'xtatadi, frontrunning hujumiga qarshi esa snapshot olish tartibini tasodifiylashtirish yoki kechiktirish tavsiya etilgan [4]. Model qatlamida adversarial robustness faqat adaptiv hujumlar bilan tekshirilganda ishonchli baholanadi [3], xavfsizlikka yo'naltirilgan qo'shimcha o'qitish esa backdoorni kafolatli olib tashlamasligi mumkin [5]. API qatlamida logit va logprob chiqishlarini cheklash extraction xarajatini oshiradi [6], differensial maxfiylik va o'qitish ma'lumotlarini saralash yodlab qolish xavfini kamaytiradi [7], biroq bu choralar modelning foydaliligi bilan murosani talab qiladi.

LLM ilova qatlamida OWASP prompt injectionning to'liq oldini olish usuli mavjudligi noma'lumligini qayd etadi [2], shuning uchun tizimli yondashuvlar ahamiyat kasb etmoqda. Preprint maqomidagi CaMeL yondashuvi boshqaruv va ma'lumot oqimini ajratish orqali AgentDojo vazifalarining 77 foizini isbotlanadigan xavfsizlik bilan bajargan, himoyasiz tizimda bu ko'rsatkich 84 foiz bo'lgan [13]; demak, xavfsizlik foydalilikning muayyan pasayishi evaziga ta'minlanadi. Agentlarga minimal vakolat berish, tashqi kontentni ishonchsiz deb hisoblash, xavfsizlik va foydalilikni birgalikda o'lchash zarur [12]. NIST mavjud himoya usullari to'liq kafolat bermasligini ta'kidlagani sababli [1], red teaming va uzluksiz monitoring bir martalik emas, doimiy jarayon sifatida yuritilishi kerak.

Xulosa

Tahlil natijalari AI modellariga qarshi hujumlar hayotiy siklning barcha qatlamlarini qamrab olishini va ularning bir qismi uchun hujumchiga faqat so'rov yuborish yoki kontent joylash kifoya ekanini ko'rsatdi. Himoya choralari qatlamga xos bo'lib, ularning har biri foydalilik, aniqlik

yoki xarajat bilan murosani talab qiladi. Ustuvor tavsiyalar: ma’lumotlar va modellar kelib chiqishini nazorat qilish; himoyani adaptiv hujumlar va past FPR metrikalari bilan baholash; API chiqishlarini cheklash; LLM agentlarida minimal vakolat va tizimli izolyatsiyani qo‘llash; red teaming va monitoringni doimiy yuritish.

Foydalanilgan adabiyotlar

1. A. Vassilev, A. Oprea, A. Fordyce, H. Anderson, X. Davies, and M. Hamin, “Adversarial machine learning: A taxonomy and terminology of attacks and mitigations,” NIST, Gaithersburg, MD, USA, NIST AI 100-2e2025, Mar. 2025, doi: 10.6028/NIST.AI.100-2e2025.

2. OWASP GenAI Security Project, “OWASP Top 10 for LLM Applications 2025,” ver. 2025, Nov. 18, 2024. [Online]. Available: https://genai.owasp.org/llm-top-10/

3. F. Croce and M. Hein, “Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks,” in Proc. 37th ICML, PMLR, vol. 119, 2020, pp. 2206–2216.

4. N. Carlini et al., “Poisoning web-scale training datasets is practical,” in Proc. IEEE Symp. Security Privacy (SP), 2024, pp. 407–425, doi: 10.1109/SP54263.2024.00179.

5. E. Hubinger et al., “Sleeper agents: Training deceptive LLMs that persist through safety training,” arXiv:2401.05566, 2024 (preprint).

6. N. Carlini et al., “Stealing part of a production language model,” in Proc. 41st ICML, PMLR, vol. 235, 2024, pp. 5680–5705.

7. N. Carlini et al., “Extracting training data from large language models,” in Proc. 30th USENIX Security Symp., 2021, pp. 2633–2650.

8. N. Carlini, S. Chien, M. Nasr, S. Song, A. Terzis, and F. Tramèr, “Membership inference attacks from first principles,” in Proc. IEEE Symp. Security Privacy (SP), 2022, pp. 1897–1914, doi: 10.1109/SP46214.2022.9833649.

9. K. Greshake, S. Abdelnabi, S. Mishra, C. Endres, T. Holz, and M. Fritz, “Not what you’ve signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection,” in Proc. 16th ACM Workshop Artif. Intell. Security (AISec), 2023, pp. 79–90, doi: 10.1145/3605764.3623985.

10. A. Zou, Z. Wang, N. Carlini, M. Nasr, J. Z. Kolter, and M. Fredrikson, “Universal and transferable adversarial attacks on aligned language models,” arXiv:2307.15043, 2023 (preprint).

11. W. Zou, R. Geng, B. Wang, and J. Jia, “PoisonedRAG: Knowledge corruption attacks to retrieval-augmented generation of large language models,” in Proc. 34th USENIX Security Symp., 2025, pp. 3827–3844.

12. E. Debenedetti, J. Zhang, M. Balunović, L. Beurer-Kellner, M. Fischer, and F. Tramèr, “AgentDojo: A dynamic environment to evaluate prompt injection attacks and defenses for LLM agents,” in Proc. NeurIPS, Datasets and Benchmarks Track, vol. 37, 2024, doi: 10.52202/079017-2636.

13. E. Debenedetti et al., “Defeating prompt injections by design,” arXiv:2503.18813, 2025 (preprint).

KIBERXAVFSIZLIK TIZIMLARINI AI BILAN INTEGRATSIYALASH MUAMMOLARI VA YECHIMLARI

Bozorov S.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda sun’iy intellekt (AI) usullarini kiberxavfsizlik tizimlariga integratsiyalashda yuzaga keladigan beshta asosiy muammo - ma’lumotlar sifati, baholash metodologiyasi, soxta ogohlantirishlar va izohlanish, concept drift hamda AI komponentining o‘zi hujum nishoniga aylanishi - 2020–2025-yillardagi taqrizdan o‘tgan tadqiqotlar va NIST, OWASP hujjatlari asosida mezonli tahlil qilingan. Muammolar integratsiya bosqichlari bo‘yicha tizimlashtirilib, har biriga mos yechim va uning cheklovi qiyoslangan. Tahlil natijasida integratsiya muvaffaqiyati model aniqligidan ko‘ra baholash, ekspluatatsiya va boshqaruv jarayonlarining sifatiga bog‘liqligi asoslangan.

Kalit so‘zlar: kiberxavfsizlik, sun’iy intellekt, intrusion detection, SIEM/SOC, false positive, concept drift, AI xavfsizligi.

Аннотация. В тезисе на основе рецензируемых исследований 2020–2025 гг. и документов NIST и OWASP проведён критериальный анализ пяти основных проблем интеграции методов искусственного интеллекта (ИИ) в системы кибербезопасности: качества данных, методологии оценки, ложных срабатываний и объяснимости, дрейфа концепций, а также уязвимости самого ИИ-компонента к атакам. Проблемы систематизированы по этапам интеграции, для каждой сопоставлены решения и их ограничения. Показано, что успех интеграции зависит не столько от точности модели, сколько от качества процессов оценки, эксплуатации и управления.

Ключевые слова: кибербезопасность, искусственный интеллект, обнаружение вторжений, SIEM/SOC, ложные срабатывания, дрейф концепций, безопасность ИИ.

Kirish

Imzo asosidagi himoya vositalari asosan oldindan ma’lum hujumlarni aniqlagani sababli tarmoq trafigi, loglar va fayllardagi yangi naqshlarni aniqlash uchun mashinali o‘qitish (ML) va chuqur o‘qitish (DL) usullari kiberxavfsizlik tizimlariga integratsiyalashmoqda. Ilmiy manbalar tahlili asosida ML inson tomonidan bajariladigan tahlilga nisbatan afzalliklarga ega bo‘lsada, uning real tizimlarda joriy etilishi hali dastlabki bosqichda ekani va tadqiqot hamda amaliyot o‘rtasida sezilarli uzilish mavjudligi qayd etilgan [1]. NIST AI RMF 1.0 hujjatida ishonchli AI tizimining xususiyatlari qatorida “xavfsiz va barqaror”, “izohlanadigan va talqin qilinadigan” hamda “haqqoniy va ishonchli” bo‘lish talablari belgilangan va risklarni boshqarish GOVERN, MAP, MEASURE, MANAGE funksiyalari orqali tashkil etilgan [2].

Muammo shundaki, laboratoriyada yuqori aniqlik ko‘rsatgan model real infratuzilmaga ulanganda ma’lumotlar sifati, ogohlantirishlar oqimi, vaqt o‘tishi bilan o‘zgaruvchan tahdidlar va AI komponentining o‘ziga qaratilgan hujumlar tufayli kutilgan samarani bermasligi mumkin. Tadqiqot maqsadi - AI ni kiberxavfsizlik tizimlariga integratsiyalashdagi asosiy muammolarni integratsiya bosqichlari bo‘yicha tizimlashtirish va ularning yechimlarini tekshirilgan natijalar asosida cheklovlari bilan birga qiyoslash. Vazifalar: muammolarni tanlash va tasniflash; har bir muammo bo‘yicha miqdoriy dalillarni aniqlash; yechimlarni bosqichlar va boshqaruv qatlami bo‘yicha moslashtirish.

Tadqiqot usuli

Tadqiqotda adabiyotlarni mezonli tahlil qilish usuli qo‘llanilgan; tajriba o‘tkazilmagan va yangi algoritm taklif etilmagan. Manbalar uchta mezon asosida tanlangan: (1) taqrizdan o‘tgan nufuzli konferensiya yoki jurnal (USENIX Security, IEEE S&P, IEEE EuroS&P, ACM AISec, NeurIPS, ACM DTRAP) yoki rasmiy tashkilot (NIST, OWASP) nashri ekanligi; (2) muammo yoki yechimni tasdiqlovchi miqdoriy yoki empirik natija mavjudligi; (3) integratsiyaning muayyan bosqichiga bevosita aloqadorligi. Preprint faqat taqrizdan o‘tgan muqobil topilmagan holda, maqomi ko‘rsatilib ishlatilgan. Muammolar sababi, oqibati, yechimi va yechim cheklovi bo‘yicha qiyoslangan. Manbadagi natijalar havola bilan, tahliliy xulosalar esa “tahlil natijasiga ko‘ra” iborasi bilan berilgan.

Asosiy qism

Muammolarni tanlash mezoni - integratsiyaning beshta bosqichini (ma’lumot yig‘ish, model ishlab chiqish va baholash, SIEM/SOC ga joriy etish, ekspluatatsiya, monitoring) qoplash va har biri uchun empirik dalil mavjudligi. Kiberxavfsizlik tizimlarini AI bilan integratsiyalash muammolari va yechimlarining qiyosiy tavsifi 1-jadvalda, ularning bosqichlar bo‘yicha joylashuvi 1-rasmda keltirilgan.

Ma’lumotlar sifati. Top-konferensiyalardagi 30 ta maqola tahlilida sampling bias 60%, data snooping 57% ishlarda aniqlangan [3]. Keng qo‘llaniladigan CICIDS2017 datasetida yozuvlarning 25,9% i TCP artefaktlari ekani, trafikning 20% dan ortig‘ini qayta yorliqlash zarurligi ko‘rsatilgan; tuzatishdan keyin Random Forest ning umumiy accuracy va vaznli F1 qiymati 0,99 da qolgani holda, Bot sinfi uchun F1 0,60 dan 0,99 gacha, Web Attack XSS uchun 0,18 dan 0,79 gacha o‘zgargan [4]. Demak, agregat ko‘rsatkichlar kam uchraydigan hujum sinflaridagi xatolarni yashiradi.

Baholash metodologiyasi va hisoblash xarajati. Tahlil qilingan ishlarning 47% ida faqat laboratoriya sharoitida baholash, 33% ida noto‘g‘ri samaradorlik metrikalari qayd etilgan [3]. Base rate fallacy tufayli 99% TPR va 1% FPR da ham hujum va normal holat nisbati 1:100 bo‘lsa, 99 ta haqiqiy ogohlantirishga 100 ta soxta ogohlantirish to‘g‘ri keladi. Mirai trafigida autoencoder ansambliga asoslangan Kitsune 0,001 FPR da 0,882 TPR ga erishgan bo‘lsa, oddiy statistik boxplot usuli 0,996 TPR ko‘rsatgan va hisoblash jihatidan ancha yengil bo‘lgan [3].

Soxta ogohlantirishlar va izohlanish. SOC tahlilchilari ishtirokidagi tadqiqotda (so‘rovnoma n = 20, intervyu n = 21) 14 nafar respondent monitoring vositalari tez-tez false positive berishini tasdiqlagan, faqat 2 nafari AI/ML asosidagi vositalardan foydalangan, past qo‘llanish sabablaridan biri sifatida esa soxta ogohlantirishlar ko‘rsatilgan; ogohlantirishlar ishonchli, izohlanadigan, analitik, kontekstli va o‘tkaziladigan bo‘lishi talab qilingan [5]. Xavfsizlikda DL modellari uchun oltita mashhur izohlash usuli zararli dastur va zaiflik aniqlash vazifalarida aniqlik, to‘liqlik, samaradorlik va barqarorlik mezonlari bo‘yicha baholanganda, usullar o‘rtasida sezilarli farqlar aniqlangan [6]; demak, izoh usulini tanlashning o‘zi ham tekshiruv talab qiladi.

Concept drift. Bir yillik ma’lumotda o‘qitilgan Android zararli dastur klassifikatorining F1 qiymati olti oylik ekspluatatsiyada 0,99 dan 0,76 gacha pasaygan; yetti yillik ma’lumotda baholangan faol o‘qitish usuli eng yaxshi bazaviy usulga nisbatan FNR ni 14% dan 9% gacha, FPR ni 0,86% dan 0,48% gacha kamaytirgan [7].

AI komponentining hujum sathi. NIST taksonomiyasida predictive va generativ AI tizimlariga qarshi evasion, poisoning, maxfiylik va suiiste’mol hujumlari, shuningdek, AI agentlari

xavfsizligi tasniflangan [8]. OWASP 2025-yil ro‘yxatida prompt injection (LLM01) birinchi, maxfiy ma’lumotlarning sizishi (LLM02) va ortiqcha vakolat (LLM06) ham asosiy xavflar qatorida keltirilgan [9]. Bilvosita prompt injection model o‘qiydigan hujjat yoki veb-sahifaga yashirilgan ko‘rsatma orqali real LLM ilovalarida ma’lumot o‘g‘irlash imkonini bergan [10]. AgentDojo benchmarkida (97 vazifa, 629 xavfsizlik testi) LLM agentlar hujumsiz sharoitda vazifalarning 66% idan kamini bajargan, mavjud hujumlar eng yaxshi agentlarga nisbatan 25% dan kam holatda muvaffaqiyatli bo‘lgan [11]. Tahlil natijasiga ko‘ra, log, e-mail yoki tiket matnlarini o‘qiydigan LLM asosidagi SOC yordamchilari ham shu turdagi ishonchsiz kontentni qayta ishlagani sababli bilvosita prompt injection xavfiga duch keladi.

1-jadval

Kiberxavfsizlik tizimlarini AI bilan integratsiyalash muammolari va yechimlarining

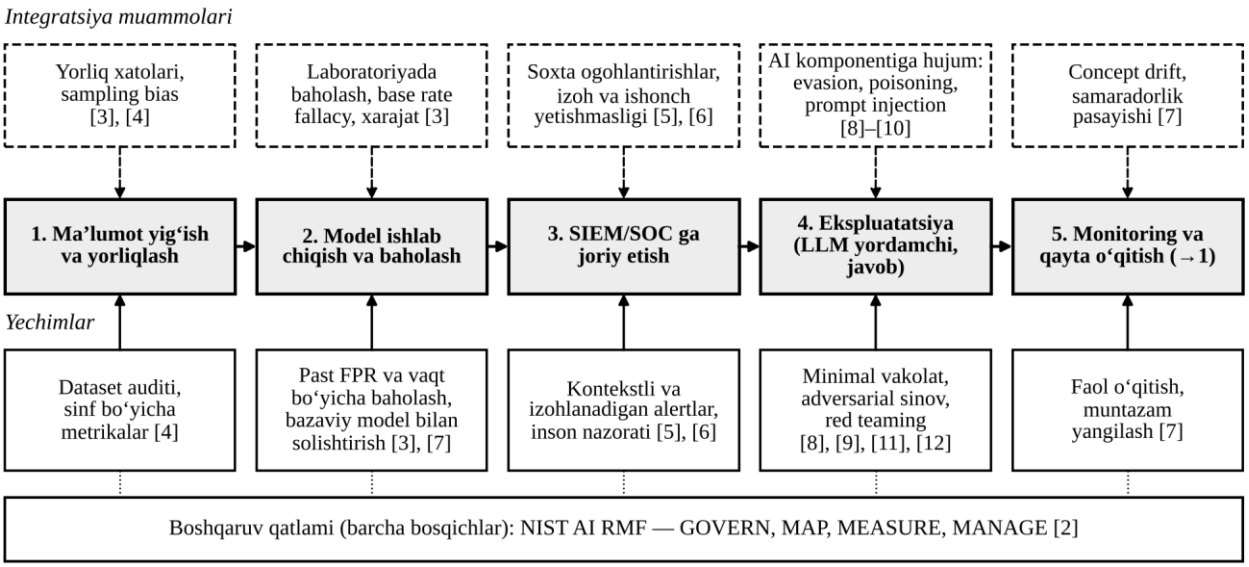
Muammo	Sababi	Oqibat	Yechim	Yechim cheklovi
Ma’lumotlar sifati	Yorliq xatolari, sampling bias	Kam uchraydigan hujumlarda xato	Dataset auditi, sinf bo‘yicha F1	Qo‘lda tekshiruv qimmat
Baholash metodologiyasi	Laboratoriyada baholash, base rate fallacy	Real muhitda samaradorlik pasayadi	Past FPR va vaqt bo‘yicha baholash, bazaviy model bilan solishtirish	Real trafik ma’lumotiga kirish cheklangan
Soxta ogohlantirish, izohlanish	Kontekstsiz, izohsiz alertlar	Tahlilchi yuki, ishonch yo‘qolishi	Kontekstli va izohlanadigan alert, inson nazorati	Izoh usullari natijasi farq qiladi
Concept drift	Tahdid va ilovalarning o‘zgarishi	F1 va FNR yomonlashuvi	Faol o‘qitish, muntazam yangilash	Yorliqlash xarajati saqlanadi
AI komponenti hujum nishoni	Evasion, poisoning, prompt injection	Aniqlashni chetlash, ma’lumot sizishi	Minimal vakolat, tizimli izolyatsiya, red teaming	To‘liq yechim noma’lum, foydalilik pasayadi

1-jadval tahlili shuni ko‘rsatadiki, beshta muammodan to‘rttasi (ma’lumotlar sifati, baholash, soxta ogohlantirishlar, drift) modelning arxitekturasi bilan emas, balki ma’lumotlar va ekspluatatsiya jarayonlari bilan bog‘liq [3]–[7]. Tahlil natijasiga ko‘ra, integratsiyada murakkabroq model tanlashdan oldin ma’lumotlar auditi, real sharoitga yaqin baholash protokoli va SOC ish oqimiga mos ogohlantirish formati ta’minlanishi lozim; aks holda yuqori laboratoriya natijasi amaliy samaraga aylanmaydi.

1-rasmda integratsiya besh bosqichli zanjir sifatida ko‘rsatilgan: har bir bosqichga xos muammo yuqoridan, unga mos yechim pastdan bog‘langan, monitoring bosqichi esa yangi ma’lumot va tahlilchi baholari orqali birinchi bosqichga qaytadi [7]. Barcha bosqichlarni qamrab oluvchi boshqaruv qatlami NIST AI RMF funksiyalariga tayanadi [2]; tahlil natijasiga ko‘ra, bu qatlam bo‘lmasa yechimlar alohida-alohida qo‘llanib, ularning ta’siri o‘lchanmay qoladi.

Yechimlarning samaradorligi va cheklovlari

Ma’lumotlar bosqichida dataset auditi va sinf bo‘yicha metrikalardan foydalanish agregat accuracy yashiradigan xatolarni ochib beradi [4], biroq yorliqlarni qo‘lda tekshirish katta mehnat talab qiladi.



1-rasm. Integratsiya muammolari va yechimlari

Baholash bosqichida natijalarni past FPR rejimida, vaqt bo‘yicha bo‘lingan ma’lumotda va oddiy bazaviy usullar bilan solishtirib berish tavsiya etilgan [3], [7]. SOC bosqichida ogohlantirishlarning kontekstli va izohlanadigan bo‘lishi tahlilchi ishonchini oshirishning sharti sifatida ko‘rsatilgan [5], ammo izoh usullarining o‘zi turli natija berishi mumkinligi sababli ular ham baholanishi kerak [6]. Drift sharoitida faol o‘qitish xatolarni kamaytiradi [7], lekin yorliqlash xarajatini butunlay yo‘qotmaydi.

AI komponentini himoyalashda OWASP prompt injectionning to‘liq oldini olish usuli mavjudligi noma’lumligini qayd etadi [9]. Preprint maqomidagi CaMeL yondashuvi boshqaruv va ma’lumot oqimini ajratish orqali AgentDojo vazifalarining 77% ini isbotlanadigan xavfsizlik bilan bajargan, himoyasiz tizimda bu ko‘rsatkich 84% bo‘lgan [12]; demak, tizimli izolyatsiya foydalilikning muayyan pasayishi evaziga ta’minlanadi. SOC dagi LLM yordamchilarga minimal vakolat berish, avtomatik javob choralarini inson tasdig‘i bilan cheklash va AI komponentini muntazam adversarial sinovdan o‘tkazish zarur [8], [9], [11].

Xulosa

Tahlil natijalari kiberxavfsizlik tizimlarini AI bilan integratsiyalashdagi asosiy to‘siqlar model arxitekturasidan ko‘ra ma’lumotlar sifati, baholash metodologiyasi, ogohlantirishlarning amaliy yaroqliligi va vaqt o‘tishi bilan samaradorlik pasayishi bilan bog‘liqligini, AI komponentining o‘zi esa yangi hujum yuzasini hosil qilishini ko‘rsatdi. Ustuvor tavsiyalar: dataset auditi va sinf bo‘yicha metrikalar; past FPR va vaqt bo‘yicha baholash; kontekstli, izohlanadigan ogohlantirishlar va inson nazorati; faol o‘qitish orqali muntazam yangilash; LLM komponentlarida minimal vakolat va red teaming; barcha bosqichlarni NIST AI RMF asosidagi boshqaruv jarayoniga birlashtirish. Har bir yechim xarajat yoki foydalilik bilan murosani talab qilgani sababli ularning ta’siri doimiy o‘lchab borilishi lozim.

Foydalanilgan adabiyotlar

1. G. Apruzzese et al., “The role of machine learning in cybersecurity,” Digit. Threats: Res. Pract., vol. 4, no. 1, pp. 1–38, 2023, doi: 10.1145/3545574.

2. E. Tabassi, “Artificial intelligence risk management framework (AI RMF 1.0),” NIST, Gaithersburg, MD, USA, NIST AI 100-1, Jan. 2023, doi: 10.6028/NIST.AI.100-1.

3. D. Arp et al., “Dos and don’ts of machine learning in computer security,” in Proc. 31st USENIX Security Symp., 2022, pp. 3971–3988.

4. G. Engelen, V. Rimmer, and W. Joosen, “Troubleshooting an intrusion detection dataset: The CICIDS2017 case study,” in Proc. IEEE Security and Privacy Workshops (SPW), 2021, pp. 7–12, doi: 10.1109/SPW53761.2021.00009.

5. B. A. Alahmadi, L. Axon, and I. Martinovic, “99% false positives: A qualitative study of SOC analysts’ perspectives on security alarms,” in Proc. 31st USENIX Security Symp., 2022, pp. 2783–2800.

6. A. Warnecke, D. Arp, C. Wressnegger, and K. Rieck, “Evaluating explanation methods for deep learning in security,” in Proc. IEEE Eur. Symp. Security Privacy (EuroS&P), 2020, pp. 158–174, doi: 10.1109/EuroSP48549.2020.00018.

7. Y. Chen, Z. Ding, and D. Wagner, “Continuous learning for Android malware detection,” in Proc. 32nd USENIX Security Symp., 2023, pp. 1127–1144.

8. A. Vassilev, A. Oprea, A. Fordyce, H. Anderson, X. Davies, and M. Hamin, “Adversarial machine learning: A taxonomy and terminology of attacks and mitigations,” NIST, Gaithersburg, MD, USA, NIST AI 100-2e2025, Mar. 2025, doi: 10.6028/NIST.AI.100-2e2025.

9. OWASP GenAI Security Project, “OWASP Top 10 for LLM Applications 2025,” ver. 2025, Nov. 18, 2024. [Online]. Available: https://genai.owasp.org/llm-top-10/

10. K. Greshake, S. Abdelnabi, S. Mishra, C. Endres, T. Holz, and M. Fritz, “Not what you’ve signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection,” in Proc. 16th ACM Workshop Artif. Intell. Security (AISec), 2023, pp. 79–90, doi: 10.1145/3605764.3623985.

11. E. Debenedetti, J. Zhang, M. Balunović, L. Beurer-Kellner, M. Fischer, and F. Tramèr, “AgentDojo: A dynamic environment to evaluate prompt injection attacks and defenses for LLM agents,” in Proc. NeurIPS, Datasets and Benchmarks Track, vol. 37, 2024, doi: 10.52202/079017-2636.

12. E. Debenedetti et al., “Defeating prompt injections by design,” arXiv:2503.18813, 2025 (preprint).

КИБЕРБЕЗОПАСНОСТЬ И НАДЁЖНОСТЬ IoT-ИНФРАСТРУКТУРЫ СИСТЕМЫ «УМНЫЙ ГОРОД»: СОВРЕМЕННЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Мурадова А.А.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий
Шарапова Н.А.
Бухарский государственный технический университет

Аннотация. В статье рассматриваются современные проблемы обеспечения кибербезопасности и надёжности IoT-инфраструктуры систем «Умный город». Рассмотрены основные виды киберугроз, оказывающих влияние на конфиденциальность, целостность и доступность данных, а также на устойчивость функционирования IoT-устройств и сетевой инфраструктуры. Проанализированы перспективы применения методов искусственного интеллекта и машинного обучения для обнаружения аномалий, прогнозирования отказов и повышения устойчивости IoT-инфраструктуры.

Ключевые слова: IoT, Интернет вещей, «Умный город», кибербезопасность, информационная безопасность, надёжность, IoT-инфраструктура, киберугрозы, обнаружение аномалий, машинное обучение, искусственный интеллект, телекоммуникационные сети, отказоустойчивость.

Annotatsiya. Ushbu maqola Smart City tizimlari uchun IoT infratuzilmasining kiberxavfsizligi va ishonchliligini ta'minlashdagi dolzarb muammolarni ko‘rib chiqadi. Unda ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligiga, shuningdek, IoT qurilmalari va tarmoq infratuzilmasining barqarorligiga ta’sir qiluvchi asosiy kibertahdid turlari ko‘rib chiqiladi. Shuningdek, anomaliyalarni aniqlash, nosozliklarni bashorat qilish va IoT infratuzilmasining barqarorligini oshirish uchun sun’iy intellekt va mashinani o'rganish usullaridan foydalanish imkoniyatlari tahlil qilinadi.

Kalit so'zlar: IoT, Internet ashyolari, Smart City, kiberxavfsizlik, axborot xavfsizligi, ishonchlilik, IoT infratuzilmasi, kibertahdidlar, anomaliyalarni aniqlash, mashinani o‘rganish, sun’iy intellekt, telekommunikatsiya tarmoqlari, nosozliklarga chidamlilik.

Введение

Стремительное развитие цифровых технологий и концепции «Умный город» приводит к широкому внедрению систем Интернета вещей (Internet of Things, IoT) в различные сферы городской инфраструктуры. Интеллектуальные системы мониторинга транспорта, энергоснабжения, водоснабжения, освещения, экологического контроля, общественной безопасности и управления городскими объектами формируют единую распределённую информационно-телекоммуникационную инфраструктуру. Основу такой инфраструктуры составляют большое количество IoT-устройств, сенсоров, шлюзов, беспроводных и проводных сетей передачи данных, серверных и облачных платформ, обеспечивающих сбор, передачу, обработку и хранение информации [1].

Одновременно с расширением IoT-инфраструктуры увеличивается количество потенциальных уязвимостей и киберугроз. Большое число территориально распределённых устройств, ограниченные вычислительные и энергетические ресурсы сенсоров, использование беспроводных каналов связи, неоднородность сетевых протоколов и необходимость постоянного обмена данными создают дополнительные условия для

возникновения угроз информационной безопасности. Компрометация одного IoT-устройства или сетевого узла потенциально может оказать влияние на функционирование связанных элементов инфраструктуры и привести к нарушению доступности городских сервисов.

Особую актуальность приобретает проблема обеспечения не только кибербезопасности, но и надёжности IoT-инфраструктуры. Кибератаки могут сопровождаться увеличением сетевой нагрузки, задержек передачи, потерь пакетов, нарушением маршрутизации, временной недоступностью устройств и снижением качества предоставляемых услуг. В результате информационная безопасность и техническая надёжность IoT-сети оказываются взаимосвязанными характеристиками, которые целесообразно рассматривать комплексно. Перспективным направлением является использование методов машинного обучения и искусственного интеллекта для выявления аномального поведения, классификации сетевых событий, прогнозирования отказов IoT-устройств и оценки состояния телекоммуникационной инфраструктуры [2].

Методы исследования

В исследовании применён комплекс теоретических, статистических и вычислительных методов, направленных на анализ современных угроз кибербезопасности и оценку надёжности IoT-инфраструктуры систем «Умный город».

Метод системного анализа использовался для изучения архитектуры IoT-инфраструктуры, включающей сенсорные устройства, шлюзы, телекоммуникационные сети, серверные и облачные платформы. Метод классификации и сравнительного анализа применялся для систематизации основных видов кибератак, включая DDoS-атаки, несанкционированный доступ, подмену данных, перехват сетевого трафика и компрометацию IoT-устройств. Методы статистического анализа использовались для исследования параметров функционирования IoT-сети. Методы теории надёжности применялись для оценки вероятности безотказной работы IoT-устройств, интенсивности отказов, средней наработки до отказа (MTTF), среднего времени восстановления (MTTR) и коэффициента готовности. Методы машинного обучения рассматривались для выявления аномального поведения устройств и сетевого трафика. Алгоритмы Random Forest и XGBoost могут применяться для классификации сетевых событий, Isolation Forest - для обнаружения аномалий, а рекуррентные нейронные сети LSTM и GRU - для анализа временных последовательностей и прогнозирования изменения состояния IoT-устройств. Метод интегральной оценки использовался для разработки подхода к совместному анализу показателей кибербезопасности и надёжности IoT-инфраструктуры [3].

Методы оценки качества моделей предусматривали использование Accuracy, Precision, Recall, F1-score и AUC-ROC для задач классификации и обнаружения аномалий. Комплексное применение указанных методов позволяет исследовать взаимосвязь между киберугрозами, техническим состоянием IoT-устройств и надёжностью телекоммуникационной инфраструктуры. Предложенный методологический подход создаёт основу для разработки интеллектуальных систем мониторинга, обнаружения аномалий и прогнозирования потенциальных нарушений функционирования сервисов «Умного города».

Результаты исследования и их обсуждение

В результате проведённого анализа установлено, что обеспечение кибербезопасности IoT-инфраструктуры систем «Умный город» представляет собой

комплексную задачу, связанную не только с защитой информации, но и с поддержанием надёжности, доступности и устойчивости функционирования телекоммуникационной сети. Распределённая архитектура IoT, большое количество подключённых устройств и непрерывный обмен данными между сенсорами, шлюзами и серверными платформами создают условия, при которых нарушение работы отдельного элемента может отрицательно повлиять на качество предоставляемых городских сервисов [4].

На основании системного и сравнительного анализа выделены основные категории угроз, способных повлиять на функционирование IoT-инфраструктуры «Умного города». К ним относятся атаки на доступность сетевых сервисов, компрометация устройств, несанкционированный доступ, перехват и модификация данных, а также нарушение целостности передаваемой информации. Особую опасность представляют распределённые атаки типа DDoS, которые могут приводить к перегрузке сетевых ресурсов и увеличению времени обработки запросов. Компрометация сенсорных устройств способна привести к передаче ложных измерений, а изменение данных мониторинга - к формированию ошибочных решений системами автоматизированного управления городской инфраструктурой. Для систематизации выявленных угроз предлагается использовать классификацию, представленную в таблице 1.

Таблица 1

Основные угрозы кибербезопасности IoT-инфраструктуры систем «Умный город»

Вид угрозы	Возможное воздействие	Контролируемые параметры
DDoS-атаки	Перегрузка сетевых ресурсов, снижение доступности	Объём трафика, задержка, доступность
Несанкционированный доступ	Нарушение конфиденциальности и целостности данных	События аутентификации, журналы доступа
Подмена данных	Передача недостоверной информации	Отклонение измерений, целостность сообщений
Перехват трафика	Утечка информации, возможность последующей модификации	События безопасности, состояние защищённых соединений
Компрометация IoT-устройств	Изменение поведения устройства, использование его в атаке	Сетевые аномалии, загрузка ресурсов, состояние устройства
Нарушение работы протоколов	Потеря пакетов, увеличение задержки, нарушение обмена	Потери пакетов, задержка, ошибки соединения

Следует учитывать, что кибератаки могут приводить не только к физическому или программному отказу устройства, но и к временному нарушению доступности сервиса. Поэтому при оценке функционирования «Умного города» целесообразно отдельно анализировать технические отказы, нарушения безопасности и последствия инцидентов для предоставления услуг [5,6].

Для повышения эффективности мониторинга IoT-инфраструктуры перспективно использование алгоритмов машинного обучения, позволяющих выявлять сложные зависимости между параметрами сетевого трафика, состоянием оборудования и событиями безопасности. Random Forest и XGBoost могут применяться для классификации наблюдений по заранее определённым категориям. Isolation Forest и Autoencoder могут

использоваться для выявления нетипичных наблюдений при ограниченном количестве размеченных примеров. Модели LSTM и GRU представляют интерес для анализа временных последовательностей, поскольку позволяют учитывать изменение сетевых параметров во времени.

В рамках экспериментальной проверки предлагается сформировать набор данных, включающий нормальные режимы работы устройств, сетевые перегрузки, технические неисправности и примеры киберинцидентов. Обучающая и тестовая выборки должны разделяться с учётом временной последовательности наблюдений, чтобы исключить утечку данных и завышение качества модели. Эффективность алгоритмов следует оценивать по метрикам Precision, Recall, F1-score и AUC-ROC. Особое значение имеет показатель Recall для выявления киберинцидентов, поскольку пропуск опасного события может привести к длительному нарушению работы городской инфраструктуры. Вместе с тем необходимо контролировать количество ложноположительных срабатываний, которые увеличивают нагрузку на систему мониторинга и специалистов по информационной безопасности [7].

На рисунке 1 показан иллюстративный сценарий изменения задержки, потерь пакетов и доступности IoT-сети.

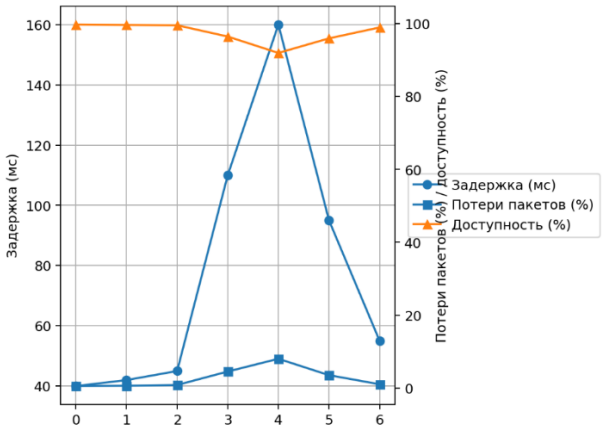


Рис. 1. График изменения задержки, потерь пакетов и доступности при нормальной нагрузке и моделируемых инцидентах (0-2 нормальная нагрузка, 3-4 инцидент, 5-6 восстановление)

График предназначен для демонстрации трёх этапов функционирования сети: Этап 0–2 - нормальная нагрузка: параметры сети относительно стабильны. Этап 3–4 - моделируемый инцидент: задержка и потери пакетов увеличиваются, доступность снижается. Этап 5–6 - восстановление: параметры постепенно приближаются к нормальным значениям. В примере задержка достигает 160 мс, потери пакетов - 8%, а доступность снижается до 92%. График показывает, как совместный мониторинг сетевых параметров может помочь выявить ухудшение состояния IoT-инфраструктуры. Однако подобная динамика сама по себе не доказывает наличие кибератаки: аналогичные изменения могут быть вызваны перегрузкой сети или техническим отказом [8,9].

Сравнение алгоритмов машинного обучения. Сравнение Random Forest, XGBoost и LSTM по Accuracy, Precision, Recall, F1-score и AUC-ROC. Таблица 2 показывает пример сравнения Random Forest, XGBoost и LSTM по пяти стандартным метрикам классификации.

Таблица 2

Значения параметров для сравнительного эксперимента

Алгоритм	Accuracy	Precision	Recall	F1-score	AUC-ROC
Random Forest	94,0%	93,0%	91,0%	92,0%	96,0%

XGBoost	96,0%	95,0%	94,0%	94,5%	98,0%
LSTM	95,0%	94,0%	96,0%	95,0%	97,0%

Метрики рассчитываются следующим образом: Accuracy - доля правильных классификаций среди всех наблюдений. Precision - доля действительно положительных случаев среди всех случаев, классифицированных как положительные. Recall - доля обнаруженных положительных случаев среди всех фактически положительных случаев. F1-score - гармоническое среднее Precision и Recall. AUC-ROC - площадь под ROC-кривой, характеризующая способность модели различать два класса. В приведённом примере XGBoost имеет наибольшие значения Accuracy и AUC-ROC, тогда как LSTM демонстрирует наиболее высокий Recall [10].

Заключение

В результате проведённого исследования рассмотрены современные проблемы обеспечения кибербезопасности и надёжности IoT-инфраструктуры систем «Умный город». Установлено, что увеличение количества подключённых устройств, расширение сетевого взаимодействия и интеграция интеллектуальных сервисов сопровождаются ростом потенциальных уязвимостей и усложнением задач защиты городской цифровой инфраструктуры.

Проведённый анализ показал, что киберугрозы могут оказывать существенное влияние не только на конфиденциальность и целостность информации, но и на доступность IoT-устройств, качество передачи данных и устойчивость функционирования телекоммуникационной сети. В работе предложен комплексный подход к оценке состояния IoT-инфраструктуры, основанный на совместном анализе параметров надёжности, доступности, качества доставки данных и признаков потенциальных инцидентов безопасности. Рассмотрена возможность применения интегрального показателя, позволяющего объединить разнородные характеристики функционирования IoT-узлов и использовать их для мониторинга состояния инфраструктуры. Практическая применимость данного показателя требует дальнейшей экспериментальной проверки и обоснования весовых коэффициентов.

Перспективным направлением повышения эффективности защиты IoT-систем является применение методов машинного обучения и искусственного интеллекта. Использование алгоритмов Random Forest, XGBoost, LSTM и методов обнаружения аномалий позволяет исследовать возможности автоматической классификации сетевых событий, выявления отклонений от нормального режима работы и прогнозирования потенциальных отказов устройств. Практическая значимость предложенного подхода заключается в возможности его дальнейшего использования при разработке интеллектуальных систем мониторинга и диагностики IoT-инфраструктуры городского освещения, транспортных систем, экологического контроля и управления энергетическими ресурсами. Комплексный анализ параметров безопасности и надёжности может способствовать более раннему выявлению потенциальных нарушений и повышению устойчивости предоставления цифровых городских услуг. Таким образом, обеспечение кибербезопасности IoT-инфраструктуры систем «Умный город» требует перехода от изолированного обнаружения угроз к комплексному управлению безопасностью, надёжностью и доступностью сетевых ресурсов.

Список литератур

1. Kim K., Alshenaifi I. M., Ramachandran S., Zia T., Almorjan A. Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey // Sensors. 2023. Vol. 23, No. 7. DOI: 10.3390/s23073681.

2. Ali J., Singh S. K., Jiang W., Alenezi A. M., Islam M., Daradkeh Y. I., Mehmood A. A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks // Computer Communications. 2024. DOI: 10.1016/j.comcom.2024.108000.

3. Omrany H., Al-Obaidi K. M., Hossain M., Alduais N. A. M., Al-Duais H. et al. IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction // Discover Cities. 2024. Vol. 1. DOI: 10.1007/s44327-024-00002-w.

4. Kaur K., Kaur A., Gulzar Y., Gandhi V. Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies // Frontiers in Computer Science. 2024. Vol. 6. DOI: 10.3389/fcomp.2024.1420680.

5. Mishra N., Islam S. K. H., Zeadally S. A survey on security and cryptographic perspective of Industrial-Internet-of-Things//Internet of Things. 2024. Vol. 25. DOI: 10.1016/j.iot.2023.101037.

6. Fagan M., Megas K. N., Marron J., Brady K. G., Cuthill B. B., Herold R., Lemire D., Hoehn N. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST Special Publication 800-213. Gaithersburg: National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.800-213.

7. Boeckl K., Fagan M., Fisher W., Lefkovitz N., Megas K., Nadeau E. M., Piccarreta B. M., O‘Rourke D. G., Scarfone K. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NISTIR 8228. Gaithersburg: National Institute of Standards and Technology, 2019. DOI: 10.6028/NIST.IR.8228.

8. European Union Agency for Cybersecurity (ENISA). Good Practices for Security of IoT: Secure Software Development Lifecycle. 2019. DOI: https://doi.org/10.2824/742784.

9. Nandhini N., Manikandan V., Manavaalan G., Elango S., Jeevakarunya C., Kumar P. V. A Survey on Intrusion Detection System in Smart City: Security Concerns // 2023 7th International Conference on Computer Applications in Electrical Engineering-Recent Advances (CERA). 2023. P. 1–6. DOI: 10.1109/CERA59325.2023.10455491

10. Borse P. B., Meesala S. K. Review of IoT-enabled Smart Cities: Cybersecurity Threat Detection Using Cloud Computing//2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). 2024. P. 1–11. DOI: https://doi.org/10.1109/ICCCNT61001.2024.10725673.

SUN’IY INTELLEKT VOSITASIDA SHAKLLANUVCHI SINTETIK TAHDIDLARNI FILTRLASH VA RAQAMLI SHAXS XAVFSIZLIGINI TA’MINLASH USULLARI

Raximov B.N., Yusupov B.K.
O‘zbekiston Respublikasi Mudofaa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ushbu qaqolada sun’iy intellekt vositasida shakllanuvchi sintetik tahdidlarni filtrlash va raqamli shaxs xavfsizligini ta’minlash usullari tahlil qilinib, ularni birlashtiruvchi ko‘p bosqichli MS-SFCBD usuli taklif etilgan. Usul sintetik yuz detektori, uning bo‘sag‘asini haqiqiy namunalarda split-konformal kalibrlash va bekor qilinuvchi BioHash shablonidan iborat. Ochiq DeepFakeFace (1 200 shaxs) va LFW (6 000 juft) ma’lumotlarida qayta sozlangan ViT-B/16 detektori AUC = 0,907 ga erishdi; JPEG siqishida qat’iy bo‘sag‘aning xato rad etish darajasi 18,1% dan 51,9% gacha oshdi, konformal kalibrlash esa uni nominal 5% da ushlab turdi. Xavfsizlik kafolati faqat aniq shartlarda mumkinligi ko‘rsatildi: kalibrlash haqiqiy foydalanuvchilarni xato rad etish darajasiga kafolat beradi, BioHash shablonining qaytarilmasligi esa tokenning maxfiyligiga bog‘liq.

Kalit so‘zlar: sun’iy intellekt xavfsizligi, sintetik tahdidlar, deepfake aniqlash, raqamli shaxs xavfsizligi, konformal kalibrlash, BioHashing, bekor qilinuvchi biometriya, MS-SFCBD.

Аннотация. В статье проанализированы методы фильтрации синтетических угроз, формируемых средствами искусственного интеллекта, и обеспечения безопасности цифровой личности, а также предложен объединяющий их многоэтапный метод MS-SFCBD. Метод включает детектор синтетических лиц, сплит-конформную калибровку его порога на подлинных образцах и отзываемый шаблон BioHash. На открытых данных DeepFakeFace (1 200 личностей) и LFW (6 000 пар) дообученный ViT-B/16 достиг AUC = 0,907; при JPEG-сжатии доля ложных отказов фиксированного порога выросла с 18,1% до 51,9%, тогда как конформная калибровка удержала её на номинальном уровне 5%. Показано, что гарантии безопасности возможны лишь при определённых условиях: калибровка гарантирует долю ложных отказов подлинным пользователям, а необратимость шаблона BioHash зависит от секретности токена.

Ключевые слова: безопасность искусственного интеллекта, синтетические угрозы, обнаружение дипфейков, безопасность цифровой личности, конформная калибровка, BioHashing, отзываемая биометрия, MS-SFCBD.

Kirish

Zamonaviy raqamli xizmatlarda - davlat boshqaruvi, bank-moliya operatsiyalari va korporativ tarmoqlarda - shaxsni kamera hamda mikrofon orqali masofadan tasdiqlash asosiy xavfsizlik omiliga aylandi. Diffuziya modellari, GAN va katta til modellari ishonarli yuz, ovoz va xabarlarni deyarli bepul yaratish imkonini berdi [1]; NIST kiberhujumlarga to‘siqlarning pasayishini generativ modellar keltirib chiqaradigan yangi xavflar qatoriga kiritadi [2], odamlar esa sun’iy yaratilgan mediani ishonchli ajrata olmaydi [3]. Shaxsni tasdiqlash bo‘yicha zamonaviy ko‘rsatmalar firibgarlikka oid talablarni kengaytirmoqda [4].

Sun’iy intellekt vositasida shakllanuvchi sintetik tahdidlarni filtrlash va raqamli shaxsni himoyalash usullarini to‘rtta asosiy guruhga ajratish mumkin:

Sintetik tasvirlarni aniqlash. Fazoviy detektorlar va oldindan o‘qitilgan katta modellar

xususiyatlariga asoslangan sinflagichlar sintetik tasvirlarni ajratadi [5, 6]; chastotaviy tahlil generatorning tanlash izlarini ochadi [7]. Bunday usullar taqsimot ichida yuqori aniqlik beradi, ammo ko‘rilmagan generatorlarga va siqish hamda shovqinga chidamsiz [8].

Jonlilik va taqdimot hujumlarini aniqlash. Teri rangi signalidagi yurak urishini tahlil qilish (rPPG) [9, 10] va yuz taqdimot hujumlarini aniqlash usullari [11] ekrandan qayta ko‘rsatish va chop etilgan tasvirlarga qarshi samarali, ammo demografik xolislik muammosi saqlanadi [12] va ular kameraga to‘g‘ridan-to‘g‘ri kiritilgan sintetik oqimga mo‘ljallanmagan.

Kelib chiqishni tasdiqlash. Suv belgisi va kontent kelib chiqishi belgilari hamkor generatorlar mahsulotini belgilaydi, ammo ularni olib tashlash yoki soxtalashtirish mumkin [13].

Biometrik shablonlarni himoyalash. BioHashing va fuzzy commitment kabi usullar [14, 15, 16] saqlanayotgan shablonni bekor qilinuvchi va qaytarilmas qiladi, biroq sensorga berilgan namuna haqiqiy deb faraz qilinadi.

Yechilishi kerak bo‘lgan muammo. Mavjud ilmiy tadqiqot ishlarida uchta kamchilik kuzatiladi:

- detektor bo‘sag‘asi o‘quv ma’lumotida qat’iy belgilanadi va sharoit o‘zgarganda haqiqiy foydalanuvchilarga tushadigan yuk nazoratdan chiqadi;
- shablon himoyasining qaytarilmasligi odatda token modelisiz ta’kidlanadi;
- aniqlash va shablonni himoyalash bir-biridan uzilgan holda tadqiq qilinadi.

Mavzu doirasida olib borilgan tadqiqot maqsadi – sintetik tahdidlarni kalibrlangan bo‘sag‘a bilan filtrlovchi va raqamli shaxs shablonini bekor qilinuvchi BioHash bilan himoyalovchi ko‘p bosqichli MS-SFCBD usulini ishlab chiqish, uning qaysi xavfsizlik xossalarini kafolatlay olishini ochiq ma’lumotlarda eksperimental aniqlash va baholashdan iborat.

Mavjud usullar tahlili va masalaning qo‘yilishi

Hujumchi himoyachiga noma’lum generator yaratgan sintetik yuz tasvirini taqdim etishi yoki oqimga kiritishi, siqish va shovqin kabi keyingi ishlovlarni qo‘llashi, joylashtirilgan detektorga qarshi gradient hujumini uyushtirishi hamda shablonlar bazasini, kuchli holatda esa foydalanuvchi tokenini ham qo‘lga kiritishi mumkin deb faraz qilinadi. Himoyachi tasvirga olish zanjirini va tekshiruv serverini nazorat qiladi, ko‘p miqdorda haqiqiy namunalarga ega, ammo belgilangan hujum namunalari kam. 1-jadvalda usullar guruhlari taqqoslangan.

Masala quyidagicha qo‘yiladi: (I) detektor generatorlar va keyingi ishlovlar bo‘yicha qanchalik umumlashtiradi; (II) qaror bo‘sag‘asini shunday kalibrlash mumkinmi, sharoit o‘zgarganda ham haqiqiy foydalanuvchilarga tushadigan yuk o‘zgarmasin; (III) BioHash shablonining bekor qilinuvchanlik, bog‘lanmaslik va qaytarilmaslik xossalari o‘lchanganda qanday bo‘ladi.

1-jadval

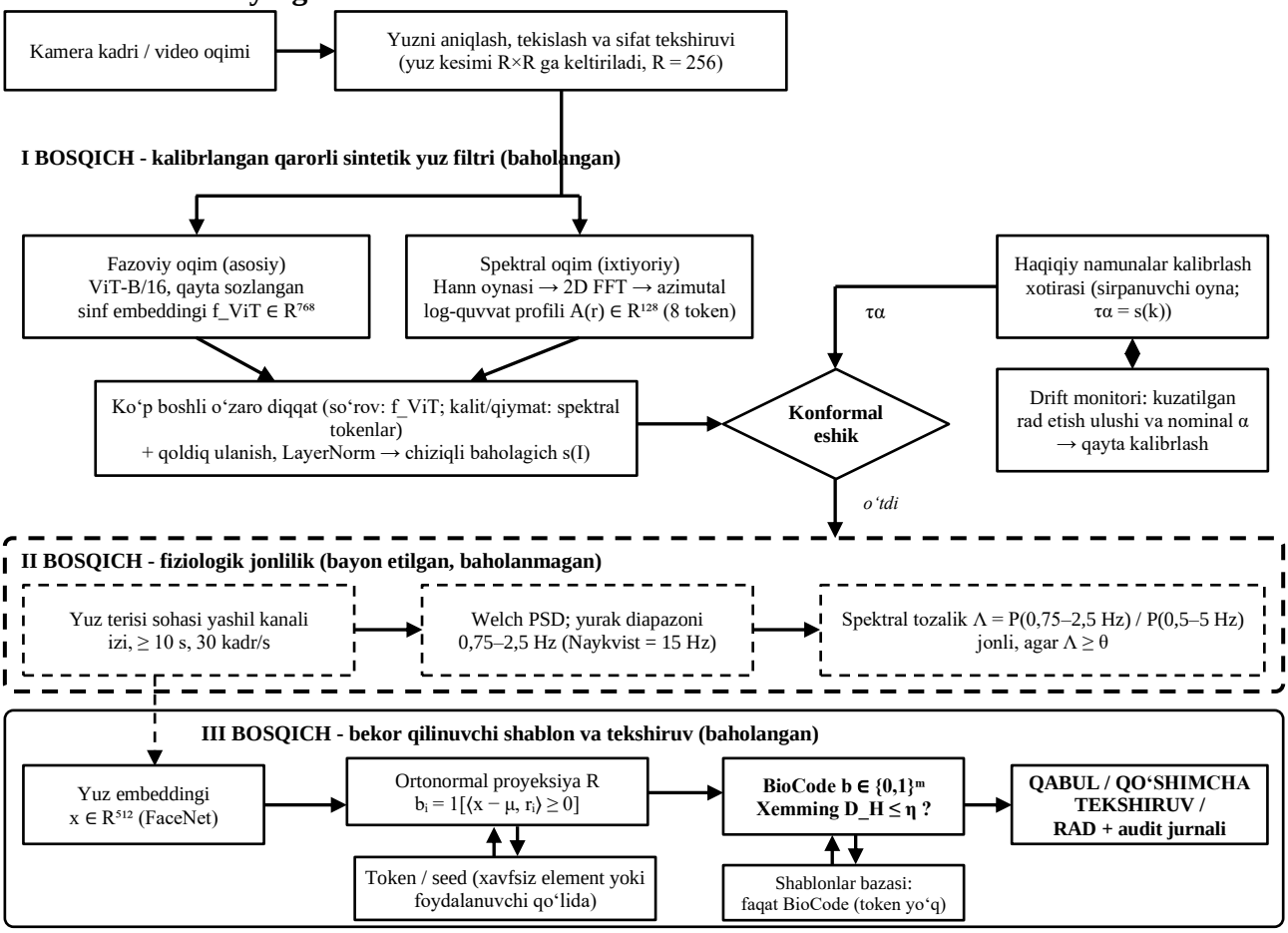
Mavjud usullar va taklif etilayotgan MS-SFCBD usulning qiyosiy tahlili

№	Usullar nomi	Kuchli tomoni	Kamchiliklari
1.	Fazoviy va asos-model detektorlari [5, 6]	Taqsimot ichida yuqori aniqlik; oldindan o‘qitilgan xususiyatlar o‘tadi	Ko‘rilmagan generator va keyingi ishlovda pasayadi
2.	Chastotaviy tahlil [7]	Generator izlarini ochadi	Siqish va shovqinga bardoshsiz
3.	Jonlilik va taqdimot hujumini aniqlash [9, 10, 11]	Chop etish va qayta ko‘rsatish hujumlariga qarshi	Oqim in’ektsiyasiga mo‘ljallanmagan; demografik xolislik [12]

№	Usullar nomi	Kuchli tomoni	Kamchiliklari
4.	Suv belgisi va kelib chiqish [13]	Hamkor generatorlarni belgilaydi	Olib tashlash va soxtalashtirish mumkin
5.	Shablon himoyasi [14, 15, 16]	Bekor qilinuvchanlik, bog‘lanmaslik	Kirish haqiqiy deb faraz qilinadi; token buzilishi
6.	Taklif etilayotgan MS-SFCBD usuli	Aniqlash + konformal kalibrlash + shablon himoyasi	Jonlilik bosqichi baholanmagan

Ovoz va matn kanallari ushbu maqoladigai ko‘rib chiqayotgan tadqiqot jarayonida ko‘rib chiqilmadi va baholash amalga oshirilmadi.

Taklif etilayotgan MS-SFCBD usuli



1-rasm. MS-SFCBD usulining uch bosqichli arxitekturasi

Usul uch bosqichdan iborat (1-rasm). *I bosqich* sintetik yuzni filtrlaydi: yuz kesimi 256×256 o‘lchamga keltiriladi va ImageNet-21k da oldindan o‘qitilgan ViT-B/16 [17] qayta sozlanib, uning 768 o‘lchamli sinf embeddingidan baho s(I) hisoblanadi. Ixtiyoriy spektral oqim - kulrang tasvirning azimut bo‘yicha integrallangan logarifmik quvvat spektri A(r) - sakkizta tokenga bo‘linib, o‘zaro diqqat (cross-attention) orqali fazoviy embedding bilan birlashtirilishi mumkin.

Konformal kalibrlash. n ta haqiqiy kalibrlash tasvirining baholari $s_1,\ldots,s_n$ bo‘lsin. Bo‘sag‘a $\tau_\alpha = s_{(k)}$, bunda $k = \lceil (n+1)(1-\alpha) \rceil$. Yangi haqiqiy baho kalibrlash baholari bilan almashinuvchan bo‘lsa, $\Pr[s(I) \le \tau_\alpha \mid \text{haqiqiy}] \ge 1-\alpha$ shartining chekli tanlanmada bajarilishi kafolatlanadi. Ikki daraja $\alpha_s > \alpha_r$ baho o‘qini o‘tish, qo‘shimcha tekshiruv va rad etish zonalariga bo‘ladi; kalibrlash oynasi uzluksiz yangilanadi, drift monitori esa kuzatilgan rad etish ulushini α bilan solishtiradi. Bu kafolat faqat haqiqiy foydalanuvchilarga tegishli: sintetik tasvirlarni ushlash quvvati detektorga

bog‘liq va o‘lchanishi kerak.

II bosqich fiziologik jonlilikni teri yashil kanalidagi yurak urishi signalining spektral tozaligi $\Lambda = P(0{,}75–2{,}5\ Hz)/P(0{,}5–5\ Hz)$ bo‘yicha tekshiradi. Ko‘z mikrotitrashi kabi 15 Hz dan yuqori tashkil etuvchilar chiqarib tashlangan, chunki ular 30 kadr/s kameraning Naykvist chastotasidan yuqori. Bu bosqich bayon etilgan, ammo ochiq video ma’lumotlar bo‘lmagani uchun aniqligi baholanmagan.

III bosqich yuz embeddingi x ni (FaceNet, 512 o‘lcham) aholi o‘rtachasi μ bilan markazlashtirib, token hosil qilgan ortonormal yo‘nalishlar r_i ga proyeksiyalaydi: $b_i = 1[\langle x-\mu, r_i\rangle \geq 0]$. Tekshiruv normallashtirilgan Xemming masofasi $D_H \leq \eta$ shartiga asoslanadi. Asosiy loyiha qoidasi: token BioCode bazasidan alohida - xavfsiz elementda yoki foydalanuvchi qo‘lida saqlanadi.

Amaliy tadqiqot va tajriba

Tajribalar ochiq ma’lumotlarda o‘tkazildi: DeepFakeFace dan 1 200 ta shaxsga mos to‘plam (har birida bitta haqiqiy surat va uchta sintetik nusxa: Stable Diffusion inpainting, InsightFace almashtirish, matndan tasvir; jami 4 800 tasvir) va LFW ning 6 000 ta tekshiruv jufti. Bo‘linishlar shaxslar bo‘yicha ajratildi (672 o‘quv, 168 validatsiya, 360 sinov). Barcha tasvirlar 256×256 ga keltirildi; JPEG (Q = 90, 70, 50) va Gauss shovqini faqat sinov tasvirlariga qo‘llandi. Ish nuqtasi validatsiyadagi teng xatolik bo‘sag‘asida belgilandi, FAR - sintetik tasvirning haqiqiy deb qabul qilinishi, FRR - haqiqiy tasvirning rad etilishi.

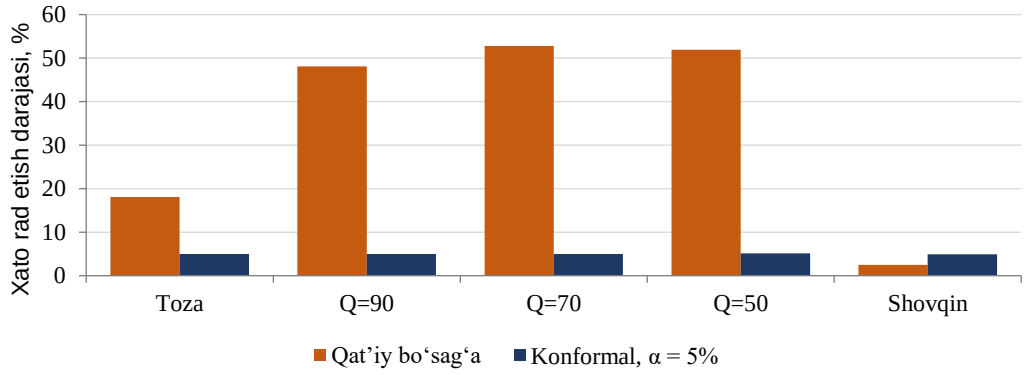
2-jadval

Aniqlash va kalibrlash natijalari (360 ta inson yuzi tasviri ma’lumotlari asosida sinovdan o‘tkazildi)

Ko‘rsatkich	S1 Qayta sozlangan ViT	P ViT + spektral cross-attention
AUC, taqsimot ichida	0,907	0,859
AUC, ko‘rilmagan generator (o‘rtacha)	0,816	0,779
FAR / FRR, %	18,0 / 18,1	22,5 / 18,9
FRR, %: JPEG Q = 50, qat’iy bo‘sag‘a	51,9	48,1
FRR, %: JPEG Q = 50, konformal (α = 5%)	5,1	5,0
Aniqlik, %: FGSM, ε = 2/255	20,4	29,6

Aniqlash. Qayta sozlangan ViT (S1) AUC = 0,907 (95% IO 0,890–0,921) ga erishdi, muzlatilgan ViT va chiziqli zond esa 0,791 ni berdi. Spektral oqim yordam bermadi: u yolg‘iz o‘zi AUC = 0,673 beradi, ViT bilan cross-attention orqali birlashtirish (P) esa 0,859 ga olib keldi, ya’ni ViT ning o‘zidan yomon. Bitta generatorni chetlab qoldirishda S1 ning AUC si o‘rtacha 0,816 gacha tushdi (2-jadval). Aniqlash oxirida FAR va FRR taxminan 18,0% bo‘lib, bu amaliy joylashtirish uchun yetarli emas.

Siqish va kalibrlash. Toza ma’lumotda sozlangan qat’iy bo‘sag‘a JPEG Q = 50 da haqiqiy tasvirlarning 51,9% ini rad etdi (toza sharoitda 18,1%). Konformal bo‘sag‘a har bir sharoitda nominal darajani saqladi: α = 5% da FRR toza sharoitda 5,0%, JPEG Q = 50 da 5,1% (2-rasm). Buning narxi - α = 1% da sintetik tasvirlarning 62,8% i qabul qilinishi: kalibrlash xato byudjetini barqaror qiladi, ammo aniqlash quvvatini oshirmaydi. White-box FGSM hujumi ε = 2/255 da S1 aniqligini 82,5% dan 20,4% gacha tushirdi.



2-rasm. S1 ning xato rad etish darajasi: qat'iy va konformal bo'sag'a.

Shablon himoyasi. BioHash (m = 512) bir xil token bilan EER = 0,87% beradi (himoyalanmagan 0,80%), har bir foydalanuvchi o'z tokeni bilan esa 0,17%. Bir yuz uchun yangi token bilan hosil qilingan kodlar orasidagi Xemming masofasi 0,499, Pirson korrelyatsiyasi 0,002, ya'ni shablon to'liq bekor qilinadi va bog'lanmaydi. Biroq token va BioCode ma'lum bo'lsa, tiklangan vektor himoyalanmagan moslashtirishdan 97,5% hollarda o'tdi, token bo'lmasa esa hech qachon (0,0%): qaytarilmaslik tokenning maxfiyligiga bog'liq. GF(2^8) maydonida to'g'ridan-to'g'ri proyeksiya moslashtirishni buzdi (EER 49,0%), Reed–Solomon fuzzy commitment esa 22,4% bit xatoligida ishlamadi (GAR ≈ 0%).

Hisoblash vaqti va resurs sarfi. Bitta tasvir uchun qayta sozlangan ViT RTX 2070 SUPER da 8,7 ms, olti yadroli CPU da 141 ms oladi; spektral oqim, baholagich va BioHash proyeksiyasi 1 ms dan kam qo'shadi.

Aniqlangan muammo va keyingi olib borilishi kerak bo'ladigan tadqiqotlar

Baholash to'plami kichik (1 200 shaxs), o'zaro yaqin uchta generatorni qamraydi va qoldiq ma'lumotlar xolisligini o'z ichiga olishi mumkin, shuning uchun mutlaq aniqliklarni real sharoitdagi ko'rsatkich deb bo'lmaydi. II bosqich baholanmagan, ovoz va matn kanallari qamralmagan. Konformal kafolat jonli va kalibrlash ma'lumotlari almashinuvchan ekanini talab qiladi. Buzg'inchi kalibrlash ma'lumotlarini zaharlashi mumkin. Adversarial baholash bir qadamli FGSM bilan cheklangan. Keyingi bosqichda jonlilik video ma'lumotlarda baholanadi, adversarial o'qitish va kamera in'ektsiyasini aniqlash qo'shiladi, FaceForensics++ va Celeb-DF da tekshiriladi.

Xulosa

Xulosa qilib aytadigan bo'lsa ushbu maqolada sun'iy intellekt vositasida shakllanuvchi sintetik tahdidlarni filtrlash va raqamli shaxs xavfsizligini ta'minlash usullari tahlil qilinib, ularni birlashtiruvchi MS-SFCBD usuli taklif etildi. Qayta sozlangan ViT-B/16 sintetik yuzlarni AUC = 0,907 bilan aniqladi, spektral oqim foyda bermadi. Split-konformal kalibrlash haqiqiy foydalanuvchilarni xato rad etish darajasini siqish sharoitida ham nominal qiymatda ushladi. BioHash bekor qilinuvchan va bog'lanmaydigan shablon beradi, ammo uning qaytarilmasligi tokenning maxfiyligiga to'liq bog'liq, GF(2^8) dagi to'g'ridan-to'g'ri arifmetika esa himoya bermaydi. Shu sababli xavfsizlik kafolati mutlaq emas, shartli ravishda u kalibrlash ma'lumotlarining haqiqiyligi va tokenning maxfiyligiga tayanadi. Natijalar dastlabki xarakterga ega va bo'lib u ko'p parametrli mezonlarda tasdiqlanishi va baholanishi kerak.

Foydalanilgan adabiyotlar ro'yxati

1. Croitoru F. A. va boshq. Deepfake Media Generation and Detection in the Generative AI Era: A Survey and Outlook // ACM Computing Surveys. – 2026. – Vol. 58, No. 15. – P. 1–35.

– DOI: 10.1145/3833867.

2. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. – NIST AI 600-1. – 2024. – DOI: 10.6028/NIST.AI.600-1.

3. Frank J. va boshq. A Representative Study on Human Detection of Artificially Generated Media Across Countries // IEEE Symposium on Security and Privacy (SP). – 2024. – P. 55–73. – DOI: 10.1109/sp54263.2024.00159.

4. Temoshok D. va boshq. Digital Identity Guidelines. – NIST SP 800-63-4. – NIST, 2025. – DOI: 10.6028/NIST.SP.800-63-4.

5. Corvi R. va boshq. On The Detection of Synthetic Images Generated by Diffusion Models // ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – 2023. – P. 1–5. – DOI: 10.1109/icassp49357.2023.10095167.

6. Ojha U., Li Y., Lee Y. J. Towards Universal Fake Image Detectors that Generalize Across Generative Models // IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). – 2023. – P. 24480–24489. – DOI: 10.1109/cvpr52729.2023.02345.

7. Frank J. va boshq. Leveraging Frequency Analysis for Deep Fake Image Recognition // ICML, PMLR vol. 119. – 2020. – arXiv:2003.08685.

8. Wang T. va boshq. Deepfake Detection: A Comprehensive Survey from the Reliability Perspective // ACM Computing Surveys. – 2024. – Vol. 57, No. 3. – P. 1–35. – DOI: 10.1145/3699710.

9. Verkruysse W., Svaasand L. O., Nelson J. S. Remote plethysmographic imaging using ambient light // Optics Express. – 2008. – Vol. 16, No. 26. – Art. 21434. – DOI: 10.1364/oe.16.021434.

10. de Haan G., Jeanne V. Robust Pulse Rate From Chrominance-Based rPPG // IEEE Transactions on Biomedical Engineering. – 2013. – Vol. 60, No. 10. – P. 2878–2886. – DOI: 10.1109/tbme.2013.2266196.

11. Sheikhfathollahi M. va boshq. A survey of deep learning for face presentation attack detection // Neurocomputing. – 2025. – Vol. 652. – Art. 131136. – DOI: 10.1016/j.neucom.2025.131136.

12. Fang M. va boshq. Fairness in face presentation attack detection // Pattern Recognition. – 2024. – Vol. 147. – Art. 110002. – DOI: 10.1016/j.patcog.2023.110002.

13. Saberi M. va boshq. Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks // ICLR. – 2024. – arXiv:2310.00076.

14. Jin A. T. B., Ling D. N. C., Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number // Pattern Recognition. – 2004. – Vol. 37, No. 11. – P. 2245–2255. – DOI: 10.1016/j.patcog.2004.04.011.

15. Teoh A., Goh A., Ngo D. Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2006. – Vol. 28, No. 12. – P. 1892–1901. – DOI: 10.1109/tpami.2006.250.

16. Juels A., Wattenberg M. A fuzzy commitment scheme // Proceedings of the 6th ACM conference on Computer and communications security. – 1999. – P. 28–36. – DOI: 10.1145/319709.319714.

17. Dosovitskiy A. va boshq. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale // ICLR. – 2021. – arXiv:2010.11929.

KIBERXAVFSIZLIKNI TA’MINLASHDA SUN’IY INTELLEKTNING O‘RNI VA ISTIQBOLDAGI RIVOJLANISH YO‘NALISHLARI

Irgasheva D.Y., Shakarov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining kiberxavfsizlikni ta’minlashdagi imkoniyatlari, xususan, kiberhujumlarni aniqlash, tasniflash va prognozlashdagi qo‘llanilishi tahlil qilinadi. Shuningdek, sun’iy intelekt va mashinaviy o‘qitish texnologiyalarining samaradorligi, mavjud muammolari hamda sun’iy intellekt asosida shakllanayotgan yangi turdagi kiberhujumlar tahlil qilinib, ushbu yo‘nalishning istiqbolli rivojlanish tendensiyalari yoritiladi.

Kalit so‘zlar: Sun’iy intellekt, kiberxavfsizlik, mashinaviy o‘rganish, chuqur o‘rganish, Federativ o‘rganish, Mustahkamlovchi o‘rganish, Tushuntiriladigan sun’iy intellekt.

Аннотация. В настоящих тезисах анализируются возможности технологий искусственного интеллекта и машинного обучения в обеспечении кибербезопасности, в частности их применение для обнаружения, классификации и прогнозирования кибератак. Кроме того, рассматриваются эффективность и существующие проблемы применения технологий искусственного интеллекта и машинного обучения, а также анализируются новые виды кибератак, формирующиеся на основе технологий искусственного интеллекта. Особое внимание уделяется перспективным тенденциям развития данного направления и основным направлениям его дальнейшего совершенствования.

Ключевые слова: искусственный интеллект, кибербезопасность, машинное обучение, глубокое обучение, федеративное обучение, обучение с подкреплением, объяснимый искусственный интеллект.

Kirish

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi axborot tizimlari va tarmoq infratuzilmalarining kengayishiga olib kelishi bilan birga, kiberxavfsizlikka tahdidlarning ko‘lami va murakkabligining ortishiga ham sabab bo‘lmoqda. Ayniqsa, yangi va tez o‘zgaruvchan kiberhujumlarni an’anaviy, qat’iy qoidalarga asoslangan usullar yordamida o‘z vaqtida aniqlash va ularga tezkor javob berish muayyan cheklovlarni yuzaga keltirmoqda. Shu nuqtayi nazardan, sun’iy intellekt texnologiyalaridan foydalanish kiberxavfsizlik tizimlarining tahdidlarni aniqlash, tahlil qilish va oldindan baholash imkoniyatlarini kengaytiruvchi istiqbolli yo‘nalishlardan biri hisoblanadi.

Sun’iy intellekt, xususan, mashinaviy o‘rganish va chuqur o‘rganish usullari katta hajmdagi ma’lumotlardan qonuniyatlarni aniqlash, anomal xatti-harakatlarni ajratish hamda kiberhujumlarni tasniflash imkonini beradi. Bundan tashqari, federativ o‘rganish va mustahkamlovchi o‘rganish kabi yondashuvlar taqsimlangan muhitlarda ma’lumotlar maxfiyligini ta’minlash va moslashuvchan himoya strategiyalarini shakllantirish imkoniyatlarini kengaytirmoqda. [1]

Shu bilan birga, sun’iy intellektning kiberxavfsizlikdagi imkoniyatlarini baholashda uning qo‘llanilish yo‘nalishlari bilan bir qatorda, mavjud cheklovlari va yangi turdagi tahdidlarni yuzaga keltirish ehtimolini ham hisobga olish zarur. Shu sababli, mazkur tezisda sun’iy intellektning kiberxavfsizlikdagi asosiy qo‘llanilish sohalari, sun’iy intelekt va mashinaviy o‘qitish asosidagi

yondashuvlarning imkoniyatlari va muammolari hamda ushbu yo‘nalishning istiqbolli rivojlanish tendensiyalari tahlil qilinadi.

Asosiy qism

Sun’iy intellekt texnologiyalarining kiberxavfsizlikdagi qo‘llanilishi tahdidlarni aniqlash, tahlil qilish va ularga javob berish jarayonlarini avtomatlashtirish imkonini bermoqda. Kiberhujumlarning murakkablashuvi, xususan, uzoq muddat davom etuvchi va yashirin xarakterdagi hujumlarning ko‘payishi xavfsizlik tizimlaridan katta hajmdagi ma’lumotlarni tezkor qayta ishlash hamda anomal holatlarni aniqlash imkoniyatini talab etmoqda. Shu nuqtayi nazardan, sun’iy intellektning kiberxavfsizlikdagi asosiy qo‘llanilish sohalarini quyidagicha guruhlash mumkin.

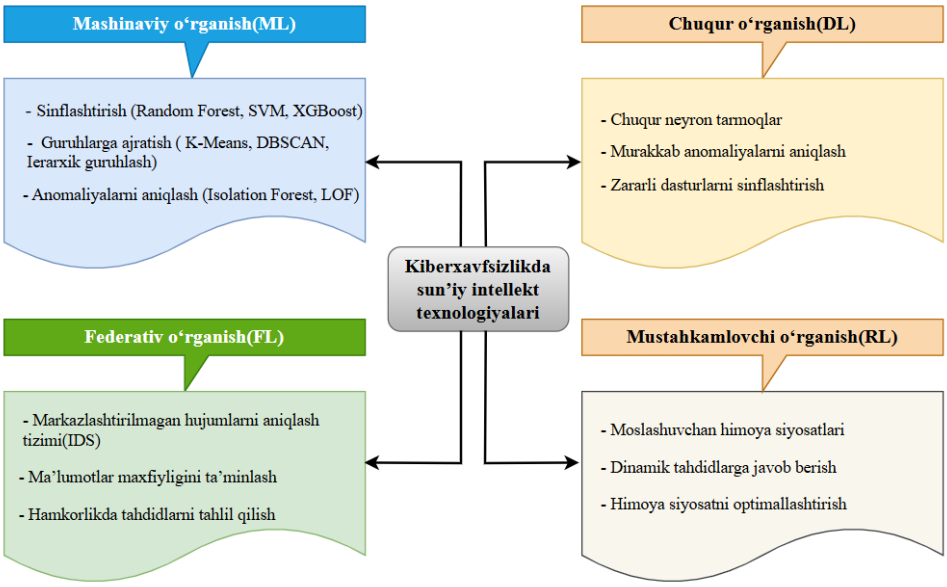
1-jadval

Kiberxavfsizlikda sun’iy intellektning asosiy qo‘llanilish sohalari

№	Qo‘llanilish sohasi	Tavsif
1	Hujumni aniqlash va oldini olish tizimlari (IDPS)	Sun’iy intellekt asosidagi IDPS tizimlari mashinaviy o‘rganish yordamida tarmoq trafikini kuzatadi va kiber tahdidlarni ko‘rsatishi mumkin bo‘lgan anomal holatlarni aniqlaydi.
2	Zararli dasturlarni aniqlash va tahlil qilish	Sun’iy intellekt asosidagi yechimlar chuqur o‘rganish modellari yordamida zararli dasturlarni ularning xatti-harakatlariga qarab aniqlaydi va tasniflaydi.
3	Tahdidlarni tahlil qilish va bashoratlash	Sun’iy intellekt tizimlari turli manbalardan ma’lumotlarni yig‘adi va o‘tmishdagi hodisalarni tahlil qilib, kelajakdagi tahdidlarni bashorat qiladi.
4	Foydalanuvchi xatti-harakatlarini tahlil qilish (UBA)	Sun’iy intellekt tizimlari tarmoq va tizimlarda foydalanuvchilarning xatti-harakatlarini kuzatadi hamda noodatiy faoliyatlarni aniqlaydi.
5	IoT xavfsizligida sun’iy intellekt	IoT qurilmalar soni ortib borayotganligi sababli, sun’iy intellekt ushbu ekotizimlarda tahdidlarni avtomatik aniqlash va ularga javob berishni ta’minlaydi hamda ulangan qurilmalarni kiberxavflardan himoya qiladi.

Jadvaldan ko‘rinib turibdiki, sun’iy intellekt kiberxavfsizlikning turli bosqichlarida - tarmoq hujumlarini aniqlashdan tortib, zararli dasturlarni tahlil qilish, tahdidlarni bashoratlash, foydalanuvchi xatti-harakatlarini baholash va IoT qurilmalarini himoyalashgacha bo‘lgan jarayonlarda qo‘llanilmoqda. Bunda sun’iy intelekt texnologiyalarining asosiy afzalligi katta hajmdagi ma’lumotlardan foydalanib, normal va anomal faoliyat o‘rtasidagi farqlarni aniqlash hamda tahdidlarni avtomatlashtirilgan tarzda tasniflash imkoniyatidir.

Kiberxavfsizlik vazifalarini hal etishda sun’iy intellektning turli yondashuvlari qo‘llaniladi. Xususan, mashinaviy o‘rganish, chuqur o‘rganish, federativ o‘rganish va mustahkamlovchi o‘rganish yondashuvlari turli xavfsizlik vazifalariga mos ravishda foydalaniladi. [2] Ularning qo‘llanilish xususiyatlari 1-rasmda umumlashtirilgan.



1-rasm. Kiberxavfsizlikda ML, DL, FL va RL ning qo‘llanilishi

Mashinaviy o‘rganish usullari, jumladan, Random Forest (RF) [3], Support Vector Machine (SVM) [3] va Naïve Bayes (NB) [3], asosan tasniflash, klasterlash va anomal holatlarni aniqlash vazifalarida qo‘llaniladi. Chuqur o‘rganish usullari murakkab va katta hajmdagi ma’lumotlardan foydalanib, anomal faoliyat hamda zararli dasturlarni aniqlash imkoniyatlarini kengaytiradi. Federativ o‘rganish ma’lumotlarni markazlashtirmagan holda modelni o‘qitish orqali maxfiylikni saqlashga yo‘naltirilgan bo‘lsa, mustahkamlovchi o‘rganish dinamik muhitda himoya strategiyalarini shakllantirish va xavfsizlik qarorlarini optimallashtirishga xizmat qiladi.

Mazkur yondashuvlarning rivojlanishi bilan bir qatorda, sun’iy intellektning kiberxavfsizlikdagi qo‘llanilishida yangi ilmiy yo‘nalishlar ham shakllanmoqda. Ayniqsa, model qarorlarini tushuntirish, adversarial ta’sirlarga chidamlilik, IoT muhitida xavfsizlikni ta’minlash va xavfsizlik jarayonlarini avtomatlashtirish kabi masalalar dolzarb bo‘lib qolmoqda.



2-rasm. Kiberxavfsizlikda sun’iy intellektning asosiy rivojlanish yo‘nalishlari

2-rasmda keltirilgan yo‘nalishlar orasida izohlanadigan sun’iy intellekt (XAI) [5], adversarial mashinaviy o‘rganish [6], IoT xavfsizligidagi sun’iy intelekt [7], avtonom xavfsizlik

operatsiya markazlari hamda sun’iy intelekt asosidagi tahdidlar razvedkasi alohida ahamiyatga ega. Izohlanuvchi sun’iy intelekt xavfsizlik tizimlari tomonidan qabul qilinayotgan qarorlarning izohlanishini oshirishga xizmat qilsa, adversarial mashinaviy o‘rganish modellarni ataylab shakllantirilgan qarama-qarshi ma’lumotlar ta’siridan himoyalash masalasini o‘rganadi. Avtonom xavfsizlik tizimlari esa tahdidlarni aniqlash va ularga javob berish jarayonlarini yanada avtomatlashtirishga yo‘naltirilmoqda.

Shunday qilib, sun’iy intellektning kiberxavfsizlikdagi rivojlanishi faqat mavjud hujumlarni aniqlash bilan cheklanmay, tahdidlarni oldindan baholash, xavfsizlik qarorlarini avtomatlashtirish va yangi avlod himoya mexanizmlarini shakllantirishga tomon yo‘nalmoqda.

Xulosa

Xulosa qilib aytganda, sun’iy intellekt texnologiyalari zamonaviy kiberxavfsizlik tizimlarining ajralmas qismiga aylanib bormoqda. Ushbu tadqiqot natijalari shuni ko‘rsatadiki, mashinaviy o‘qitish, chuqur o‘rganish, federativ o‘rganish va mustahkamlovchi o‘rganish kabi yondashuvlar kiberhujumlarni aniqlash va oldini olish jarayonlarini sezilarli darajada takomillashtiradi. Ayniqsa, sun’iy intellektning katta hajmdagi ma’lumotlar asosida qonuniyatlarni aniqlash va tahdidlarni oldindan bashorat qilish qobiliyati an’anaviy reaktiv xavfsizlik tizimlariga nisbatan ancha samarali ekanligi aniqlandi. Shu bilan birga, sun’iy intelekt texnologiyalari yordamida xavfsizlik jarayonlarini avtomatlashtirish, inson omiliga bog‘liqlikni kamaytirish va real vaqt rejimida tezkor qarorlar qabul qilish imkoniyati kengaymoqda.

Biroq, sun’iy intellektni kiberxavfsizlikda qo‘llash bilan bog‘liq muammolar ham mavjud bo‘lib, ular orasida model shaffofligi, adversarial hujumlarga chidamlilik va etik masalalar alohida ahamiyat kasb etadi. Tadqiqot shuni ko‘rsatadiki, kelajakda izohlanadigan sun’iy intellekt (XAI), adversarial mashinaviy o‘rganish, avtonom xavfsizlik tizimlari hamda kvant texnologiyalariga mos kriptografik yechimlar kiberxavfsizlikning asosiy rivojlanish yo‘nalishlari bo‘lib xizmat qiladi. Shu sababli, sun’iy intellekt asosidagi tizimlarni yanada takomillashtirish, ularning ishonchliligi va barqarorligini oshirish hamda real sharoitlarga moslashtirish dolzarb ilmiy va amaliy vazifalardan biri hisoblanadi.

Foydalanilgan adabiyotlar

1. Aslan Ö., Aktuğ S. S., Ozkan-Okay M., Yilmaz A. A. & Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics 12, 1333 (2023)

2. Zhang W., Gu, X., Tang L., Yin Y., Liu D. & Zhang Y. Application of machine learning, deep learning and optimization algorithms in geoengineering and geoscience: Comprehensive review and future challenge. Gondwana Res 109, 1–17 (2022).

3. Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowl Inf Syst 67, 1–87 (2025).

4. Shakya A. K., Pillai G. & Chakrabarty S. Reinforcement learning algorithms: A brief survey. Expert Syst Appl 231, 120495 (2023).

5. Mathews S. M., ‘‘Explainable artificial intelligence applications in NLP, 2168 biomedical, and malware classification: A literature review,’’ in Intelli2169 gent Computing. Cham, Switzerland: Springer, 2019, pp. 1269–1292, doi: 2170 10.1007/978-3-030-22868-2_90

6. Andrew Ross and Finale Doshi-Velez, 2018. Improving the adversarial robustness and interpretability of deep neuralnetworks by regularizing their input gradients. In Proc. of AAA.

7. Dusmurod Kilichev, Wooseong Kim. 2026. Real-time intrusion detection in IoT networks: A hybrid framework of offline ML and online DL. Internet of Things 102039.

FAYL METAMA’LUMOTLARINI RAQAMLI KRIMINALISTIK TAHLIL QILISH VA ULARNING SOXTALASHTIRILGANLIGINI ANIQLASH USULLARI

Sodiqova D.J.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Maqolada axborot-kommunikatsiya tizimlarida saqlanadigan va uzatiladigan fayllarning metama’lumotlarini raqamli kriminalistik tahlil qilish masalalari ko‘rib chiqilgan. Fayl tizimi, fayl ichki tuzilmasi va operatsion tizim jurnallari darajasidagi metama’lumotlar tasniflangan, ularni soxtalashtirishning asosiy usullari tahlil qilingan. Vaqt belgilarining o‘zaro mosligi, ichki va tashqi metama’lumotlarning muvofiqligi hamda jurnal artefaktlari bilan solishtirishga asoslangan kompleks aniqlash algoritmi taklif etilgan. Algoritmda belgilarning vaznli yig‘indisi asosida ishonchsizlik koeffitsienti hisoblanadi va uning chegaraviy qiymat bilan solishtirilishi orqali faylning soxtalashtirilganligi to‘g‘risida xulosa chiqariladi.

Kalit so‘zlar: raqamli kriminalistika, fayl metama’lumotlari, vaqt belgilari, soxtalashtirish, anti-kriminalistika, NTFS, EXIF, raqamli dalil.

Аннотаци: В статье рассмотрены вопросы цифрового криминалистического анализа метаданных файлов, хранимых и передаваемых в информационно-коммуникационных системах. Приведена классификация метаданных уровня файловой системы, внутренней структуры файла и журналов операционной системы, проанализированы основные способы их фальсификации. Предложен комплексный алгоритм выявления фальсификации, основанный на проверке взаимного соответствия временных меток, согласованности внутренних и внешних метаданных и сопоставлении с журнальными артефактами. В алгоритме вычисляется коэффициент недостоверности как взвешенная сумма признаков, сравнение которого с пороговым значением позволяет сделать вывод о фальсификации файла.

Ключевые слова: цифровая криминалистика, метаданные файлов, временные метки, фальсификация, антикриминалистика, NTFS, EXIF, цифровое доказательство.

Bugungi kunda axborot-kommunikatsiya tizimlarida yaratilayotgan har bir elektron hujjat, tasvir yoki multimedia fayli o‘zi haqidagi qo‘shimcha ma’lumotlar - metama’lumotlar bilan birga saqlanadi. Ular faylning yaratilgan va o‘zgartirilgan vaqti, muallifi, yaratishda foydalanilgan qurilma va dasturiy ta’minot, hatto geografik joylashuv haqida ham ma’lumot beradi. Shu sababli metama’lumotlar kiberjinoyatlarni tergov qilishda voqealar ketma-ketligini tiklash va shaxsni aniqlash uchun eng muhim raqamli dalillardan biri hisoblanadi [5, 6].

Shu bilan birga, metama’lumotlarni maxsus vositalar yordamida o‘zgartirish oson bo‘lib, huquqbuzarlar undan izlarni yashirish yoki soxta alibi yaratish maqsadida foydalanadi. Bunday harakatlar anti-kriminalistika deb ataladi va raqamli dalillarning ishonchliligiga bevosita tahdid soladi [2, 9]. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunida kiberhodisalarni aniqlash va tergov qilish vazifalari belgilanganligi [1] ham ushbu yo‘nalishning dolzarbligini ko‘rsatadi. Mazkur maqolaning maqsadi - fayl metama’lumotlarining soxtalashtirilganligini aniqlash usullarini tizimlashtirish va ular asosida kompleks tahlil algoritmini taklif etishdan iborat.

Fayl metama’lumotlarining turlari va kriminalistik ahamiyati

Kriminalistik nuqtai nazardan fayl metama’lumotlarini saqlanish joyiga ko‘ra uch darajaga ajratish maqsadga muvofiq (1-jadval). Bu darajalar bir-biridan mustaqil ravishda shakllanganligi sababli, ularni o‘zaro solishtirish soxtalashtirishni aniqlashning asosiy manbai bo‘lib xizmat qiladi.

1-jadval

Fayl metama’lumotlarining darajalar bo‘yicha tasnifi

Daraja	Asosiy atributlar	Kriminalistik ahamiyati
Fayl tizimi	NTFS: $STANDARD_INFORMATION ($SI) va $FILE_NAME ($FN) atributlaridagi MACB vaqt belgilari, hajm, egasi	Faylning tizimda paydo bo‘lishi va o‘zgarishlar vaqtini aniqlash
Fayl ichki tuzilmasi	EXIF/XMP (tasvirlar), docProps/core.xml va app.xml (Office hujjatlari), PDF Info lug‘ati	Muallif, qurilma, dasturiy ta’minot, asl yaratilgan vaqt
Operatsion tizim artefaktlari	$UsnJrnl, $LogFile, Prefetch, LNK fayllar, ro‘yxatga olish kitobi (registry)	Fayl ustida bajarilgan amallar tarixini mustaqil tasdiqlash

Fayl tizimi darajasidagi metama’lumotlar foydalanuvchi uchun eng oson o‘zgartiriladigan qatlam hisoblanadi. Ichki metama’lumotlar fayl formati standartlarida belgilanadi, masalan, tasvirlar uchun EXIF 3.0 standarti [10]. Jurnal artefaktlari esa operatsion tizim tomonidan avtomatik yuritiladi va ularni izsiz o‘zgartirish ancha murakkab [3, 4].

Metama’lumotlarni soxtalashtirishning asosiy usullari

Amaliyotda metama’lumotlarni soxtalashtirish quyidagi usullar orqali amalga oshiriladi: vaqt belgilarini maxsus utilitalar yoki SetFileTime kabi tizim funksiyalari yordamida o‘zgartirish (timestomping); EXIF va hujjat xossalari maydonlarini tahrirlovchi dasturlar bilan qayta yozish; tizim soatini vaqtincha o‘zgartirib fayl yaratish; metama’lumotlarni to‘liq o‘chirib tashlash. Tadqiqotlar shuni ko‘rsatadiki, foydalanuvchi darajasidagi vositalar odatda faqat $SI atributini o‘zgartiradi, $FN atributi va jurnal yozuvlari esa o‘zgarishsiz qoladi [2, 3]. Aynan shu nomuvofiqlik soxtalashtirishni aniqlash uchun asos bo‘ladi [11].

Vaqt belgilarining ichki mosligini tekshirish usuli

NTFS fayl tizimida $FN atributi asosan fayl yaratilganda yoki ko‘chirilganda yangilanadi. Shu sababli $SI yaratilgan vaqtining $FN yaratilgan vaqtidan oldin bo‘lishi soxtalashtirish belgisi hisoblanadi. Bundan tashqari, NTFS vaqt belgilari 100 nanosekund aniqlikda saqlanadi, ko‘plab utilitalar esa sekund kasr qismini nolga tenglashtiradi; kasr qismining aynan nolga teng bo‘lishi ham shubhali belgi sifatida qaraladi [2, 3].

Ichki va tashqi metama’lumotlar muvofiqligini tekshirish usuli

Tasvirning EXIF DateTimeOriginal maydoni, hujjatning dcterms:created va dcterms:modified maydonlari fayl tizimi vaqt belgilari bilan solishtiriladi. Mantiqiy ziddiyatlar, masalan, o‘zgartirilgan vaqtning yaratilgan vaqtdan oldin bo‘lishi, tahrirlar soni (cp:revision) bilan umumiy tahrirlash vaqti (TotalTime) o‘rtasidagi nomutanosiblik yoki yaratuvchi dasturiy ta’minot versiyasining sana bilan mos kelmasligi soxtalashtirishni ko‘rsatadi.

Jurnal artefaktlari bilan solishtirish usuli

$UsnJrnl jurnalidagi FILE_CREATE, BASIC_INFO_CHANGE yozuvlari va $LogFile tranzaksiyalari faylning haqiqiy tarixini mustaqil ravishda tasdiqlaydi [4]. Agar vaqt belgisi

o‘zgartirilgan bo‘lsa, jurnalda BASIC_INFO_CHANGE yozuvi qoladi va uning vaqti faylning da’vo qilingan yaratilish vaqtiga mos kelmaydi.

Intellektual tahlil usullari

So‘nggi yillarda katta hajmdagi artefaktlar ichidan anomaliyalarni avtomatik aniqlash uchun mashinali o‘qitish usullari qo‘llanilmoqda [7, 8]. Ularning afzalligi - ko‘p sonli belgilarni bir vaqtda hisobga olish, kamchiligi esa natijalarni sudda tushuntirib berish qiyinligidir. Ko‘rib chiqilgan usullarning qiyosiy tavsifi 2-jadvalda keltirilgan.

2-jadval

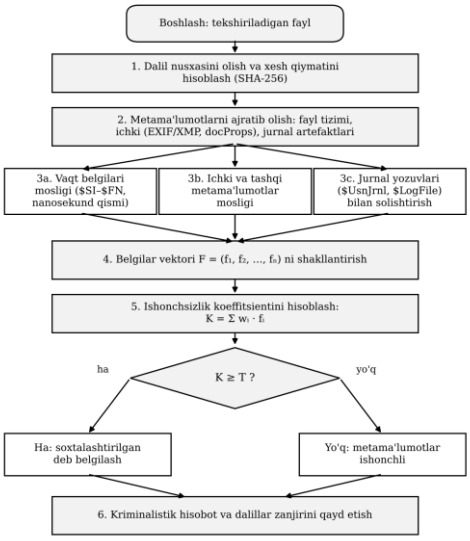
Soxtalashtirishni aniqlash usullarining qiyosiy tavsifi

Usul	Aniqlaydigan holat	Afzalligi	Cheklovi
Vaqt belgilari ichki mosligi	$SI < $FN, nol kasr qism	Tezkor, qo‘shimcha ma’lumot talab etmaydi	Past darajali vositalar $FN ni ham o‘zgartirishi mumkin
Ichki va tashqi muvofiqlik	EXIF/docProps va fayl tizimi ziddiyati	Formatlar bo‘yicha universal	Metama’lumot o‘chirilgan bo‘lsa qo‘llanilmaydi
Jurnal artefaktlari	BASIC_INFO_CHANGE, haqiqiy yaratilish vaqti	Yuqori ishonchlilik	Jurnallar cheklangan hajmda, eskilari o‘chadi
Intellektual tahlil	Murakkab va noodatiy anomaliyalar	Katta hajmda avtomatlashtirish	O‘qitish ma’lumotlari va izohlash muammosi

Yuqoridagi usullarning har biri alohida qo‘llanilganda cheklovlarga ega bo‘lganligi sababli, maqolada ularni yagona tizimga birlashtiruvchi algoritm taklif etiladi (1-rasm). Algoritm har bir tekshiruv natijasini $f_i \in [0,1]$ belgisi ko‘rinishida ifodalaydi va ishonchsizlik koeffitsientini quyidagicha hisoblaydi:

$$K = \Sigma\, w_\text{i} \cdot f_\text{i},\ \ \Sigma\, w_\text{i} = 1,\ \ i = 1, \dots, n, \qquad (1)$$

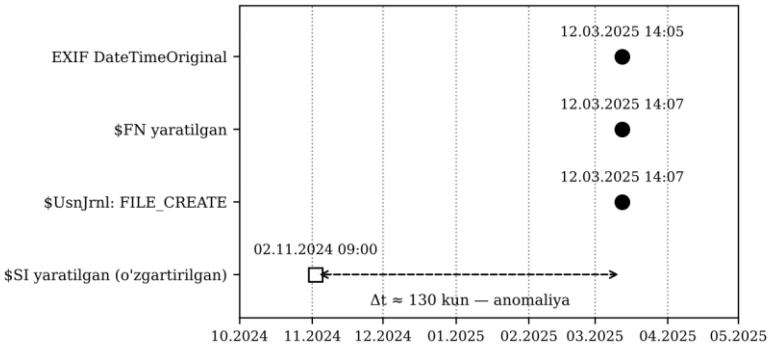
bu yerda w_i - i-belgining vazni bo‘lib, u tegishli artefaktning o‘zgartirishga chidamliligiga qarab tanlanadi. $K \geq T$ shart bajarilganda (T - chegaraviy qiymat) fayl metama’lumotlari soxtalashtirilgan deb topiladi. Vaqt farqiga asoslangan belgilar uzluksiz ko‘rinishda hisoblanadi: $f = \min(1;\ |\Delta t| / \tau)$, bu yerda τ- ruxsat etilgan farq (masalan, 24 soat).



1-rasm. Fayl metama’lumotlarining soxtalashtirilganligini aniqlash algoritmi

Algoritmning birinchi bosqichida dalil nusxasi olinib, uning SHA-256 xesh qiymati qayd etiladi. Bu tahlil jarayonida dalilning o‘zgarmaganligini kafolatlaydi va dalillar zanjirini saqlash talablariga javob beradi [9]. Keyingi bosqichlarda uch darajadagi metama’lumotlar parallel tekshiriladi va natijalar yagona belgilar vektoriga birlashtiriladi.

Algoritmning ishlashini ko‘rsatish uchun NTFS bo‘limida saqlangan JPEG tasvir misolida namunaviy tahlil keltiriladi. Tasvirning $SI yaratilgan vaqti 02.11.2024 qilib o‘zgartirilgan, ammo EXIF, $FN va $UsnJrnl ma’lumotlari 12.03.2025 sanani ko‘rsatadi (2-rasm).



2-rasm. Namunaviy fayl vaqt belgilarining vaqt o‘qidagi joylashuvi

Belgilar qiymatlari va ishonchsizlik koeffitsientini hisoblash natijasi 3-jadvalda keltirilgan. Tasvir fayli uchun hujjat xossalari belgisi qo‘llanilmaydi va nolga teng deb olinadi.

3-jadval

Namunaviy fayl uchun ishonchsizlik koeffitsientini hisoblash

№	Belgi	Vazn w_i	Qiymat f_i	$w_i \cdot f_i$
f_1	$SI yaratilgan vaqti $FN dan oldin	0,30	1	0,30
f_2	$SI vaqtining kasr qismi nolga teng	0,15	1	0,15
f_3	EXIF va $SI vaqtlari farqi ($\tau$ = 24 soat)	0,20	1	0,20
f_4	$UsnJrnl da BASIC_INFO_CHANGE yozuvi mavjud	0,25	1	0,25
f_5	Hujjat xossalari ziddiyati	0,10	0	0,00
	Ishonchsizlik koeffitsienti K	1,00		0,90

Hisoblangan K = 0,90 qiymati T = 0,5 chegaradan katta bo‘lganligi sababli fayl metama’lumotlari soxtalashtirilgan deb topiladi. Muhim jihat shundaki, xulosa bitta belgiga emas, balki uch mustaqil darajadagi dalillarning o‘zaro tasdig‘iga asoslanadi. Bu natijani ekspert xulosasida asoslab berishni osonlashtiradi.

Xulosa

Maqolada fayl metama’lumotlari fayl tizimi, fayl ichki tuzilmasi va operatsion tizim artefaktlari darajalari bo‘yicha tasniflandi, ularni soxtalashtirishning asosiy usullari va aniqlash usullari tahlil qilindi. Taklif etilgan kompleks algoritm turli darajadagi metama’lumotlarni o‘zaro solishtirish va belgilarning vaznli yig‘indisi asosida qaror qabul qilishga imkon beradi. Algoritm alohida usullarning cheklovlarini qisman bartaraf etadi va xulosaning shaffofligini ta’minlaydi. Keyingi ishlarda vazn koeffitsientlarini real ma’lumotlar to‘plami asosida optimallashtirish va algoritmni bulutli muhitdagi fayllarga moslashtirish rejalashtirilgan.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 2022-yil 15-aprel.

2. Palmbach D., Breitinger F. Artifacts for detecting timestamp manipulation in NTFS on Windows and their reliability // Forensic Science International: Digital Investigation. – 2020. – Vol. 32. – 300920.

3. Galhuber M., Luh R. Time for Truth: Forensic Analysis of NTFS Timestamps // Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021). – ACM, 2021.

4. Oh J., Lee S., Hwang H. NTFS Data Tracker: Tracking file data history based on $LogFile // Forensic Science International: Digital Investigation. – 2021.

5. Al-Dhaqm A. et al. Digital forensics subdomains: The state of the art and future directions // IEEE Access. – 2021. – Vol. 9.

6. Casino F. et al. Research trends, challenges, and emerging topics in digital forensics: A review of reviews // IEEE Access. – 2022. – Vol. 10.

7. Du X. et al. SoK: Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation // Proceedings of ARES 2020. – ACM, 2020.

8. Breitinger F. et al. DFRWS EU 10-year review and future directions in Digital Forensic Research // Forensic Science International: Digital Investigation. – 2024. – Vol. 48.

9. Gruber J., Hargreaves C., Freiling F. Contamination of digital evidence: Understanding an underexposed risk // Forensic Science International: Digital Investigation. – 2023. – Vol. 44.

10. CIPA DC-008-2023. Exchangeable image file format for digital still cameras: Exif Version 3.0. – Camera & Imaging Products Association, 2023.

11. NIST IR 8354. Digital Investigation Techniques: A NIST Scientific Foundation Review. – National Institute of Standards and Technology, 2022.

MODERN PROBLEMS OF CYBERSECURITY AND METHODS OF SOLVING THEM

Sodiqova D.J., Sodikov U.B.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotatsiya: Ushbu maqolada raqamli texnologiyalar jadal rivojlanayotgan sharoitda kiberxavfsizlik sohasida yuzaga kelayotgan zamonaviy muammolar - fishing hujumlari, to‘lov talab qiluvchi zararli dasturlar, shaxsga doir ma’lumotlarning sizib chiqishi, sun’iy intellekt yordamida amalga oshiriladigan hujumlar va “narsalar interneti” qurilmalarining zaifliklari tahlil qilingan. Tahdidlar tasnifi jadval ko‘rinishida keltirilgan, ko‘p qatlamli himoya usuli hamda kiberhodisalarga javob berish sikli taklif etilgan. Maqolada foydalanuvchilarning raqamli savodxonligini oshirish muhim himoya omili ekanligi asoslab berilgan.

Kalit so‘zlar: kiberxavfsizlik, kibertahdid, fishing, zararli dastur, ransomware, ko‘p faktorli autentifikatsiya, shifrlash, raqamli savodxonlik.

Аннотация: В статье анализируются современные проблемы кибербезопасности в условиях стремительного развития цифровых технологий: фишинговые атаки, программы-вымогатели, утечки персональных данных, атаки с применением искусственного интеллекта и уязвимости устройств «интернета вещей». Приведена классификация угроз в табличной форме, предложены многоуровневый метод защиты и цикл реагирования на киберинциденты. Обосновано, что повышение цифровой грамотности пользователей является важным фактором защиты.

Ключевые слова: кибербезопасность, киберугроза, фишинг, вредоносное программное обеспечение, программа-вымогатель, многофакторная аутентификация, шифрование, цифровая грамотность.

Today, almost every area of human life - education, healthcare, banking, public administration and everyday communication - is closely tied to digital systems. Mobile phones, online payment systems, e-government services and distance learning platforms have made life more convenient, but they have also created new risks. Data theft, account hijacking and the disruption of systems can cause serious harm to individuals, organisations and the state.

The Republic of Uzbekistan pays great attention to this field. In particular, the Law “On Cybersecurity” adopted in 2022 established the legal basis for protecting information systems and resources [1]. Therefore, studying cybersecurity problems and developing ways to address them is an urgent task. The purpose of this article is to systematise modern cyber threats and to propose an effective method of protection against them.

Cybersecurity is a set of measures aimed at protecting information systems, networks, software and data from unauthorised access, modification, destruction or disruption. International practice bases information security on three core principles: confidentiality (only authorised persons can view the data), integrity (the data has not been altered) and availability (the system works when it is needed) [2, 3].

Modern cyber threats. Annual reports of international organisations identify ransomware, social engineering and attacks targeting data as among the most widespread threats in recent years [4]. The main types of threats and the corresponding countermeasures are presented in Table 1.

Table 1

Classification of modern cyber threats and protective measures

Threat type	Essence	Main protective measures
Phishing	Tricking users into revealing passwords and card details through fake messages, websites or links	Checking links, multi-factor authentication, staff training
Ransomware	Encrypting files and demanding payment to unlock them	Regular backups, software updates, EDR tools
Data leaks	Personal and commercial data falling into the hands of outsiders	Encryption, restricting access rights, monitoring
DDoS attack	Flooding a server with fake requests to stop the service	Traffic filtering, reserve capacity, CDN services
AI-based attacks	Fake voice and video (deepfakes), automated phishing texts	Confirming information through a second channel, digital literacy
IoT device vulnerabilities	Default passwords and outdated software in cameras and "smart" home devices	Changing default passwords, a separate network segment, updates

Among these threats, social engineering holds a special place, because it exploits human trust rather than a technical weakness. For example, calling on behalf of a "bank employee" to ask for an SMS code, or sending a fake message about a "prize", are common tricks. The development of artificial intelligence tools makes such deception even more convincing: it is now possible to imitate the voice of a familiar person or to generate fake letters without a single mistake.

*The multi-layered protection method***.** No single tool can guarantee complete security. For this reason, the principle of "defence in depth" is applied in practice: even if an attacker overcomes one layer, the next layer stops them. The multi-layered protection method proposed in this article is shown in Figure 1. At its centre lies the most valuable asset - data, which is protected by encryption and backup copies. The outer layer consists of organisational policies and users' awareness.

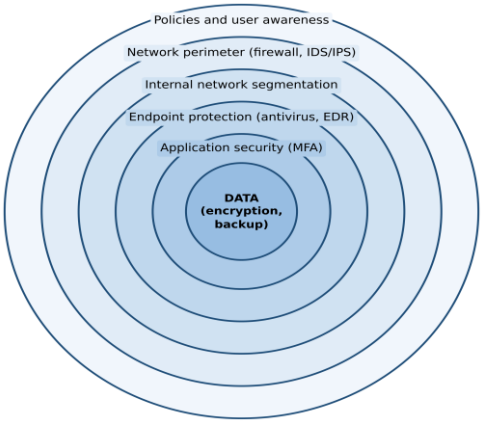


Figure 1. The multi-layered (defence-in-depth) protection method

Responding to cyber incidents. In any system, the possibility of an incident always remains. Therefore, a response procedure developed in advance minimises the damage. A six-stage cycle based on NIST recommendations is shown in Figure 2 [5]. The conclusions drawn at the last stage are fed back into the preparation stage, so that the protection system is continuously improved.

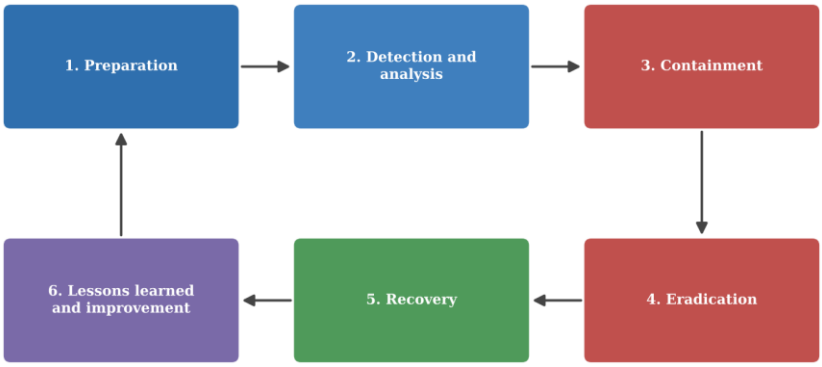


Figure 2. The cyber incident response cycle

Practical recommendations for users. Cybersecurity is the responsibility not only of specialists but of every user. The main recommendations for different categories of users are summarised in Table 2.

Table 2

Practical recommendations by user category

User category	Recommended measures
Pupils and young people	Use strong and separate passwords for each service; do not disclose personal information on social networks; do not open unfamiliar links
Parents and teachers	Monitor children's online activity; use parental control tools; include digital safety topics in lessons
Organisations	Introduce a security policy; train staff regularly; prepare backups and an incident response plan
All users	Enable multi-factor authentication; update the operating system and applications on time; never share SMS codes or card details with anyone

Conclusion

The analysis presented in this article shows that modern cyber threats are becoming increasingly complex and actively exploit the human factor as well as technical weaknesses. New technologies such as artificial intelligence and the Internet of Things expand the possibilities for protection, but they also create new risks. In these conditions, effective protection can be achieved by applying the multi-layered protection method, by preparing an incident response procedure in advance and, most importantly, by improving the digital literacy of users, especially young people. Teaching the basics of cybersecurity in school education is an important condition for building a safe digital society in the future.

References

1. Law of the Republic of Uzbekistan "On Cybersecurity". No. O'RQ-764, 15 April 2022.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
3. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. - Pearson, 2020.
4. ENISA Threat Landscape 2024. - European Union Agency for Cybersecurity, 2024.
5. NIST. The NIST Cybersecurity Framework (CSF) 2.0. - National Institute of Standards and Technology, 2024.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: APPROACHES, CHALLENGES, AND FUTURE DIRECTIONS

Barotova Z.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Abduvoxidov D.
Prosecutor General's Office of the Republic of Uzbekistan.

Annotatsiya. Sun'iy intellektning kiberxavfsizlikka integratsiyasi an'anaviy mudofaa mexanizmlarini o'zgartirdi, bu esa kibertahdidlarni aqlli aniqlash, tasniflash va ularga javob berish imkonini berdi. Sun'iy intellektga asoslangan tizimlar katta hajmdagi tarmoq ma'lumotlarini tahlil qilish, anomaliyalarni aniqlash va potensial hujumlarni ajoyib tezlik va aniqlik bilan bashorat qilish uchun ilg'or mashinali o'qitish, chuqur o'qitish va mustahkamlovchi o'qitish texnikalaridan foydalanadi. Biroq, o'sib borayotgan samaradorligiga qaramay, kiberxavfsizlikda AI bir qator dolzarb muammolarga duch keladi, jumladan, ma'lumotlar nomutanosibligi, qarama-qarshi manipulyatsiya, talqin qilinmaslik va maxfiylikni saqlovchi o'qitish tizimlariga ehtiyoj. Bundan tashqari, axloqiy boshqaruv, shaffoflik va model ishonchliligi bilan bog'liq muammolar AI asosidagi yechimlarni keng ko'lamda joylashtirishga to'sqinlik qilmoqda. Ushbu tadqiqot ushbu muammolarni chuqur o'qitishni ta'minlaydi, shu bilan birga ularni hal qilishda Explainable AI (XAI), Federatsiyalangan o'qitish (FL) va gibrid intellekt yondashuvlarining muhim rolini ta'kidlaydi. Tahlil shuningdek, AIga asoslangan kiberxavfsizlikning kelajagi paydo bo'layotgan tahdidlar bilan mustaqil ravishda rivojlanishi mumkin bo'lgan moslashuvchan, shaffof va ishonchli modellarni ishlab chiqishga bog'liqligini ta'kidlaydi.

Kalit so'zlar: Sun'iy intellekt, Mashinali o'qitish, Kiberxavfsizlik, Explainable AI (XAI), Avtonom mudofaa tizimlari.

Аннотация. Внедрение искусственного интеллекта (ИИ) в сферу кибербезопасности трансформировало традиционные механизмы защиты, обеспечив возможность интеллектуального обнаружения и классификации киберугроз, а также реагирования на них. Системы на базе ИИ используют передовые методы машинного обучения, глубокого обучения и обучения с подкреплением для анализа огромных объемов сетевых данных, выявления аномалий и прогнозирования потенциальных атак с высокой скоростью и точностью. Однако, несмотря на растущую эффективность, применение ИИ в кибербезопасности сопряжено с рядом серьезных проблем, включая дисбаланс данных, уязвимость к состязательным атакам (манипуляциям), недостаточную интерпретируемость моделей и потребность в методах обучения, обеспечивающих конфиденциальность данных. Кроме того, вопросы этического регулирования, прозрачности и надежности моделей по-прежнему сдерживают масштабное внедрение решений на основе ИИ. В данном исследовании проводится углубленный анализ этих проблем и подчеркивается ключевая роль таких подходов, как объяснимый искусственный интеллект (XAI), федеративное обучение (FL) и гибридный интеллект, в их решении. Также отмечается, что будущее кибербезопасности с использованием ИИ зависит от разработки адаптивных, прозрачных и надежных моделей, способных автономно эволюционировать по мере появления новых угроз.

Ключевые слова: искусственный интеллект, машинное обучение, кибербезопасность, объяснимый искусственный интеллект (XAI), автономные системы защиты.

Introduction

The development of technology and the Internet has had an impact on many areas. In today's digital world, cybersecurity is not only a problem for governments and financial systems, but also for the core infrastructure of many industries, such as personal privacy and business continuity. The increasing complexity and scale of cyber threats have made it difficult to work with security mechanisms for IoT systems and cloud systems. As it has become increasingly difficult to predict and detect these threats using signature-based and static methods, the cybersecurity industry has begun to use Artificial Intelligence and Machine Learning as an important tool to enhance cyber defense capabilities.

AI and ML technologies offer dynamic and adaptive solutions for detecting, classifying, and responding to threats. Unlike traditional methods, AI and ML systems have the ability to learn from a constantly evolving data set to recognize new attack patterns and anomalies. From real-time threat detection and behavior analysis to automating incident response and increasing threat intelligence, AI and ML have transformed cybersecurity operations into more resilient intelligent systems. Modern cybersecurity demands speed and accuracy in detecting attacks. AI and ML algorithms excel in these areas by leveraging the power of big data to analyze massive amounts of information from network traffic, system logs, and external threat feeds in real time. One of the most significant advantages of AI/ML-based systems is their ability to detect previously unknown threats (zero-day attacks) through anomaly detection and pattern recognition. By continuously learning from new data, these models evolve to recognize even the most sophisticated attack vectors, offering a layer of defense that static, signature-based systems cannot achieve.

This article reviews the role, achievements, challenges, limitations and future directions of AI and ML in cybersecurity.

Main part

Artificial Intelligence has emerged as a cornerstone of modern cybersecurity efforts, offering a transformative approach to detecting, responding to, and mitigating threats. AI’s role in cybersecurity revolves around three key pillars:threa tdetection, automation, and intelligent decision-making. AI plays a central role in intelligent decision-making, empowering cybersecurity systems to act more autonomously and proactively. Through techniques such as predictive analytics, AI can forecast potential threats and vulnerabilities before they materialize, allowing organizations to take preemptive actions to safeguard their networks. This capability is crucial in today’s threat landscape, where attackers often employ advanced tactics and deception techniques to bypass traditional defenses [1]. AI’s role in cybersecurity is not limited to reactive measures. It also contributes to proactive defense strategies, such as threat hunting and forensic analysis, where AI systems can comb through vast amounts of historical data to identify emerging threats or trace the origins of an attack [2].

Table 1

The role of AI in cybersecurity [3]

Consepts	Definition
Reducing False Positives	AI has capability to decrease the occurrence of incorrect identification in security. Conventional security systems frequently provide erroneous

	alerts, resulting in a state of exhaustion from excessive warnings and the possibility of disregarding genuine dangers.
Behavioral Analytics	AI demonstrates exceptional profiency in behavioral analytics, which compasses the examination of user behavior patterns and network activity. AI sytems can identify security threats by comparing current activity to a standard baseline and detecting any abnormal security procedure may overlook.
Threat Detection	AI facilitates the implementation of advanced and resize thread detection. ML algorithms have the capabilities to examine large data sets and detect trends, abnormalities and potential threats in real time.
Automated Incident Response	AI enabes the streamlining of incident response procedures. AI posses the capacity to acquire knowledge from past data and adjust their response based on new information, enabling them to promptly and efficiently address required to discover, contain and resolve a security breach.

Machine Learning (ML) is one of the most influential technologies in modern cybersecurity. ML algorithms enable systems to automatically learn from data without being explicitly programmed, making them highly effective in dynamic and complex environments like cybersecurity [4]. ML techniques are broadly categorized into three paradigms: supervised learning, unsupervised learning, and reinforcement learning. Each paradigm has unique applications and advantages in the context of cybersecurity.

Supervised learning in IDS relies on labeled datasets that contain pre-classified examples of both benign and malicious network traffic. This method employs classification algorithms such as decision trees, support vector machines (SVM), random forest, and deep neural networks (DNNs) to learn attack patterns from historical data and make predictions on new traffic [5].

Unlike supervised learning, unsupervised learning does not require labeled datasets. Instead, it analyzes patterns and structures in network traffic, allowing IDS/IPS to detect previously unseen attacks and anomalies. This approach is particularly effective for identifying zero-day exploits, advanced persistent threats (APTs), and insider threats, which may not follow known attack patterns.

Challenges in ai-driven cybersecurity

Despite the remarkable progress in Artificial Intelligence (AI) based cybersecurity, several technical, ethical, and operational challenges still hinder its large-scale deployment. These challenges arise from the dynamic nature of cyber threats, the limitations of AI algorithms, and the scarcity of high-quality data. The key challenges are discussed below.

Data quality, Imbalance and Availability. AI models are heavily data-dependent; their performance largely relies on the quality, diversity, and representativeness of training datasets. However, in cybersecurity, acquiring comprehensive and labeled data remains one of the most significant obstacles. Most available datasets, such as NSL-KDD**,** CICIDS2017**,** and UNSW-NB15**,** contain outdated attack signatures or synthetic traffic, which fail to capture the complexity of real-world scenarios [6].

Adversial attacks on AI models. AI models, particularly deep learning architectures, are themselves vulnerable to **adversarial attacks**. These attacks involve subtle perturbations or manipulations of input data that can deceive the model into making incorrect predictions. For example, an attacker could slightly modify network traffic features to evade detection by an IDS.

Such vulnerabilities can be catastrophic in cybersecurity environments, where even a single misclassification may lead to a successful breach.

Lack of Explainability and Transparency. One of the major limitations of AI-based cybersecurity systems is their "black-box" nature. Deep neural networks can achieve high accuracy, yet their decision-making process is often opaque to human analysts. This lack of explainability raises concerns regarding accountability and trust, especially in critical infrastructures such as banking, healthcare, or defense systems.

Real-time detection and computational complexity. Cyber attacks often unfold within milliseconds, necessitating real-time detection and response capabilities. However, most deep learning models are computationally intensive, requiring significant processing power, memory, and latency that may not be feasible for real-time operation in large-scale network environments.

Privacy security and ethical concerns. AI-based systems often require large volumes of user and network data for model training. This raises privacy and ethical concerns, as sensitive information might be exposed or misused during data collection, labeling, or model sharing processes. Furthermore, model inversion attacks can potentially reconstruct private information from trained models, leading to secondary privacy violations.

Integrating and deployment challenges. Integrating AI into existing cybersecurity infrastructures is non-trivial. Many organizations rely on legacy security systems that are incompatible with modern AI-driven frameworks. Moreover, deploying AI in critical systems demands extensive validation, continuous monitoring, and adaptive retraining to cope with concept drift the evolution of attack patterns over time. Without these measures, the performance of AI models can degrade rapidly, leading to undetected intrusions or false alarms.

Table 2

Challenges' description and mitigation

Challenge	Description	Mitigation
Data Imbalance	Rare attacks underrepresented in datasets	Synthetic data generation, resampling, federated learning
Adversarial Vulnerability	Manipulated inputs mislead models	Adversarial training, robust optimization
Lack of Explainability	Difficult to interpret decisions	Explainable AI (LIME, SHAP)
Real-Time Limitations	High latency and computational cost	Edge AI, lightweight models
Privacy Concerns	Risk of data leakage	Differential privacy, federated learning
Integration Issues	Compatibility with legacy systems	Continuous retraining, hybrid frameworks

Conclusion and future directions

Artificial intelligence has revolutionized the cybersecurity landscape by enhancing the capability to detect, classify, and mitigate complex cyber threats in real time. Through advanced models such as deep learning, reinforcement learning, and generative AI, the field has witnessed substantial progress in intrusion detection, malware classification, and behavioral analysis. However, despite these achievements, significant challenges remain in terms of data quality, model interpretability, adversarial robustness, and ethical governance. Addressing these limitations is essential to ensure the trustworthiness and long-term sustainability of AI-driven defense mechanisms.

Looking ahead, the future of FSIEM cybersecurity will be defined by the integration of multiple advanced paradigms. First, Generative AI and Large Language Models (LLMs) will play an increasing role in automated threat analysis, intelligent reporting, and autonomous decision-making within security operations centers. Meanwhile, Explainable and Trustworthy AI (XAI-T) will be central to building transparent systems that allow human analysts to understand and verify model reasoning. The adoption of Federated Learning and Privacy-Preserving AI will further ensure secure collaboration across distributed environments without exposing sensitive data.

In conclusion, the next decade will witness a convergence of AI, quantum computing, and ethical governance, forming an ecosystem of intelligent, transparent, and autonomous cybersecurity solutions. Continuous innovation, coupled with strong regulatory and ethical oversight, will be the cornerstone for ensuring a secure digital future.

References

1. Kumar S, Gupta U, Singh AK, Singh AK (2023) Artificial intelligence: revolutionizing cyber security in the digital era. J Comput Mech Manag 2(3):31–42.

2. Prasad R, Rohokale V, Prasad R, Rohokale V(2020) Artificial intelligence and machine learning in cyber security. Cyber security: the lifeline of information and communication technology. Springer, Cham, pp 231–247.

3. Hossain, R. (2024). Adopting Industry 4.0: A Strategic Solution for Transforming Smart Bangladesh: Prospective Connections, Opportunities, and Challenges. Pakistan Journal of Life and Social Sciences.

4. Ozkan-Ozay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, Beloev I (2024) A comprehensive sur vey: evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEE Access 12:12229.

5. Lysenko S, Bobro N, Korsunova K, Vasylchyshyn O, Tatarchenko Y (2024) The role of artificial intelli gence in cybersecurity: automation of protection and detection of threats. Econ Aff 69:43–51.

6. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, 2016.

AI-NATIVE CYBERSECURITY COVERAGE GAPS IN INDUSTRIAL AI SYSTEMS: A REPRODUCIBLE CROSSWALK OF MITRE ATLAS AND ATT&CK FOR ICS

Shanning Fu, Bekmuratov D.K.
National Research University "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers"

Annotatsiya. Sanoat sun'iy intellektidagi ayrim hujum usullari ICS xavfsizlik bilim bazalarida faqat qisman ifodalanadi. MITRE ATLAS v2026.09 va ATT&CK for ICS v19.2 ning 181 × 89 (16 109) quyi darajadagi texnika juftligi taqqoslandi. TF-IDF, MiniLM va BGE nomzodlarni aniqladi; muvofiqlik mexanizm va bevosita nishon dalillari bilan baholandi. Dastlabki protokol 23 ta yaqin analog, 148 ta qisman moslik va 10 ta ehtimoliy bo‘shliqni ko‘rsatdi. Bir mustaqil ekspert dastlabki tasnif yorliqlarini ko‘rmasdan 551 ta juftlikni baholab, o‘nta bo‘shliqni saqlab qoldi (214 ta juftlik), ammo faqat yettita yaqin analogni qat'iy tasdiqladi. Bu natija semantik yaqinlik hujum mexanizmlari ekvivalentligini anglatmasligini ko‘rsatadi; ekspert tahlili maqsadli sezgirlik tekshiruvidir.

Kalit so‘zlar: sanoat SI kiberxavfsizligi; MITRE ATLAS; ATT&CK for ICS; freymvorklararo moslik; ekspert bahosi.

Аннотация. Некоторые атаки на промышленный искусственный интеллект лишь частично отражены в базах знаний по безопасности ICS. Мы сопоставили 181 × 89 (16 109) пар конечных техник MITRE ATLAS v2026.09 и ATT&CK for ICS v19.2. TF-IDF, MiniLM и BGE находили кандидатов, а соответствие определялось отдельно по механизмам и непосредственным целям. Исходный протокол выделил 23 близких аналога, 148 частичных соответствий и 10 предполагаемых пробелов. Один независимый эксперт оценил 551 пару без доступа к исходным меткам: все десять пробелов сохранились (214 пар), но строгая эквивалентность подтвердилась только для семи близких аналогов. Семантическая близость не равнозначна эквивалентности действий; экспертные результаты представляют собой целевой анализ чувствительности.

Ключевые слова: кибербезопасность промышленного ИИ; MITRE ATLAS; ATT&CK for ICS; сопоставление фреймворков; экспертная оценка.

Introduction

Industrial AI extends operational technology with models, training data, prompts and agent-operated tools, adding attack mechanisms that traditional industrial security taxonomies may not distinguish [3,4]. MITRE ATLAS records adversarial-AI techniques [1], while ATT&CK for ICS describes attacks in industrial environments [2]. Prior work has analyzed ATLAS/ICS gaps, industrial adversarial-AI threats and the representation of cyber-physical attacks [5-9]; semantic approaches already support security knowledge-base mapping [10].

However, similar descriptions need not imply equivalent adversary actions. We ask: (RQ1) which ATLAS techniques have close ICS analogues; (RQ2) which have only partial correspondence or candidate gaps; and (RQ3) how these patterns vary across overlapping Predictive, Generative and Agentic AI labels. Our contribution is a fixed-version, hierarchy-aware protocol that separates candidate retrieval from mechanism-level coverage adjudication, with targeted expert sensitivity testing.

Materials and Methods

Using a 2 October 2026 cutoff, we froze ATLAS v2026.09 and ATT&CK for ICS v19.2 [1,2]. The leaf rule retained sub-techniques and standalone techniques without children, yielding 181 ATLAS and 89 ICS units (16,109 pairs). Only official names and descriptions were embedded. Structural attributes remained separate; 69 ATLAS strings nevertheless retained residual internal Markdown link syntax, which may affect ranking. The original inputs and scores were not silently changed.

We ranked each ATLAS unit against all ICS units using TF-IDF (unigrams/bigrams) and two unfine-tuned, L2-normalized encoders: all-MiniLM-L6-v2 (mean pooling) and bge-base-en-v1.5 (CLS pooling) [11-14]. For MiniLM and BGE, Top-3 overlap defined strong consensus; overlap only in Top-10 defined moderate consensus; and no Top-10 overlap defined isolation. No absolute cosine threshold was used. Eight exact-name anchors checked retrieval. A frozen 3,643-pair audit queue covered P0=8, P1=255, P2=733, P3=378 and P4=2,269 selected candidates.

Mechanism and immediate target correspondence were assessed separately in the model-assisted audit and assigned yes/partial/no/unclear labels; tactic and asset metadata supplied contextual evidence. An ATLAS node was Close when at least one pair had mechanism=yes and target=yes; Partial when a material mechanism relation remained but no pair met that strict rule; Candidate Gap when all audited mechanisms were no; otherwise Unresolved. Model-assisted reapplication checked rule reproducibility, not human inter-rater reliability.

One independent domain expert reviewed 268 label-blinded pairs (214 gap candidates, 24 decisive close pairs and 30 sampled partial pairs). A second round examined 283 other pairs for 16 challenged close nodes, giving 551 unique judgments. The follow-up did not reveal previous labels or scores but did disclose why the nodes were selected. The original 148 Partial nodes were not exhaustively expert-reviewed; the expert-derived distribution is therefore a targeted sensitivity result, not a new gold standard.

Results

All retrieval methods found the eight exact-name anchors within Top-10; Recall@1 was 0.875 for TF-IDF, 0.750 for MiniLM and 1.000 for BGE. MiniLM and BGE agreed on Top-1 for 77/181 nodes (42.5%), with 158 strong-consensus, 23 moderate-consensus and zero isolation cases. Yet close analogues were rare even under strong consensus (Fig. 1).

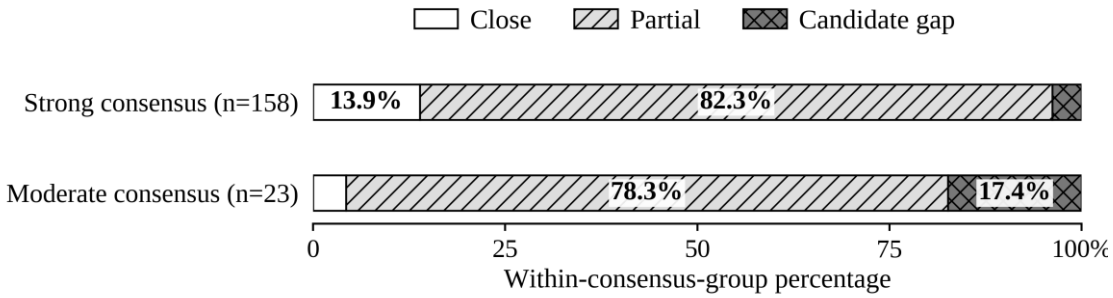


Fig. 1. Retrieval consensus versus protocol class; within-group percentages (Strong: 22 Close/130 Partial/6 Gap; Moderate: 1/18/4).

The frozen protocol yielded 23 Close, 148 Partial and 10 Candidate Gap cases (Table 1). In 551 selected comparisons, expert agreement with the model-assisted labels was 84.4% for mechanism (κ=0.517) and 49.9% for target (κ=0.126). All 214 audited pairs across the ten candidate-gap nodes were judged mechanism=no. Among 23 protocol Close nodes, only seven retained an expert yes/yes pair; the other 16 became Partial after the expert examined all their

remaining candidates. The expert sensitivity distribution is thus 7 Close/164 Partial/10 Gap/0 Unresolved.

Table 1

Frozen-protocol classes and targeted expert sensitivity (N=181).

Basis	Close	Partial	Candidate gap	Unresolved
Protocol	23 (12.7%)	148 (81.8%)	10 (5.5%)	0
Expert-1 sensitivity	7 (3.9%)	164 (90.6%)	10 (5.5%)	0

Across the overlapping ATLAS platform labels, the Close/Partial/Candidate Gap counts were 6/55/7 for Predictive AI (N=68), 6/75/7 for Generative AI (N=88), and 7/104/7 for Agentic AI (N=118). These are descriptive within-platform counts, not independent-group comparisons.

The ten audited Candidate AI-Native Coverage Gaps were Train Proxy via Gathered AI Artifacts, Train Proxy via Replication, Use Pre-Trained Model, Consumer Hardware, Domains, Adversarial AI Attack Implementations, Generative AI, Adversarial AI Attacks, Reputational Harm, and Autonomous Attack-Path Adaptation. These are candidate knowledge-representation gaps, not confirmed vulnerabilities or measured failures of operational defenses.

Discussion and Limitations

The main finding is retrieval–coverage non-equivalence: semantic models consistently find related descriptions, but a close analogue requires matching adversary mechanisms and immediate targets. Expert review makes the boundary visible: 16 of 23 protocol Close nodes moved to Partial, whereas all ten candidate gaps remained stable within the audited pool. This favors graded knowledge-base cross-references over automatic binary matches and clarifies that knowledge representation coverage is not the same as deployed defensive coverage.

The inference remains version- and audit-pool-specific. Although all 16,109 pairs were scored, only 3,643 selected pairs received mechanism audit. Residual Markdown markup in 69 ATLAS strings may influence retrieval. One expert assessed targeted high-consequence cases; neither all original Partial nodes nor all 16,109 possible pairs received independent mechanism judgments. No attack exploitability or mitigation effectiveness was tested.

Conclusion

A version-pinned ATLAS–ICS crosswalk separated lexical/neural retrieval from behavioral adjudication and found Partial Coverage to be the dominant relationship. The frozen protocol yielded 23/148/10/0, while targeted expert sensitivity gave 7/164/10/0; all ten candidate gaps remained stable among audited candidates. This provides a reproducible baseline for studying how AI-specific threat knowledge is represented as both frameworks evolve.

Data availability. The frozen 16,109-pair scores, 3,643-pair audit, code, and expert-validation records are retained in the versioned project archive and are available from the corresponding author on reasonable request.

References

1. MITRE ATLAS, “ATLAS Data Release v2026.09,” 2026. https://github.com/mitre-atlas/atlas-data/releases.

2. MITRE ATT&CK, “ICS ATT&CK v19.2” (STIX data, released 5 Aug. 2026). https://github.com/mitre-attack/attack-stix-data/blob/master/ics-attack/ics-attack-19.2.json.

3. B. Strom et al., “MITRE ATT&CK: Design and Philosophy,” MITRE, 2020.

4. K.-K. Kim et al., “Cybersecurity Opportunities and Risks of Artificial Intelligence in Industrial Control Systems: A Survey,” Computer Modeling in Engineering & Sciences, 146(2), 5, 2026, doi:10.32604/cmes.2026.077315.

5. S. A. Rana, “Adversarial Artificial Intelligence in Industrial Control Systems: A Consequence-Oriented Gap Analysis of MITRE ATLAS,” SSRN, 2026, doi:10.2139/ssrn.6055035 [preprint].

6. S. A. Rana, “Beyond MITRE ATLAS: Defining Adversarial AI Techniques for Industrial Control Systems,” SSRN, 2026, doi:10.2139/ssrn.6810543 [preprint].

7. M. A. Khan, “Adversarial AI in ICS/OT: The Next Cyber Threat to Critical Infrastructure,” SSRN, 2026, doi:10.2139/ssrn.6741039 [preprint].

8. M. Mc Cabe and S. H. Houmb, “Enhancing the MITRE ATT&CK Framework for Cyber-Physical Systems Using Insights from Advanced Persistent Threats,” Applied Sciences, 16(4), 1815, 2026, doi:10.3390/app16041815.

9. N. Sachpelidis-Brozos et al., “Hacking intelligence: Mapping the anatomy of adversarial threats in artificial intelligence with MITRE ATLAS,” Computer Science Review, 61, 100923, 2026, doi:10.1016/j.cosrev.2026.100923.

10. H. Lee et al., “Enhancing RMF and ATT&CK Mapping Accuracy Through Integration of Sentence-BERT and Mitigation Parameters,” Electronics, 15(6), 1248, 2026, doi:10.3390/electronics15061248.

11. N. Reimers and I. Gurevych, “Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks,” EMNLP-IJCNLP, 2019, doi:10.18653/v1/D19-1410.

12. W. Wang et al., “MiniLM: Deep Self-Attention Distillation for Task-Agnostic Compression of Pre-Trained Transformers,” NeurIPS 33, 2020.

13. Sentence Transformers, “all-MiniLM-L6-v2: Model Card.” https://huggingface.co/sentence-transformers/all-MiniLM-L6-v2.

14. BAAI, “bge-base-en-v1.5: Model Card.” https://huggingface.co/BAAI/bge-base-en-v1.5.

ZARARLI DASTURIY TA’MINOTNI MASHINALI O‘QITISH USULLARI ASOSIDA ANIQLASHNING ZAMONAVIY MUAMMOLARI

Fayziyeva D.S., Yakubova D.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Mazkur maqolada zararli dasturiy ta’minotni mashinali o‘qitish usullari asosida aniqlash tizimlarining ishonchliligiga ta’sir etuvchi dolzarb muammolar tahlil qilingan: ma’lumotlarni vaqt mezoni asosida noto‘g‘ri ajratish, sinflar nisbatining real muhitga mos kelmasligi, ma’lumotlarning sizib o‘tishi, model samaradorligining pasayishi, raqib hujumlari, yorliqlarning beqarorligi va bashoratlarni izohlash imkoniyatlarining cheklanganligi. Ushbu muammolarni bartaraf etish uchun vaqtga asoslangan baholash, past yolg‘on musbat qarorlar darajasida aniqlash samaradorligini o‘lchash, yorliqlar ishonchliligini tekshirish va modellarni nazorat ostida qayta o‘qitishni birlashtiruvchi tajriba protokoli taklif etilgan.

Kalit so‘zlar: zararli dasturiy ta’minot, mashinali o‘qitish, vaqtga asoslangan baholash, ma’lumotlarning sizib o‘tishi, konsepsiya siljishi, raqib hujumlari, yorliqlar sifati, tushuntiriluvchanlik.

Аннотация. В статье проанализированы актуальные проблемы, влияющие на надёжность систем обнаружения вредоносного программного обеспечения на основе машинного обучения: некорректное временное разделение данных, несоответствие распределения классов реальным условиям, утечка данных, снижение эффективности моделей со временем, состязательные атаки, нестабильность меток и ограниченная интерпретируемость прогнозов. Предложен экспериментальный протокол, объединяющий временное разделение данных, оценку полноты обнаружения при низком уровне ложноположительных решений, проверку достоверности меток и контролируемое переобучение моделей.

Ключевые слова: вредоносное программное обеспечение, машинное обучение, временная оценка, утечка данных, дрейф концепции, состязательные атаки, качество меток, интерпретируемость.

Kirish

Zararli fayllar hajmining ortishi avtomatlashtirilgan aniqlash tizimlarining ahamiyatini oshirmoqda. Kaspersky ma’lumotlariga ko‘ra, 2025-yilda uning aniqlash tizimlari kuniga o‘rtacha 500 mingta zararli faylni qayd etgan, bu avvalgi davrga nisbatan 7 foizga yuqori (2024-yil noyabridan 2025-yil oktabrigacha). Statistika Kaspersky Security Network kuzatuvlariga asoslangan bo‘lib, uni dunyodagi barcha zararli dasturlar, noyob oilalar yoki O‘zbekistonda qayd etilgan kiberhodisalar soni sifatida talqin qilish to‘g‘ri emas [1].

O‘zbekistonda kiberxavfsizlik sohasini tartibga soluvchi asosiy hujjatlardan biri 2022-yil 15-aprelda qabul qilingan O‘RQ-764-sonli «Kiberxavfsizlik to‘g‘risida»gi Qonun bo‘lib, unda kibertahdid, kiberhujum va kiberhimoya tushunchalari hamda tegishli huquqiy munosabatlar asoslari belgilangan [2].

Mashinali o‘qitish usullari zararli dasturlarni avtomatik tasniflash imkonini kengaytiradi, biroq laboratoriyadagi yuqori natija real muhitdagi ishonchlilikni kafolatlamaydi: tafovut ma’lumotlar, baholash metodologiyasi, yorliqlar sifati va hujumchilarning qarshi choralaridan kelib chiqishi mumkin.

Shu munosabat bilan maqolaning asosiy tadqiqot masalasi mashinali o‘qitish modelining yuqori test ko‘rsatkichlari qaysi sharoitlarda uning amaliy ishonchliligini yetarli darajada aks ettirmasligini aniqlashdan iborat.

Asosiy qism

Anderson va Roth tomonidan ishlab chiqilgan EMBER ma’lumotlar to‘plami Windows Portable Executable (PE) fayllaridan ajratilgan statik xususiyatlarni o‘z ichiga olib, jami 1,1 millionta namunadan iborat: o‘qitish qismida 900 mingta namuna (300 mingta zararli, 300 mingta zararsiz va 300 mingta yorliqlanmagan), test qismida 200 mingta namuna (100 mingtadan zararli va zararsiz) mavjud. Demak, o‘qitish to‘plamidagi barcha namunalar yorliqlangan emas [3].

Arp va hammualliflari kompyuter xavfsizligida mashinali o‘qitishdan foydalanishdagi o‘nta tipik metodologik xatoni tizimlashtirgan. Ma’lumotlar to‘plamining noto‘g‘ri shakllantirilishi, yorliqlar sifatining pastligi, o‘qitish va test ma’lumotlari o‘rtasida axborot sizib o‘tishi hamda soxta korrelyatsiyalar model samaradorligini asossiz yuqori baholashga olib kelishi mumkinligi ko‘rsatilgan [4].

TESSERACT tadqiqotida zararli dasturlarni tasniflashga ta’sir etuvchi fazoviy va vaqtga oid tarafkashliklar o‘rganilgan: birinchisi o‘qitish va amaliy muhit taqsimotlarining mos kelmasligi, ikkinchisi ma’lumotlarning xronologik noto‘g‘ri tashkil etilishi bilan bog‘liq. Uchta klassifikator taxminan 129 mingta Android ilovasida baholangan; natijalarni Windows PE fayllariga miqdoriy tatbiq etib bo‘lmaydi, biroq vaqt xususiyatlarini hisobga olish tamoyili muhim metodologik asos hisoblanadi [5].

Baholash mezonlari va sinflar nomutanosibligi

Zararli dasturlarni aniqlash modellarini faqat umumiy to‘g‘ri tasniflash ulushi (*Accuracy*) asosida baholash yetarli emas. Modelning samaradorligini har tomonlama aniqlash uchun bir nechta baholash mezonlaridan kompleks foydalanish zarur [5].

Asosiy mezonlar quyidagi formulalar orqali ifodalanadi:

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = TPR = \frac{TP}{TP+FN} \quad (2)$$

$$FPR = \frac{FP}{FP+TN} \quad (3)$$

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \quad (4)$$

Bu yerda:

- TP (True Positive) - zararli deb to‘g‘ri tasniflangan namunalar soni;
- FP (False Positive) - zararsiz bo‘lishiga qaramay, zararli deb tasniflangan namunalar soni;
- TN (True Negative) - zararsiz deb to‘g‘ri tasniflangan namunalar soni;
- FN (False Negative) - zararli bo‘lishiga qaramay, zararsiz deb tasniflangan namunalar soni.

Sinflar nomutanosibligining ta’sirini shartli misolda ko‘rish mumkin. Faraz qilaylik, 100 mingta fayldan iborat to‘plamning 1 foizi zararli, modelning TPR ko‘rsatkichi 95 foiz, FPR esa 1 foiz bo‘lsin. Bunda model 1 000 ta zararli fayldan 950 tasini to‘g‘ri aniqlaydi, biroq 99 mingta zararsiz faylning 990 tasini ham zararli deb noto‘g‘ri tasniflaydi. Natijada Precision taxminan 49 foizni tashkil etadi.

Shu sababli Precision, Recall, F1-mezon, PR-AUC va ROC-AUC bilan bir qatorda, oldindan belgilangan past FPR darajasidagi TPR, turli vaqt oraliqlaridagi F1-mezon hamda bitta faylni tahlil qilish vaqti ham qayd etilishi lozim.

Qaror chegarasi validatsiya to‘plamida tanlanishi kerak; barcha holatlar uchun yagona maqbul FPR chegarasi mavjud emas, u fayllar oqimi hajmi, xavfsizlik talablari va tahlilchilar imkoniyatiga bog‘liq.

Ma’lumotlar siljishi va model samaradorligining pasayishi

Jordaney va hammualliflari taklif etgan Transcend yondashuvi o‘qitish davridagi va amaliy foydalanishdagi ma’lumotlarni statistik taqqoslab, model samaradorligi pasayishi ehtimolini aniqlaydi; u Android va Windows zararli dasturlari misolida tekshirilgan [6]. Taqsimotning o‘zgarishi yangi faylning zararli ekanligini isbotlamaydi, balki qo‘shimcha tahlil yoki ekspert tekshiruvini talab qiladi.

Ma’lumotlar taqsimotidagi o‘zgarishlarni to‘g‘ri tavsiflash uchun quyidagi ehtimollik taqsimotlarini farqlash muhim:

- $P(X)$ - belgilar taqsimoti;
- $P(Y)$ - sinflar taqsimoti;
- $P(Y|\ X)$ - belgilar va yorliqlar o‘rtasidagi shartli bog‘liqlik.

Bu taqsimotlarning o‘zgarishi bir xil hodisa emas, shuning uchun barchasini «konsepsiya siljishi» deb atash noto‘g‘ri: bu atama asosan belgilar va yorliqlar o‘rtasidagi shartli bog‘liqlikning o‘zgarishini bildiradi.

Ishonchlilikni saqlash uchun ma’lumotlarni keyingi vaqt davrlari bo‘yicha alohida baholash va qayta o‘qitishni nazorat ostida tashkil etish zarur: yangi yorliqlar tekshirilishi, yangi model esa mustaqil keyingi-davr to‘plamida avvalgi model bilan taqqoslanishi lozim [6]. Tekshirilmagan shubhali fayllarni o‘qitish ma’lumotlariga kiritish modelni zaharlash xavfini ham oshirishi mumkin [7].

Raqib hujumlari va tahdid modelini shakllantirish

NIST 2025-yilda e’lon qilgan hisobotda bashoratlovchi sun’iy intellekt tizimlariga qarshi raqib hujumlari tasniflangan: aniqlashdan qochish (*evasion*), o‘qitish ma’lumotlarini zaharlash (*poisoning*) va maxfiylikka qarshi hujumlar. Ular o‘rganish bosqichi, hujumchining maqsadi, imkoniyatlari va model haqidagi bilim darajasi bo‘yicha farqlanadi. Hisobotda keng qo‘llaniladigan himoya usullari mutlaq xavfsizlikni kafolatlamasligi ta’kidlangan [7].

Demetrio va hammualliflari Windows PE fayllariga funksionallikni saqlovchi o‘zgartirishlar kiritib, statik detektorlardan qochish imkoniyatlarini tadqiq qilgan; *white-box* va *black-box* sharoitlari farqlangan. Natijalarni «kichik o‘zgartirishlar detektorlarni doimo chalg‘itadi» deb umumlashtirib bo‘lmaydi: muvaffaqiyat model, fayl va hujumchi imkoniyatlariga bog‘liq [8].

Shu sababli tajribalardan oldin tahdid modeli (hujumchining bilim darajasi, o‘zgartirish mumkin bo‘lgan fayl qismlari, so‘rovlar soni, funksionallikni tekshirish usuli, muvaffaqiyat mezonlari) belgilanishi lozim. Muvaffaqiyat faqat dastlab to‘g‘ri aniqlangan va funksionalligini saqlagan namunalar doirasida hisoblanadi; sinovlar ruxsat bilan, izolyatsiyalangan laboratoriya muhitida o‘tkaziladi.

Yorliqlar sifati va model bashoratlarining tushuntiriluvchanligi

Zhu va hammualliflari VirusTotal ma’lumotlaridan foydalangan 115 ta ilmiy maqolani tahlil qilgan hamda 14 mingdan ortiq fayl bo‘yicha 65 ta antivirus dvigatelining kundalik

yorliqlarini bir yil kuzatgan. Dvigatellar o‘rtasida kelishmovchiliklar, yorliqlarning vaqt davomida o‘zgarishi va ayrim guruhlar natijalari o‘rtasida kuchli korrelyatsiya aniqlangan [9].

Demak, bir nechta dvigatelning bir xil xulosasi mustaqil dalillar mavjudligini bildirmaydi. Yorliqlarni ovoz berish yoki chegaraviy qiymat bilan birlashtirish barqarorlikni oshirishi mumkin, biroq noto‘g‘ri chegara xatolarga olib kelishi mumkin.

Shu bois har bir namuna uchun yorliq manbasi, tekshirish sanasi va birlashtirish qoidasi qayd etilishi, noaniq namunalar ajratilishi, keyinroq olingan xulosalar esa avvalgi davr uchun ishlatilmasligi zarur [4].

Model bashoratlarini tushuntirish uchun SHAP usulidan foydalanish mumkin; u alohida belgilarning hissasini baholaydi [10]. Biroq SHAP izohi faylning zararli ekanligini isbotlamaydi va sababiy bog‘liqlikni tasdiqlamaydi, shu sababli u ekspert tekshiruvini qo‘llab-quvvatlovchi yordamchi vosita sifatida ishlatilishi kerak.

Taklif etilayotgan baholash protokoli

Birinchi bosqich - tadqiqot vazifasi va qo‘llanish doirasini belgilash. Tadqiqot obyekti va aniqlash vazifasi aniq belgilanadi: masalan, Windows PE fayllarini ikkilik tasniflash Android ilovalarini tahlil qilish yoki zararli dastur oilalarini tasniflashdan alohida ko‘riladi.

Ikkinchi bosqich - ma’lumotlarning kelib chiqishini hujjatlashtirish. Har bir to‘plamning manbasi, kuzatuv va yorliqlash sanasi, platforma turi va sinflar nisbati qayd etiladi.

Uchinchi bosqich - takroriy va o‘xshash namunalarni aniqlash. Xeshlar yordamida bir xil namunalar aniqlanadi, o‘xshash fayllar tekshiriladi va ularni qismlarga ajratish qoidalari belgilanadi.

To‘rtinchi bosqich - ma’lumotlarni vaqt bo‘yicha ajratish. O‘qitish, validatsiya va test to‘plamlari xronologik tartibda shakllantiriladi; belgilarni tanlash, parametrlarni moslash va qaror chegarasini belgilash faqat o‘qitish hamda validatsiya ma’lumotlari asosida amalga oshiriladi.

Beshinchi bosqich - modellarni bir xil sharoitlarda taqqoslash. Bazaviy va taklif etilayotgan modellar bir xil ma’lumotlar, belgilar, yorliqlar va hisoblash sharoitlarida xolis taqqoslanadi.

Oltinchi bosqich - samaradorlik va resurs sarfini baholash. Precision, Recall, F1-mezon, PR-AUC, ROC-AUC, past FPR sharoitidagi TPR, tahlil vaqti va resurs sarfi, shuningdek keyingi vaqt davrlaridagi natijalar alohida qayd etiladi.

Yettinchi bosqich - raqib hujumlariga chidamlilikni tekshirish. Oldindan belgilangan tahdid modeli asosida funksionallikni saqlovchi raqib o‘zgartirishlariga qarshi sinovlar o‘tkaziladi, natijalar sharoitlari va cheklovlari bilan keltiriladi.

Sakkizinchi bosqich - ekspert tekshiruvi va nazoratli qayta o‘qitish. Noto‘g‘ri tasniflangan va noaniq namunalar ekspert tekshiruviga yuboriladi; qayta o‘qitilgan model mustaqil test to‘plamida baholanadi, zarurat tug‘ilsa avvalgi modelga qaytish imkoniyati saqlanadi.

Takrorlanuvchanlik uchun ma’lumotlar versiyasi, kutubxonalar, tasodifiylik urug‘lari, parametrlar va qaror chegarasi ko‘rsatilishi lozim. Mahalliy tashkilotlarda joriy etishdan oldin qonuniy asosda to‘plangan ma’lumotlarda alohida validatsiya zarur; xorijiy to‘plamlardagi natijalar O‘zbekiston sharoiti uchun bevosita baho bo‘lmaydi.

Xulosa

Zararli dasturiy ta’minotni mashinali o‘qitish asosida aniqlash tizimlarining amaliy ishonchliligi nafaqat algoritmga, balki ma’lumotlar sifati, vaqt bo‘yicha ajratish, baholash mezonlari, yorliqlar barqarorligi va hujumchi imkoniyatlariga ham bog‘liq. Yuqori umumiy test ko‘rsatkichi real ishonchlilikni kafolatlamaydi, shu sababli past FPR darajasidagi samaradorlik,

keyingi davr ma’lumotlaridagi sifat va raqib o‘zgartirishlariga chidamlilik alohida baholanishi zarur.

Taklif etilgan protokol bu tekshiruvlarni birlashtiradi; uning amaliy samaradorligi keyingi bosqichda qonuniy asosda shakllantirilgan mahalliy ma’lumotlar to‘plamida bazaviy model bilan taqqoslab baholanishi lozim.

Foydalanilgan adabiyotlar

1. Kaspersky. The Number of the Year: Kaspersky Detected Half a Million Malicious Files Daily in 2025. Rasmiy press-reliz, 2-dekabr 2025-yil.

2. O‘zbekiston Respublikasi. Kiberxavfsizlik to‘g‘risidagi Qonun, 2022-yil 15-aprel, O‘RQ-764-son. LexUZ. URL: https://lex.uz/docs/-5960604

3. Anderson H. S., Roth P. EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. 2018. arXiv:1804.04637. DOI: 10.48550/arXiv.1804.04637.

4. Arp D. et al. Dos and Don’ts of Machine Learning in Computer Security. 31st USENIX Security Symposium, 2022, pp. 3971–3988.

5. Pendlebury F., Pierazzi F., Jordaney R., Kinder J., Cavallaro L. TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time. 28th USENIX Security Symposium, 2019, pp. 729–746.

6. Jordaney R., Sharad K., Dash S. K., Wang Z., Papini D., Nouretdinov I., Cavallaro L. Transcend: Detecting Concept Drift in Malware Classification Models. 26th USENIX Security Symposium, 2017, pp. 625–642.

7. Vassilev A., Oprea A., Fordyce A., Anderson H., Davies X., Hamin M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025, March 2025. DOI: 10.6028/NIST.AI.100-2e2025. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf

8. Demetrio L., Coull S. E., Biggio B., Lagorio G., Armando A., Roli F. Adversarial EXEmples: A Survey and Experimental Evaluation of Practical Attacks on Machine Learning for Windows Malware Detection. ACM Transactions on Privacy and Security, 2021, vol. 24, no. 4, article 27. URL: https://arxiv.org/abs/2008.07125

9. Zhu S., Shi J., Yang L., Qin B., Zhang Z., Song L., Wang G. Measuring and Modeling the Label Dynamics of Online Anti-Malware Engines. 29th USENIX Security Symposium, 2020, pp. 2361–2378. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/zhu

10. Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions. Advances in Neural Information Processing Systems 30, 2017.

SIEM TIZIMLARIDA MASHINALI O‘QITISH ALGORITMLARI: XAVFSIZLIK HODISALARINI ANIQLASH VA BOSHQARISHNI KUCHAYTIRISH

Samarov X.K., **Nizomov A.O.**
Muhammad Al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti

Annotatsiya: Ushbu maqolada kiberxavfsizlik tahdidlarini aniqlash va ularga samarali javob berishda SIEM (xavfsizlik axborotlari va hodisalarini boshqarish) tizimlariga mashinali o‘qitish (Machine Learning, ML) algoritmlarini integratsiya qilish imkoniyatlari o‘rganildi. An’anaviy SIEM tizimlarining mavjud muammolari tahlil qilinib, tizim jurnallari va tarmoq trafigini tahlil qilish orqali anomaliyalarni aniqlash, noma’lum tahdidlarni bashorat qilish hamda noto‘g‘ri ogohlantirishlarni kamaytirish usullari ko‘rib chiqildi. Shuningdek, mashinali o‘qitish yordamida xavfsizlik hodisalarini monitoring qilish va axborot resurslarini himoya qilish samaradorligini oshirishga qaratilgan ba’zi usullar ko‘rib chiqildi.

Kalit so‘zlar: kiberxavfsizlik tahdidlari, mashinali o‘qitish, SIEM, axborot xavfsizligini boshqarish, hodisalarga javob berish, muhim infratuzilma.

Abstract: This article explores the integration of Machine Learning (ML) algorithms into Security Information and Event Management (SIEM) systems to improve cybersecurity threat detection, analysis, and response. As cyber threats become increasingly complex, traditional SIEM systems face challenges in identifying sophisticated attacks and minimizing false positives. The study examines how ML algorithms can analyze system logs, network traffic, and historical security data to detect anomalies, identify previously unknown threats, and enhance real-time monitoring. Furthermore, it discusses the role of predictive analytics and automated incident response in improving the efficiency and adaptability of SIEM systems. The integration of ML technologies offers promising opportunities to strengthen information security, optimize security event management, and provide more effective protection against evolving cyber threats.

Keywords: cyber threats, machine learning, SIEM, information security management, incidentresponse, critical infrastructure.

Kirish

Raqamli texnologiyalarning jadal rivojlanishi kiberxavfsizlik tahdidlarini ham kuchaytirmoqda. Zararli dasturlar, ransomware va uzoq muddatli ilg‘or tahdidlar (APT) tashkilotlarning ma’lumotlari va tizimlariga tobora ko‘proq xavf solmoqda. Bunday sharoitda axborot xavfsizligini faqat himoya devorlari va antivirus dasturlari bilan ta’minlash yetarli emas. Tashkilotlarga xavfsizlik hodisalarini markazlashtirilgan holda yig‘ib, tahlil qiladigan va ularga tezda javob beradigan tizimlar kerak. Shu vazifani bajaradigan vosita SIEM (Security Information and Event Management) tizimi hisoblanadi.

SIEM tizimlari xavfsizlik operatsion markazlarining (SOC) asosiy vositasi bo‘lib, turli manbalardan kelayotgan loglarni yig‘adi, normallashtiradi va korrelyatsiya qiladi. Biroq an’anaviy SIEM yechimlari asosan oldindan yozilgan qoidalar va signaturalarga tayanadi. Bu yondashuv ma’lum hujumlarni aniqlashda samarali bo‘lsa-da, yangi va yashirin tahdidlarni o‘tkazib yuborishi mumkin. Shu bilan birga, qoidalarning ko‘pligi analitiklarga juda ko‘p yolg‘on ogohlantirishlar yetkazadi, natijada muhim signallar shovqin ichida qolib ketadi. Mashinali o‘qitish (ML) algoritmlari bu muammolarga yechim bo‘lishi mumkin, chunki ular avvalgi ma’lumotlardan odatdagi xatti-harakatni o‘rganib, undan chetga chiqishlarni aniqlay oladi. Ushbu maqolada ML

algoritmlarini SIEM tizimiga integratsiya qilish orqali xavfsizlik hodisalarini aniqroq aniqlash va boshqarish imkoniyatlari tahlil qilindi.

Asosiy qism

Avvalo SIEM va mashinali o‘qitishning o‘zaro integratsiyasi va mavjud muammolari tahlil qilinadi, bu qaysi yechimlar allaqachon sinalgani va qanday bo‘shliqlar qolayotganini aniqlashga yordam beradi. Shu asosda avtomatlashtirilgan ogohlantirish tizimi ishlab chiqiladi va u real kiberhujum stsenariylarida sinovdan o‘tkaziladi. Sinov natijalari tizimni takomillashtirish uchun qayta ishlatiladi. Tizim uch manbadan olingan ma’lumotlarga tayanadi. Birinchisi korrelyatsiya qoidalari bo‘lib, ular real vaqtda kelayotgan hodisalarga qarab avtomatik harakatlarni ishga tushiradi va operatorlar tekshirishi kerak bo‘lgan hodisalar sonini kamaytiradi. Ikkinchisi ochiq formatdagi Sigma qoidalari bo‘lib, ular turli turdagi log fayllariga moslashtirilishi mumkin. Uchinchisi hodisalarga javob berish platformasi (IRP) bo‘lib, undan tizim joriy etilgandan keyingi aniqlash holatlari va javob berish vaqtlari to‘planadi. Bu ma’lumotlar tizimning amaliy samaradorligini baholash uchun ishlatiladi. Ma’lumotlar tahlilidan oldin loglar tozalanadi va yagona formatga keltiriladi. Turli manbalardan kelgan yozuvlar standart tuzilmaga o‘tkazilgach, SIEM ularni bir xil tarzda qayta ishlay oladi. Bu bosqich muhim, chunki noto‘g‘ri formatdagi ma’lumot modelning xatolariga olib keladi. Natijalar asosida qoidalar, signaturalar va mashinali o‘qitish modellari yangilanib boradi. Mashinali o‘qitish modeli MITRE ATT&CK namunalari asosida o‘qitiladi. Bu namunalar real hujum texnikalarini tasvirlaydi, shuning uchun model yangi loglarda shunga o‘xshash naqshlarni topishni o‘rganadi. Tizim real vaqt rejimida skanerlaydi va ogohlantirishni darhol beradi, bu esa birinchi darajali (L1) analitiklarning ish yukini sezilarli darajada kamaytiradi. Yakunda tizim javob stsenariylarini tavsiya qiladi va zarur bo‘lganda inson nazoratchisini ogohlantiradi. Shu tariqa avtomatik javob bilan inson qarori o‘rtasida muvozanat saqlanadi. Kiberxavfsizlik jarayoni to‘xtovsiz davom etgani uchun tizimning aniqlash qoidalari va modellari doimiy ravishda yangilanib turishi kerak.

Tizim ishini tushunish uchun avvalo ma’lumot oqimi aniq bo‘lishi kerak. Har bir ogohlantirish xom log yozuvidan boshlanadi, shuning uchun tahlil SIEM ga kirayotgan ma’lumotlarni yig‘ish va normallashtirish bilan boshlanadi. Serverlar, xavfsizlik devorlari va tarmoq qurilmalaridan kelgan yozuvlar turlicha formatda bo‘ladi: birida vaqt Unix ko‘rinishida, boshqasida matn shaklida yoziladi, bir manbada IP manzil maydoni bor, boshqasida esa u yo‘q. Bunday ma’lumot to‘g‘ridan-to‘g‘ri modelga berilsa, algoritm formatdagi farqlarni hujum belgisi deb o‘rganib qolishi mumkin. Shuning uchun har bir yozuv avval umumiy sxemaga keltiriladi: vaqt bir xil birlikda, IP manzil va port alohida maydonlarda, hodisa turi esa standart nomlar bilan belgilanadi.

Normallashtirilgan ma’lumotdan keyin xususiyatlar ajratiladi. Bu bosqichda kategorik maydonlar, masalan hodisa turi yoki protokol, LabelEncoder yordamida raqamli ko‘rinishga o‘tkaziladi. Uzatilgan ma’lumot hajmi, javob vaqti kabi sonli ko‘rsatkichlar esa StandardScaler bilan normallashtiriladi, shunda katta qiymatli maydonlar kichiklarini bosib ketmaydi. Yo‘qolgan qiymatlar to‘ldiriladi yoki yozuv olib tashlanadi. Xususiyatlar soni ham muhim: loglarda o‘nlab maydon bo‘lishi mumkin, ammo ularning hammasi aniqlash uchun foydali emas. Statistik tahlil va korrelyatsiya asosida eng ma’lumotli maydonlar tanlanadi, bu modelni soddalashtiradi va real vaqt rejimida tezroq ishlashini ta’minlaydi.

Tayyorlangan ma’lumot o‘qitish va sinov to‘plamlariga bo‘linadi. Bu yerda muhim tafsilot bor: oddiy tasodifiy bo‘linish ko‘pincha optimistik natija beradi, chunki model kelajakdagi yozuvlarni ham o‘qitish paytida ko‘rgan bo‘ladi. Shu sababli bo‘linish vaqt bo‘yicha amalga

oshiriladi, ya’ni model eski loglarda o‘qitiladi va yangi loglarda sinaladi. Bu real SIEM muhitiga yaqinroq sharoit yaratadi.

1 **Ma’lumotlarni yig‘ish va tahlil qilish**	**2** **Modelni o‘qitish va ishlab chiqish**	**3** **ML ni SIEM tizimiga integratsiya qilish**	**4** **Doimiy monitoring va takomillashtirish**	**5** **Hodisalarga javob berish va tahdidlarni yumshatish**
Log fayllar, tarmoq trafigi va tizim hodisalari kabi manbalardan ma’lumotlar yig‘iladi va ML yordamida tahlil qilinadi. ▶	Tarixiy ma’lumotlar (masalan, MITRE hujum namunalari) asosida ML algoritmlari o‘qitiladi va yangi, noma’lum tahdidlarni aniqlash qobiliyati shakllantiriladi. ▶	O‘qitilgan model SIEM tizimiga integratsiya qilinadi, bu tahdidlarni aniqlash aniqligini oshiradi va real vaqt rejimida naqshlarni tanib olish imkonini beradi. ▶	Tizim doimiy ravishda tarmoq va log ma’lumotlarini kuzatadi, yangi tahdidlarni aniqlaydi va model muntazam ravishda yangilanadi. ▶	Tahdid aniqlangandan so‘ng, tizim ogohlantirish beradi va avtomatlashtirilgan javob choralarini ko‘radi. Zararli resurslar toza holatga keltirilishi va kelajakda takrorlanishining oldi olinadi.

1-rasm. Mashinali o‘qitish algoritmlarini SIEM tizimiga integratsiya qilish va kiberxavfsizlik tahdidlarini aniqlash bosqichlari

Modellar uch guruhga bo‘linadi. Nazorat ostida o‘qitish algoritmlari, jumladan Random Forest, Decision Tree, SVM va AdaBoost, belgilangan hujum va normal yozuvlar asosida o‘rgatiladi. Ular ma’lum hujum turlarini tanish uchun yaxshi, ammo har bir hodisaning javobini oldindan bilish kerak. Nazoratsiz algoritmlar, masalan Isolation Forest va DBSCAN, belgilanmagan ma’lumotda odatdagidan ajralib turadigan yozuvlarni topadi. Ular oldin ko‘rilmagan hujumlarni aniqlashda foydali bo‘lsa-da, har bir chetga chiqish hujum degani emas, shuning uchun ularning ogohlantirishlari ko‘pincha yolg‘on bo‘ladi. Chuqur o‘qitish modellari, jumladan CNN va autoencoder, murakkab naqshlarni topishga qodir, lekin ularning hisoblash xarajati yuqori va real vaqt talabiga mos kelishi uchun optimallashtirish talab qiladi. Tizimda bu uchala guruh bir-birini to‘ldiradi: nazorat ostidagi model ma’lum tahdidlarni tez tasniflaydi, nazoratsiz model esa noma’lum holatlarni belgilaydi.

Modelning ishlash jarayoni ogohlantirish bilan yakunlanadi. Model hodisani xavfli deb topsa, u tahdid turi, manba IP manzili, vaqt va hodisalar soni bilan birga Telegram bot orqali SOC ning birinchi darajali (L1) analitiklariga yuboriladi. Xabarning to‘liq bo‘lishi muhim, chunki analitik faqat “xavf bor” degan signalni olsa, uni tekshirish uchun qo‘shimcha vaqt sarflaydi. Aniq ma’lumot bilan u darhol blokirovka qilish yoki tarmoqni tekshirish qarorini qabul qila oladi.

Tizimning samaradorligi tajribada baholanadi. Modellar bir xil ma’lumot va bir xil bo‘linishda solishtiriladi, natijalar Accuracy, Precision, Recall, F1-score va AUC-ROC ko‘rsatkichlari bilan o‘lchanadi. Biroq asosiy mezon yolg‘on ogohlantirishlar darajasi bo‘lib qoladi, chunki maqsad analitikning vaqtini tejash va haqiqiy hujumlarni o‘tkazib yubormaslikdir. Natijalar tahlil qilinganda qaysi algoritm eng yuqori Precision va F1 ko‘rsatkichini bergani, qaysi model tezroq ishlagani va ularning har biri qanday cheklovlarga ega ekani ko‘rsatiladi.

Tizimni laboratoriya sharoitidan real SOC muhitiga o‘tkazishda amaliy to‘siqlar paydo bo‘ladi. Hujum usullari va tarmoq xatti-harakati vaqt o‘tishi bilan o‘zgaradi, bu esa modelning aniqligini pasaytiradi. Bu holat tushuncha siljishi (concept drift) deb ataladi va model ishlayotgan davrda aniqlik ko‘rsatkichlarini doimiy kuzatish orqali aniqlanadi. Shuningdek, hujumchilar ataylab o‘zgartirilgan loglar bilan modelni chalg‘itishi mumkin. Analitikning ishonchi ham muhim: ogohlantirishda IP manzil, urinishlar soni va vaqt oralig‘i kabi asosiy belgilar ko‘rsatilmasa, analitik uni e’tiborsiz qoldirishi mumkin. Demak, samarali SIEM ML tizimi yuqori aniqlikka emas, balki modelni muntazam yangilash, analitik fikrini hisobga olish va natijalarni shaffof ko‘rsatishga ham tayanadi.

Xulosa

Ushbu maqolada an’anaviy SIEM tizimlarining asosiy cheklovlari, ya’ni yangi tahdidlarni aniqlashdagi zaiflik va ko‘p sonli yolg‘on ogohlantirishlar muammosi ko‘rib chiqildi. Mashinali o‘qitish algoritmlarini SIEM ish jarayoniga integratsiya qilish bu muammolarga muqobil yechim bo‘lishi mumkinligi asoslandi. Nazorat ostidagi, nazoratsiz va chuqur o‘qitish modellari bir-birini to‘ldirishi, ularning samaradorligi esa ma’lumotlarni to‘g‘ri tayyorlash, vaqt bo‘yicha to‘g‘ri baholash va muntazam qayta bog‘liqligi ko‘rsatildi. Taklif etilgan ish jarayoni ma’lumot yig‘ish va normallashtirishdan boshlanib, ML tahlili, L1 analitiklariga ogohlantirish va javob tavsiyalari bilan davom etadi. Bu yondashuv SOC analitiklarining ish yukini kamaytirib, haqiqiy o‘qitishga hujumlarga tezroq javob berishga yordam beradi.

Foydalanilgan adabiyotlar

1. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.

2. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, № 2. – P. 1153–1176.

3. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // IEEE International Conference on Data Mining (ICDM). – 2008. – P. 413–422.

4. Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A Survey of Network-based Intrusion Detection Data Sets // Computers & Security. – 2019. – Vol. 86. – P. 147–167.

5. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – P. 108–116.

MA’LUMOTLAR BAZALARIDA SHAFFOF SHIFRLASH (TDE) VA USTUN DARAJASIDAGI SHIFRLASH USULLARINING QIYOSIY TAHLILI

Irgasheva D.Y.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada ma’lumotlar bazalarida saqlanayotgan axborotni kriptografik himoyalashning ikki asosiy usuli – shaffof shifrlash (Transparent Data Encryption, TDE) va ustun darajasidagi shifrlash (Column-Level Encryption) qiyosiy tahlil qilingan. Har bir usulning ishlash tamoyili, kalitlarni boshqarish sxemasi, unumdorlikka ta’siri, tahdidlardan himoyalash darajasi va me’yoriy talablarga muvofiqligi ko‘rib chiqilgan. Tahlil natijalariga ko‘ra, axborot tizimining turiga qarab usul tanlash bo‘yicha tavsiyalar hamda ikkala usulni birgalikda qo‘llashga asoslangan gibrid yondashuv taklif etilgan.

Kalit so‘zlar: ma’lumotlar bazasi xavfsizligi, shaffof shifrlash, TDE, ustun darajasidagi shifrlash, AES, kalitlarni boshqarish, kriptografik himoya, shaxsga doir ma’lumotlar.

Аннотация: В статье проведён сравнительный анализ двух основных способов криптографической защиты информации, хранящейся в базах данных, – прозрачного шифрования данных (Transparent Data Encryption, TDE) и шифрования на уровне столбцов (Column-Level Encryption). Рассмотрены принцип работы каждого способа, схема управления ключами, влияние на производительность, степень защиты от угроз и соответствие нормативным требованиям. По результатам анализа предложены рекомендации по выбору способа в зависимости от типа информационной системы, а также гибридный подход, основанный на совместном применении обоих способов.

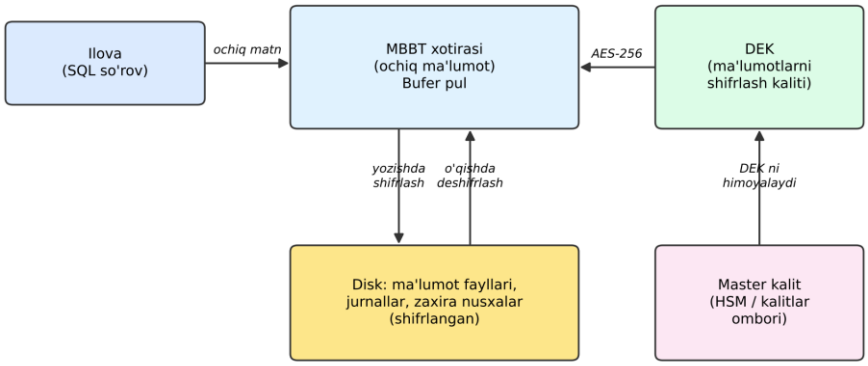
Ключевые слова: безопасность баз данных, прозрачное шифрование, TDE, шифрование на уровне столбцов, AES, управление ключами, криптографическая защита, персональные данные.

Raqamli transformatsiya jarayonida ta’lim, sog‘liqni saqlash, bank-moliya va davlat boshqaruvi sohalaridagi axborot tizimlari katta hajmdagi shaxsga doir ma’lumotlarni ma’lumotlar bazalarida saqlamoqda. Bunday bazalar kiberjinoyatchilarning asosiy nishoniga aylangan: disk yoki zaxira nusxaning o‘g‘irlanishi, bulut xizmatidagi konfiguratsiya xatosi yoki ichki xodimning ruxsatsiz harakati natijasida millionlab yozuvlar oshkor bo‘lishi mumkin.

O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni hamda xalqaro PCI DSS va GDPR talablari saqlanayotgan ma’lumotlarni kriptografik himoyalashni muhim chora sifatida belgilaydi. Amaliyotda buning uchun ikki asosiy usul keng qo‘llaniladi: butun bazani fayl darajasida shifrlovchi TDE va alohida maxfiy maydonlarni shifrlovchi ustun darajasidagi shifrlash. Ushbu maqolaning maqsadi – ikkala usulni bir xil mezonlar asosida taqqoslab, ularni tanlash bo‘yicha amaliy tavsiyalar ishlab chiqishdir.

Shaffof shifrlash (TDE) usulining ishlash tamoyili, TDE usuli Microsoft SQL Server, Oracle Database, MySQL (InnoDB) va PostgreSQL ning ayrim distributivlarida qo‘llab-quvvatlanadi. Uning mohiyati shundaki, ma’lumotlar bazasini boshqarish tizimi (MBBT) sahifalarni diskka yozishda shifrlaydi va xotiraga o‘qishda avtomatik deshifrlaydi. Shu sababli usul “shaffof” deb ataladi: ilova va foydalanuvchi uchun hech narsa o‘zgarmaydi, SQL so‘rovlarni qayta yozish talab etilmaydi.

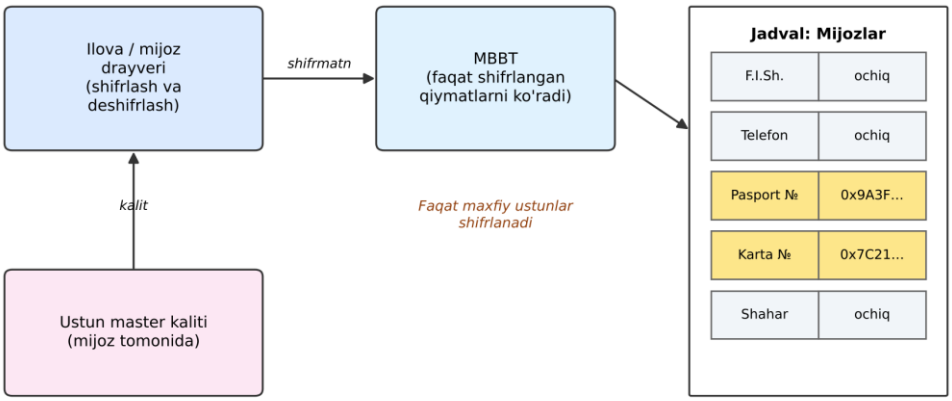
TDE ikki bosqichli kalit ierarxiyasiga asoslanadi (1-rasm). Ma’lumotlar AES-256 algoritmi bilan ma’lumotlarni shifrlash kaliti (DEK) yordamida shifrlanadi, DEK esa o‘z navbatida master kalit bilan himoyalanadi. Master kalit sertifikat, kalitlar ombori yoki apparat xavfsizlik moduli (HSM) da saqlanadi. Bu sxema kalitni almashtirishni (rotatsiya) osonlashtiradi: master kalit yangilanganda butun bazani qayta shifrlash shart emas, faqat DEK qayta shifrlanadi.



1-rasm. TDE usulining ishlash sxemasi va kalit ierarxiyasi

TDE ning asosiy afzalligi – ma’lumot fayllari, tranzaksiya jurnallari va zaxira nusxalar o‘g‘irlanganda ularni boshqa serverda ochib bo‘lmasligidir. Biroq usulning muhim cheklovi bor: MBBT xotirasida ma’lumotlar ochiq holda bo‘ladi, shu bois tizimga qonuniy kirish huquqiga ega ma’mur (DBA), SQL-in’eksiya orqali kirgan buzg‘unchi yoki ruxsati keng xodim ma’lumotlarni ochiq ko‘ra oladi.

Ustun darajasidagi shifrlash usuli. Ustun darajasidagi shifrlashda jadvaldagi barcha ma’lumotlar emas, balki faqat maxfiy ustunlar – pasport raqami, bank karta raqami, tibbiy tashxis, maosh kabi maydonlar shifrlanadi (2-rasm). Bu usul ikki ko‘rinishda amalga oshiriladi: server tomonida (masalan, PostgreSQL pgcrypto kengaytmasi yoki SQL Server ENCRYPTBYKEY funksiyasi) va mijoz tomonida (SQL Server Always Encrypted, MongoDB Queryable Encryption).



2-rasm. Mijoz tomonida ustun darajasidagi shifrlash sxemasi

Mijoz tomonidagi shifrlashda kalit hech qachon serverga uzatilmaydi, shu sababli MBBT va uning ma’muri faqat shifrmatnni ko‘radi. Bu usul ichki tahdidlar va bulut provayderiga ishonch muammosini hal qiladi. Ammo shifrlangan ustun bo‘yicha saralash, oraliq (BETWEEN, LIKE) bo‘yicha qidiruv va agregat funksiyalar cheklanadi. Tasodifiy (randomized) shifrlash eng yuqori himoyani beradi, lekin qidiruvga imkon bermaydi; deterministik shifrlash esa tenglik bo‘yicha qidiruvga ruxsat beradi, biroq chastota tahliliga nisbatan zaifroq.

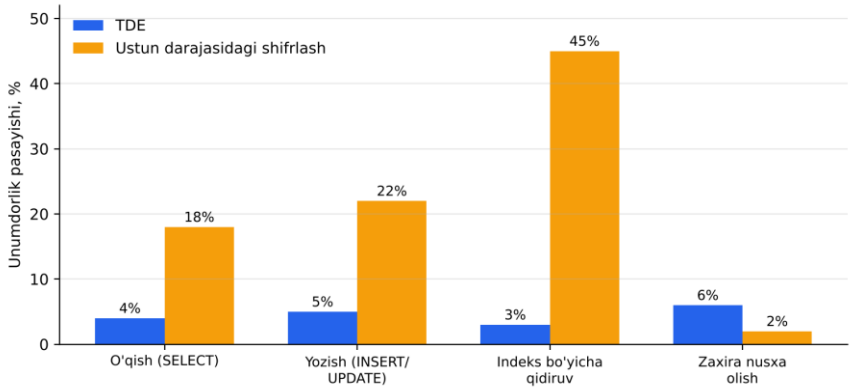
Ikkala usul himoya ko‘lami, ilovaga ta’siri, kalitlarni boshqarish murakkabligi va unumdorlik nuqtai nazaridan taqqoslandi. Natijalar 1-jadvalda umumlashtirilgan.

1-jadval

TDE va ustun darajasidagi shifrlashning qiyosiy tavsifi

Mezon	TDE (shaffof shifrlash)	Ustun darajasidagi shifrlash
Himoya darajasi	Butun ma’lumotlar bazasi, jurnal va zaxira fayllari	Faqat tanlangan maxfiy ustunlar
Himoyalanadigan holat	Saqlanayotgan ma’lumot (data at rest)	Saqlanayotgan, uzatilayotgan va xotiradagi ma’lumot
Ilovaga ta’siri	O‘zgartirish talab etilmaydi	Ilova yoki drayver darajasida o‘zgartirish kerak
Ma’mur (DBA)dan himoya	Yo‘q – ma’mur ochiq ma’lumotni ko‘radi	Bor – kalit mijoz tomonida bo‘lsa
Unumdorlikka ta’siri	Past (taxminan 3–6 %)	O‘rta va yuqori (so‘rov turiga bog‘liq)
Indeks va qidiruv	To‘liq saqlanadi	Cheklangan (deterministik shifrlashda tenglik bo‘yicha qidiruv)
Kalitlarni boshqarish	Oddiy: bitta DEK va master kalit	Murakkab: har bir ustun uchun alohida kalit
Joriy etish narxi	Past	Yuqori
Me’yoriy talablarga muvofiqlik	Umumiy talablar (PCI DSS, GDPR, shaxsga doir ma’lumotlar qonuni)	Nozik ma’lumotlarga qo‘yiladigan qat’iy talablar

Unumdorlik nuqtai nazaridan TDE apparat tezlashtirishi (AES-NI ko‘rsatmalari) tufayli tizimga deyarli sezilmaydigan yuk beradi. Ustun darajasidagi shifrlashda esa har bir yozuvni alohida shifrlash va deshifrlash, shuningdek, indekslardan to‘liq foydalana olmaslik so‘rovlarni sezilarli sekinlashtiradi. 3-rasmda adabiyotlar va ishlab chiqaruvchilar hujjatlarida keltirilgan taxminiy ko‘rsatkichlar asosida unumdorlik pasayishi taqqoslangan.



3-rasm. Operatsiya turlari bo‘yicha unumdorlik pasayishi

Rasmda, eng katta farq indeks bo‘yicha qidiruvda kuzatiladi. Zaxira nusxa olishda esa ustun darajasidagi shifrlash ustunlikka ega, chunki ma’lumotlarning katta qismi ochiq qoladi va qo‘shimcha shifrlash amali bajarilmaydi.

Tahlil shuni ko‘rsatadiki, ikkala usul bir-birini inkor etmaydi, balki to‘ldiradi. TDE fizik tashuvchilar va zaxira nusxalar o‘g‘irlanishidan himoya qilsa, ustun darajasidagi shifrlash eng nozik ma’lumotlarni hatto ma’murdan ham yashiradi. Shu sababli yuqori xavf darajasidagi tizimlar uchun gibrid yondashuv – butun bazaga TDE va eng maxfiy ustunlarga qo‘shimcha shifrlash qo‘llash maqsadga muvofiq. Axborot tizimi turlariga ko‘ra tavsiyalar 2-jadvalda keltirilgan.

2-jadval

Axborot tizimi turiga ko‘ra shifrlash usulini tanlash

Foydalanish holati	TDE	Ustun shifrlash	Tavsiya etilgan yondashuv
Ta’lim muassasasi axborot tizimi	+	±	TDE
Bank va to‘lov tizimlari	+	+	Gibrid
Tibbiyot ma’lumotlari bazasi	+	+	Gibrid
Bulutli MBBT (uchinchi tomon ma’muri)	±	+	Ustun shifrlash
Eski (legacy) ilovalar	+	–	TDE

Qaysi usul tanlanishidan qat’i nazar, kalitlarni boshqarish himoyaning eng muhim bo‘g‘ini bo‘lib qoladi. Kalitlarni ma’lumotlardan alohida, HSM yoki markazlashgan kalitlar boshqaruvi tizimida saqlash, ularni muntazam almashtirish va kirish huquqlarini vazifalar bo‘linishi tamoyili asosida taqsimlash tavsiya etiladi. Shuningdek, shifrlash SQL-in’eksiyaga qarshi himoya, kirish nazorati va audit jurnallarini almashtirmasligini, balki ular bilan birga qo‘llanishini hisobga olish lozim.

Xulosa

Maqolada ma’lumotlar bazalarini kriptografik himoyalashning ikki asosiy usuli qiyosiy tahlil qilindi. TDE joriy etilishi oson, ilovani o‘zgartirishni talab etmaydigan va unumdorlikka kam ta’sir qiluvchi usul bo‘lib, saqlanayotgan ma’lumotlarni fizik o‘g‘irlikdan himoyalashda samarali. Ustun darajasidagi shifrlash esa joriy etilishi murakkabroq bo‘lsa-da, ichki tahdidlar va bulut provayderiga nisbatan ishonch muammosini hal qiladi.

Ta’lim muassasalari kabi o‘rta xavf darajasidagi tizimlar uchun TDE yetarli darajadagi himoyani ta’minlaydi, bank, tibbiyot va bulutli tizimlarda esa gibrid yondashuvni qo‘llash tavsiya etiladi. Kelgusida kvant kompyuterlari tahdidini hisobga olib, kalitlarni himoyalashda postkvant kriptografik algoritmlarga o‘tish masalasi dolzarb bo‘lib qoladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. 02.07.2019, O‘RQ-547-son.

2. NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management. – Gaithersburg: NIST, 2020.

3. NIST FIPS 197. Advanced Encryption Standard (AES). – Gaithersburg: NIST, 2001 (updated 2023).

4. Microsoft. Transparent Data Encryption (TDE) and Always Encrypted. SQL Server Documentation. – learn.microsoft.com.

5. Oracle. Database Advanced Security Guide: Transparent Data Encryption. – docs.oracle.com.

6. PCI Security Standards Council. Payment Card Industry Data Security Standard, v4.0. – 2022.

7. Popa R.A., Redfield C.M.S., Zeldovich N., Balakrishnan H. CryptDB: Protecting Confidentiality with Encrypted Query Processing // Proc. 23rd ACM SOSP. – 2011. – P. 85–100.

8. Naveed M., Kamara S., Wright C.V. Inference Attacks on Property-Preserving Encrypted Databases // Proc. ACM CCS. – 2015. – P. 644–655.

9. Ganiev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. – Toshkent: Fan va texnologiya, 2016.

АЛГОРИТМЫ И МОДЕЛИ ДЛЯ ОБНАРУЖЕНИЯ ИСКУССТВЕННО СОЗДАННЫХ ВИЗУАЛЬНЫХ ОБЪЕКТОВ

Хакимбеков Д.Т.
Университет “Новый Узбекистан”

Annotatsiya. Maqolada sun’iy intellekt yordamida yaratilgan vizual obyektlarni - deepfake va sun’iy generatsiya qilingan tasvirlarni - aniqlash algoritmlari va modellari tahlil qilinadi. To‘rtta xorijiy manbaning qiyosiy tahlili asosida mavjud detektorlarning asosiy muammolari umumlashtiruvchanlik (generalization) va bardoshlilik (robustness) ekanligi ko‘rsatiladi. CNN (ResNet18) yordamida olingan fazoviy belgilarni va tez Furye almashtirishi (FFT) yordamida olingan chastota belgilarini birlashtiruvchi gibrid model taklif etiladi.

Kalit so‘zlar: sun’iy intellekt, deepfake aniqlash, sun’iy yaratilgan tasvirlar, konvolyutsion neyron tarmoq (CNN), FFT, gibrid model, umumlashtiruvchanlik.

Аннотация. В работе рассматриваются алгоритмы и модели обнаружения визуальных объектов, созданных с помощью искусственного интеллекта, включая дипфейки и синтетические изображения. На основе сравнительного анализа четырёх зарубежных источников показано, что главными проблемами существующих детекторов являются обобщаемость и устойчивость. Предложена гибридная модель, объединяющая пространственные признаки, извлекаемые свёрточной нейронной сетью ResNet18, и частотные признаки, получаемые с помощью быстрого преобразования Фурье (FFT).

Ключевые слова: искусственный интеллект, обнаружение дипфейков, синтетические изображения, свёрточная нейронная сеть (CNN), быстрое преобразование Фурье, гибридная модель, обобщаемость.

Введение

В последние годы генеративные состязательные сети (GAN) и диффузионные модели (DM) достигли уровня, при котором создаваемые ими изображения и видео практически неотличимы от подлинных для человеческого глаза [1], [3]. Наряду с применением в искусстве, дизайне и научной визуализации это порождает серьёзные риски: распространение дезинформации, подделку личности, мошенничество и несанкционированное воспроизведение контента, защищённого авторским правом [1], [3], [4]. Современные методы генерации минимизируют заметные артефакты, поэтому эффективность традиционных способов обнаружения снижается, а задача выявления искусственно созданных визуальных объектов стала одной из центральных в компьютерном зрении и информационной безопасности [7].

Объектом исследования является визуальный контент (изображения и видео), созданный с помощью искусственного интеллекта; предметом - алгоритмы и модели его обнаружения. Цель работы - сравнительный анализ существующих подходов и обоснование гибридной модели обнаружения, ориентированной на обобщаемость. Задачи: классифицировать основные подходы, представленные в современной литературе; выявить их сильные и слабые стороны; обосновать место гибридной модели, объединяющей CNN и анализ в частотной области [7].

Методология исследования

Работа выполнена методом сравнительного анализа. Отобраны четыре зарубежных источника [1]–[4], которые анализировались по следующим критериям: (1) тип предлагаемого метода или модели; (2) используемые признаки (пространственные, частотные, глубокие, мультимодальные); (3) наборы данных, на которых проводилась проверка; (4) результаты по обобщаемости и устойчивости; (5) ограничения. Выводы из каждого источника сопоставлялись между собой, что позволило выделить общие тенденции и научные пробелы, а на их основе определить место предлагаемой гибридной модели [7].

Обзор существующих подходов

Zhang и соавторы систематизируют область по используемым признакам и разделяют проблему на две части: обнаружение синтетических изображений, созданных GAN и DM, и обнаружение дипфейков, т. е. манипуляций с лицом и подмены личности. Методы для изображений делятся на опирающиеся на пространственную область, частотную область, кросс-доменное объединение признаков и мультимодальные подходы «изображение–текст». Методы обнаружения дипфейков классифицируются по пространственным, пространственно-временным, биологическим (направление взгляда, положение головы, пульс) и идентификационным признакам [1].

Laurier и соавторы рассматривают обнаружение как постоянную «игру в кошки-мышки» между генеративными моделями и детекторами. Детекторы, созданные для GAN, нередко оказываются неработоспособными на изображениях диффузионных моделей, поскольку природа артефактов различается; небольшое изменение архитектуры генератора может устранить высокочастотные отличия, на которые опирается детектор. В качестве эффективных для эпохи диффузии авторы называют методы на основе ошибки реконструкции (DIRE, AEROBLADE, LaRE) и детекторы на базе CLIP [3]. Следует учесть, что эта работа является препринтом, не прошедшим рецензирование. Близкий вывод содержится в исследовании Corvi и соавторов, посвящённом обнаружению изображений, созданных диффузионными моделями: специфика следов этих генераторов отличается от следов GAN, и это необходимо учитывать при обучении детекторов [6].

Raza и соавторы сопоставляют парадигмы - глубокое обучение, классическое машинное обучение и традиционную обработку изображений. Главный вывод: при переходе на другой набор данных (кросс-датасетная оценка) точность стабильно падает на 10–15 % как у трансформеров, так и у CNN и традиционных методов. Это означает, что детекторы запоминают артефакты сжатия, характерные для конкретного набора данных, а не общие свойства синтетических медиа. По данным [2], падение составляет 11,33 % для трансформеров (ADT), 7,61 % для MCX-API, 16,50 % для CNN (XceptionNet) и в среднем 13,00 % для традиционных методов. Авторы также отмечают, что лишь малая часть проанализированных работ оценивает устойчивость к состязательным атакам [2].

Bianco и соавторы представляют практический эксперимент: модели VGG-19, ResNet-50 и ViT, обученные методом transfer learning, отличают произведения искусства, созданные человеком, от искусственных с точностью выше 95 % (лучший результат у ViT - около 0,976). С помощью Grad-CAM авторы визуализируют области, влияющие на решение, и тем самым демонстрируют интерпретируемость (XAI). Однако модель оценивалась лишь на одном внутреннем тестовом наборе, а подлинные и синтетические изображения взяты из разных источников, поэтому высокая точность может частично

отражать различие источников - то самое ограничение обобщаемости, о котором предупреждают Raza и соавторы [2, 4].

Результаты и обсуждение

Результаты сравнительного анализа сведены в таблице 1. Несмотря на разнообразие используемых признаков, все источники независимо друг от друга приходят к одной центральной проблеме - обобщаемости и устойчивости [1]–[3].

Таблица 1

Сравнительный анализ источников и предлагаемой модели [7]

Источник	Тип работы	Основной подход	Сильная сторона	Ограничение
Zhang и др. [1]	Обзор	Классификация по признакам: пространственные, частотные, кросс-доменные, «изображение–текст»	Широкая и систематическая карта области	Сравнение качественное; единого бенчмарка нет
Raza и др. [2]	Критический обзор	Оценка с ориентацией на практику: точность, вычислительная стоимость, обобщаемость	Количественно показано падение точности на 10–15 % при смене датасета	Часть цифр спорна; текст требует редактирования
Laurier и др. [3]	Обзор (диффузия)	«Кошки-мышки»: ошибка реконструкции, CLIP, частотные признаки	Учёт эпохи диффузии и состязательных атак	Препринт без рецензирования; нет количественной таблицы
Bianco и др. [4]	Эмпирическая работа	Transfer learning (VGG-19, ResNet-50, ViT) + Grad-CAM	Чёткая методика и интерпретируемость (XAI)	Только in-distribution тест; смещение по источнику данных
Предлагаемая модель [7]	Гибридная модель	CNN (ResNet18) + FFT, объединение признаков	Обобщаемость за счёт взаимодополняющих признаков	Требуется кросс-датасетная и состязательная проверка

Первый результат - недостаточная обобщаемость: падение точности на 10–15 % в кросс-датасетных условиях [2] описывается Laurier и соавторами как «гонка вооружений» [3], а Zhang и соавторами - как фундаментальная нерешённая проблема области [1]. Второй результат - недостаточная устойчивость: JPEG-сжатие, изменение размера и повторная обработка в социальных сетях снижают качество обнаружения, а состязательные атаки

практически не оцениваются [1]–[3]. Третий результат - несовершенство практики оценки: Raza и соавторы требуют многомерной оценки, учитывающей не только точность, но и вычислительную стоимость и кросс-датасетную обобщаемость [2]; тест Bianco и соавторов лишь на внутреннем наборе показывает именно эту слабость [4]. Четвёртый результат - интерпретируемость: методы на общих признаках дают высокую точность, но трудно объяснимы [1], тогда как Grad-CAM позволяет частично решить эту задачу [4].

Предлагаемая гибридная модель

Выявленные пробелы обосновывают гибридную модель, предложенную авторами [7]. Литература показывает, что пространственные и частотные признаки взаимно дополняют друг друга. CNN-подходы (Xception, ResNet, VGG) хорошо выявляют видимые несоответствия в структуре лица и текстуре, но зависят от обучающих данных и теряют эффективность на незнакомых наборах [1], [2]. Частотные методы (DCT, FFT) обнаруживают высокочастотные артефакты, характерные для процесса генерации и невидимые в пространственной области, но не учитывают семантическую информацию [1]–[3]. Поскольку каждое из семейств охватывает то, что упускает другое, а кросс-доменное объединение признаков превосходит однодоменное обнаружение, их совместное использование является обоснованным выбором [1]–[3], [7].

Модель имеет двухпоточную архитектуру с блоком объединения признаков (feature fusion). Первый поток на основе CNN (ResNet18) извлекает из кадров пространственные признаки - нарушения текстуры и неестественные структуры лица. Второй поток анализирует спектр, полученный с помощью быстрого преобразования Фурье (FFT), и выявляет высокочастотные артефакты, скрытые в пространственной области. Признаки обоих потоков объединяются и передаются в классификационный слой, который определяет, является ли контент подлинным или синтетическим [7]. Таким образом, модель охватывает более широкий спектр артефактов, чем одиночная сеть, и устраняет ограничение, отмеченное в обзорах: CNN-модели не видят частотные аномалии, а чисто частотные методы - семантику [2], [7].

Заключение

Анализ четырёх работ [1]–[4] с разных позиций приводит к одному выводу: обнаружение искусственно созданных визуальных объектов сегодня ограничивается не нехваткой полезных признаков, а неспособностью детекторов обобщаться за пределы условий обучения. Предложенная гибридная модель, объединяющая пространственные и спектральные признаки в одном детекторе [7], может быть расширена для кросс-датасетной устойчивости, учёта временных и мультимодальных признаков и работы в условиях состязательных атак. Эффективность модели нуждается в экспериментальном подтверждении. Дальнейшие исследования целесообразно направить на: (1) проверку модели на нескольких наборах данных (кросс-датасет); (2) учёт наряду с точностью вычислительной стоимости и интерпретируемости; (3) интеграцию временных признаков видео и аудиовизуальных мультимодальных сигналов; (4) повышение устойчивости к состязательным атакам [2], [7].

Список литературы

1. Zhang Y., Pang Z., Huang S., Wang C., Zhou X. Unmasking AI-created visual content: a review of generated images and deepfake detection technologies // Journal of King Saud University – Computer and Information Sciences. 2025. Vol. 37. Art. 148.

2. Raza A., Basit A., Amin A., Arfeen Z.A., Masud M.I., Fayyaz U., Jumani T.A. A comprehensive review of deepfake detection techniques: from traditional machine learning to advanced deep learning architectures // AI. 2026. Vol. 7, No. 2. Art. 68.

3. Laurier L., Giulietta A., Octavia A., Cleti M. The Cat and Mouse Game: The Ongoing Arms Race Between Diffusion Models and Detection Methods. arXiv preprint arXiv:2410.18866. 2024.

4. Bianco T., Castellano G., Scaringi R., Vessio G. Identifying AI-generated art with deep learning // Proceedings of the 2nd Workshop on Artificial Intelligence and Creativity (CREAI). CEUR-WS. 2023. Vol. 3519.

5. Khakimbekov D.T. Hybrid Deepfake Detection Using CNN and Frequency Domain Analysis. Tashkent: New Uzbekistan University, 2025.

6. Corvi S., Cozzolino D., Zingarini G., Poggi G., Nagano K., Verdoliva L. On the detection of synthetic images generated by diffusion models // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). 2023.

7. Xakimbekov D.T., Usmanbayev D.Sh. Sun’iy generatsiya qilingan vizual obyektlarni aniqlash usullari tahlili // Muhandislik va iqtisodiyot. 2026. № 10. B. 399–403.

LOKAL BULUTLI TIZIMLARDA AXBOROT XAVFSIZLIGI TAHDIDLARI MODELINI QURISH VA HIMOYA TALABLARINI SHAKLLANTIRISH

Sapayev Sh.R.
O‘zbekiston Respublikasi Harbiy xavfsizlik va Mudofaa universitetining
Axborot kommunikatsiya texnologiyalari va harbiy aloqa institute

Annotatsiya. Maqolada xizmat doirasida foydalanishga mo‘ljallangan lokal bulutli tizimlar uchun tahdidlar modelini qurish metodikasi ko‘rib chiqilgan. Tizim ma’lumotlar oqimi diagrammasi (DFD) va ishonch chegaralari bo‘yicha tavsiflanib, tahdidlar STRIDE tasnifi asosida aniqlanadi, xavf ehtimol va ta’sir bo‘yicha baholanadi hamda himoya talablariga aylantiriladi. Tahdidlarni aniqlash, xavfni hisoblash va talablarni shakllantirish algoritmlari, xavf matritsasi va sakkizta asosiy himoya talabi keltirilgan. Metodika tizim arxitekturasini loyihalashdan oldingi bosqich sifatida qo‘llanadi.

Kalit so‘zlar: tahdidlar modeli, STRIDE, ma’lumotlar oqimi diagrammasi, ishonch chegarasi, xavfni baholash, himoya talablari, lokal bulutli tizim, axborot xavfsizligi.

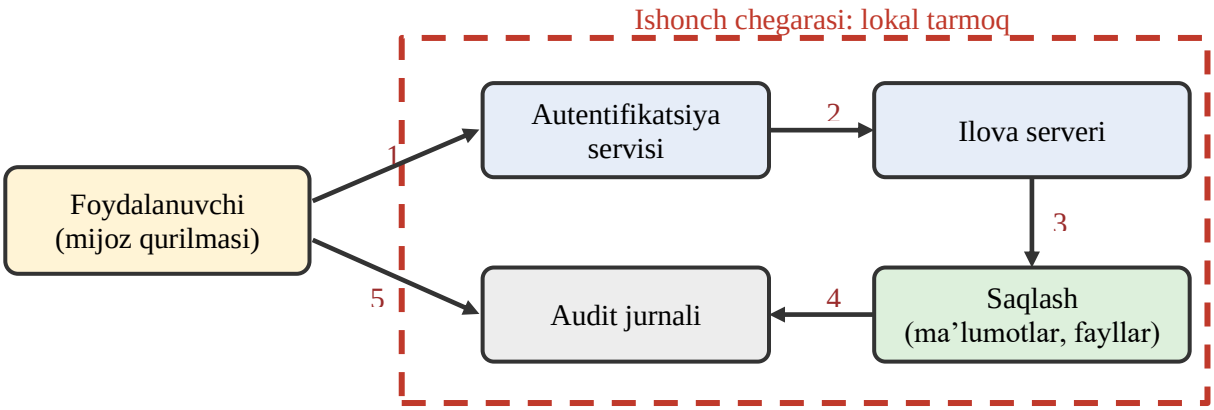
Аннотация. В статях рассмотрена методика построения модели угроз для локальных облачных систем служебного назначения. Система описывается диаграммой потоков данных (DFD) и границами доверия, угрозы выявляются по классификации STRIDE, риск оценивается по вероятности и ущербу и преобразуется в требования защиты. Приведены алгоритмы выявления угроз, расчёта риска и формирования требований, матрица риска и восемь основных требований защиты.

Ключевые слова: модель угроз, STRIDE, диаграмма потоков данных, граница доверия, оценка риска, требования защиты, локальная облачная система, информационная безопасность.

Lokal bulutli tizim tashkilotning o‘z tarmog‘ida joylashgani uchun tashqi provayderga bog‘liqlik kamayadi, ammo xavfsizlik muammolari yo‘qolmaydi: ichki foydalanuvchi suiiste’moli, noto‘g‘ri sozlangan kirish huquqlari, ma’lumotlarning saqlash joyidan sizib chiqishi, jurnallarning o‘zgartirilishi kabi tahdidlar saqlanib qoladi [1, 2]. Xavfsizlik choralari ko‘pincha tizim ishlab chiqilgandan so‘ng, tasodifiy tarzda qo‘shiladi. Tahdidlar modeli esa loyihalash bosqichida nimadan va nima uchun himoyalanish kerakligini aniq belgilab beradi [3].

Buning uchun ma’lumotlar oqimi diagrammasi (DFD) quriladi: unda tashqi ishtirokchilar (foydalanuvchi), jarayonlar (autentifikatsiya va ilova serverlari), ma’lumotlar saqlash joylari va ular orasidagi oqimlar ko‘rsatiladi (1-rasm). Eng muhim element ishonch chegarasi: ma’lumot ikki xil ishonch darajasidagi zona orasidan o‘tgan joylarda - mijoz qurilmasidan lokal tarmoqqa tahdid ehtimoli eng yuqori bo‘ladi. Shu sababli har bir oqim va chegarani kesib o‘tuvchi nuqta alohida tahlil qilinadi.

Tizimga bo‘ladigan tahdidlarni STRIDE tasnifi bo‘yicha ko‘rib chiqaylik. STRIDE tasnifi tahdidlarni buziladigan xavfsizlik xususiyatiga qarab oltita guruhga ajratadi: soxtalashtirish (Spoofing), o‘zgartirish (Tampering), inkor etish (Repudiation), axborotning oshkor bo‘lishi (Information disclosure), xizmat ko‘rsatishdan to‘xtatish (Denial of service) va huquqlarni oshirish (Elevation of privilege) [3, 4]. Har bir guruh uchun lokal bulutli tizimdagi tipik misollar va asosiy himoya yo‘nalishi 1-jadvalda keltirilgan. Bulutli xizmatlar uchun keng tarqalgan tahdidlar Bulut xavfsizligi alyansi (CSA) hisobotida ham ro‘yxatlangan.



1- rasm. Tizim komponentlari o'rtasidagi ma'lumotlar oqimi va ishonch chegarasi

1-jadval

STRIDE tahdidlari va lokal bulutli tizimdagi misollar

t/r	Tahdid	Buziladigan xususiyat	Lokal bulutli tizimdagi misol	Himoya yo'nalishi
1	Soxtalashtirish (S)	Autentifikatsiya	Boshqa xodim nomidan kirish, parolni taxmin qilish	Kuchli (ko'p omilli) autentifikatsiya
2	O'zgartirish (T)	Yaxlitlik	Fayl yoki so'rovni uzatishda o'zgartirish	Shifrlangan kanal, yaxlitlik tekshiruvi
3	Inkor etish (R)	Inkor etilmaslik	Harakatni bajarganini inkor etish, jurnalni o'chirish	Himoyalangan audit jurnali
4	Oshkor bo'lishi (I)	Maxfiylik	Saqlangan ma'lumotni nusxalash, sizib chiqish	Saqlashda shifrlash, kalit boshqaruvi
5	Xizmatdan to'xtatish (D)	Mavjudlik	Serverni so'rovlar bilan to'ldirish	So'rovlarni cheklash, zaxira
6	Huquqlarni oshirish (E)	Avtorizatsiya	Oddiy foydalanuvchining administrator huquqini olishi	Minimal huquq, rollar bo'yicha boshqaruv

Bunday turdagi tahdidlar xavfini baholash va talablarni shakllantirish bir nechta algoritmlardan foydalaniladi:

1-algoritm. Tahdidlarni aniqlash. Bunda tizim uchun DFD quriladi, ishonch chegaralari belgilanadi. Har bir element - tashqi ishtirokchi, jarayon, saqlash, oqim uchun unga mos STRIDE guruhlari tanlanadi. Shundan so'ng har bir mos juftlik (element, guruh) uchun aniq tahdid stsenariysi ishlab chiqilib, tahdidlar ro'yxati identifikator bilan raqamlanadi.

2-algoritm. Xavfni hisoblash va ustuvorlashtirish. Bundan har bir tahdid uchun ehtimol L va ta'sir I 1 dan 5 gacha shkala bo'yicha baholanadi va $R = L \cdot I$ fo'rmula bo'yicha xavf hisoblanadi. Ushbu hisoblash natijasiga ko'ra daraja belgilanadi: $R \leq 4$ – past, 5–9 – o'rta, 10–16 – yuqori, $R \geq 17$ – jiddiy (2-diagramma). Ushbu belgilangan tahdidlar R kamayish tartibida saralanadi va jiddiy va yuqori xavflar birinchi navbatda bartaraf etiladi.

3-algorit. Himoya talablarini shakllantirish va tekshirish. Har bir ustuvor tahdid uchun uni kamaytiruvchi nazorat chorasi standart katalogidan tanlanadi va Nazorat chorasi tekshiriladigan talab ko'rinishida yoziladi. Shunday qilib, keyingi qadamda talab tahdid identifikatoriga bog'lanadi, shunda har bir tahdid kamida bitta talab bilan yopilgani ko'rinadi. Chora

qo‘llangandan so‘ng qoldiq xavf R′ qayta hisoblanadi hamda R′ qabul qilinadigan darajadan yuqori bo‘lsa, 1-qadamga qaytiladi.

Ehtimol (L)	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Ta’sir (I)				

2-diagramma. Xavf matritsasi. (yashil – past, sariq – o‘rta, to‘q sariq – yuqori, qizil – jiddiy)

Metodikaning ishlashini ko‘rsatish uchun 1-rasmdagi oqimlar bo‘yicha oltita tahdid uchun shartli baholash keltirilgan (2-jadval). Ehtimol va ta’sir qiymatlari namuna sifatida olingan. Jadvaldan ko‘rinib turibdiki, eng yuqori xavf kirish nuqtasidagi (1-oqim) autentifikatsiya hamda saqlangan ma’lumotning oshkor bo‘lishi tahdidlariga to‘g‘ri keladi. Ichki foydalanuvchi tomonidan ma’lumotni nusxalash lokal tizimlarda tashqi hujumdan kam xavf emas, shuning uchun tahlilda ichki xodim ham potentsial hujumchi sifatida hisobga olinadi [5].

2-jadval

Tahdidlarning namunaviy xavf baholari

№	Tahdid stsenariysi	Oqim	STRIDE	L	I	R	Daraja
1	O‘g‘irlangan yoki taxmin qilingan hisob bilan kirish	1	S	4	4	16	Yuqori
2	Tarmoq kanalida ma’lumotni tinglash	1, 2	I	3	5	15	Yuqori
3	Saqlangan ma’lumotni ichki xodim tomonidan nusxalash	3	I	3	5	15	Yuqori
4	Oddiy foydalanuvchi huquqini oshirish	2	E	2	5	10	Yuqori
5	Audit jurnalini o‘zgartirish yoki o‘chirish	4, 5	R	2	4	8	O‘rta
6	Autentifikatsiya servisini so‘rovlar bilan to‘ldirish	1	D	3	3	9	O‘rta

Shu natijalar asosida talablar ustuvorlashtiriladi: birinchi navbatda T1–T4 (autentifikatsiya, shifrlangan kanal, saqlashda shifrlash va huquqlar nazorati), so‘ng T5–T8 amalga oshiriladi. Har bir talab bajarilgandan keyin tahdid xavfi qayta baholanadi.

Aniqlangan tahdidlardan ISO/IEC 27001, ISO/IEC 27017 va NIST SP 800-53 kataloglariga tayangan holda 3-jadvaldagi umumiy talablar kelib chiqadi. Ular lokal bulutli tizim uchun minimal asos bo‘lib, tizim arxitekturasi ushbu talablarni qondiradigan qilib loyihalanadi. Autentifikatsiya talabi NIST SP 800-63B tavsiyalariga mos bo‘lib, shaxsni bir necha omil bilan, jumladan biometrik omil bilan tasdiqlashni nazarda tutadi [6, 7].

3-jadval

Lokal bulutli tizim uchun himoya talablari

№	Talab	Yopiladigan tahdid
1	Ko‘p omilli autentifikatsiya; kirish urinishlari soni cheklanishi	S
2	Barcha tarmoq aloqasi shifrlangan va yaxlitligi tekshiriladigan kanal orqali	T, I

3	Saqlanadigan ma’lumot shifrlangan; kalitlar ma’lumotdan alohida boshqariladi	I
4	Rollar bo‘yicha boshqaruv va minimal huquq tamoyili	E, I
5	Barcha muhim harakatlar o‘zgartirib bo‘lmaydigan audit jurnaliga yoziladi	R
6	Tarmoq segmentatsiyasi; “hech kimga ishonmaslik” (zero trust) tamoyili	S, E, D
7	So‘rovlarni cheklash, resurslar nazorati va zaxira nusxalash	D
8	Zaifliklarni muntazam tekshirish va yangilash	T, E

Ushbu tizimda autentifikatsiya masalasi ham muhim o‘rin tutadi. Foydalanuvchi autentifikatsiyasi lokal tizimning kirish nuqtasi bo‘lgani uchun hujumchilar birinchi navbatda shunga e’tibor qaratadi. Parolga asoslangan tizimlarda keng tarqalgan hujumlar: parolni taxmin qilish va to‘liq saralash (brute force), boshqa tizimdan sizib chiqqan hisob ma’lumotlarini sinab ko‘rish (credential stuffing), fishing orqali parolni aldab olish, sessiya identifikatorini o‘g‘irlash (session hijacking) hamda tarmoqda “o‘rtadagi odam” hujumi. Biometrik omil qo‘shilganda soxta tasvir hujumlari paydo bo‘ladi. Shu sababli bir omilli autentifikatsiya yetarli emas va uni ko‘p omilli qilish NIST SP 800-63B da tavsiya etilgan [8].

Lokal tizimda xodimlar tarmoq ichida joylashgani uchun ichki tahdid alohida ahamiyatga ega. Ichki tahdid manbalari uch xil: ataylab zarar yetkazuvchi xodim, beparvolik tufayli xato qilgan xodim va hisobi hujumchi tomonidan egallangan xodim. Uchala holatda ham tizim nuqtai nazaridan hujum ruxsatli foydalanuvchi nomidan bajariladi, shuning uchun faqat kirishni nazorat qilish yetarli emas. Himoya Saltzer va Schroeder tomonidan ta’riflangan tamoyillarga tayanadi: minimal huquq (har kim faqat ishi uchun zarur huquqqa ega), vazifalarni ajratish (muhim amal bir kishining qo‘lida emas) va to‘liq vositachilik (har bir kirish har safar tekshiriladi) [9].

4-jadval

Ichki tahdid stsenariylari va nazorat choralari

t/r	Stsenariy	Qanday namoyon bo‘ladi	Nazorat chorasi
1	Ma’lumotni nusxalash	Katta hajmdagi fayllarni yuklab olish	Hajm bo‘yicha ogohlantirish, minimal huquq
2	Huquqni suiiste’mol qilish	Administrator o‘z huquqlarini kengaytiradi	Vazifalarni ajratish, ikki kishi tasdig‘i
3	Jurnalni o‘zgartirish	Izlarni yashirish uchun yozuvlarni o‘chirish	Faqat qo‘shiladigan jurnal, alohida saqlash
4	Hisob egallanishi	Boshqa kishi xodim nomidan kiradi	Ko‘p omilli autentifikatsiya, sessiya nazorati
5	Beparvolik	Noto‘g‘ri sozlash, ruxsatni noto‘g‘ri berish	Sozlamalarni tekshirish, o‘qitish

Shifrlash faqat kalitlar to‘g‘ri boshqarilgandagina himoya beradi. NIST SP 800-57 kalit hayot sikli bosqichlarini belgilaydi [8, 9]: kalitni hosil qilish, tarqatish, saqlash, foydalanish, almashtirish (rotation), bekor qilish va yo‘q qilish. Asosiy qoidalar: kalit shifrlangan ma’lumot bilan bir joyda saqlanmaydi; kalitdan foydalanish huquqi cheklanadi va jurnalga yoziladi; har bir kalit uchun foydalanish muddati (kriptodavr) belgilanadi va u tugagach kalit almashtiriladi; kalit buzilgan deb gumon qilinsa, u zudlik bilan bekor qilinadi va unga bog‘liq ma’lumot qayta shifrlanadi. Lokal tizimda kalit boshqaruvi ayniqsa muhim, chunki ma’lumot va kalit bir tashkilot ichida bo‘lib, bir ma’mur har ikkalasiga ham kirish imkoniga ega bo‘lishi mumkin. Shuning uchun

kalitga kirish ma’lumotga kirishdan alohida nazorat qilinadi va muhim amallar uchun vazifalarni ajratish tamoyili qo‘llaniladi. Kalit zaxira nusxasi ham himoyalangan bo‘lishi kerak: aks holda u eng zaif halqaga aylanadi.

Lokal tarmoq ichida joylashganli – bu xavfsizlik to‘laqonli kafolangan degani emas. Bitta buzilgan qurilma butun tarmoqda erkin harakatlanishi mumkin. NIST SP 800-207 tavsiya etgan zero trust yondashuvida tarmoqdagi joylashuv avtomatik ishonch bermaydi. Har bir so‘rov foydalanuvchi, qurilma va kontekst bo‘yicha tekshiriladi [10]. Amaliyotda bu tarmoqni zonalarga bo‘lish (segmentatsiya) va zonalar orasida faqat zarur oqimlarga ruxsat berishni bildiradi (5-jadval). Bunda foydalanuvchi zonasidan faqat autentifikatsiya va ilova servislariga murojaat qilishiga imkon beriladi. Ma’lumotlarni saqlash zonasiga esa faqat ilova serveri kira oladi.

5-jadval

Tarmoq zonalari va ruxsat etilgan oqimlar (namuna)

t/r	Zona	Tarkibi	Kimdan ruxsat	Himoya
1	Foydalanuvchi zonasi	Xodimlar kompyuterlari	Hech kimdan (boshlovchi)	Qurilma tekshiruvi
2	Servis zonasi	Autentifikatsiya va ilova serverlari	Foydalanuvchi zonasidan	Shifrlangan kanal, so‘rovlarni cheklash
3	Ma’lumot zonasi	Saqlash, ma’lumotlar bazasi	Faqat ilova serveridan	Shifrlash, to‘liq izolyatsiya
4	Boshqaruv zonasi	Administrator vositalari, jurnal	Ajratilgan administrator qurilmalaridan	Qo‘shimcha omil, to‘liq audit

Xavfsizlik hodisasi sodir bo‘lganda uni aniqlash va tahlil qilish jurnallar sifatiga bog‘liq. NIST SP 800-92 ga ko‘ra har bir yozuv kim, nima qilgani, qachon, qayerdan va natijasi qanday bo‘lganini aks ettirishi kerak [8-10]. Jurnal o‘zgartirishdan himoyalanadi: yozuvlar faqat qo‘shiladi, har bir yozuv oldingisiga xesh orqali bog‘lanadi, jurnal asosiy tizimdan alohida joyda saqlanadi. Jurnal avtomatik tahlil qilinib, shubhali hodisalar - ketma-ket muvaffaqiyatsiz kirish, g‘ayrioddiy vaqtdagi kirish, katta hajmli yuklab olish uchun ogohlantirish beriladi. Hodisaga javob jarayoni NIST SP 800-61 bo‘yicha to‘rt bosqichdan iborat: tayyorgarlik; aniqlash va tahlil; cheklash, bartaraf etish va tiklash; hodisadan keyingi tahlil. Tayyorgarlik bosqichida mas’ul shaxslar, aloqa kanallari va zaxira nusxadan tiklash tartibi oldindan belgilanadi. Hodisadan keyingi tahlil natijalari tahdidlar modeliga qaytariladi. Talab yozilgani uni bajarilgan degani emas: har bir talab uchun tekshirish usuli belgilanadi (6-jadval). Texnik xavfsizlik sinovi va baholash usullari NIST SP 800-115 da keltirilgan [9, 10]. Tekshirish natijasi talabning bajarilganini yoki bajarilmaganini ko‘rsatadi va qoldiq xavfni qayta baholash uchun asos bo‘ladi.

6-jadval

Himoya talablarini tekshirish usullari

Talab	Tekshirish usuli	Dalil
T1 Ko‘p omilli autentifikatsiya	Kirish urinishlarini sinash, parolni saralash sinovi	Sinov hisoboti
T2 Shifrlangan kanal	Tarmoq trafigini tahlil qilish, sertifikat va protokol versiyasini tekshirish	Tahlil natijasi
T3 Saqlashda shifrlash	Diskdagi ma’lumotni to‘g‘ridan to‘g‘ri o‘qishga urinish, kalit saqlanishini ko‘rib chiqish	Konfiguratsiya auditi

T4 Rollar va minimal huquq	Foydalanuvchi huquqlarini ro‘yxatga olish, ruxsatsiz amallarni sinash	Huquqlar jadvali
T5 Audit jurnali	Jurnalni o‘zgartirishga urinish, yaxlitlik tekshiruvi	Jurnal va sinov natijasi
T6–T8 Segmentatsiya, zaxira, yangilash	Zonalararo oqimlarni sinash, tiklash mashqi, zaiflik skaneri	Hisobot va mashq natijasi

Tahdidlar modeli bir marta tuzilib qolmaydi, chunki tizim va tahdidlar o‘zgaradi. Model quyidagi hollarda qayta ko‘rib chiqiladi.

7-jadvalda 2-jadvaldagi eng yuqori xavfli tahdidlar uchun shartli qoldiq xavf keltirilgan. Misol uchun ko‘p omilli autentifikatsiya hisob egallash ehtimolini L = 4 dan 2 gacha kamaytiradi, ta’sir esa o‘zgarmaydi: R = 16 dan 8 gacha. Ichki xodim tomonidan nusxalash ehtimoli minimal huquq va hajm bo‘yicha ogohlantirish bilan kamayadi, ta’sirni esa shifrlash va kalitni alohida saqlash kamaytiradi.

7-jadval

Nazorat choralaridan keyin qoldiq xavf (shartli baholash)

t/r	Tahdid	Boshlang‘ich L·I = R	Nazorat chorasi	Qoldiq L·I = R′	Daraja
1	Hisob egallash	4·4 = 16	T1	2·4 = 8	O‘rta
2	Kanalni tinglash	3·5 = 15	T2	1·5 = 5	O‘rta
3	Ichki nusxalash	3·5 = 15	T3, T4	2·3 = 6	O‘rta
4	Huquq oshirish	2·5 = 10	T4, T8	1·4 = 4	Past

Ko‘rinib turibdiki, barcha tahdidlar “o‘rta” va undan past darajaga tushgan; qoldiq xavf qabul qilinadigan darajadan yuqori bo‘lsa, qo‘shimcha chora tanlanadi yoki xavf tashkilot rahbariyati tomonidan ongli ravishda qabul qilinadi.

Xavfni qabul qilish mezonlari oldindan belgilanadi [11]. Odatda jiddiy xavf qabul qilinmaydi va zudlik bilan kamaytiriladi; yuqori xavf belgilangan muddat ichida kamaytirish rejasi bilan yuritiladi; o‘rta xavf monitoring ostida qoldiriladi; past xavf esa qabul qilinadi. Qabul qilingan har bir qoldiq xavf mas’ul shaxs nomi va sanasi bilan reestrga yoziladi, shunda keyinchalik xavfsizlik darajasi pasayganda uning sababini aniqlash mumkin bo‘ladi. Shuningdek, baholarning shartli ekanini unutmaslik kerak: ehtimol va ta’sir qiymatlari tizim o‘zgarishi bilan o‘zgaradi, shuning uchun ular har yangilanishda qayta ko‘riladi.

Tahdidlar modeli hujjatlashtirilmasa, undan foydalanib bo‘lmaydi va uni yangilash qiyinlashadi. Shu sababli barcha tahdidlar yagona reestrda yuritiladi (8-jadval). Reestr har bir tahdid uchun javobgar shaxsni, nazorat chorasi holatini va qoldiq xavfni ko‘rsatadi, shuning uchun u ham xavfsizlik mutaxassislari, ham tizim ishlab chiquvchilari uchun yagona ma’lumot manbai bo‘ladi. Reestrdagi har bir yozuv himoya talabi bilan bog‘lanadi (izlanuvchanlik): talabsiz qolgan tahdid ham, tahdidsiz yozilgan talab ham modeldagi nuqson belgisi hisoblanadi.

8-jadval

Tahdidlar reestrining tavsiya etilgan maydonlari

t/r	Maydon	Mazmuni	Misol
1	Identifikator	Tahdidning noyob raqami	TH-01
2	Element va oqim	DFD dagi qaysi element yoki oqimga tegishli	Autentifikatsiya servisi, 1-oqim
3	STRIDE guruhi	Tahdid turi	S (soxtalashtirish)

4	Stsenariy	Tahdid qanday amalga oshirilishi	O‘g‘irlangan hisob bilan kirish
5	L, I, R	Ehtimol, ta’sir, xavf	4, 4, 16
6	Talab	Tahdidni yopuvchi talab raqami	T1
7	Javobgar va muddat	Chorani amalga oshiruvchi, sanasi	Tizim administratori, chorak oxirigacha
8	Holat va qoldiq xavf	Bajarilgan yoki jarayonda, R′	Bajarilgan, R′ = 8

Model ham chegaralarga ega: u faqat ko‘rib chiqilgan tahdidlarni qamrab oladi va yangi, oldindan noma’lum hujumlarni aniqlay olmaydi. Shu sababli tahdidlar modeli boshqa choralar bilan, ya’ni muntazam zaiflik sinovlari, jurnallarni monitoring qilish va hodisalarga javob mashqlari bilan to‘ldirilishi kerak.

Keyingi bosqichda aniqlangan talablar tizim modullariga taqsimlanadi va har bir modul uchun xavfsizlik topshirig‘i shakllantiriladi. Shundan so‘ng arxitektura qarori talablar bilan bog‘liq holda asoslanadi: har bir arxitektura elementi qaysi tahdidni yopishi izlanuvchanlik jadvali orqali ko‘rinib turadi. Bunday yondashuv xavfsizlikni tizimga keyinchalik qo‘shiladigan emas, loyihalashning ajralmas qismi sifatida ta’minlaydi.

Xulosa

Lokal bulutli tizim uchun tahdidlar modelini DFD, STRIDE, hujum daraxti va xavfni ehtimol-ta’sir bo‘yicha baholashga asoslab qurish tizim xavfsizligi talablarini asosli va tekshiriladigan shaklda belgilash imkonini beradi. Taklif etilgan uchta algoritm tahdidlarni aniqlashdan boshlab hujum yo‘llarini tahlil qilish, qoldiq xavfni baholash va modelni yangilashgacha bo‘lgan jarayonni qamrab oladi. Tahlil ichki tahdid, kalit boshqaruvi, tarmoq segmentatsiyasi va audit jurnalini alohida e’tiborga loyiq yo‘nalishlar sifatida ko‘rsatdi, sakkizta asosiy talab esa tizim arxitekturasini loyihalash uchun boshlang‘ich asos bo‘ladi.

Foydalanilgan adabiyotlar

1. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: opportunities and challenges. Information Sciences. 2015;305:357-383.

2. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011;34(1):1-11.

3. Shostack A. Threat modeling: designing for security. Indianapolis: Wiley; 2014. 624 p.

4. Kohnfelder L, Garg P. The threats to our products. Microsoft Interface. 1999.

5. Cloud Security Alliance. Top threats to cloud computing: Pandemic Eleven. CSA; 2022.

6. NIST SP 800-30 Rev. 1. Guide for conducting risk assessments. Gaithersburg: NIST; 2012.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: ISO; 2022.

8. NIST SP 800-53 Rev. 5. Security and privacy controls for information systems and organizations. Gaithersburg: NIST; 2020.

9. ISO/IEC 27017:2015. Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Geneva: ISO; 2015.

10. NIST SP 800-63B. Digital identity guidelines: authentication and lifecycle management. Gaithersburg: NIST; 2017.

11. Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture. NIST SP 800-207. Gaithersburg: NIST; 2020.

SUN’IY INTELLEKT YORDAMIDA TARMOQ KIBERHUJUMLARINI ANIQLASH: CIC-IDS2017 TO‘PLAMIDA RANDOM FOREST MODELINI BAHOLASH

Jaxongirov M.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada tarmoq oqimlari xususiyatlari asosida kiberhujumlarni aniqlashda mashinaviy o‘qitish usullarini qo‘llash masalasi ko‘rib chiqiladi. CIC-IDS2017 ochiq to‘plami oshkora tozalash protokoli asosida qayta ishlandi (2 517 883 ta oqim, 15 sinf) va 100 ta daraxtli Random Forest modeli ko‘p sinfli tasniflash uchun o‘qitildi. Test to‘plamida umumiy aniqlik 0,9982, macro-F1 esa 0,8614 ni tashkil etdi; hujum va normal trafikni ajratishda recall 0,9949, noto‘g‘ri ijobiy aniqlash ulushi 0,073% bo‘ldi. Xatolar tahlili yuqori umumiy aniqlik kam uchraydigan sinflar (Bot, XSS, SQL Injection, Infiltration) bo‘yicha past sifatni yashirishini ko‘rsatdi va modelni sinflar kesimidagi ko‘rsatkichlar bilan baholash zarurligini asosladi.

Kalit so‘zlar: kiberxavfsizlik, hujumlarni aniqlash tizimi, mashinaviy o‘qitish, Random Forest, tarmoq trafigi, CIC-IDS2017, sinflar nomutanosibligi.

Аннотация. В статье рассматривается применение методов машинного обучения для обнаружения кибератак по признакам сетевых потоков. Открытый набор данных CIC-IDS2017 обработан по прозрачному протоколу очистки (2 517 883 потока, 15 классов), модель Random Forest из 100 деревьев обучена для многоклассовой классификации. На тестовой выборке общая точность составила 0,9982, macro-F1 - 0,8614; при разделении атак и нормального трафика полнота (recall) равна 0,9949, доля ложноположительных срабатываний - 0,073 %. Анализ ошибок показал, что высокая общая точность скрывает низкое качество распознавания редких классов (Bot, XSS, SQL Injection, Infiltration), что обосновывает необходимость оценки модели по показателям для каждого класса.

Ключевые слова: кибербезопасность, система обнаружения вторжений, машинное обучение, Random Forest, сетевой трафик, CIC-IDS2017, несбалансированность классов.

Kirish

Raqamli xizmatlar, bulutli infratuzilmalar va masofaviy ulanishlarning kengayishi tarmoqqa qaratilgan hujumlar sonini va xilma-xilligini oshirmoqda. An’anaviy hujumlarni aniqlash tizimlari (IDS) asosan ma’lum hujum signaturalari va qoidalariga tayanadi: ular ma’lum tahdidlarni ishonchli aniqlaydi, biroq o‘zgartirilgan yoki yangi hujumlarga sekin moslashadi. Shu sababli tarmoq oqimlarining statistik xususiyatlaridan normal va zararli faoliyat o‘rtasidagi farqni o‘rganadigan mashinaviy o‘qitish usullari faol tadqiq etilmoqda [1, 3].

Ochiq ma’lumotlar to‘plamlarida e’lon qilinayotgan natijalarning ko‘pchiligi 99% dan yuqori aniqlikni ko‘rsatadi. Ammo bunday natijalar sinflar nomutanosibligi, takroriy yozuvlar va baholash usulidagi kamchiliklar tufayli ko‘pincha ortiqcha optimistik bo‘ladi [4, 5]; xususan, CIC-IDS2017 to‘plamida yorliqlash va oqimlarni shakllantirishdagi xatolar aniqlangan [4].

Tadqiqotning maqsadi – CIC-IDS2017 to‘plamida Random Forest modelini takrorlanadigan metodika asosida baholash va umumiy aniqlik ortida yashiringan xatolar tuzilmasini aniqlash. Ishning hissasi: (1) ma’lumotlarni tozalashning har bir bosqichi miqdoriy ko‘rsatilgan oshkora protokol; (2) ko‘p sinfli va ikki sinfli baholash natijalari; (3) eng ko‘p uchraydigan xatolar va metodik cheklovlar tahlili.

Ma’lumotlar to‘plami va metodika

Tajribada Kanada kiberxavfsizlik instituti tomonidan yaratilgan CIC-IDS2017 to‘plamidan foydalanildi. Unda normal trafik bilan birga DoS/DDoS, brute-force, botnet, veb-hujum, port skanerlash va infiltratsiya hujumlari CICFlowMeter vositasi yordamida olingan oqim xususiyatlari ko‘rinishida berilgan [1]. Ma’lumotlarga ishlov berish quyidagi bosqichlarda bajarildi:

1) MachineLearningCSV papkasidagi 8 ta CSV fayl birlashtirildi (2 830 743 ta yozuv, 78 ta xususiyat va yorliq), ustun nomlaridagi ortiqcha bo‘shliqlar va veb-hujum yorliqlaridagi buzilgan belgilar tuzatildi;

2) cheksiz (Inf) yoki yetishmayotgan (NaN) qiymatli 2 867 ta hamda mazmunan yaroqsiz manfiy qiymatli (masalan, oqim davomiyligi) 2 925 ta yozuv olib tashlandi; Init_Win_bytes ustunlaridagi −1 qiymati «oyna o‘lchami mavjud emas» ma’nosini bildirgani uchun saqlandi;

3) Fwd Header Length ustunining aynan nusxasi va bitta qiymatli 8 ta ustun chiqarildi, natijada 69 ta raqamli xususiyat qoldi; IP manzil va vaqt tamg‘asi kabi identifikatorlar ishlatilmadi;

4) 307 068 ta takroriy yozuv olib tashlandi, natijada 2 517 883 ta yozuv qoldi;

5) ma’lumotlar sinflar nisbatini saqlagan holda (stratifikatsiya) 80/20 nisbatda o‘qitish (2 014 306 ta) va test (503 577 ta) to‘plamlariga ajratildi (random_state = 42).

Model sifatida Random Forest tanlandi: u bootstrap tanlanmalarda o‘qitilgan ko‘plab qaror daraxtlarining ovozlarini birlashtiradi, jadval ko‘rinishidagi xususiyatlar bilan yaxshi ishlaydi va xususiyatlarni masshtablashni talab qilmaydi [2]. Model Python tilida scikit-learn (1.9.1) kutubxonasi yordamida n_estimators = 100, random_state = 42 sozlamalari bilan o‘qitildi; class_weight standart qiymatda qoldirildi, gipersozlamalar tanlanmadi [6]. Yakuniy ko‘rsatkichlar faqat model tanlashda ishlatilmagan test qismida hisoblandi.

Baholash mezonlari

Hujum ijobiy sinf deb olinganda quyidagi ko‘rsatkichlar hisoblandi:

$$\text{Precision} = TP / (TP + FP), \qquad \text{Recall} = TP / (TP + FN), \tag{1}$$

$$F1 = 2 \cdot \text{Precision} \cdot \text{Recall} / (\text{Precision} + \text{Recall}), \tag{2}$$

bu yerda TP – to‘g‘ri aniqlangan hujum, FP – hujum deb belgilangan normal yozuv, FN – aniqlanmay qolgan hujum. Ko‘p sinfli holatda macro-F1 barcha sinflar F1 qiymatlarining oddiy o‘rtachasi bo‘lib, kam uchraydigan sinflarga ham teng vazn beradi. Ikki sinfli ko‘rsatkichlar ko‘p sinfli bashoratlardan BENIGN dan boshqa barcha sinflarni «hujum» deb birlashtirish orqali olindi. Qo‘shimcha ravishda noto‘g‘ri ijobiy aniqlash ulushi FPR = FP / (FP + TN) hisoblandi, chunki aynan u xavfsizlik operatorlarining ish yukini belgilaydi [5].

Tajriba natijalari

Tozalashdan keyingi sinflar taqsimoti va test natijalari 1-jadvalda keltirilgan. Takroriy yozuvlar sinflar bo‘yicha notekis taqsimlangan: SSH-Patator yozuvlarining 45,5%, PortScan yozuvlarining 42,9% olib tashlandi, DDoS uchun bu ulush atigi 0,02% bo‘ldi. Test to‘plamining 83,1% ini normal trafik tashkil etadi.

1-jadval

Sinflar bo‘yicha yozuvlar soni va test natijalari

Sinf	Tozalashdan keyin	Test namunalari	Precision	Recall	F1
BENIGN	2 092 335	418 467	0,9990	0,9993	0,9991
DoS Hulk	172 688	34 538	0,9975	0,9975	0,9975
DDoS	127 995	25 599	0,9998	0,9996	0,9997

Sinf	Tozalashdan keyin	Test namunalari	Precision	Recall	F1
PortScan	90 694	18 139	0,9896	0,9888	0,9892
DoS GoldenEye	10 281	2 056	0,9990	0,9937	0,9963
FTP-Patator	5 927	1 186	0,9992	1,0000	0,9996
DoS slowloris	5 385	1 077	0,9926	0,9916	0,9921
DoS Slowhttptest	5 228	1 046	0,9923	0,9904	0,9914
SSH-Patator	3 217	643	1,0000	0,9922	0,9961
Bot	1 948	390	0,8794	0,7103	0,7858
Web Attack – Brute Force	1 470	294	0,7360	0,8061	0,7695
Web Attack – XSS	652	130	0,4000	0,2923	0,3378
Infiltration*	35	7	0,8000	0,5714	0,6667
Web Attack – Sql Injection*	21	4	1,0000	0,2500	0,4000
Heartbleed*	7	1	1,0000	1,0000	1,0000
Jami / macro o‘rtacha	2 517 883	503 577	0,9190	0,8389	0,8614
Vaznli o‘rtacha	–	–	0,9982	0,9982	0,9982

Ko‘p sinfli tasnifda umumiy aniqlik va weighted-F1 0,9982, macro-F1 esa 0,8614 bo‘ldi. To‘qqizta sinfda (BENIGN, DoS/DDoS turlari, Patator hujumlari, PortScan) F1 0,98 dan yuqori; eng past natijalar XSS (0,3378), SQL Injection (0,4000), Infiltration (0,6667), Brute Force (0,7695) va Bot (0,7858) sinflarida kuzatildi. Ikki sinfli ko‘rinishdagi chalkashlik matritsasi 2-jadvalda berilgan: precision 0,9964, recall 0,9949, F1 0,9957, FPR esa 0,0729% (418 467 ta normal yozuvdan 305 tasi).

2-jadval

Ikki sinfli chalkashlik matritsasi (test to‘plami)

Haqiqiy \ Bashorat	BENIGN	Hujum	Jami
BENIGN	418 162 (TN)	305 (FP)	418 467
Hujum	431 (FN)	84 679 (TP)	85 110

Xatolar tahlili shuni ko‘rsatdi: aniqlanmay qolgan 431 ta hujumning 388 tasi (90,0%) uchta sinfga – PortScan (194), Bot (113) va DoS Hulk (81) – to‘g‘ri keladi; 305 ta noto‘g‘ri ogohlantirishning 298 tasi (97,7%) normal trafikning aynan shu sinflar deb belgilanishidan iborat (PortScan – 188, DoS Hulk – 72, Bot – 38). PortScan va BENIGN o‘rtasidagi chalkashlik ikki yo‘nalishda deyarli teng (194 va 188), bu qisqa skanerlash oqimlarining oqim darajasidagi statistikasi normal qisqa ulanishlarga yaqinligini ko‘rsatadi. Veb-hujumlar ichida XSS yozuvlarining 83 tasi (63,8%) Brute Force deb, Brute Force yozuvlarining 55 tasi (18,7%) XSS deb tasniflangan; ikkala hujum ham bitta veb-ilovaga yuborilgan HTTP so‘rovlari ketma-ketligi bo‘lgani uchun ularning oqim xususiyatlari o‘xshash bo‘lishi mumkin.

Random Forest hisoblagan xususiyat muhimligi bo‘yicha birinchi o‘rinlarni paket uzunligi statistikasi egalladi: Packet Length Variance (0,0735), Bwd Packet Length Std (0,0717), Packet Length Std (0,0653), Avg Bwd Segment Size (0,0554). Bu xususiyatlarning bir qismi o‘zaro funksional bog‘liq bo‘lgani uchun muhimlik ular o‘rtasida taqsimlanadi; natija sababiy bog‘liqlikni emas, faqat model qaysi xususiyatlardan ko‘proq foydalanganini ko‘rsatadi.

Muhokama va cheklovlar

Birinchidan, normal trafik ulushi yuqori bo‘lgani sababli umumiy aniqlik (0,9982) hujum sinflaridagi sifatni aks ettirmaydi: macro-F1 bilan farq 0,137 ni tashkil etadi. Ikkinchidan, Heartbleed (1 ta), SQL Injection (4 ta) va Infiltration (7 ta) sinflari test to‘plamida juda kam namunaga ega, ularning ko‘rsatkichlari (jumladan, Heartbleed uchun F1 = 1,0) tasodifiy xarakterga ega. Uchinchidan, natijalar bitta tasodifiy ajratishga asoslangan; kross-validatsiya o‘tkazilmagani sababli ko‘rsatkichlar dispersiyasi baholanmagan. To‘rtinchidan, tasodifiy ajratishda bir hujum seansining o‘xshash oqimlari ikkala to‘plamga tushishi mumkin; takroriy yozuvlarni olib tashlash bu xavfni kamaytiradi, lekin bartaraf etmaydi, shuning uchun natijalar optimistik baho hisoblanadi [5]. Beshinchidan, xususiyatlari bir xil, ammo yorliqlari turlicha bo‘lgan 1 394 ta yozuv saqlab qolingan, CIC-IDS2017 yorliqlashida esa ma’lum xatolar mavjud [4]; laboratoriya muhitida yaratilgan to‘plam natijalarini real tarmoqqa bevosita ko‘chirib bo‘lmaydi.

Xulosa

Tajriba Random Forest modeli CIC-IDS2017 to‘plamida normal trafik va hujumlarni yuqori sifat bilan ajratishini ko‘rsatdi (recall 0,9949, precision 0,9964, FPR 0,073%). Biroq ko‘p sinfli tasnifda macro-F1 (0,8614) umumiy aniqlikdan sezilarli past bo‘lib, xatolarning asosiy qismi PortScan – BENIGN, Bot – BENIGN va XSS – Brute Force juftliklarida to‘plangan. Demak, hujumlarni aniqlash modellarini faqat accuracy bilan emas, sinflar kesimidagi precision, recall, F1 va mutlaq xatolar soni orqali baholash zarur. Keyingi bosqichda sinflar og‘irligini hisobga olish (class_weight), stratifikatsiyalangan kross-validatsiya hamda kunlar bo‘yicha ajratilgan mustaqil test o‘tkazish rejalashtirilgan.

Foydalanilgan adabiyotlar

1. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – P. 108–116.

2. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32.

3. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, No. 2. – P. 1153–1176.

4. Engelen G., Rimmer V., Joosen W. Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study // IEEE Security and Privacy Workshops (SPW). – 2021. – P. 7–12.

5. Arp D., Quiring E., Pendlebury F. et al. Dos and Don’ts of Machine Learning in Computer Security // Proceedings of the 31st USENIX Security Symposium. – 2022. – P. 3971–3988.

6. Pedregosa F., Varoquaux G., Gramfort A. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. – 2011. – Vol. 12. – P. 2825–2830.

AXBOROT TIZIMLARI ANOMALIYALARINI SUN'IY IMMUN TIZIMLAR ASOSIDA ANIQLASH ALGORITMI

Usmanbayev D.Sh.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti.

Annotatsiya: Ushbu maqolada axborot tizimiga tarmoqdan bo‘ladigan tahdidlar, hujumlarni amalga oshirish bosqichlari va aniqlash usullari, suqilib kirishlarni aniqlash va bartaraf etish tizimlari tadqiq va tahlil qilingan. Tahlil natijasiga ko‘ra, su'niy immun tizimiga asoslangan anomaliyalarni aniqlash tizimidan foydalanish qulayligi hamda samaradorligi yuqoriligi bilan ajralib turishi aniqlandi. Anomaliyalarini sun'iy immun tizimlar asosida aniqlash mexanizm va algoritmi tadqiq etildi.

Kalit so‘zlar: sun'iy immun tizimlar, suqilib kirishlarni aniqlash tizimi, suqilib bartaraf etish tizimi, ma'lumotlar to‘plami, NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset.

Abstract: This article examines and analyzes network-based threats to information systems, the stages of executing attacks, methods for their detection, and systems for identifying and mitigating intrusions. The analysis indicates that anomaly detection systems based on artificial immune systems are particularly advantageous due to their ease of use and high effectiveness. Furthermore, the mechanisms and algorithms for detecting anomalies using artificial immune systems were investigated.

Key words: artificial immune system, intrusion detection system, prevention detection system, dataset, NSL-KDD ISCX Dataset, CSIC 2010 Dataset, Enron Dataset.

Kirish

Tarmoq trafigini tasniflash jarayonida dolzarb muammolardan biri anomal so‘rovlarni aniqlash hisoblanadi, ushbu masalalarni hal qilishda mashinali o‘qitishga asoslangan anomaliyalarni aniqlash tizimlari yuqori samaradorlikni ko‘rsatmoqda. Yangi qo‘llanilayotgan usullar va texnologiyalarni ishonchliligi va samaradorligi, hamda ularni real vaqt rejimida amalga oshirish bilan bog‘liq masalalar noaniq bo‘lib qolmoqda, mashinali o‘qitish texnologiyasiga asoslangan istiqbolli yo‘nalishlardan biri sun'iy immun tizimlarini qo‘llagan holda suqilib kirishlarni aniqlash tizimini ishlab chiqish dolzarb hisoblanadi.

Anomaliyalarni aniqlashda foydalanilgan usullar, tizim ishida o‘zgarishlarga olib keluvchi jarayonlar tajovuzkor tomonidan amalga oshirilmayotganligini aniqlashga yo‘naltirilgan. Anomaliyalar qidiruv usullari quyidagi jadvallarda ko‘rsatilgan.

Usullar ikki guruhga ajratiladi: nazorat ostidagi ta'lim bilan amalga oshiriladigan (“o‘qituvchi yordamida o‘qitish”) va nazoratsiz ta'lim orqali amalga oshiriladigan (“o‘qituvchi yordamidamisiz o‘qitish”). Ular orasidagi asosiy farq nazorat ostidagi ta'lim usullarida baxolashni belgilangan hususiyatlaridan foydalaniladi va o‘qitish vaqti belgilanadi.

Nazoratsiz ta'limda baxolash hususiyatlari vaqt davomida o‘zgarishi mumkin, o‘qitish jarayoni doimiy amalga oshiriladi.

Ikkinchi yo‘nalishning maqsadi (suqilib kirishlarni aniqlash) – suqilib kirishni amalga oshirish bosqichi sifatida aniqlangan (xavfsizlik administrator yoki IDSni o‘qitish vqtidagi ekspert)lardan, hodisalar ketma ketligini qidirsih. Suqilib kirishlarni qidiruv usullari jadvalda ko‘rsatilgan. Hozirgi kunda, faqat nazorat ostidagi ta'lim usuli farqlanadi.

Hozirgi paytda amalga oshirilgan IDSlardagi usullar obrazlarni aniqlashning umumiy g‘oyalariga asoslanadi. Ularga ko‘ra, ekspert bahosi asosida anomaliyani aniqlash uchun normal faoliyat olib borayotgan axborot tizimini obrazi shakllantiriladi. Uning o‘zgarishi tizimining anomal faoliyat olib borayotganini bildiradi. Anomaliya aniqlangandan va uning darajasi baxolangandan so‘ng o‘zgarishning tabiati haqida ma’lumotlar shakllantiriladi: ular suqilib kirishning oqibatlarimi yoki ruxsat etilgan harakatlarmi. Suqilib kirishlarni aniqlash uchun obraz(signatura)lardan foydalaniladi, lekin bunda xujumchining oldindan ma’lum bo‘lgan harakatlarigina bartaraf etiladi.

1-jadval

Anomaliyalarni aniqlash - nazorat ostidagi ta’lim

Aniqlash usullari	Foydalaniladigan tizimlar	Usullar tavsifi
Qoidalarni modellashtirish	W & S	Aniqlash tizimi, o‘quv jarayoni davomida tizimining normal holatini ifodolovchi qoidalar majmuini shakllantiradi. Ruxsatsiz harakatlarni qidiruv bosqichida, tizim olingan qoidalardan foydalanadi va yetarlicha muvofiqlik aniqlanmasa anomal holat aniqlanganligi haqida signal beradi.
Tasvirlovchi statistika	IDES, NIDES, EMERLAND, JiNao, HayStack	O‘qitish himoya qilinayotgan tizimning ko‘plab ko‘rsatkichlarini oddiy tasvirlovchi statistikadan maxsus strukturaga jamlashga asoslanadi. Anomaliyalarni aniqlash uchun ikki vektor ko‘rsatkichlar -joriy va saqlangan qiymatar o‘rtasidagi “masofa” hisoblanadi. Olingan masofa yetarlicha katta bo‘lsa tizimdagi holat anomaliya hisoblanadi.
Neyron tarmoqlar	Hyperview	Ishlatiladigan neyron tarmoqlarning tuzilishi turlicha. Lekin barcha ta’lim berish hollari, tizimining normal holatini ifodalovchi ma’lumotlari asosida amalga oshiriladi. Olingan neyron tarmoq keyinchalik tizimnning anomaligini baholash uchun ishlatiladi. Neyron tarmog‘ining chiqishdagi ma’lumotlari anmaliya borligini bildiradi.

2-jadval

Anomaliyalarni aniqlash - nazoratsiz ta’lim orqali

Aniqlash usullari	Foydalaniladigan tizimlar	Usullar tavsifi
Ko‘plab holatlarni modellashtirish	DPEM, JANUS, Bro	Tiziming normal ko‘rinishi, chegaralangan holatlar va ular orasidagi o‘tish majmui ko‘rinishida tasvirlanadi.
Tasvirlovchi statistika	MIDAS, NADIR, Haystack, NSM	Nazorat ostidagi ta’lim usuliga o‘xshash.

3-jadval

Ruxsat etilmagan hatti xarakatlarni aniqlash - nazorat ostidagi ta’lim

Aniqlash usullari	Foydalaniladigan tizimlar	Usullar tavsifi

Hollatlarni modellashtirish	USTAT, IDIOT	Suqilib kirish holat ketma-ketligi ko‘rinishida tasvirlanadi, holat - himoya qilinayotgan tizimning baholash hususiyatlarining qilymatlar vektori. Ushbu ketma-ketlikning borligi suqilib kirish mavjudligi uchun zarur va yetarli shart. Suqilib kirishni tasvirlashni asosan ikki usulini mavjud: 1) hodisalarni oddiy zanjir ko‘rinishida; 2) Petr tarmoqlaridan foydalanib, tugunlar - hodisalar.
Ekspert tizimlar	NIDES, EMERLAND, MIDAS, DIDS	Ekspert tizimlar suqilib kirish jarayonini turli qoidalar majmui ko‘rinishida tasvirlaydi. Tez-tez ishlab chiqarish tizimlari ishlatiladi.
Qoidalarni modellashtirish	NADIR, HayStack, JiNao, ASAX, Bro	Ekspert tzimilarining oddiy variant.
Sintaktik tahlil	NSM	Aniqlash tizimi tomonidan, quyi tizimlar va himoya qilinayotgan kompleks tizimlari o‘rtasida uzatiladigan simvollar kombinatsiyasini aniqlash maqsadida ularni sintaktik qismalrga ajratiladi.

Suqulib kirishlarni aniqlash tizimlarini rivojlantirishning yangi yo‘nalishidan biri sun’iy immun tizimlari (SIT) asosida adaptiv algoritmlarni ishlab chiqish hisoblanadi. Ushbu ishda tavsiya etilgan mashinali o‘qitish modellaridan biri sun’iy immun tizimiga (SIT) asoslangan model sanaladi. Uning funksional va dasturiy qo‘shimchalarini tavsiflashdan oldin, asosiy talablarni shakllantirish zarur, ularning bajarilishi tizim samaradorligining zarur darajasini ta’minlashga imkon beradi.

Sun’iy immun tizimiga qo‘yiladigan talablar

Sun’iy immun tizimi uchun umumlashtirilgan tamoyillardan kelib chiqqan holda to‘plamlarni tasniflash muammosini hal qilishni amalga oshiradigan sun’iy immun tizimi quyida keltirilgan talablarga javob berishi kerak:

- tahlil qilinadigan ob’ektlarni saqlash. Tasniflashning vazifasi ma’lumotlarni saqlashning yagona formatini nazarda tutadi, uning asosida sun’iy immun tizimlari o'qitiladi, hamda uni keyinchalik ishga tushiriladi.

- ma’lumotlar unifikatsiyasi. Axborot almashish va uzatish tizimlarining ko'p turlari mavjud. Loyihalashtiriladigan sun’iy immun tizimi uchun tahlil qilinadigan format turini farqi bo'lmasligi lozim: TCP protokoli orqali yoki HTTP protokoli orqali kelgan ma’lumotlar bloki bo'lishidan qat’iy nazar.

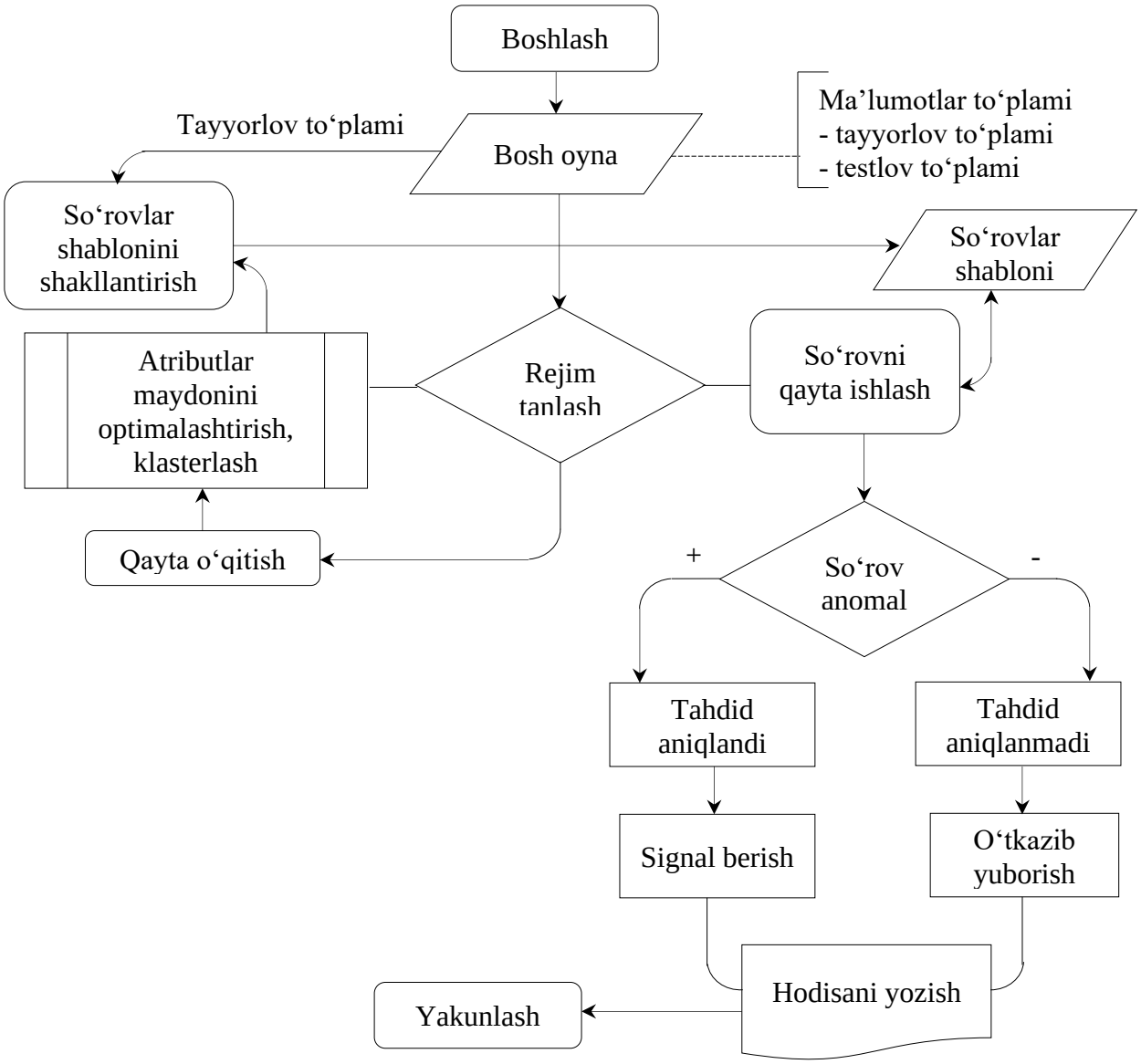
- ma’lumotlarni qayta ishlashning ko‘lami. Loyihalashtirilgan tizim kichik hajmdagi ma’lumotlarni ham, ularning massivlarini ham teng darajada qayta ishlashi kerak. Ekvivalentlik qayta ishlash tamoyillaridagi bir xillikni anglatadi.

- tuzilmaviy ko‘lamlik. Sun’iy immun tizimini tashkil etuvchi ko'p sonli elementlarning mavjudligi butun axborot tizimi va xususan suqulib kirishni aniqlash tizimi doirasida hisoblashlarni parallellashtirish muammosini hal qilishni nazarda tutadi.

- shovqinlarga bardoshlilik. Sun’iy immun tizimi tahlil qilinadigan ob'ektlardan foydali belgilarni (xususiyatlarni) sifatli ajratib olishi va belgilangan vazifalar bo'yicha ma’lumotlarni samarali tasniflashi lozim.

Taklif etilgan tizim ikkita rejimda ishlaydi - o‘qitish va tasniflash.

Birinchi holatda, taklif qilingan ma’lumotlar to‘plamlari bo‘yicha bir nechta modellarni o‘qitilish amalga oshiriladi, ikkinchi holatda, tizimning to‘g‘ri ishlashini tekshiradigan so‘rovlar tahlili. Tizimning ishlashi natijasi yakuniy mashinali o‘qitish modeli hisoblanadi, o‘qitish tanlanmasiga kiritilmagan misollarni tahlil qilishda eng yaxshi natijalarni ko‘rsatdi - ushbu vazifani korrelyatsiya bloki amalga oshiradi.



1-rasm. SIT ga asoslangan hujumni aniqlash tizimi algoritmi

O‘qitish va testlash formal algoritmi quyidagi qadamlar ketma-ketlikka ega:

1 - qadam. Tadqiq qilingan so‘rovlar to‘plami olinadi, ikkita kichik to‘plamga (namunalarga) bo‘linadi: o‘qitish va test.

2 - qadam. So‘rovlar kortejlari atributlar fazosi bilan shakllantiriladi.

3 - qadam. Kortejlarni binarlash va ulardan to‘g‘ri burchakli A matritsani yaratish.

4 - qadam. Singulyar bo‘lish usulidan foydalanib, 3 - bosqichda olingan ma’lumotlardan iborat bo‘lgan A matritsasi olinadi, atributlarning muhim kombinatsiyalari shakllantiriladi.

5 - qadam. Muhim atributlar ajratiladi, klaster markazlarini alohida to‘plamga (G gen kutubxonasi) ajratgan holda so‘rovlarni klasterlash jarayoni amalga oshiriladi.

6 - qadam. 5 - bosqichda olingan so‘rovlar to‘plami va sun’iy immun tizimi yordamida anomal so‘rovlarning yangi to‘plami (G to‘plami) hosil qilinadi.

7 - qadam. Singulyar taqsimlashni teskari akslantirishdan, shuningdek round yaxlitlash usulidan foydalanib, xususiyatlarning atribut fazosidan G va G' to‘plamlarning elementlari boshlang‘ich atributli (1-qadam kabi) anomal so‘rovlarga almashtiriladi.

8 - qadam. Anomal so‘rovlarining test to‘plamidan foydalanib, algoritmning ishlash samaradorligi baholanadi.

Xulosa

Xulosa qilib shuni ta’kidlash mumkinki mazkur maqolada hujumlarni va anomaliyalarni aniqlash tizimining axborot xavfsizligini ta’minlashdagi roli, uning afzalliklari va kamchiliklari tahlili keltirilgan. Bundan tashqari, taklif etilayotgan adaptiv algoritm bo‘yicha ishlaydigan suqilib kirishlarni aniqlash tizimlari, shu jumladan sun’iy immun tizimi korxona lokal taqmoq tarkibida qo‘llanilishi mumkinligini ta’kidlash mumkin.

Foydalanilgan adabiyotlar

1. Usmanbayev D. Improving and evaluating methods network attack anomaly detection //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – C. 1-5.

2. Bozorov, Suhrobjon, and Doniyor Usmanbayev. Balanced ANN and majority based voting approach for building IDS. AIP Conference Proceedings. Vol. 3377. No. 1. AIP Publishing LLC, 2025.

3. Usmanbayev D. S. Kiberxavfsizlik: IT Infratuzilmasini Himoya Qilishning Zamonaviy Usullari //Green Economy and Development. – T. 3. – №. 5. – C. 665738.

4. Mirpulatovich, K. M., Zakirovna, T. N., Gulnora, K., & Ismoilovna, U. D. S. (2019). Methodology for Developing a Mandatory Security Policy Based on Two Value Chains. Methodology, 6(11).

5. Shuxratovich, U. D. Kaspersky Threat Intelligence Services Analysis. Galaxy International Interdisciplinary Research Journal, 13(1), 90-93.

6. Shukhratovich, Usmanbayev D. Specific Features Of The Structure And Operation Of Network Attack Detection Systems. JournalNX, vol. 8, no. 04, 2022, pp. 224-228, doi:10.17605/OSF.IO/EYNQ2.

SANOAT TARMOQLARIDA KIBERXAVFSIZLIK XAVFLARINI MINIMALLASHTIRISH MODELI VA ALGORITMI

G‘ulomov Sh.R., Mirzoyev A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada sanoat boshqaruv tizimlari (ICS/SCADA) va sanoat buyumlar interneti (IIoT) tarmoqlarida kiberxavfsizlik xavflarini baholash va kamaytirish masalasi ko‘rib chiqiladi. Tarmoq hujum grafi ko‘rinishida ifodalanib, tugunlar zaifligi, tahdidning tugunga yetib borish ehtimoli va hujum turiga bog‘liq zarar yagona qoldiq xavf funksiyasida birlashtirilgan. Himoya choralarini tanlash kechikish, qurilma resurslari, byudjet va texnologik jarayon uzluksizligi cheklovlari ostidagi optimallashtirish masalasi sifatida qo‘yilgan va uning NP-murakkabligi asoslangan. Masalani tez yechish uchun passiv monitoring, anomaliyalarni aniqlash va har qadamda eng foydali himoya chorasini tanlashga asoslangan besh bosqichli algoritm taklif etilgan. Shartli misolda algoritm xavfni 83,5 % ga kamaytirib, barcha variantlarni tekshirish orqali topilgan optimal yechimga (85,4 %) yaqinlashdi.

Kalit so‘zlar: sanoat tarmoqlari, ICS, SCADA, IIoT, kiberxavfsizlik xavfi, hujum grafi, xavfni minimallashtirish, binar optimallashtirish, mikro-segmentatsiya, IEC 62443.

Аннотация. В статье рассматривается задача количественной оценки и минимизации рисков кибербезопасности в промышленных системах управления (ICS/SCADA) и сетях промышленного Интернета вещей (IIoT). Сеть представлена в виде графа атак, а уязвимость узлов, вероятность достижения узла угрозой и зависящий от типа атаки киберфизический ущерб объединены в единую функцию остаточного риска. Выбор мер защиты сформулирован как задача бинарной оптимизации при ограничениях на задержку реального времени, ресурсы узлов, бюджет и непрерывность технологического процесса; показана её NP-трудность. Для оперативного решения предложен пятиэтапный адаптивный алгоритм, основанный на пассивном мониторинге, обнаружении аномалий и жадной эвристике. На условном расчётном примере алгоритм снизил исходный риск на 83,5 %, что близко к оптимальному решению, найденному полным перебором (85,4 %).

Ключевые слова: промышленные сети, ICS, SCADA, IIoT, киберриск, граф атак, минимизация рисков, бинарная оптимизация, микросегментация, IEC 62443.

Kirish

Sanoat 4.0 konsepsiyasi doirasida energetika, tog‘-kon, neft-gaz, kimyo sanoati va suv ta’minoti kabi muhim infratuzilma obyektlarining texnologik jarayonlarni boshqarish tizimlari korporativ tarmoqlar va bulutli platformalar bilan tobora ko‘proq integratsiyalashmoqda. IT va OT tarmoqlari konvergensiyasi masofaviy monitoring va uskunalar holatini bashoratlash imkonini bersa-da, ilgari fizik izolyatsiyalangan boshqaruv tarmoqlarini maqsadli (APT) hujumlar uchun ochiq qilib qo‘yadi [1, 2]. O‘zbekistonda muhim axborot infratuzilmasi obyektlarini himoya qilish masalalari “Kiberxavfsizlik to‘g‘risida”gi Qonun bilan tartibga solinadi [3].

Sanoat tarmoqlarida xavfsizlik ustuvorligi korporativ tizimlardan farq qiladi: birinchi o‘rinda jarayonning uzluksizligi (foydalanuvchanlik), keyin buyruq va telemetriya ma’lumotlarining yaxlitligi, so‘ngra maxfiylik turadi [1]. Modbus TCP, DNP3, IEC 60870-5-104 kabi keng tarqalgan protokollarning bazaviy versiyalarida kriptografik autentifikatsiya va yaxlitlik nazorati yo‘q. Himoyalangan yechimlar (DNP3 Secure Authentication, IEC 62351 standartlari,

OPC UA ning o‘rnatilgan xavfsizlik rejimlari) mavjud bo‘lsa-da, eski uskunalar ko‘pligi sababli ular amalda kam qo‘llaniladi. PLC, RTU va IED qurilmalari cheklangan hisoblash resursiga ega va 15–20 yil davomida ekspluatatsiya qilinadi, shu bois ularga og‘ir himoya vositalarini o‘rnatib bo‘lmaydi, tarmoqqa kiritilgan qo‘shimcha kechikish esa deterministik boshqaruv siklini buzishi mumkin.

Hujum graflari asosida xavfni baholash usullari [4, 5], mashinaviy o‘qitishga asoslangan ICS hujum detektorlari [6] hamda ularni sinash uchun stend va ma’lumotlar to‘plamlari [7] yetarlicha o‘rganilgan. Biroq himoya choralarini tanlashda sanoat tarmog‘ining real vaqt va resurs cheklovlari ko‘pincha hisobga olinmaydi. Ushbu ishning maqsadi - xavfni baholash va himoya choralarini tanlashni sanoat cheklovlari bilan birgalikda ifodalovchi matematik model hamda uni tezkor yechuvchi algoritmni taklif etishdan iborat. Ishning yangiligi shundaki, zaiflik bahosiga protokolning dizayn nuqsonlari ham kiritilgan, himoya choralarini tanlash esa kechikish, resurs, byudjet va texnologik uzluksizlik cheklovlari bilan yagona masala sifatida qo‘yilgan.

Asosiy qism. 1. Sanoat tarmog‘i sathlari va tahdidlar

Tahlil uchun Purdue referens arxitekturasi [8] va IEC 62443 standartining zona va kanal (zone/conduit) tushunchalari [9] asos qilib olindi (1-jadval). Quyi sathlarga yaqinlashgan sari vaqt talablari qat’iylashadi, muvaffaqiyatli hujumning fizik oqibatlari esa og‘irlashadi.

1-jadval

Sanoat tarmog‘i sathlari, protokollari va ularga xos tahdidlar

Purdue sathi	Qurilmalar	Protokollar	Xos tahdidlar
0 – fizik jarayon	datchiklar, aktuatorlar	4–20 mA, HART, IO-Link	signalni soxtalashtirish, fizik ta’sir
1 – bazaviy boshqaruv	PLC, RTU, IED	Modbus, PROFINET, DNP3, EtherNet/IP	buyruq in’yeksiyasi, PLC dasturini o‘zgartirish, replay
2 – supervizor boshqaruv	SCADA, HMI, muhandislik stansiyasi	OPC UA, IEC 60870-5-104, MMS	MITM (ARP spoofing), HMI da yolg‘on ma’lumot, DoS
3 – ishlab chiqarish operatsiyalari	MES, Historian	SQL, HTTPS, MQTT	ransomware, ruxsatsiz kirish
3.5 – DMZ	tarmoqlararo ekran, jump-server	SSH, RDP, VPN	hisob ma’lumotlarini o‘g‘irlash, lateral movement
4–5 – korporativ tarmoq	ERP, ofis tizimlari	HTTP(S), e-mail	fishing, dastlabki kirish nuqtasi

Xavfni minimallashtirishning matematik modeli

Tarmoqni yo‘naltirilgan graf $G = (\Omega, E)$ ko‘rinishida tasvirlaymiz: $\Omega = \{v_1, \ldots, v_n\}$ - tugunlar (PLC, RTU, HMI, SCADA serveri, shlyuzlar) to‘plami, E - ular orasidagi aloqa kanallari, $A = \{a_1, \ldots, a_m\}$ - tahdid turlari, $S = \{s_1, \ldots, s_K\}$ - himoya choralari. Quyida v_i tugun qisqacha i-tugun deb yuritiladi.

Har bir tugun uchun q_i - uni ekspluatatsiya qilish ehtimoli kiritiladi. CVSS bali zaiflik og‘irligini bildiradi, lekin ehtimol emas, shu bois ma’lum zaifliklar uchun EPSS kabi ehtimoliy baholar [10], protokolning dizayn nuqsonlari (masalan, autentifikatsiya yo‘qligi) uchun esa alohida d_i parametri qo‘llanadi. Zaifliklar o‘zaro mustaqil deb faraz qilinsa:

$$q_i = 1 - (1 - d_i) \prod_{c \in \mathrm{CVE}_i} (1 - p_c) \qquad (1)$$

bu yerda p_c - c-zaiflikning ekspluatatsiya qilinish ehtimoli, CVE_i - tugundagi ma’lum zaifliklar to‘plami. Natijada CVE qayd etilmagan, ammo autentifikatsiyasiz Modbus orqali boshqariladigan PLC ham nolga teng bo‘lmagan zaiflikka ega bo‘ladi.

a_j hujum i-tugunda muvaffaqiyatli amalga oshganda yetkaziladigan zarar hujum turiga bog‘liq bo‘ladi:

$$C_{ij} = w_1 C_{ij}^{\text{tech}} + w_2 C_{ij}^{\text{fin}} + w_3 C_{ij}^{\text{safe}} \quad (2)$$

bu yerda C^{tech} - jarayon to‘xtashidan kelib chiqadigan operatsion yo‘qotish, C^{fin} - uskunani tiklash xarajati, C^{safe} - xodimlar va atrof-muhit uchun xavf (har biri 0–100 shkalada); $w_1 + w_2 + w_3 = 1$ vaznlari korxona ekspertlari tomonidan, masalan, AHP usulida aniqlanadi.

Boshqaruv o‘zgaruvchisi sifatida binar matritsa $X = \|x_{ik}\|$ olinadi: agar k-chora i-tugunda yoki unga olib boruvchi kanalda qo‘llansa, $x_{ik} = 1$, aks holda $x_{ik} = 0$. $\eta_{jk} \in [0, 1)$ - k-choraning a_j hujumni neytrallash samaradorligi; choralar ta’siri o‘zaro mustaqil deb olinadi. U holda qoldiq xavf funksiyasi quyidagicha bo‘ladi:

$$R(X) = \sum_{i=1}^{n} \sum_{j=1}^{m} P_{ij}(X)\, q_i\, C_{ij} \prod_{k=1}^{K} (1 - \eta_{jk}\, x_{ik}) \quad (3)$$

bu yerda $P_{ij}(X)$ - a_j tahdidning hujum grafi bo‘ylab i-tugunga yetib borish ehtimoli bo‘lib, Bayes hujum grafi [5] yordamida hisoblanadi. U X ga bog‘liq: mikro-segmentatsiya grafdagi ayrim yo‘llarni uzadi va P_{ij} ni kamaytiradi.

Optimallashtirish masalasi quyidagicha shakllantiriladi:

$$\min_{X \in \{0,1\}^{n \times K}} R(X) \quad (4)$$

cheklovlar:

$$\sum_{i \in l} \sum_{k=1}^{K} \tau_{ik}\, x_{ik} \le \Delta t_l^{\max}, \ \forall l \in L \quad (5)$$

$$\sum_{k=1}^{K} r_{ik}\, x_{ik} \le r_i^{\max}, \ \forall i \in \Omega \quad (6)$$

$$\sum_{i=1}^{n} \sum_{k=1}^{K} c_{ik}\, x_{ik} \le B \quad (7)$$

$$\varphi_f(X) = 0, \ \forall f \in W \quad (8)$$

Bu yerda L - kritik boshqaruv konturlari to‘plami (har bir $l \in L$ kontur tarkibidagi tugunlar to‘plami), τ_{ik} - choraning konturga kiritadigan kechikishi (passiv choralar uchun $\tau_{ik} \approx 0$), r_{ik} va $r_i^{\max}$ - choraning tugundagi resurs sarfi va tugunning bo‘sh resursi, c_{ik} - narx, B - byudjet, W - legitim trafik oqimlari to‘plami; agar X konfiguratsiyasi f oqimni bloklasa, $\varphi_f(X) = 1$, aks holda 0. (8) shart himoya choralari texnologik jarayonni to‘xtatib qo‘ymasligini ta’minlaydi.

Bitta chora turi ($K = 1$) va o‘zgarmas P_{ij} bo‘lgan xususiy holda (3) funksiya X ga nisbatan chiziqli bo‘lib, (7) cheklov bilan birga klassik ryukzak (knapsack) masalasiga aylanadi. Demak, (4)–(8) masala NP-murakkab va uni real vaqtda aniq yechish o‘rniga evristik usul zarur.

Xavfni dinamik minimallashtirish algoritmi.

Algoritm besh bosqichdan iborat.

1-bosqich. Passiv inventarizatsiya. Kontrollerlar ishini buzmaslik uchun faol skanerlash qo‘llanilmaydi: kommutatorlarning SPAN portlaridan olingan trafik nusxasi asosida tugunlar, ular orasidagi aloqa matritsasi va legitim oqimlar to‘plami W aniqlanib, hujum grafi quriladi. Kam faol qurilmalar trafikda ko‘rinmasligi mumkinligi sababli natija aktivlar reestri bilan solishtiriladi.

2-bosqich. Protokol tahlili va anomaliyalarni aniqlash. DPI moduli Modbus va DNP3 paketlaridan funksiya kodlari (masalan, Modbus 0x06 va 0x10 yozish buyruqlari), registr manzillari va qiymatlarini ajratadi; shifrlangan OPC UA trafigida faqat meta-ma’lumotlar (seans parametrlari, chastota, hajm) tahlil qilinadi. Statistik anomaliyalar Isolation Forest [11], jarayon qiymatlari vaqt qatoridagi og‘ishlar esa LSTM-avtoenkoderning tiklash xatoligi bo‘yicha aniqlanadi. Chegaraviy qiymatlar normal trafikning validatsiya qismida ruxsat etilgan soxta signal darajasiga ko‘ra tanlanadi.

3-bosqich. Xavfni yangilash. Aniqlangan hodisalar asosida P_{ij} ehtimollari Bayes hujum grafida aposterior qayta hisoblanadi [5] va (3) bo‘yicha joriy xavf R topiladi.

4-bosqich. Himoya choralarini tanlash. Agar joriy xavf ruxsat etilgan darajadan oshsa ($R > R^{thr}$), ochko‘z evristika qo‘llanadi: har qadamda (5)–(8) cheklovlarni qanoatlantiruvchi (i, k) juftliklar uchun foydalilik koeffitsiyenti hisoblanadi:

$$U_{ik} = \Delta R_{ik} / (\tau_{ik}/\Delta t^{\max} + c_{ik}/B + \varepsilon) \quad (9)$$

bu yerda ΔR_{ik} - chora qo‘shilganda xavfning kamayishi (har tanlovdan keyin qayta hisoblanadi), Δt^{max} - kritik konturlar uchun ruxsat etilgan kechikishlarning eng kichigi, $\varepsilon > 0$ - nolga bo‘lishdan saqlovchi kichik son. Eng katta U_{ik} ga ega chora tanlanadi va jarayon xavf kamaymay qolguncha yoki mumkin bo‘lgan chora qolmaguncha davom etadi. Har qadamda ko‘pi bilan nK ta nomzod tekshiriladi, qadamlar soni ham nK dan oshmaydi, demak R funksiyasi ko‘pi bilan $O(n^2K^2)$ marta hisoblanadi. Tanlangan choralar SDN kontrolleri va zona chegaralaridagi sanoat ekranlari orqali qo‘llanadi.

Shuni hisobga olish kerakki, passiv monitoring hujumni faqat aniqlaydi va birinchi zararli paket nishonga yetib borishi mumkin. Shu sababli yozish buyruqlarini oq ro‘yxat asosida filtrlash kabi profilaktik choralar kanallarda oldindan (in-line) qo‘llanadi, aniqlashdan keyingi javob esa hujumning keyingi bosqichlarini to‘xtatishga xizmat qiladi. Aniqlashdan javobgacha bo‘lgan vaqt alohida ko‘rsatkich sifatida baholanishi lozim.

5-bosqich. Moslashish. Hodisa ma’lumotlari SIEM tizimiga uzatiladi, hujum grafi, η_{jk} baholari va anomaliya modellari yangilanadi.

4. Hisoblash misoli. Model va algoritm ishlashini ko‘rsatish uchun shartli misol ko‘rib chiqildi: 4 ta tugun (v_1 - muhandislik stansiyasi, v_2 - SCADA serveri, v_3 - nasos PLC si, v_4 - himoya klapani PLC si), 3 ta tahdid (a_1 - Modbus buyruq in’yeksiyasi, a_2 - MITM, a_3 - DoS) va 4 ta himoya chorasi (2-jadval). Ikki kritik kontur $\{v_2, v_3\}$ va $\{v_2, v_4\}$ uchun Δt^{max} = 0,6 ms, PLC larning bo‘sh resursi 25 %, kompyuterlarniki (v_1, v_2) 30 %, byudjet B = 24 shartli birlik. q = (0,62; 0,55; 0,80; 0,80), C_{ij} qiymatlari 30–95, P_{ij} esa 0,25–0,70 oralig‘ida shartli ravishda tanlandi. Soddalik uchun P_{ij} o‘zgarmas deb olinib, segmentatsiya ta’siri η orqali hisobga olindi, (8) shart esa barcha choralar uchun bajariladi deb faraz qilindi.

2-jadval.

Misoldagi himoya choralari parametrlari (ikki qiymat berilganda: kompyuter / PLC)

Himoya chorasi	η(a1)	η(a2)	η(a3)	τ, ms	Resurs, %	Narx
s1 – SDN mikro-segmentatsiya	0,40	0,50	0,60	0,05	5 / 0	2
s2 – passiv DPI + ML monitoring	0,55	0,45	0,40	0	0	2
s3 – yozish buyruqlari oq ro‘yxat filtri	0,70	0,20	0,30	0,30	10 / 0	3
s4 – yengil MAC-autentifikatsiya	0,80	0,85	0,10	0,10 / 0,45	10 / 40	2 / 3

Himoyasiz holatda xavf R_0 = 198,5 shartli birlikni tashkil etadi. Barcha 2^{16} = 65 536 variantni to‘liq saralash natijasida optimal yechim R^* = 29,1 topildi (xavf 85,4 % ga kamaydi). Ochko‘z algoritm 11 qadamda, xavf funksiyasini atigi 99 marta hisoblab, R = 32,8 natijaga erishdi (83,5 % kamayish), ya’ni optimaldan farqi 1,9 foiz punktni tashkil etdi. Farq shundan iboratki, algoritm dastlabki qadamlarda v_1 tugunida passiv monitoringni tanladi va byudjetning qolgan qismi v_4 dagi filtr uchun yetmay qoldi; bu ochko‘z yondashuvga xos kamchilikdir. Ikkala yechimda ham s_4 PLC larda tanlanmadi, chunki u (6) resurs cheklovini buzadi; bu og‘ir himoya vositalarini kontrollerlarga emas, kanal va shlyuzlarga joylashtirish zarurligini ko‘rsatadi. Konturlardagi qo‘shimcha kechikish 0,5 ms dan oshmadi.

Ta’kidlash joizki, bu misol algoritm mantiqini tushuntirish uchun xizmat qiladi va uning amaliy samaradorligini isbotlamaydi. Keyingi bosqichda model OpenPLC asosidagi sinov stendida hamda SWaT kabi ochiq ma’lumotlar to‘plamlarida [7, 12] tekshirilib, aniqlik, soxta signallar ulushi, maksimal kechikish va jitter ko‘rsatkichlari baholanishi rejalashtirilgan.

Xulosa

Olib borilgan tadqiqot natijasida quyidagi xulosalarga kelindi. Sanoat tarmoqlarida himoya choralarini tanlashda ularning samaradorligi bilan birga tarmoqqa kiritadigan kechikishi, qurilma resursiga va texnologik jarayon uzluksizligiga ta’sirini ham hisobga olish zarur. Taklif etilgan model tugun zaifligini (ma’lum CVE zaifliklari va protokol dizayn nuqsonlari), hujum turiga bog‘liq zararni va himoya choralari ta’sirini yagona qoldiq xavf funksiyasida birlashtiradi NP-murakkab bo‘lgani, ya’ni tugunlar soni ortganda barcha variantlarni tekshirish amalda imkonsiz bo‘lgani sababli, har qadamda eng foydali himoya chorasini tanlaydigan tezkor algoritm taklif etildi. Shartli misolda bu algoritm xavfni 83,5 % ga kamaytirdi, bu esa barcha variantlarni tekshirib topilgan eng yaxshi natijaga juda yaqin. Shuningdek, og‘ir himoya vositalarini PLC larga emas, tarmoq kanallari va shlyuzlarga joylashtirish maqsadga muvofiqligi aniqlandi. Olingan natijalarimdan O‘zbekistondagi muhim infratuzilma obyektlarida himoya choralarini rejalashtirishda foydalanish mumkin.

Foydalanilgan adabiyotlar

1. Stouffer K., Pease M., Tang C. et al. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. – Gaithersburg: NIST, 2023.

2. Humayed A., Lin J., Li F., Luo B. Cyber-physical systems security – a survey // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 6. – P. 1802–1831.

3. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764-son, 2022-yil 15-aprel.

4. Ou X., Govindavajhala S., Appel A.W. MulVAL: A logic-based network security analyzer // Proc. 14th USENIX Security Symposium. – 2005.

5. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using Bayesian attack graphs // IEEE Transactions on Dependable and Secure Computing. – 2012. – Vol. 9, No. 1. – P. 61–74.

6. Kravchik M., Shabtai A. Detecting cyber attacks in industrial control systems using convolutional neural networks // Proc. Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC). – ACM, 2018. – P. 72–83.

7. Conti M., Donadel D., Turrin F. A survey on industrial control system testbeds and datasets for security research // IEEE Communications Surveys & Tutorials. – 2021. – Vol. 23, No. 4. – P. 2248–2294.

8. Williams T.J. The Purdue enterprise reference architecture // Computers in Industry. – 1994. – Vol. 24, No. 2–3. – P. 141–158.

9. IEC 62443-3-2:2020. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design. – Geneva: IEC, 2020.

10. Jacobs J., Romanosky S., Edwards B., Adjerid I., Roytman M. Exploit Prediction Scoring System (EPSS) // Digital Threats: Research and Practice. – 2021. – Vol. 2, No. 3.

11. Liu F.T., Ting K.M., Zhou Z.-H. Isolation forest // Proc. 8th IEEE International Conference on Data Mining (ICDM). – 2008. – P. 413–422.

12. Goh J., Adepu S., Junejo K.N., Mathur A. A dataset to support research in the design of secure water treatment systems // Critical Information Infrastructures Security (CRITIS 2016). LNCS, vol. 10242. – Springer, 2017. – P. 88–99.

ZERO TRUST ARXITEKTURASI: PERIMETR HIMOYASIDAN UZLUKSIZ TEKSHIRUVGA O‘TISHNING DOLZARB MUAMMOLARI

Xolimtayeva I.U.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti,
Xamdamov D.B.
O‘R HX va MU Axborot-kommunikatsiya texnologiyalari va harbiy aloqa instituti

Annotatsiya. Maqolada an’anaviy perimetrga asoslangan himoya modelining bulutli, gibrid va masofaviy ish muhitidagi cheklovlari hamda Zero Trust (nol ishonch) arxitekturasiga o‘tish zarurati tahlil qilinadi. NIST SP 800-207 standarti tamoyillari va CISA yetuklik modeli asosida o‘tish jarayonidagi asosiy muammolar – eski tizimlarning mosligi, identifikatsiya infratuzilmasiga tushadigan yuklama, mikrosegmentatsiya va siyosatlarni loyihalash murakkabligi, uzluksiz monitoring uchun telemetriya, shuningdek tashkiliy va me’yoriy to‘siqlar tizimlashtiriladi. O‘zbekiston axborot tizimlari uchun bosqichma-bosqich o‘tish yo‘l xaritasi taklif etiladi.

Kalit so‘zlar: Zero Trust, nol ishonch arxitekturasi, perimetr himoyasi, uzluksiz tekshiruv, identifikatsiya va kirishni boshqarish, mikrosegmentatsiya, ko‘p faktorli autentifikatsiya, kiberxavfsizlik.

Аннотация. В статье анализируются ограничения традиционной периметровой модели защиты в облачной, гибридной и удалённой рабочей среде, а также необходимость перехода к архитектуре нулевого доверия (Zero Trust). На основе принципов стандарта NIST SP 800-207 и модели зрелости CISA систематизированы ключевые проблемы перехода: совместимость унаследованных систем, нагрузка на инфраструктуру идентификации, сложность микросегментации и проектирования политик, телеметрия для непрерывного мониторинга, а также организационные и нормативные барьеры. Предложена дорожная карта поэтапного перехода для информационных систем Узбекистана.

Ключевые слова: нулевое доверие, архитектура Zero Trust, защита периметра, непрерывная проверка, управление идентификацией и доступом, микросегментация, многофакторная аутентификация, кибербезопасность.

Kirish

Uzoq yillar davomida korporativ tarmoqlar himoyasi “qal’a va xandaq” tamoyiliga tayanib keldi: tashqi chegarada tarmoqlararo ekranlar, VPN-shlyuzlar va hujumlarni aniqlash tizimlari o‘rnatilib, ichki tarmoq ishonchli zona deb qabul qilindi. Bulutli xizmatlar, masofaviy ish, shaxsiy mobil qurilmalar va uchinchi tomon integratsiyalarining kengayishi natijasida bunday aniq chegara amalda yo‘qoldi. Perimetrni bir marta yorib o‘tgan yoki haqiqiy hisob ma’lumotlarini qo‘lga kiritgan buzg‘unchi ichki tarmoqda deyarli to‘siqsiz harakatlanib, muhim resurslarga yetib borish imkoniga ega bo‘ladi.

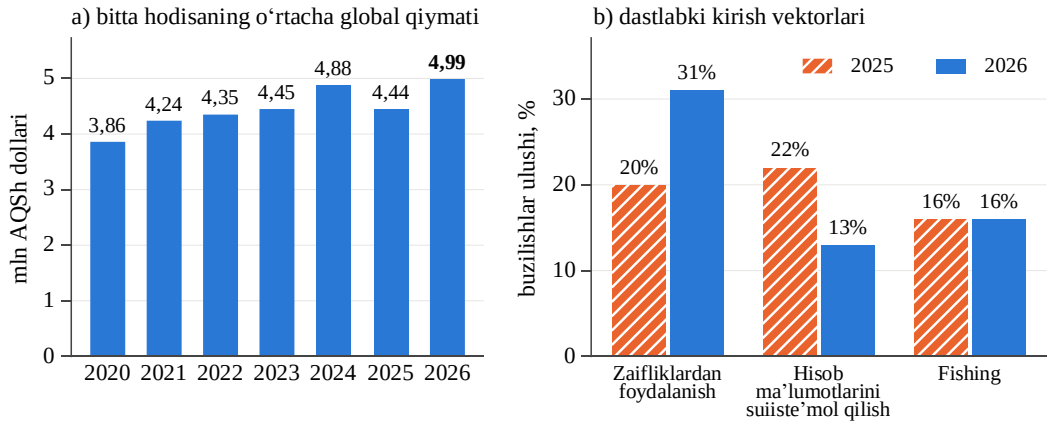
Ushbu muammoga javob sifatida 2010-yilda Forrester Research tahlilchisi J. Kindervag Zero Trust modelini taklif etgan, Google kompaniyasi esa BeyondCorp loyihasida korporativ ilovalarga kirishni tarmoqdagi joylashuvdan to‘liq ajratgan. 2020-yilda AQSh Standartlar va texnologiyalar milliy instituti (NIST) SP 800-207 hujjatida Zero Trust arxitekturasini (ZTA)

tarmoqdagi joylashuv yoki aktivga egalik asosida hech qanday yashirin ishonch berilmaydigan himoya modeli sifatida rasmiy ta’rifladi.

Muammoning dolzarbligi so‘nggi statistik ma’lumotlarda yaqqol ko‘rinadi (1-rasm). Verizon kompaniyasining 2026-yilgi hisobotiga ko‘ra, zaifliklardan foydalanish 31 foiz holatda dastlabki kirish vektori bo‘lgan. Hisob ma’lumotlarini suiiste’mol qilishning dastlabki vektor sifatidagi ulushi qisman metodika o‘zgargani sababli 22 foizdan 13 foizga tushgan bo‘lsa-da, u hujum zanjirining biror bosqichida 39 foiz buzilishlarda qayd etilgan. IBM va Ponemon Institute tadqiqotida bitta ma’lumotlar sizib chiqishi hodisasining o‘rtacha global qiymati 2026-yilda 12 foizga oshib, rekord darajadagi 4,99 mln AQSh dollariga yetgan.

O‘zbekistonda ham vaziyat keskinlashmoqda: Raqamli texnologiyalar vazirligi ma’lumotiga ko‘ra, kiberxavfsizlik uzeli orqali bartaraf etilgan tahdidlar soni 2024-yildagi 7 mln dan 2025-yilda 107 mln dan ortiqqa yetgan, 2026-yil 27–30-yanvar kunlari esa uchta davlat idorasining axborot tizimlariga uyushtirilgan hujumlar natijasida 60 mingga yaqin fuqaroning ma’lumotlari tarqalgan.

Tadqiqotning maqsadi – perimetr modelidan ZTAga o‘tish jarayonida yuzaga keladigan dolzarb muammolarni tizimlashtirish va ularni bartaraf etishning amaliy yo‘nalishlarini asoslashdan iborat.



1-rasm. Kiberxavfsizlik hodisalari ko‘rsatkichlari dinamikasi: a) IBM ma’lumotlari; b) Verizon DBIR ma’lumotlari

Asosiy qism. NIST SP 800-207 ga ko‘ra, ZTA quyidagi tamoyillarga tayanadi: barcha ma’lumot manbalari va hisoblash xizmatlari resurs sifatida qaraladi; har qanday aloqa tarmoqdagi joylashuvidan qat’i nazar himoyalanadi; resursga kirish har bir seans uchun alohida beriladi; kirish to‘g‘risidagi qaror subyekt identifikatori, qurilma holati, xulq-atvor va muhit atributlarini hisobga oluvchi dinamik siyosat asosida qabul qilinadi; tashkilot barcha aktivlarning yaxlitligi va xavfsizlik holatini uzluksiz kuzatadi; autentifikatsiya va avtorizatsiya kirishdan oldin qat’iy amalga oshiriladi; tarmoq va aloqalar holati haqidagi ma’lumotlar to‘planib, himoyani takomillashtirishda foydalaniladi. Perimetr modeli bilan qiyosiy tavsif 1-jadvalda keltirilgan.

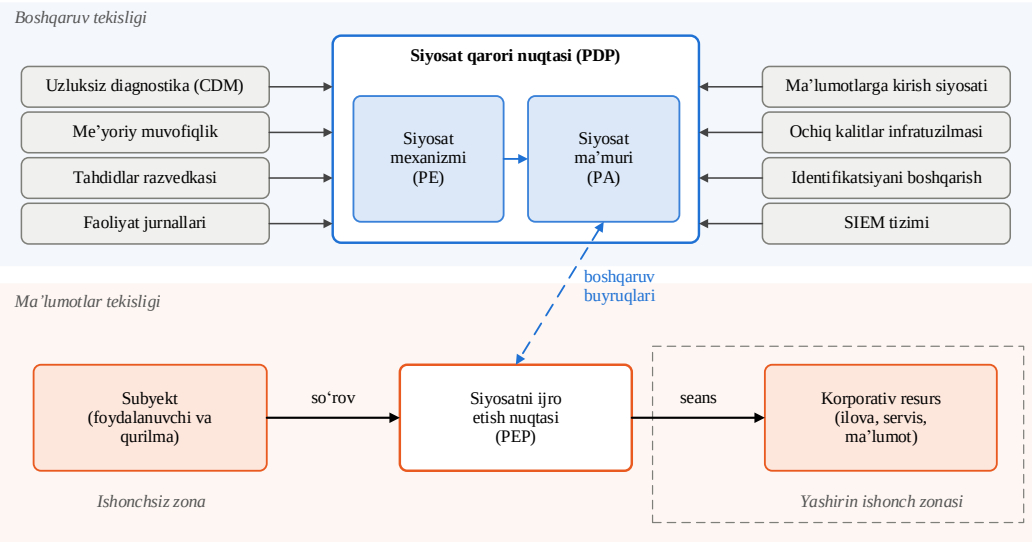
1-jadval

Perimetr modeli va Zero Trust yondashuvining qiyosiy tavsifi

Mezon	Perimetr modeli	Zero Trust yondashuvi
Ishonch asosi	Tarmoqdagi joylashuv (“ichki” yoki “tashqi”)	Subyekt identifikatori, qurilma holati va kontekst
Tekshiruv	Tarmoqqa kirishda bir marta	Har bir seans va so‘rovda, uzluksiz

Mezon	Perimetr modeli	Zero Trust yondashuvi
Himoya obyekti	Tarmoq chegarasi	Alohida resurs: ilova, servis, ma’lumot
Ichki trafik	Ishonchli deb hisoblanadi, ko‘pincha shifrlanmaydi	Ishonchsiz deb hisoblanadi, shifrlanadi va autentifikatsiyalanadi
Kirish huquqlari	Keng va statik	Minimal (least privilege) va dinamik
Buzilish oqibati	Ichki tarmoq bo‘ylab erkin lateral harakat	Zarar alohida segment doirasida cheklanadi

Arxitekturaning mantiqiy yadrosini siyosat mexanizmi (Policy Engine, PE), siyosat ma’muri (Policy Administrator, PA) va siyosatni ijro etish nuqtasi (Policy Enforcement Point, PEP) tashkil etadi (2-rasm). PE tashqi manbalardan – uzluksiz diagnostika, tahdidlar razvedkasi, faoliyat jurnallari, identifikatsiya tizimlari va boshqalardan kelgan signallar asosida kirish to‘g‘risida qaror qabul qiladi, PA uni aniq sozlamalarga aylantiradi, PEP esa subyekt va resurs o‘rtasidagi ulanishni ochadi, kuzatadi va yopadi.



2-rasm. Zero Trust arxitekturasining mantiqiy komponentlari (NIST SP 800-207 asosida tuzilgan)

Amaliy joriy etishda AQSh Kiberxavfsizlik va infratuzilma xavfsizligi agentligining (CISA) yetuklik modeli keng qo‘llaniladi. Uning 2.0-versiyasi besh ustunni, shuningdek ko‘rinuvchanlik va tahlil, avtomatlashtirish va orkestratsiya, boshqaruv kabi kesishuvchi imkoniyatlarni o‘z ichiga oladi; har bir ustun bo‘yicha yetuklik an’anaviy, boshlang‘ich, ilg‘or va optimal bosqichlarda baholanadi. Ustunlar bo‘yicha boshlang‘ich va maqsadli holat 2-jadvalda umumlashtirilgan.

2-jadval

CISA yetuklik modeli ustunlari bo‘yicha an’anaviy va optimal holat tavsifi

Ustun	An’anaviy bosqich	Optimal bosqich
Identifikatsiya	Parol yoki oddiy MFA, statik kirish huquqlari	Fishingga chidamli MFA, xavf asosida uzluksiz tekshiruv

Ustun	An’anaviy bosqich	Optimal bosqich
Qurilmalar	Aktivlar ro‘yxati to‘liq emas, holati qo‘lda tekshiriladi	Qurilmalar holati real vaqtda kuzatiladi va kirish qaroriga ta’sir qiladi
Tarmoqlar	Yirik perimetr, ichki trafik ko‘pincha shifrlanmaydi	Mikroperimetrlar, barcha trafik shifrlanadi
Ilovalar va ish yuklamalari	Kirish lokal va statik avtorizatsiyaga asoslanadi	Har bir murojaatda uzluksiz avtorizatsiya
Ma’lumotlar	Qo‘lda inventarizatsiya, statik kirish	Avtomatik tasniflash, saqlash va uzatishda shifrlash, dinamik kirish

NIST NCCoE markazining 2025-yilda yakunlangan SP 1800-35 qo‘llanmasida 24 ta ishlab chiqaruvchi bilan hamkorlikda tijoriy texnologiyalar asosida 19 ta namunaviy ZTA yaratilgan. Bu Zero Trust bitta mahsulotni sotib olish bilan emas, balki ko‘plab tizimlarni integratsiyalash orqali erishiladigan strategiya ekanini ko‘rsatadi. Tahlil natijasida perimetr himoyasidan uzluksiz tekshiruvga o‘tishda quyidagi asosiy muammolar aniqlandi.

Birinchidan, eski (legacy) tizimlarning mosligi. Ko‘plab davlat va korporativ axborot tizimlari zamonaviy autentifikatsiya protokollarini (SAML, OpenID Connect) va ko‘p faktorli autentifikatsiyani qo‘llab-quvvatlamaydi, dastur kodiga kiritilgan parollar va eskirgan tarmoq protokollaridan foydalanadi. Gartner kompaniyasining 2024-yilgi so‘roviga ko‘ra, tashkilotlarning 63 foizi Zero Trust strategiyasini to‘liq yoki qisman joriy etgan bo‘lsa-da, ko‘pchiligida u infratuzilmaning yarmi yoki undan kam qismini qamrab oladi va umumiy risklarning to‘rtdan bir qismidan ko‘pini kamaytirmaydi.

Ikkinchidan, identifikatsiya infratuzilmasiga tushadigan yuklama. ZTAda identifikatsiya provayderi va siyosat qarori nuqtasi asosiy ishonch markaziga aylanadi, shu sababli ularning buzilishi barcha bog‘liq tizimlarga zanjir bo‘ylab ta’sir qiladi. 2026-yil yanvaridagi hodisadan so‘ng OneID yagona identifikatsiya tizimi foydalanuvchilarining parollari yangilanib, himoya vositalari kuchaytirilgani markazlashgan autentifikatsiya tizimlarini alohida himoyalash zarurligini ko‘rsatadi.

Uchinchidan, mikrosegmentatsiya va siyosatlarni loyihalash murakkabligi. Har bir resurs uchun aniq kirish siyosatini belgilash aktivlar, foydalanuvchilar va ma’lumot oqimlarining to‘liq inventarizatsiyasini talab qiladi. Haddan tashqari qat’iy siyosatlar biznes-jarayonlarni to‘xtatib qo‘yadi, haddan tashqari keng siyosatlar esa yangi arxitekturani amalda perimetr modeliga qaytaradi.

To‘rtinchidan, uzluksiz tekshiruv uchun telemetriya va tahlil. Har bir so‘rov bo‘yicha dinamik qaror qabul qilish qurilma holati, foydalanuvchi xulq-atvori va tarmoq hodisalari haqidagi katta hajmdagi ma’lumotlarni real vaqtda tahlil qilishni talab qiladi. Bu hisoblash resurslari, soxta ogohlantirishlar, kirishdagi kechikish va xodimlar shaxsiy ma’lumotlarining maxfiyligi bilan bog‘liq masalalarni keltirib chiqaradi. IBM tadqiqotida xavfsizlik sohasida sun’iy intellekt va avtomatlashtirishdan keng foydalangan tashkilotlarda bitta hodisaning o‘rtacha qiymati 4,00 mln dollarni, ulardan foydalanmaganlarda esa 5,93 mln dollarni tashkil etgan.

Beshinchidan, ma’lumotlar va aloqa kanallarining kriptografik himoyasi. ZTAning “har qanday aloqa himoyalanadi” tamoyiliga qaramay, IBM tadqiqotiga ko‘ra, ma’lumotlari sizib chiqqan tashkilotlarning yarmidan ko‘pi maxfiy ma’lumotlarni saqlash va uzatishda shifrlamagan.

Shu bois ichki trafikni mTLS orqali shifrlash, kalitlarni markazlashgan boshqarish va milliy kriptografik standartlarga muvofiqlik ZTAning ajralmas qismi hisoblanadi.

Oltinchidan, tashkiliy, kadr va me'yoriy to'siqlar. Gartner ma'lumotiga ko'ra, Zero Trust joriy etilgandan keyin har besh tashkilotdan uchtasi xarajatlar, ikkitasi esa xodimlarga bo'lgan ehtiyoj ortishini kutadi. Kompaniya 2023-yilda 2026-yilga kelib yirik korxonalarning atigi 10 foizi yetuk va o'lchanadigan Zero Trust dasturiga ega bo'lishini prognoz qilgan. AQShda federal idoralar uchun Zero Trust maqsadlari va muddatlari 2022-yilda maxsus memorandum bilan belgilangan. O'zbekistonda "Kiberxavfsizlik to'g'risida"gi Qonun sohaning umumiy huquqiy asosini yaratgan bo'lsa-da, ZTAni joriy etish bo'yicha milliy yetuklik modeli va metodik tavsiyalarni ishlab chiqish dolzarb vazifa bo'lib qolmoqda.

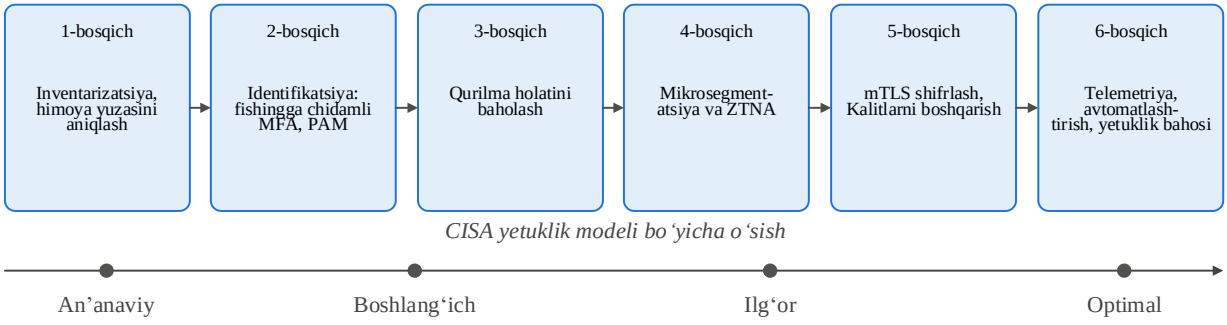
Aniqlangan muammolar va ularni bartaraf etish choralari 3-jadvalda umumlashtirilgan.

3-jadval

Zero Trustga o'tishdagi asosiy muammolar va ularni bartaraf etish choralari

Muammo	Tavsiya etiladigan choralar	CISA ustuni
Eski tizimlarning mosligi	Proksi-shlyuzlar (PEP) orqali himoyalash, bosqichma-bosqich modernizatsiya	Ilovalar va ish yuklamalari
Identifikatsiya infratuzilmasiga yuklama	FIDO2/WebAuthn, qisqa muddatli tokenlar, imtiyozli hisoblarni boshqarish (PAM), identifikatsiya provayderini alohida himoyalash	Identifikatsiya
Mikrosegmentatsiya va siyosatlar murakkabligi	Ma'lumot oqimlarini xaritalash, siyosatlarni avval kuzatuv rejimida sinash	Tarmoqlar
Telemetriya hajmi va tahlil	SIEM/UEBA tizimlari, javob choralarini avtomatlashtirish	Ko'rinuvchanlik va tahlil; avtomatlashtirish
Shifrlanmagan trafik va ma'lumotlar	mTLS, kalitlar hayot siklini markazlashgan boshqarish, milliy kriptografik standartlar	Tarmoqlar; ma'lumotlar
Tashkiliy va me'yoriy to'siqlar	Milliy yetuklik modeli va metodik tavsiyalar, mutaxassislar tayyorlash	Boshqaruv

Shu asosda axborot tizimlarida ZTAga o'tishning olti bosqichli yo'l xaritasi taklif etiladi (3-rasm). Unda avval eng muhim resurslar aniqlanib, identifikatsiya ustuni mustahkamlanadi, so'ngra qurilmalar, tarmoq va ma'lumotlar himoyasi bosqichma-bosqich kengaytiriladi; har bir bosqich CISA modeli bo'yicha yetuklikning keyingi darajasiga o'tishga xizmat qiladi.



3-rasm. Zero Trust arxitekturasiga bosqichma-bosqich o'tishning taklif etilayotgan yo'l xaritasi

Xulosa

Zero Trust arxitekturasi himoya mantig‘ini “so‘rov qayerdan kelmoqda?” degan savoldan “kim, qaysi qurilmadan, qanday holatda va qaysi resursga murojaat qilmoqda?” degan savolga o‘tkazadi. Tadqiqot shuni ko‘rsatdiki, perimetr modelidan ZTAga o‘tish bir martalik texnik loyiha emas, balki eski tizimlarni moslashtirish, identifikatsiya infratuzilmasini mustahkamlash, siyosatlarni aniq loyihalash, telemetriya va kriptografik himoyani rivojlantirishni talab qiluvchi ko‘p yillik evolyutsion jarayondir. Zero Trust kiberxavfni to‘liq yo‘q qilmaydi, ammo buzilish ehtimoli va uning oqibatlarini sezilarli darajada cheklaydi. Davlat raqamli xizmatlari jadal kengayayotgan O‘zbekiston sharoitida ZTAni eng muhim tizimlar va identifikatsiya ustunidan boshlab bosqichma-bosqich joriy etish hamda milliy yetuklik modelini ishlab chiqish maqsadga muvofiq.

Foydalanilgan adabiyotlar:

1. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. – Cambridge: Forrester Research, 2010.
2. Ward R., Beyer B. BeyondCorp: A New Approach to Enterprise Security // ;login:. – 2014. – Vol. 39, № 6. – P. 6–11.
3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. – Gaithersburg: NIST, 2020. – DOI: 10.6028/NIST.SP.800-207.
4. Verizon. 2026 Data Breach Investigations Report. – Verizon Business, 2026.
5. Verizon. 2025 Data Breach Investigations Report. – Verizon Business, 2025.
6. IBM, Ponemon Institute. Cost of a Data Breach Report 2026. – Armonk: IBM, 2026.
7. Kiberhujum oqibatida 15 mln emas, 60 mingga yaqin fuqaro ma’lumotlari tarqalgan – vazir // Spot.uz. – 2026-yil 12-fevral. – URL: https://www.spot.uz/oz/2026/02/12/cyberattack
8. CISA. Zero Trust Maturity Model. Version 2.0. – Washington: Cybersecurity and Infrastructure Security Agency, 2023.
9. NIST NCCoE. Implementing a Zero Trust Architecture. NIST Special Publication 1800-35. – Gaithersburg: NIST, 2025. – DOI: 10.6028/NIST.SP.1800-35.
10. Gartner. Top 3 Recommendations From the 2024 State of Zero-Trust Adoption Survey. – Stamford: Gartner Research, 2024.
11. Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026. – Gartner Press Release, 23.01.2023.
12. Office of Management and Budget. M-22-09. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. – Washington: Executive Office of the President, 2022.
13. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 15.04.2022, O‘RQ-764-son // Qonunchilik ma’lumotlari milliy bazasi. – URL: https://lex.uz/docs/5960604

WEB APPLICATION VULNERABILITY DETECTION METHODS: A COMPARATIVE ANALYSIS OF SAST, DAST, IAST AND MANUAL TESTING

Toshpulatov Sh.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract. The paper presents a comparative analysis of the main methods for detecting security vulnerabilities in web applications: static (SAST), dynamic (DAST) and interactive (IAST) application security testing, as well as manual testing. For each method, the operating principle, detection coverage, false positive and false negative rates, and its place in the software development life cycle are examined. The capabilities of hybrid and machine learning-based approaches are reviewed, and the need to apply these methods jointly within a complementary multi-layered testing model is substantiated.

Keywords: web application security, vulnerability detection, SAST, DAST, IAST, manual testing, penetration testing, SQL injection, XSS.

Annotatsiya. Maqolada veb-ilovalardagi zaifliklarini aniqlashning asosiy usullari – statik (SAST), dinamik (DAST) va interaktiv (IAST) tahlil hamda qo‘lda testlash qiyosiy tahlil qilinadi. Har bir usulning ishlash tamoyili, aniqlash qamrovi, yolg‘on ijobiy va yolg‘on manfiy natijalar darajasi hamda dasturiy ta’minotni ishlab chiqishning hayotiy siklidagi o‘rni yoritiladi. Gibrid va mashinali o‘qitishga asoslangan yondashuvlarning imkoniyatlari ko‘rib chiqilib, usullarni ko‘p qatlamli testlash modeli doirasida birgalikda qo‘llash zarurati asoslanadi.

Kalit so‘zlar: veb-ilova xavfsizligi, zaifliklarni aniqlash, SAST, DAST, IAST, qo‘lda testlash, penetratsion test, SQL in’eksiya, XSS.

Introduction

Today, a large share of e-government, banking, education and commerce services is delivered through web applications. Because a web application is permanently reachable from external networks, any software defect in it can become an attack vector. SQL injection, cross-site scripting (XSS), flaws in authentication and authorization mechanisms, and security misconfigurations are consistently reported as the most widespread vulnerability classes. Detecting a vulnerability during development costs far less than remediating it in a system already in production; therefore, choosing and positioning detection methods correctly is an important practical problem.

The scientific literature offers a wide range of vulnerability detection approaches. According to systematic mapping studies, they can be grouped into static, dynamic, hybrid and machine learning-based categories [1]. In industrial practice, these approaches are implemented as SAST, DAST and IAST tools and as manual penetration testing. The aim of this work is to compare these methods against a common set of criteria and to substantiate a model for applying them jointly.

Main part

Static analysis (SAST, Static Application Security Testing) inspects an application’s source code, bytecode or intermediate representation without executing the program. Its core techniques include lexical analysis and pattern matching, control flow graph construction, data flow analysis and taint analysis. In taint analysis, untrusted data sources (request parameters, cookies, headers) are marked, and the tool tracks whether such data reaches dangerous sinks (SQL queries, HTML

output) without sanitization. A survey of static approaches for detecting SQL injection and XSS shows that data flow tracking is the most promising direction, while correctly modelling sanitization routines and handling the features of dynamic languages remain the main challenges [2].

The strengths of SAST are its applicability at the earliest stage of the software life cycle, theoretically complete coverage of all code paths, and precise localization of a vulnerability down to the file and line. Its weaknesses include a high proportion of false positives, blindness to the runtime environment and server configuration, and reduced accuracy for dynamically typed languages such as PHP and JavaScript. Studies evaluating static analysis tools on web applications show that results differ substantially from tool to tool and that relying on a single tool is insufficient [3].

Dynamic analysis (DAST, Dynamic Application Security Testing) follows a black-box principle: the tool sends HTTP requests to a running application and analyses its responses. The process typically consists of automated crawling, discovery of entry points, injection of crafted payloads and fuzzing. DAST is independent of the programming language and framework, detects vulnerabilities that are actually exploitable as well as environment-related issues such as server settings, HTTP security headers and TLS configuration, and produces relatively few false positives. At the same time, its coverage depends on the quality of crawling: pages behind authentication, multi-step business workflows and complex stateful interfaces are often left untested. In addition, DAST does not point to the exact location of the flaw in the code and can be applied only once the application is deployed.

Interactive analysis (IAST, Interactive Application Security Testing) combines ideas from static and dynamic approaches at runtime. A dedicated agent is installed in the application's execution environment (JVM, .NET CLR, Node.js) and monitors data flow from inside the application while functional tests or DAST traffic are running. As a result, each finding is linked simultaneously to the HTTP request that triggered it and to the exact line of code, which considerably reduces false positives and simplifies continuous integration into the CI/CD pipeline. The limitations of IAST are its dependence on supported languages and platforms, the agent's impact on application performance, and the fact that it only examines code paths actually executed during testing, so the quality of its results is directly tied to test coverage.

Manual testing comprises penetration testing and security-focused code review performed by a specialist, usually following methodologies such as the OWASP WSTG. Automated tools are practically unable to detect business logic flaws (for example, tampering with a payment amount or bypassing workflow steps), broken authorization via insecure direct object references (IDOR), or the chaining of several minor weaknesses into a single attack – these tasks require human reasoning. Manual testing is also necessary to validate and triage the findings of automated tools. It has been shown that combining SAST tools with manual testing improves the vulnerability detection methodology, increasing the number of true vulnerabilities found and reducing false results [4]. The drawbacks of this method are its dependence on the specialist's expertise, high cost, low repeatability and difficulty in scaling to large code bases.

In recent years, hybrid approaches have been actively developed to overcome the limitations of individual methods. A methodology and case study on blending static and dynamic analysis demonstrate that the two methods complement each other and that their joint use broadens detection coverage [5]. An approach to website vulnerability detection based on static and dynamic analysis [6] and comprehensive systems that integrate both types of analysis into a single platform

[7] have been developed along the same lines. Machine learning-based methods are applied mainly at the attack detection stage: it has been shown that fusing multiple feature sets makes it possible to classify XSS and SQL injection attacks with high accuracy [8]. However, such models remain sensitive to the quality of training data, the explainability of their results, and evasion by attackers through adversarial samples.

A comparative overview of the reviewed methods against the main criteria is given in Table 1.

Table 1

Comparative characteristics of vulnerability detection methods

Criterion	SAST	DAST	IAST	Manual testing
Object of analysis	Source code, bytecode	Running application	Application at runtime (via agent)	Application, code, logic
Life cycle stage	Coding, build	Testing, staging, production	Integration and testing	Pre-release, periodic
Source code access	Required	Not required	Agent installation required	Optional
Code coverage	High	Low – medium	Depends on test coverage	Selected parts
False positives	High	Low	Very low	Very low
Business logic flaws	Not detected	Limited	Limited	Detected
Environment and configuration errors	Not detected	Detected	Partially	Detected
Vulnerability localization	File, line	URL, parameter	URL and code line	Described in report
Automation (CI/CD)	Full	High	Full	Low

As the table shows, no single method is superior across all criteria: SAST leads in code coverage and early detection, DAST in environment-related issues and a low false positive rate, IAST in accuracy and automation, and manual testing in detecting business logic vulnerabilities. Consequently, in practice it is advisable to combine them within a multi-layered model. In the proposed model, SAST is applied when code is written and changes are merged (pull requests), IAST during functional testing, DAST in the staging environment, and manual penetration testing before release and periodically thereafter. All findings are aggregated in a unified vulnerability management system, and vulnerabilities confirmed by more than one method are given priority. This approach is particularly relevant for government and financial web resources in the national segment, as it allows the level of security to be raised systematically under limited resources.

Conclusion

The SAST, DAST, IAST and manual testing methods for detecting web application vulnerabilities are based on different principles, and each has its own detection coverage and limitations. The analysis shows that relying on a single method leaves certain classes of

vulnerabilities unaddressed. Hybrid approaches that combine static and dynamic analysis, as well as machine learning-based methods, can increase detection effectiveness, but they cannot replace the involvement of a specialist in identifying business logic flaws. Therefore, a multi-layered model that applies automated tools and manual testing jointly at different stages of the software life cycle is the most appropriate solution for ensuring web application security.

References:

1. Rahman K., Izurieta C. A Mapping Study of Security Vulnerability Detection Approaches for Web Applications // Euromicro Conference on Software Engineering and Advanced Applications (SEAA). – 2022. – DOI: 10.1109/SEAA56994.2022.00081.
2. Gupta M.K., Govil M.C., et al. Static analysis approaches to detect SQL injection and cross site scripting vulnerabilities in web applications: A survey // International Conference on Recent Advances and Innovations in Engineering (ICRAIE). – 2014. – DOI: 10.1109/ICRAIE.2014.6909173.
3. Ehichoya O., Nnaemeka C.C. Evaluation of Static Analysis on Web Applications // arXiv preprint. – 2022. – DOI: 10.48550/arXiv.2212.12308.
4. Elrowayati A.A., Fadeel A. SAST Tools and Manual Testing to Improve the Methodology of Vulnerability Detection in Web Applications // The International Journal of Engineering & Information Technology (IJEIT). – 2024. – Vol. 12, No. 1. – DOI: 10.36602/ijeit.v12i1.480.
5. Nunes P., Fonseca J., et al. Blending Static and Dynamic Analysis for Web Application Vulnerability Detection: Methodology and Case Study // IEEE Access. – 2025. – DOI: 10.1109/ACCESS.2024.3522094.
6. Popereshnyak S., Horokh B.D. An approach to website vulnerability detection based on static and dynamic analysis // Problems in Programming. – 2025. – No. 4. – DOI: 10.15407/pp2025.04.041.
7. Gündoğdu A., Güven E.Y. WebScan: A Comprehensive Static and Dynamic Analysis Approach for Web Application Security // International Conference on New Technologies, Mobility and Security (NTMS). – 2025. – DOI: 10.1109/NTMS65597.2025.11076695.
8. Bakır R. UniEmbed: A Novel Approach to Detect XSS and SQL Injection Attacks Leveraging Multiple Feature Fusion with Machine Learning Techniques // Arabian Journal for Science and Engineering. – 2025. – DOI: 10.1007/s13369-024-09916-4.

SUN’IY INTELLEKT ASOSIDA FISHING HUJUMLARINI ANIQLASH: GIBRID DATASET, REST API VA TELEGRAM BOT INTEGRATSIYASI

Abduraufova M.S.
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti

Annotatsiya. Maqolada elektron xat va URL belgilarini birgalikda tahlil qilish orqali fishing xatlarni aniqlash yondashuvi o‘rganiladi. Beshta ochiq email korpusi va UCI “Phishing Websites” datasetidan sinf belgisi bo‘yicha sun’iy juftlash usulida 79 627 ta yozuvli gibrid dataset shakllantirildi va Evidently yordamida tahlil qilindi. Ijobiy sinfning 88,5% i spam korpuslaridan olingani sababli asosiy to‘plam “fishing va spam” sinfi sifatida talqin qilinadi. Takrorlanuvchi namunalar bo‘yicha guruhlangan 5-fold kross-validatsiyada 40 belgili eksperimental Random Forest modeli 96,18 ± 0,68% aniqlikka erishdi. Biroq alohida o‘qitilgan email va URL modellarini kech birlashtirish deyarli shu natijani (96,04%) berdi: ustunlik sun’iy juftlash sharoitidagi ikki mustaqil signal yig‘indisidan iborat. Spam chiqarib tashlangan “faqat fishing” to‘plamida gibrid model F1 = 94,69% ko‘rsatdi. Real vaqtda hisoblanadigan 20 belgili amaliy model (92,52 ± 0,62%) REST API va OCR qo‘llab-quvvatlaydigan Telegram botga integratsiya qilindi. Qoidaviy qatlam test to‘plamida FPR ni 44,3% gacha oshirgani uchun faqat ogohlantirish sifatida qoldirildi.

Kalit so‘zlar: fishing, spam, kiberxavfsizlik, mashinali o‘qitish, gibrid dataset, guruhli kross-validatsiya, Evidently, REST API, Telegram bot.

Аннотация. В статье исследуется подход к обнаружению фишинговых писем на основе совместного анализа признаков электронного письма и URL. Из пяти открытых корпусов писем и набора данных UCI «Phishing Websites» методом искусственного сопоставления по метке класса сформирован гибридный датасет из 79 627 записей, проанализированный с помощью Evidently. Поскольку 88,5% положительного класса взято из спам-корпусов, основной набор интерпретируется как класс «фишинг и спам». При 5-кратной кросс-валидации с группировкой повторяющихся образцов экспериментальная модель Random Forest на 40 признаках достигла точности 96,18 ± 0,68%. Однако позднее объединение отдельно обученных моделей письма и URL дало почти тот же результат (96,04%): преимущество объясняется суммой двух независимых сигналов в условиях искусственного сопоставления. На наборе «только фишинг» без спама гибридная модель показала F1 = 94,69%. Практическая модель на 20 признаках, вычисляемых в реальном времени (92,52 ± 0,62%), интегрирована в REST API и Telegram-бот с OCR. Слой правил, повысивший FPR на тестовом наборе до 44,3%, оставлен только как предупреждение.

Ключевые слова: фишинг, спам, кибербезопасность, машинное обучение, гибридный датасет, групповая кросс-валидация, Evidently, REST API, Telegram-бот.

Kirish

Masofaviy bank xizmatlari va messenjerlarning ommalashuvi bilan ijtimoiy muhandislikka asoslangan hujumlar, xususan, soxta havola yoki xat orqali login-parol va karta ma’lumotlarini o‘g‘irlashga qaratilgan fishing keng tarqalmoqda [1]. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni [2] bunday tahdidlarni aniqlash va bartaraf etishni muhim vazifa sifatida belgilaydi. Ilmiy ishlarda fishingni aniqlash odatda URL belgilari [3, 4] yoki xat matni [5] bo‘yicha alohida o‘rganiladi, amaliyotda esa hujum ko‘pincha ishontiruvchi matn va soxta havolani birga o‘z ichiga oladi. Ishning maqsadi – email va URL belgilarini birlashtirishning

ta’sirini xolis protokol asosida baholash va amaliy modelni REST API hamda Telegram bot orqali joriy etish.

Gibrid dataset

Email qismi uchun Kaggle’dagi jamlangan to‘plamdan [5, 6] beshta korpus olindi (1-jadval). Yorliqlar manbadagi holicha (0 – qonuniy, 1 – ijobiy) ishlatilgan va qo‘lda qayta tekshirilmagan. CEAS-2008, Enron-Spam [7] va SpamAssassin spam korpuslari bo‘lib, ulardagi “1” yorlig‘i spamni (jumladan, fishingni) bildiradi. Faqat Nazario va Nigerian Fraud korpuslari fishing va firibgarlik xatlaridan iborat [15]. Shunday qilib, ijobiy sinfdagi 42 433 ta xatdan 4 897 tasi (11,5%) fishing yoki firibgarlik, 37 536 tasi (88,5%) esa spam yorlig‘idagi xatdir. Demak, asosiy tajribada model sof fishingni emas, kengroq “spam va fishing” sinfini aniqlaydi. Sof fishing uchun alohida tajriba o‘tkazildi (4-bo‘lim).

1-jadval

Email korpuslari va ulardagi yorliqlar

Korpus	Manbadagi ijobiy sinf	Qonuniy (0)	Ijobiy (1)
CEAS-2008	spam	17 312	21 842
Enron-Spam	spam	15 791	13 976
SpamAssassin	spam	4 091	1 718
Nazario	fishing	–	1 565
Nigerian Fraud	firibgarlik (“419”)	–	3 332
Jami		37 194	42 433

Har bir xat uchun 10 ta belgi hisoblandi: mavzu va matn uzunligi, havola mavjudligi, to‘rt guruh kalit so‘zlar va uchta metama’lumot maydonining yo‘qligi. URL qismi uchun UCI “Phishing Websites” datasetining [3] 30 ta belgisi olindi. Real email–URL juftliklari mavjud emasligi sababli har bir ijobiy xatga tasodifiy fishing URL, qonuniy xatga esa tasodifiy qonuniy URL biriktirildi. Bunday juftlashda ikki manbaning yorliqlari oldindan moslashtirilgan bo‘ladi, shuning uchun gibrid modelning yuqori aniqligi qisman usulning o‘zidan kelib chiqadi (3-bo‘lim).

Evidently tahlili

Evidently [8] DataSummaryPreset hisobotida bo‘sh qiymatlar aniqlanmadi. DataDriftPreset bo‘yicha o‘qitish (80%) va test (20%) to‘plamlari solishtirilganda tanlangan statistik testlar va standart chegara bo‘yicha 43 ta ustunning birortasida sezilarli drift aniqlanmadi. Tahlil ikki xil takrorlanishni ham ko‘rsatdi: UCI dataseti kichik bo‘lgani uchun qayta tanlash bilan kengaytirilgan URL qismida atigi 5 782 ta noyob belgilar kombinatsiyasi bor, email qismida esa 595 ta takroriy matn (79 032 ta noyob xat) mavjud.

Baholash metodikasi va natijalar

Ma’lumotlar sizib o‘tishining (data leakage) oldini olish uchun bir xil URL kombinatsiyasi yoki bir xil email matniga ega yozuvlar bitta guruhga birlashtirildi (5 188 ta guruh) va 5-fold StratifiedGroupKFold kross-validatsiya qo‘llanildi. Uchta belgilar to‘plami (email – 10, URL – 30, gibrid – 40) uchta algoritmda solishtirildi (2-jadval): Random Forest (RF) [9], logistik regressiya (LR) va gradient bustingi (GB) [10]. Modellar scikit-learn [11] yordamida qurildi. FNR – o‘tkazib yuborilgan ijobiy xatlar, FPR – ijobiy deb belgilangan qonuniy xatlar ulushi.

Uchala algoritmda ham gibrid to‘plam bir manbali to‘plamlardan yuqori natija berdi (RF uchun URL modeliga nisbatan +1,2, email modeliga nisbatan +17,1 foiz punkt). ROC-AUC RF

uchun mos ravishda 88,32%, 99,23% va 99,50%, gibrid RF ning yig‘ma chalkashlik matritsasi: TN = 35 796, FP = 1 398, FN = 1 662, TP = 40 771. Guruhlanmagan tasodifiy 80/20 bo‘linishda esa URL modeli 99,05%, gibrid model 98,57% aniqlik ko‘rsatgan (Evidently ClassificationPreset: accuracy 0,986, precision 0,988, recall 0,985), ya’ni takrorlanishlar hisobga olinmasa natija oshib ko‘rinadi.

2-jadval

Guruhli 5-fold kross-validatsiya natijalari, % (o‘rtacha ± std)

Belgilar	Algoritm	Accuracy	F1	FPR	FNR	PR-AUC
Email	LR	66,09 ± 0,30	68,85	38,78	29,65	74,32
Email	RF	79,07 ± 0,21	80,35	22,35	19,69	90,14
Email	GB	79,91 ± 0,31	80,65	18,55	21,44	91,11
URL	LR	92,40 ± 1,51	92,82	7,38	7,79	98,21
URL	RF	94,97 ± 0,77	95,25	4,71	5,32	99,34
URL	GB	95,16 ± 1,01	95,45	5,02	4,69	99,37
Gibrid	LR	92,99 ± 1,18	93,39	6,88	7,12	98,46
Gibrid	RF	96,18 ± 0,68	96,41	3,90	3,76	99,57
Gibrid	GB	96,70 ± 0,65	96,91	3,63	3,02	99,69

Juftlash ta’sirini tekshirish uchun email va URL modellari alohida o‘qitilib, ularning skorlari log-odds yig‘indisi bilan birlashtirildi (kech birlashtirish). Bu usul 96,04 ± 0,32% aniqlik va 96,27% F1 berdi, ya’ni birgalikda o‘qitilgan gibrid model (96,18%, F1 96,41%) bilan deyarli bir xil. Demak, gibrid modelning ustunligi email va URL belgilari o‘rtasidagi o‘zaro bog‘liqlikdan emas, sinfi oldindan moslashtirilgan ikki mustaqil signalning yig‘indisidan kelib chiqadi.

Qo‘shimcha tekshiruvlar

Spamni fishingdan ajratish uchun spam yorlig‘idagi barcha xatlar chiqarib tashlandi: ijobiy sinf faqat Nazario va Nigerian Fraud xatlari (4 897 ta), salbiy sinf barcha qonuniy xatlar (37 194 ta). Qoidaviy qatlam esa xuddi shu kross-validatsiya foldlarida amaliy gibrid model bilan birga baholandi (3-jadval).

3-jadval

Faqat fishing to‘plami va qoidaviy qatlam natijalari, %

Tajriba	Precision	Recall	F1	FPR	FNR
Faqat fishing: email	84,19	77,17	80,52	1,91	22,83
Faqat fishing: URL	83,97	91,85	87,72	2,32	8,15
Faqat fishing: gibrid	97,51	92,06	94,69	0,31	7,94
Amaliy gibrid: model	93,07	92,89	92,97	7,90	7,11
Amaliy gibrid: model + qoida	71,05	95,28	81,40	44,32	4,72

Faqat fishing to‘plamida ham gibrid model eng yaxshi natija berdi (F1 = 94,69%, PR-AUC = 98,61%), lekin bu yerda ham juftlash sun’iy. Bundan tashqari, korpusga xos metama’lumot belgilari (jo‘natuvchi, sana va qabul qiluvchi maydonlarining yo‘qligi) olib tashlanganda email modelining F1 ko‘rsatkichi 80,52% dan 64,38% gacha tushdi. Demak, email modeli qisman xat mazmunini emas, korpus manbasini ajratadi. Qoidaviy qatlam recall ni 92,89% dan 95,28% gacha

oshirgan bo‘lsa-da, FPR ni 7,90% dan 44,32% gacha ko‘tardi va F1 ni 81,40% gacha tushirdi. Shu sababli qoida yakuniy qarordan chiqarildi va faqat ogohlantirish sifatida qoldirildi.

Amaliy model, REST API va bot

UCI belgilarining bir qismi (sahifa tarkibi, domen yoshi, trafik, WHOIS, DNS) havola satridan hisoblanmaydi. Birinchi versiyada ular standart qiymat bilan to‘ldirilgani sababli model havolasiz har qanday xabarga ≈0,81 skor bergan. Shu sababli har bir rejimga alohida RF modeli o‘qitildi: email (10 belgi), URL (havola satridan aniq hisoblanadigan 10 belgi) va gibrid (20 belgi). Ularning aniqligi mos ravishda 79,07 ± 0,21%, 89,54 ± 1,05% va 92,52 ± 0,62% ni tashkil etdi (gibrid: ROC-AUC 97,54%, PR-AUC 97,71%). API va botda aynan shu 20 belgili amaliy model ishlaydi, 96,18% li eksperimental model emas. RF chiqishi kalibrlangan ehtimol emas, shuning uchun u “model skori” deb ataladi (Brier 0,057, ECE 1,1%; izotonik kalibrlash Brier ni atigi 0,055 gacha yaxshiladi).

FastAPI [12] asosidagi API /analyze-email, /analyze-url, /analyze-hybrid va rejimni avtomatik tanlovchi /analyze-text endpointlariga ega. Xavf darajasi s skor bo‘yicha belgilanadi: $s \geq 0{,}80$ – HIGH, $0{,}50 \leq s < 0{,}80$ – MEDIUM, $s < 0{,}50$ – LOW. Javobda model_score, model_prediction, rule_triggered va final_decision maydonlari alohida qaytariladi. Yakuniy qaror faqat model bo‘yicha qabul qilinadi. IP manzil, qisqartirish xizmati yoki “@” belgisi aniqlansa, qarorga ta’sir qilmaydigan ogohlantirish beriladi, chunki ular ichki korporativ tizimlarda va qonuniy xizmatlarda ham uchraydi. Bot Telegram Bot API [13] asosida ishlaydi, skrinshot matnini Tesseract OCR [14] bilan ajratadi. O‘zbek va rus ma’nodosh kalit so‘zlari qo‘shilgan, lekin model ko‘p tilli emas va bu tillarda baholanmagan.

Demonstratsion sinov (smoke test)

Tizim 10 ta namunaviy xabar bilan /analyze-text orqali sinaldi (4-jadval). Bu statistik baholash emas, faqat end-to-end namoyish.

4-jadval

Demonstratsion sinov natijalari

Xabar	Rejim	Skor	Ogohlantirish	Yakuniy qaror
Fishing xat (ingliz)	EMAIL	0,83	–	fishing ✓
Oddiy xat (ingliz)	EMAIL	0,74	–	fishing ✗
Fishing xat (o‘zbek)	EMAIL	0,85	–	fishing ✓
Oddiy xat (o‘zbek)	EMAIL	0,30	–	xavfsiz ✓
IP manzilli havola	URL	0,11	IP	xavfsiz ✗
Qisqartirilgan havola	URL	0,16	qisqartirish	xavfsiz ✗
Defisli, ko‘p subdomenli	URL	0,99	–	fishing ✓
google.com	URL	0,00	–	xavfsiz ✓
Matn + fishing havola	HYBRID	0,94	–	fishing ✓
Matn + tuit.uz	HYBRID	0,17	–	xavfsiz ✓

Yakuniy qaror 10 ta holatdan 7 tasida to‘g‘ri bo‘ldi. IP manzilli va qisqartirilgan havolalar uchun model past skor berdi, foydalanuvchiga esa ogohlantirish ko‘rsatildi. Qisqa qonuniy xatdagi xato email modelining yuqori FPR ko‘rsatkichiga mos keladi.

Cheklovlar

Asosiy cheklovlar: email–URL juftliklarining sun’iyligi; ijobiy sinfning asosan spamdan iboratligi va yorliqlarning qayta tekshirilmaganligi; korpusga xos metama’lumot belgilari; UCI URL belgilarining eskirganligi (2015-yil). Kelgusida real xatlardagi havolalar asosida haqiqiy juftliklarni yig‘ish, fishing yorliqlarini qo‘lda tekshirish va o‘zbek hamda rus tilidagi test to‘plamini yaratish rejalashtirilgan.

Xulosa

79 627 ta yozuvli gibrid dataset yaratildi va Evidently yordamida tahlil qilindi. Guruhli baholash protokolida gibrid belgilar to‘plami ushbu dataset doirasida bir manbali modellarga nisbatan yuqori natija ko‘rsatdi (RF uchun 96,18 ± 0,68%). Biroq kech birlashtirish tahlili bu ustunlik sinfi moslashtirilgan ikki mustaqil signal yig‘indisidan kelib chiqishini ko‘rsatdi. Ijobiy sinfning 88,5% i spam ekani aniqlandi va sof fishing uchun alohida natijalar keltirildi. Guruhlanmagan bo‘linish natijani oshirib ko‘rsatishi va qoidaviy qatlam yolg‘on ogohlantirishlarni keskin ko‘paytirishi ham aniqlandi. Amaliy gibrid model (92,52 ± 0,62%) REST API va Telegram bot orqali joriy etildi. Natijalarni real hujumlar uchun tasdiqlash haqiqiy email–URL juftliklari va qayta tekshirilgan fishing yorliqlari asosida qo‘shimcha tadqiqotni talab etadi.

Foydalanilgan adabiyotlar

1. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. – https://apwg.org/trendsreports/

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 2022-yil 15-apreldagi O‘RQ-764-son. – https://lex.uz

3. Mohammad R., Thabtah F., McCluskey L. Phishing Websites Dataset. – UCI Machine Learning Repository, 2015.

4. Sahingoz O.K., Buber E., Demir O., Diri B. Machine learning based phishing detection from URLs // Expert Systems with Applications. – 2019. – Vol. 117. – P. 345–357.

5. Champa A.I., Rabbi M.F., Zibran M.F. Curated Datasets and Feature Analysis for Phishing Email Detection with Machine Learning // 12th International Symposium on Digital Forensics and Security (ISDFS). – 2024.

6. Alam N.A. Phishing Email Dataset. – Kaggle. – https://www.kaggle.com/datasets/naserabdullahalam/phishing-email-dataset

7. Metsis V., Androutsopoulos I., Paliouras G. Spam Filtering with Naive Bayes – Which Naive Bayes? // Third Conference on Email and Anti-Spam (CEAS). – 2006.

8. Evidently AI. Evidently: open-source ML evaluation and monitoring. – https://github.com/evidentlyai/evidently

9. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, № 1. – P. 5–32.

10. Friedman J.H. Greedy function approximation: A gradient boosting machine // The Annals of Statistics. – 2001. – Vol. 29, № 5. – P. 1189–1232.

11. Pedregosa F. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. – 2011. – Vol. 12. – P. 2825–2830.

12. FastAPI. – https://fastapi.tiangolo.com

13. Telegram Bot API. – https://core.telegram.org/bots/api

14. Smith R. An Overview of the Tesseract OCR Engine // Proc. of the 9th International Conference on Document Analysis and Recognition (ICDAR 2007). – P. 629–633.

15. Mendes P., Maia E., Praça I. MeAJOR Corpus: A Multi-Source Dataset for Phishing Email Detection. – arXiv:2507.17978, 2025.

BUYUMLAR INTERNETI TIZIMLARIDA XAVFSIZLIK MUAMMOLARI VA AUTENTIFIKATSIYALASH USULLARI

Olimov I.S., Tursunov O.O., Bo‘riyev Y.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda Buyumlar Interneti (IoT) tizimlaridagi asosiy xavfsizlik muammolari va autentifikatsiyalash usullari tahlil qilinadi. Parol, token va sertifikat, ko‘p omilli, challenge–response va kriptografik usullar qiyosiy baholanadi. Universal usul mavjud emasligi, tanlov qurilma resurslari va tahdid modeliga bog‘liq ekani ko‘rsatiladi.

Kalit so‘zlar: Buyumlar Interneti, autentifikatsiya, kiberxavfsizlik, challenge–response, kalitlarni boshqarish.

Аннотация. В тезисе анализируются основные проблемы безопасности систем Интернета вещей (IoT) и методы аутентификации. Сравниваются парольная, токенная и сертификатная, многофакторная аутентификация, механизм «запрос–ответ» и криптографические методы. Показано, что универсального метода нет, а выбор зависит от ресурсов устройства и модели угроз.

Ключевые слова: Интернет вещей, аутентификация, кибербезопасность, «запрос–ответ», управление ключами.

Kirish

Buyumlar Interneti sensorlar, ijro mexanizmlari, shlyuzlar va bulutli xizmatlarni yagona axborot muhitiga birlashtirib, aqlli uy, sanoat avtomatlashtirish, energetika, sog‘liqni saqlash va transport tizimlarining ajralmas qismiga aylangan. IoT Analytics kompaniyasining bozor tahliliga ko‘ra, dunyo bo‘yicha faol ulangan IoT qurilmalari soni 2024-yilda 18,5 mlrd tani tashkil etgan, 2025-yil yakuni uchun esa 2025-yil birinchi yarmi ma’lumotlari asosida 21,1 mlrd ta qurilma prognoz qilingan [1]. Ushbu hisob smartfon, kompyuter va planshetlarni o‘z ichiga olmaydi hamda xavfsizlik hodisalarini emas, balki faqat ulanishlar miqyosini tavsiflaydi.

Qurilmalar sonining ortishi hujum yuzasini kengaytiradi. Ilmiy adabiyotda autentifikatsiya IoT ilovalarida maxfiylik, yaxlitlik va foydalanish imkoniyatini ta’minlashning zaruriy sharti sifatida ko‘riladi [2]. NIST IoT mahsulotlarida mijozlar xavfni kamaytirish uchun foydalanishi mumkin bo‘lgan kiberxavfsizlik imkoniyatlari ko‘pincha yetishmasligini qayd etib, ishlab chiqaruvchilarga mahsulot bozorga chiqarilgunga qadar bajariladigan asosiy faoliyatlarni tavsiya qiladi [3]. Shu bois tadqiqot muammosi xavfsizlik darajasi va hisoblash xarajatlari o‘rtasidagi muvozanatni hisobga olgan holda autentifikatsiya usulini qurilma va tahdid modeliga mos tanlash bilan bog‘liq. Tezisning maqsadi IoT tizimlaridagi asosiy tahdidlarni autentifikatsiya bilan aloqasi nuqtayi nazaridan tahlil qilish va asosiy autentifikatsiyalash usullarini qiyosiy baholash.

IOT tizimlaridagi xavfsizlik muammolari

Kuchsiz yoki standart parollar. Ko‘plab iste’molchi qurilmalarining barcha nusxalari uchun bir xil standart login va parol bilan sotilishi IoTdagi ko‘plab xavfsizlik hodisalarining manbai bo‘lgan. Shu sababli ETSI EN 303 645 standarti zavod holatidan tashqari barcha holatlarda parollar qurilmaga xos yoki foydalanuvchi tomonidan belgilangan bo‘lishini va tarmoq orqali parolni tanlab topish (brute force) hujumlarini amalda samarasiz qiluvchi mexanizm mavjud bo‘lishini talab qiladi [4].

Ruxsatsiz kirish. Tarmoq interfeysi orqali qurilma funksiyalariga autentifikatsiyasiz kirish xavfsizlik konfiguratsiyasini o‘zgartirish va shaxsiy ma’lumotlarni olish imkonini beradi [4]. Autentifikatsiya subyektning haqiqiyligini tasdiqlaydi, ammo unga qaysi amallar ruxsat etilishini avtorizatsiya va kirishni boshqarish mexanizmlari belgilaydi.

Soxta qurilmalar va identifikatorni qalbakilashtirish. Qurilma faqat ochiq identifikator (seriya raqami, MAC manzil) bilan tanilsa, tajovuzkor uni nusxalab, tarmoqqa soxta tugun ulashi mumkin. Autentifikatsiya va kalit kelishuvi protokollari bo‘yicha sharhlarda soxtalashtirish, o‘rtadagi odam va qurilmani qo‘lga olish hujumlari protokol xavfsizligini baholashning asosiy mezonlari sifatida ko‘rib chiqiladi [5]. Shu bois identifikator kriptografik dalilga - qurilmaga xos maxfiy kalit, yopiq kalit yoki apparat xususiyatiga bog‘lanishi lozim.

Uzatishda tutib olish va o‘zgartirish. Simsiz kanalda uzatiladigan ma’lumotlar shifrlanmasa yoki yaxlitligi tekshirilmasa, ular tinglanishi va o‘zgartirilishi mumkin. Faqat seans boshida bajarilgan autentifikatsiya bu tahdidni bartaraf etmaydi: har bir xabar autentifikatsiyalangan shifrlash yoki xabar autentifikatsiya kodi (MAC) bilan himoyalanishi kerak.

Takroriy xabar yuborish (replay attack). Tajovuzkor avval tutib olingan haqiqiy xabarni qayta yuborib, tizimni aldashga urinadi. Xabarning kriptografik to‘g‘riligi uning yangiligini kafolatlamaydi, shuning uchun protokolda nonce, vaqt belgisi yoki ketma-ketlik raqami va ularni tekshirish qoidasi bo‘lishi zarur [5]. DTLS 1.3 yozuvlarga ketma-ketlik raqamlarini qo‘shadi, biroq qayta yuborishni aniqlash funksiyasi unda ixtiyoriy ekanini hisobga olish kerak [6].

Kalitlarni saqlash va boshqarish. Kalitlar, parollar va sertifikatlarning yopiq qismi kabi muhim xavfsizlik parametrlari doimiy xotirada xavfsiz saqlanishi, dastur kodiga qattiq yozilmasligi va qurilma sinfi bo‘yicha takrorlanmasligi kerak, chunki global kalitning oshkor bo‘lishi bir turdagi qurilmalarga keng ko‘lamli hujum imkonini beradi [4]. Kalitlarni yaratish va saqlash muammosiga apparat yechimi sifatida fizik klonlanmaydigan funksiyalar (PUF) ko‘rilmoqda, ammo ularning arxitekturasi va hujumlarga chidamliligi alohida baholanishi talab etiladi [7].

Resurslarning cheklanganligi. Batareyali sensorlar va mikrokontrollerlarda hisoblash quvvati, xotira, aloqa kengligi va energiya cheklangan, shu sababli an’anaviy internet xavfsizlik texnologiyalarini to‘g‘ridan-to‘g‘ri ko‘chirish har doim ham imkonli emas [5]. Ushbu ehtiyojga javoban NIST 2025-yilda cheklangan qurilmalar uchun Ascon oilasiga asoslangan yengil kriptografiya standartini (autentifikatsiyalangan shifrlash, xesh va XOF funksiyalari) e’lon qilgan.

Autentifikatsiyalash usullari

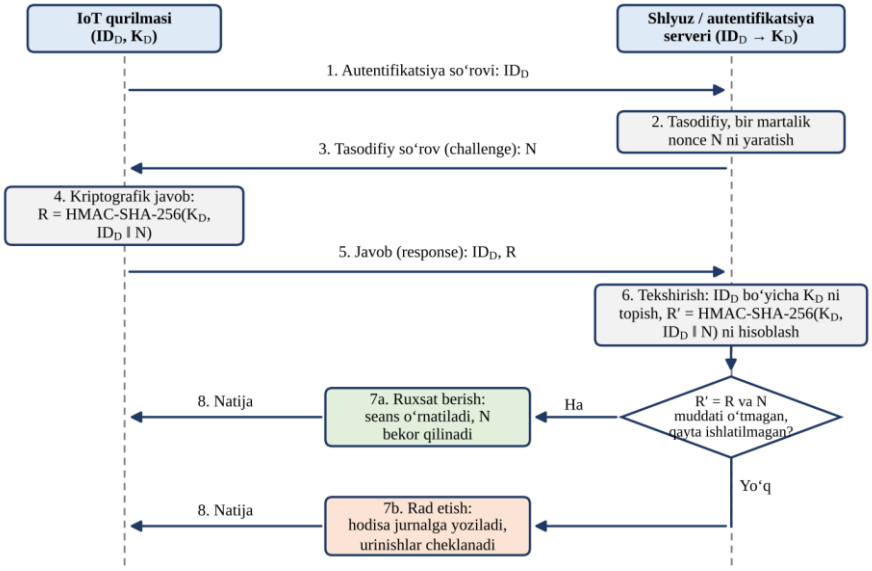
Autentifikatsiya foydalanuvchi–qurilma, qurilma–shlyuz va qurilma–bulut sathlarida bajariladi. Protokollarning hujumlarga chidamliligi hamda hisoblash va aloqa xarajatlari ular asosidagi kriptografik texnikaga bevosita bog‘liq [9]; shu nuqtayi nazardan quyidagi usullar ko‘rib chiqiladi [2].

Parolga asoslangan autentifikatsiya subyektning maxfiy satrni bilishiga tayanadi. U oddiy va qo‘shimcha apparat talab qilmaydi, ammo tanlab topish, lug‘at hujumlari va ma’lumotlar bazasi oshkor bo‘lishiga moyil. NIST SP 800-63B-4 hujjati autentifikatorlarni tanlash va boshqarish, jumladan parollarga oid talablarni belgilaydi; u asosan inson-foydalanuvchilar autentifikatsiyasiga mo‘ljallangan [10]. ETSI EN 303 645 esa mashinalararo autentifikatsiyada paroldan foydalanmaslikni tavsiya qiladi [4].

Token va raqamli sertifikatga asoslangan autentifikatsiya. Token yondashuvida subyekt ishonchli serverdan muayyan muddat va huquqlar doirasida amal qiluvchi kirish tokenini oladi.

ACE-OAuth freymvorki OAuth 2.0 va CoAP asosida bunday mexanizmni cheklangan IoT muhitiga moslashtiradi; u asosan avtorizatsiyani ta’minlaydi va tomonlar o‘rtasidagi himoyani alohida profillar orqali amalga oshiradi [11]. Sertifikatga asoslangan usulda qurilmaning ochiq kaliti ishonchli markaz imzosi bilan bog‘lanadi; bu katta tarmoqlarda masshtablanuvchanlikni oshiradi, biroq sertifikatlarni tekshirish, bekor qilish va yangilash infratuzilmasini talab etadi [5].

Ko‘p omilli autentifikatsiya (MFA) bilim, egalik va biometrik omillardan kamida ikkitasini birlashtiradi. SP 800-63B-4 yuqori ishonch darajalari uchun ko‘p omilli va fishingga chidamli autentifikatorlarga oid talablarni belgilaydi [10], ETSI EN 303 645 esa parol va bir martalik parolni birgalikda qo‘llashni misol sifatida keltiradi [4]. IoT sharoitida MFA asosan qurilmani boshqaruvchi inson (mobil ilova, bulut paneli) uchun qo‘llanadi va inson ishtirokisiz ishlaydigan sensorlarga bevosita mos kelmaydi.



1-rasm. IoT tizimida challenge–response asosidagi autentifikatsiya jarayonining umumiy sxemasi

Challenge–response mexanizmi. Tekshiruvchi tomon tasodifiy va bir martalik nonce yuboradi, isbotlovchi tomon esa maxfiy kalit yordamida unga bog‘liq kriptografik javob qaytaradi; kalitning o‘zi kanal orqali uzatilmaydi. Javob har bir urinish uchun noyob bo‘lgani sababli tutib olingan qiymatni qayta ishlatish samarasiz bo‘ladi, biroq bunday qiymatlarni ham maxfiy kanalda uzatish yaxshi amaliyot hisoblanadi [4]. Mexanizmning umumiy bosqichlari 1-rasmda keltirilgan.

Sxemada HMAC-SHA-256 misol sifatida olingan; xuddi shu bosqichlarni AES-CMAC yoki Ed25519 imzosi bilan ham qurish mumkin. Ruxsat berish uchun javob mos kelishi bilan birga nonce muddati o‘tmagan va avval ishlatilmagan bo‘lishi shart. Sxema yangi protokol emas, balki mexanizm bosqichlarining umumlashtirilgan tasviri bo‘lib, o‘zaro autentifikatsiya va seans kalitini kelishish bosqichlarini o‘z ichiga olmaydi.

Kriptografik autentifikatsiya. Simmetrik yondashuvda HMAC-SHA-256 (xesh funksiyaga asoslangan) va AES-CMAC (blokli shifrga asoslangan) xabar autentifikatsiya kodlari tomonlarning umumiy maxfiy kaliti yordamida xabar manbasi va yaxlitligini tasdiqlaydi. Ular kam hisoblash talab qiladi, lekin kalitni oldindan xavfsiz taqsimlashni talab etadi va rad etib bo‘lmaslikni (non-repudiation) ta’minlamaydi [5]. Ed25519 esa ochiq kalitli elektron raqamli imzo sxemasi bo‘lib, FIPS 186-5 standartida EdDSA tarkibida tasdiqlangan [12]: imzoni faqat yopiq kalit egasi yaratadi, ochiq kalit egasi esa uni tekshiradi. Bu vositalar kriptografik primitivlar bo‘lib, to‘liq autentifikatsiya protokoli bilan aynan bir narsa emas: protokol nonce yoki

hisoblagichlar, kalitlarni boshqarish, xatoliklarni qayta ishlash va xavfsiz kanalni o‘rnatish qoidalarini ham belgilashi kerak. Masalan, DTLS 1.3 protokoli tinglash, o‘zgartirish va xabarlarni soxtalashtirishdan himoyalangan kanalni yaratadi [6].

Qiyosiy tahlil

1-jadvalda ko‘rib chiqilgan usullar umumlashtirilgan. Baholar nisbiy xarakterga ega, chunki har bir usulning samaradorligi qurilma resurslari va tahdid modeliga bog‘liq.

1-jadval

IoT tizimlarida autentifikatsiyalash usullarining qiyosiy tavsifi

Autentifikatsiyalash usuli	Ishlash prinsipi	Afzalliklari	Cheklovlari	IoT tizimlarida qo‘llash xususiyatlari
Parolga asoslangan	Subyekt maxfiy satrni taqdim etadi, tekshiruvchi uni saqlangan qiymat bilan solishtiradi	Amalga oshirish oson, qo‘shimcha apparat talab qilmaydi	Tanlab topish, standart va takroriy parollar, bazaning oshkor bo‘lishi	Asosan foydalanuvchi interfeyslari uchun; qurilmaga xos parol va urinishlarni cheklash zarur; M2M uchun tavsiya etilmaydi [4], [10]
Token va raqamli sertifikat	Ishonchli server bergan kirish tokeni yoki sertifikatlash markazi imzolagan ochiq kalit	Markazlashgan huquq boshqaruvi, katta tarmoqlarda masshtablanuvchanlik	Token o‘g‘irlanishi; PKI, sertifikatni bekor qilish va yangilash xarajatlari	Token - ACE-OAuth orqali avtorizatsiya; sertifikat - shlyuz va resursi yetarli qurilmalarda qulayroq [11], [5]
Ko‘p omilli	Ikki va undan ortiq mustaqil omil (bilim, egalik, biometriya)	Bitta omil buzilganda ham himoya saqlanadi	Foydalanish murakkabligi, qo‘shimcha qurilma yoki kanal talabi	Qurilmani boshqaruvchi inson uchun; avtonom sensorlarga bevosita mos emas [10], [4]

Autentifikatsiyalash usuli	Ishlash prinsipi	Afzalliklari	Cheklovlari	IoT tizimlarida qo‘llash xususiyatlari
Challenge–response	Tasodifiy nonce ga maxfiy kalit asosida hisoblangan javob qaytariladi	Kalit uzatilmaydi, qayta yuborish hujumiga chidamli	Nonce sifati va holatini saqlash zarur; o‘zi kanalni shifrlamaydi	Simmetrik primitivlar bilan resursi cheklangan qurilmalarga mos [4], [5]
Kriptografik (MAC va raqamli imzo)	HMAC-SHA-256, AES-CMAC - umumiy maxfiy kalit; Ed25519 - yopiq/ochiq kalit juftligi	MAC - tez va kam resurs talab qiladi; imzo - rad etib bo‘lmaslik, maxfiy kalitni taqsimlash shart emas	MAC - kalitni xavfsiz taqsimlash talabi; imzo - ko‘proq hisoblash, ochiq kalit haqiqiyligini tasdiqlash	Qurilmaga xos kalitlar va xavfsiz saqlash (SE, TEE, PUF) bilan birga qo‘llanadi [12], [7]

Muhokama

Qiyosiy tahlil usullar bir-birini almashtirmasligini, balki turli sathlarda bir-birini to‘ldirishini ko‘rsatadi. Inson ishtirok etadigan boshqaruv interfeyslari uchun qurilmaga xos yoki foydalanuvchi belgilagan parolni ko‘p omilli autentifikatsiya bilan birga qo‘llash maqsadga muvofiq, mashinalararo aloqada esa paroldan ko‘ra qurilmaga xos kalitga asoslangan challenge–response yoki raqamli imzo mexanizmlari afzal [4]. Juda cheklangan sensorlarda simmetrik MAC va yengil kriptografiya [8] qulayroq bo‘lishi mumkin; shlyuz va resursi yetarli qurilmalarda esa sertifikatlar va Ed25519 kabi imzolar masshtablanuvchanlikni oshiradi.

Resurs-cheklangan qurilmalar uchun hisoblash va aloqa xarajatlarining pastligi, qurilmaga xos maxfiy parametrlar, kalitlarning xavfsiz saqlanishi, kriptografik algoritmlarni almashtirish imkoniyati (kriptoagillik) va urinishlarni cheklash muhim talablardir [4], [9]. Har qanday usulning amaliy xavfsizligi kalitlarni boshqarish jarayoniga tayanadi: kalitni yaratish, taqsimlash, yangilash va bekor qilish hayotiy sikl davomida nazorat qilinmasa, kuchli algoritm ham kutilgan himoyani bermaydi.

Autentifikatsiya tahdidlarning faqat bir qismini bartaraf etadi. Qayta yuborish hujumidan himoya nonce yoki hisoblagichni tekshirish qoidasini, uzatishdagi tutib olishdan himoya esa autentifikatsiyalangan shifrlash yoki DTLS 1.3 kabi xavfsiz kanalni talab qiladi [6]; dasturiy ta’minotni xavfsiz yangilash va ortiqcha interfeyslarni o‘chirish kabi choralar ham alohida zarur [4]. Mazkur tezisda amaliy o‘lchovlar o‘tkazilmagan, shu sababli usullarning ishlash vaqti va energiya sarfiga oid xulosalar manbalardagi sifat tahliliga asoslangan.

Xulosa

IoT tizimlarida autentifikatsiya ruxsatsiz kirish, soxta qurilma ulanishi va qayta yuborish hujumlariga qarshi asosiy himoya chizig‘i hisoblanadi, biroq u shifrlash, yaxlitlik nazorati va kalitlarni boshqarish choralarisiz yetarli emas. Usul tanloviga qurilmaning hisoblash, xotira va energiya resurslari, inson yoki mashina ishtiroki, tahdid modeli va kalit infratuzilmasining mavjudligi ta’sir qiladi. Xavfsizlik va resurs samaradorligi o‘rtasidagi muvozanatga simmetrik

MAC va yengil kriptografiyani cheklangan tugunlarda, raqamli imzo va sertifikatlarni esa shlyuz va server sathida qo‘llash orqali erishish mumkin. Amaliy tavsiya sifatida universal standart parollardan voz kechish, har bir qurilmaga noyob kalit berib, uni himoyalangan xotirada saqlash, mashinalararo autentifikatsiyani nonce asosidagi challenge–response mexanizmi orqali amalga oshirish hamda aloqani xavfsiz kanal protokoli bilan himoyalash taklif etiladi.

Foydalanilgan adabiyotlar

1. S. Sinha, “State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally,” IoT Analytics, Oct. 28, 2025. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/ (accessed Oct. 16, 2026).

A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, “A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions,” J. Netw. Comput. Appl., vol. 204, Art. no. 103414, 2022, doi: 10.1016/j.jnca.2022.103414.

2. M. Fagan, K. Megas, B. Cuthill, J. Marron, and B. Hoehn, “Foundational cybersecurity activities for IoT product manufacturers,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST IR 8259r1, Apr. 2026, doi: 10.6028/NIST.IR.8259r1.

3. “CYBER; Cyber security for consumer Internet of Things: Baseline requirements,” ETSI, Sophia Antipolis, France, ETSI EN 303 645 V3.1.3, Sep. 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (accessed Oct. 16, 2026).

4. M. K. Hasan, Z. Weichen, N. Safie, F. R. A. Ahmed, and T. M. Ghazal, “A survey on key agreement and authentication protocol for Internet of Things application,” IEEE Access, vol. 12, pp. 61642–61666, 2024, doi: 10.1109/ACCESS.2024.3393567.

5. E. Rescorla, H. Tschofenig, and N. Modadugu, “The Datagram Transport Layer Security (DTLS) protocol version 1.3,” IETF, RFC 9147, Apr. 2022, doi: 10.17487/RFC9147.

A. Al-Meer and S. Al-Kuwari, “Physical unclonable functions (PUF) for IoT devices,” ACM Comput. Surv., vol. 55, no. 14s, Art. no. 314, pp. 1–31, 2023, doi: 10.1145/3591464.

6. M. Sönmez Turan, K. A. McKay, D. Chang, J. Kang, and J. Kelsey, “Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST SP 800-232, Aug. 2025, doi: 10.6028/NIST.SP.800-232.

7. S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, A. Alabdulatif, and A. Alnajim, “Internet of Things authentication protocols: Comparative study,” Comput. Mater. Continua, vol. 79, no. 1, pp. 65–91, 2024, doi: 10.32604/cmc.2024.047625.

8. D. Temoshok, J. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. Richer, “Digital identity guidelines: Authentication and authenticator management,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST SP 800-63B-4, Jul. 2025, doi: 10.6028/NIST.SP.800-63B-4.

9. L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, “Authentication and authorization for constrained environments using the OAuth 2.0 framework (ACE-OAuth),” IETF, RFC 9200, Aug. 2022, doi: 10.17487/RFC9200.

10. Nat. Inst. Standards Technol., “Digital signature standard (DSS),” FIPS PUB 186-5, Feb. 2023, doi: 10.6028/NIST.FIPS.186-5.

BUYUMLAR INTERNETI TIZIMLARIDA FOYDALANUVCHILARNI AUTENTIFIKATSIYALASH USULLARINING TASNIFI VA QIYOSIY TAHLILI

Olimov I.S., Karimov A.A., Daminov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda Buyumlar Interneti (IoT) tizimlarida foydalanuvchilarni autentifikatsiyalash usullari omillar soni, kriptografik asos, arxitektura va maxfiylik darajasi bo‘yicha tasniflanadi. Parolga asoslangan, ikki va uch omilli, parolsiz hamda xesh va ECC asosidagi sxemalar xavfsizlik talablari nuqtayi nazaridan qiyosiy baholanadi. Omillar sonini oshirishning o‘zi xavfsizlikni kafolatlamasligi, usul tanlovi tahdid modeli va resurslarga bog‘liq ekani ko‘rsatiladi.

Kalit so‘zlar: Buyumlar Interneti, foydalanuvchi autentifikatsiyasi, ko‘p omilli autentifikatsiya, anonimlik, tasniflash.

Аннотация. В тезисе методы аутентификации пользователей в системах Интернета вещей (IoT) классифицируются по числу факторов, криптографической основе, архитектуре и уровню конфиденциальности. Парольные, двух- и трёхфакторные, беспарольные схемы, а также схемы на основе хеш-функций и ECC сравниваются с точки зрения требований безопасности. Показано, что увеличение числа факторов само по себе не гарантирует безопасность, а выбор метода зависит от модели угроз и ресурсов.

Ключевые слова: Интернет вещей, аутентификация пользователей, многофакторная аутентификация, анонимность, классификация.

Kirish

Buyumlar Interneti aqlli uy, sog‘liqni saqlash, sanoat va shahar infratuzilmasida sensorlar va ijro qurilmalarini masofadan boshqarish imkonini beradi. IoT Analytics kompaniyasining bozor tahliliga ko‘ra, dunyo bo‘yicha faol ulangan IoT qurilmalari soni 2024-yilda 18,5 mlrd tani tashkil etgan, 2025-yil yakuni uchun esa 21,1 mlrd ta qurilma prognoz qilingan [1]. Bu raqamlar ulanishlar miqyosini tavsiflaydi va xavfsizlik hodisalariga oid statistika hisoblanmaydi.

IoT tizimida autentifikatsiya ikki xil vazifani bajaradi: qurilmalarning bir-biriga nisbatan haqiqiyligini tasdiqlash va inson-foydalanuvchining qurilma yoki xizmatga kirish huquqini tekshirish [2]. Foydalanuvchi autentifikatsiyasining o‘ziga xos jihati shundaki, unda inson tomonidan esda saqlanadigan parol, foydalanuvchi qo‘lidagi qurilma va biometrik xususiyatlar ishtirok etadi, foydalanuvchi esa ko‘pincha Internet orqali shlyuz va sensorlarga masofadan murojaat qiladi [3]. Adabiyotda bunday sxemalar soni juda ko‘p bo‘lsa-da, ular turli mezonlar bo‘yicha tavsiflanadi, bu esa ularni taqqoslashni qiyinlashtiradi. Tezisning maqsadi - IoT tizimlarida foydalanuvchi autentifikatsiyasi usullarini yagona mezonlar asosida tasniflash va ularni xavfsizlik talablari nuqtayi nazaridan qiyosiy tahlil qilish.

Arxitektura, tahdid modeli va xavfsizlik talablari

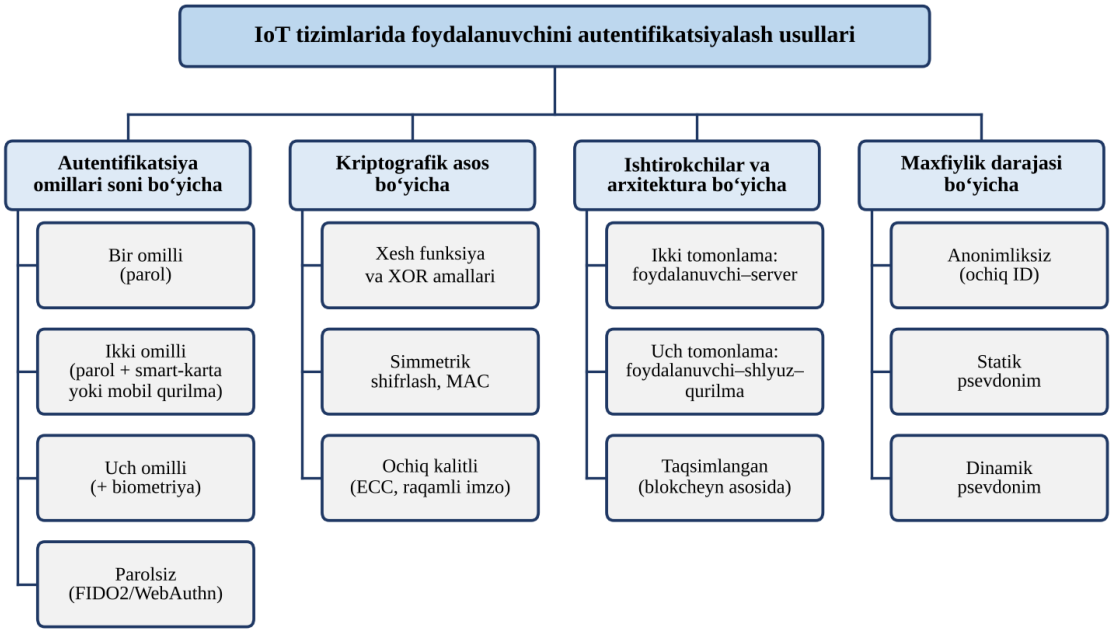
Arxitektura. Odatiy modelda to‘rt ishtirokchi bor: foydalanuvchi (smartfon yoki smart-karta bilan), shlyuz, IoT qurilmasi (sensor) va ro‘yxatdan o‘tkazish markazi. Sxemalar odatda ro‘yxatdan o‘tish, tizimga kirish (login), o‘zaro autentifikatsiya va seans kalitini kelishish hamda parol yoki biometriyani yangilash bosqichlaridan iborat bo‘ladi [4]. Aqlli uy tizimlarida foydalanuvchi qurilmalarga shlyuz orqali masofadan murojaat qiladi va bu yerda autentifikatsiya bilan birga seans kaliti ham o‘rnatilishi talab etiladi [3].

Tahdid modeli. Tahlillarda tajovuzkor ochiq kanaldagi xabarlarni tinglash, to‘sib qolish, o‘zgartirish va qayta yuborish imkoniyatiga ega deb hisoblanadi. Bundan tashqari, u yo‘qotilgan smart-karta yoki mobil qurilmadan ma’lumotlarni chiqarib olishi va parolni oflayn tanlab topishga urinishi mumkin [5]. Kuchli tahdid modelida tajovuzkor omillardan birini (masalan, parolni) allaqachon qo‘lga kiritgan deb faraz qilinadi [6]. Qurilmani qo‘lga olish, foydalanuvchi, shlyuz yoki qurilma nomidan harakat qilish va imtiyozli ichki xodim hujumlari ham alohida ko‘rib chiqiladi [3].

Xavfsizlik talablari. Asosiy talablarga o‘zaro autentifikatsiya, seans kalitini xavfsiz kelishish, foydalanuvchi anonimligi va kuzatib bo‘lmaslik, oldinga maxfiylik (forward secrecy), desinxronizatsiyaga chidamlilik va resurs tejamkorligi kiradi [5]. Ko‘p omilli sxemalar uchun qo‘shimcha ravishda omillarning bir-biridan farqliligi va mustaqilligi hamda bitta omil oshkor bo‘lganda qolganlarining himoyasi saqlanishi talab etiladi [6].

Foydalanuvchi autentifikatsiyasi usullarining tasnifi

Tahlil qilingan manbalar asosida usullar to‘rtta mezon bo‘yicha tasniflandi (1-rasm). Bu mezonlar bir-birini istisno etmaydi: har bir aniq sxema bir vaqtning o‘zida barcha to‘rt guruhga tegishli bo‘ladi.



1-rasm. IoT tizimlarida foydalanuvchini autentifikatsiyalash usullarining tasnifi

Omillar soni bo‘yicha. Bir omilli usulda faqat parol ishlatiladi; u oddiy, ammo parolni tanlab topish va standart parollar muammosiga moyil, shu bois ETSI EN 303 645 parollar qurilmaga xos yoki foydalanuvchi tomonidan belgilangan bo‘lishini talab qiladi [7]. Ikki omilli usulda parolga smart-karta yoki mobil qurilma qo‘shiladi, uch omillida esa biometriya ham ishtirok etadi. NIST SP 800-63B-4 biometriyani mustaqil autentifikator sifatida emas, balki jismoniy autentifikator bilan birga qo‘llashni nazarda tutadi [8]. Parolsiz usullarda, xususan FIDO2/WebAuthn texnologiyasida, foydalanuvchi qurilmasida saqlanadigan yopiq kalit va muayyan xizmatga bog‘langan ochiq kalitli hisob ma’lumotlari ishlatiladi [9]; SP 800-63B-4 bunday autentifikatorlarni fishingga chidamli turlar qatorida ko‘rib chiqadi [8].

Kriptografik asos bo‘yicha. Xesh funksiya va XOR amallariga asoslangan sxemalar eng kam hisoblash talab qiladi va resurs-cheklangan qurilmalar uchun keng taklif etiladi, ammo ularda oldinga maxfiylik va anonimlikni bir vaqtda ta’minlash qiyin [5]. Protokollarning hujumlarga

chidamliligi va xarajatlari ishlatilgan kriptografik texnikaga bevosita bog‘liq [10]. Elliptik egri chiziqlarga (ECC) asoslangan sxemalar kalit kelishuvi orqali oldinga maxfiylikni ta’minlashga imkon beradi, biroq ko‘proq hisoblash talab qiladi [4]; ECDSA va EdDSA raqamli imzolari FIPS 186-5 standartida belgilangan [11].

Arxitektura bo‘yicha. Ikki tomonlama sxemalarda foydalanuvchi bevosita server bilan autentifikatsiyadan o‘tadi. Uch tomonlama sxemalarda shlyuz foydalanuvchi va resurs-cheklangan qurilma o‘rtasida ishonchli vositachi bo‘ladi [3]. Markazlashgan ishonch nuqtasiga bog‘liqlikni kamaytirish uchun blokcheyn asosidagi taqsimlangan yondashuvlar, biometrik va mashinali o‘qitishga asoslangan usullar ham tadqiq etilmoqda [12].

Maxfiylik darajasi bo‘yicha. Ochiq identifikator ishlatilganda foydalanuvchini kuzatish oson. Statik psevdonim haqiqiy identifikatorni yashiradi, ammo seanslarni bir-biriga bog‘lash imkonini qoldiradi. Har seansdan keyin yangilanadigan dinamik psevdonim kuzatib bo‘lmaslikni ta’minlaydi, lekin xabar yo‘qolganda tomonlar holatining desinxronizatsiyasiga olib kelishi mumkin; bu muammoni hal qiluvchi yechimlar qo‘shimcha xotira yoki aloqa bosqichlarini talab qiladi [5].

Qiyosiy tahlil

1-jadvalda asosiy usullar umumlashtirilgan. Baholar nisbiy xarakterga ega, chunki aniq sxemaning xavfsizligi uning protokol dizayni va tahdid modeliga bog‘liq.

1-jadval

IoT tizimlarida foydalanuvchini autentifikatsiyalash usullarining qiyosiy tavsifi

Autentifikatsiyalash usuli	Ishlash prinsipi	Afzalliklari	Cheklovlari	IoT tizimlarida qo‘llash xususiyatlari
Parolga asoslangan (bir omilli)	Foydalanuvchi parolni kiritadi, server uning xesh qiymatini tekshiradi	Oddiy, qo‘shimcha qurilma talab qilmaydi	Oflayn va onlayn tanlab topish, standart parollar, fishing	Faqat past xavfli xizmatlar uchun; qurilmaga xos parol va urinishlarni cheklash zarur [7]
Ikki omilli (parol + smart-karta yoki mobil qurilma)	Parol va qurilmada saqlangan maxfiy parametrlar birgalikda ishlatiladi	Bitta omil oshkor bo‘lganda ham himoya saqlanadi	Karta yoki qurilma yo‘qolganda oflayn parol tanlash xavfi	Aqlli uy va WSN sxemalarida keng tarqalgan; shlyuz orqali ishlaydi [3], [5]
Uch omilli (+ biometriya)	Parol, qurilma va biometrik shablon birlashtiriladi	Yuqori ishonch darajasi	Biometriya maxfiy emas va almashtirib bo‘lmaydi; omillar bog‘liq bo‘lishi mumkin	Tibbiyot va muhim tizimlarda; biometrik shablonni himoyalash talab etiladi [6], [8]

Autentifikatsiyalash usuli	Ishlash prinsipi	Afzalliklari	Cheklovlari	IoT tizimlarida qo‘llash xususiyatlari
Parolsiz (FIDO2/WebAuthn)	Qurilmadagi yopiq kalit bilan xizmatga bog‘langan so‘rovga imzo qo‘yiladi	Fishingga chidamli, serverda parol saqlanmaydi	Mos autentifikator va brauzer/ilova qo‘llab-quvvatlashi kerak	Mobil ilova va bulut paneli orqali boshqaruvda qulay [9], [8]
Xesh va XOR asosidagi yengil sxemalar	Xesh qiymatlar va XOR bilan niqoblangan xabarlar almashinadi	Juda kam hisoblash va energiya talab qiladi	Oldinga maxfiylik va anonimlikni ta’minlash qiyin, desinxronizatsiya xavfi	Resursi cheklangan sensorli tarmoqlar uchun [5], [10]
ECC asosidagi sxemalar	ECDH orqali seans kaliti kelishiladi, imzo yoki MAC bilan tasdiqlanadi	Oldinga maxfiylik, kalit taqsimlash qulayligi	Ko‘proq hisoblash va aloqa xarajati	Shlyuz va mobil qurilma tomonida maqbul [4], [11]

Muhokama

Qiyosiy tahlil usullarni tanlashda “ko‘proq omil - yuqoriroq xavfsizlik” degan yondashuv yetarli emasligini ko‘rsatadi. Turli sohalardagi ko‘p omilli protokollar tahlilida ko‘pchilik sxemalarda dizayn darajasidagi kamchiliklar aniqlangan; ularning bir qismi rasmiy isbot va ekspert ko‘rigidan o‘tgan bo‘lsa-da, omillar bir-biriga bog‘liqligi yoki ma’lumot sizib chiqishiga chidamsizligi sababli zaif bo‘lib chiqqan [6]. Demak, omillar soni bilan birga ularning mustaqilligi va tahdid modelining realistikligi baholanishi lozim.

Resurs-cheklangan muhitda xesh va XOR asosidagi sxemalar samarali, ammo anonimlik, oldinga maxfiylik va desinxronizatsiyaga chidamlilik o‘rtasida murosaga borishga majbur qiladi [5]. ECC asosidagi sxemalar bu talablarni to‘liqroq qondiradi, lekin hisoblash yukini oshiradi [4]. Shu sababli amalda gibrid yondashuv maqsadga muvofiq: og‘ir amallar foydalanuvchi qurilmasi va shlyuzda, yengil simmetrik amallar esa sensor tomonida bajariladi. Sxemalarni baholashda ROR modelida formal isbot va AVISPA kabi vositalar bilan tekshirish keng qo‘llanadi [3], biroq u evristik xavfsizlik tahlilini almashtirmaydi [6]. Mazkur tezisda amaliy o‘lchovlar o‘tkazilmagan, shu sababli xarajatlarga oid xulosalar manbalardagi sifat tahliliga asoslangan.

Xulosa

IoT tizimlarida foydalanuvchi autentifikatsiyasi usullarini omillar soni, kriptografik asos, arxitektura va maxfiylik darajasi bo‘yicha tasniflash ularni yagona mezonlar asosida taqqoslash imkonini beradi. Tahlil shuni ko‘rsatadiki, omillar sonini oshirishning o‘zi xavfsizlikni kafolatlamaydi: omillarning mustaqilligi, oldinga maxfiylik, anonimlik va desinxronizatsiyaga chidamlilik birgalikda ta’minlanishi kerak. Resurs tejamkorligi va xavfsizlik o‘rtasidagi muvozanat uch tomonlama arxitekturada hisoblash yukini taqsimlash orqali erishiladi. Keyingi tadqiqotlar uchun yengil, uch omilli, anonim va desinxronizatsiyaga chidamli foydalanuvchi

autentifikatsiyasi algoritmini ishlab chiqish hamda uni formal va evristik usullarda tekshirish dolzarb yo‘nalish sifatida belgilanadi.

Foydalanilgan adabiyotlar

1. S. Sinha, “State of IoT 2025: Number of connected IoT devices growing 14% to 21.1 billion globally,” IoT Analytics, Oct. 28, 2025. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/ (accessed Oct. 16, 2026).

A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, “A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions,” J. Netw. Comput. Appl., vol. 204, Art. no. 103414, 2022, doi: 10.1016/j.jnca.2022.103414.

2. M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, “Secure remote user authenticated key establishment protocol for smart home environment,” IEEE Trans. Dependable Secure Comput., vol. 17, no. 2, pp. 391–406, 2020, doi: 10.1109/TDSC.2017.2764083.

3. M. K. Hasan, Z. Weichen, N. Safie, F. R. A. Ahmed, and T. M. Ghazal, “A survey on key agreement and authentication protocol for Internet of Things application,” IEEE Access, vol. 12, pp. 61642–61666, 2024, doi: 10.1109/ACCESS.2024.3393567.

4. J. Zhong, S. He, Z. Liu, and L. Xiong, “Lightweight anonymous authentication for IoT: A taxonomy and survey of security frameworks,” Sensors, vol. 25, no. 17, Art. no. 5594, 2025, doi: 10.3390/s25175594.

5. K. W. Ang, E. G. Chekole, and J. Zhou, “Unveiling the covert vulnerabilities in multi-factor authentication protocols: A systematic review and security analysis,” ACM Comput. Surv., vol. 57, no. 11, pp. 1–37, 2025, doi: 10.1145/3734864.

6. “CYBER; Cyber security for consumer Internet of Things: Baseline requirements,” ETSI, Sophia Antipolis, France, ETSI EN 303 645 V3.1.3, Sep. 2024. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (accessed Oct. 16, 2026).

7. D. Temoshok, J. Fenton, Y.-Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, and J. Richer, “Digital identity guidelines: Authentication and authenticator management,” Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST SP 800-63B-4, Jul. 2025, doi: 10.6028/NIST.SP.800-63B-4.

8. W3C Web Authentication Working Group, “Web Authentication: An API for accessing public key credentials - Level 2,” W3C Recommendation, Apr. 8, 2021. [Online]. Available: https://www.w3.org/TR/2021/REC-webauthn-2-20210408/ (accessed Oct. 16, 2026).

9. S. Dargaoui, M. Azrour, A. El Allaoui, A. Guezzaz, A. Alabdulatif, and A. Alnajim, “Internet of Things authentication protocols: Comparative study,” Comput. Mater. Continua, vol. 79, no. 1, pp. 65–91, 2024, doi: 10.32604/cmc.2024.047625.

10. Nat. Inst. Standards Technol., “Digital signature standard (DSS),” FIPS PUB 186-5, Feb. 2023, doi: 10.6028/NIST.FIPS.186-5.

A. Alotaibi, H. Aldawghan, and A. Aljughaiman, “A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions,” Sensors, vol. 25, no. 6, Art. no. 1649, 2025, doi: 10.3390/s25061649.

DPDK ASOSIDA ZARARLI DOMEN SO‘ROVLARINI INLINE FILTRLASH TIZIMI

Oripov P.X.
Kiberxavfsizlik markazi davlat muassasasi Kiberxavfsizlik sohasidagi ilmiy-tadqiqot bo‘limi

Annotatsiya. Maqolada tarmoqqa shaffof ko‘prik sifatida o‘rnatiladigan va zararli domenlarga murojaatni DNS darajasida bloklovchi DPDK asosidagi filtrlash tizimining arxitekturasi va ishlash usullari tavsiflanadi. Tizim har bir DNS so‘rovidagi domen nomini va uning ota-domenlarini xesh-jadvaldagi blocklist bilan solishtiradi, zararli so‘rovni tashlaydi yoki sinkhole javobi orqali foydalanuvchini bloklash sahifasiga yo‘naltiradi, DoT va DoH orqali chetlab o‘tishni cheklaydi hamda barcha so‘rovlarni tahlil uchun ClickHouse bazasida qayd etadi.

Kalit so‘zlar: DNS filtrlash, zararli domenlar, Protective DNS, DPDK, blocklist, sinkhole, DoT, DoH, ClickHouse.

Аннотация. В статье описываются архитектура и методы работы системы фильтрации на основе DPDK, которая устанавливается в сеть как прозрачный мост и блокирует обращения к вредоносным доменам на уровне DNS. Система сравнивает доменное имя каждого DNS-запроса и его родительские домены с блок-листом, хранящимся в хеш-таблице, отбрасывает вредоносный запрос или перенаправляет пользователя на страницу блокировки с помощью ответа sinkhole, ограничивает обход через DoT и DoH и регистрирует все запросы в базе данных ClickHouse для последующего анализа.

Ключевые слова: фильтрация DNS, вредоносные домены, Protective DNS, DPDK, блок-лист, sinkhole, DoT, DoH, ClickHouse.

Kirish

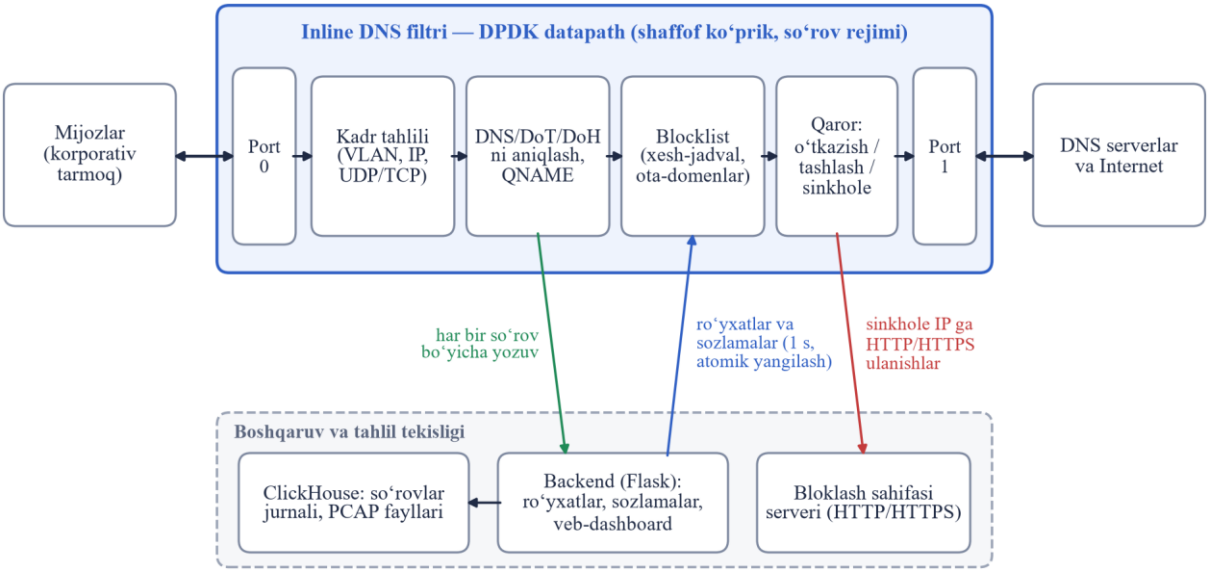
DNS (Domain Name System) internetning asosiy xizmatlaridan biri bo‘lib, domen nomlarini IP manzillarga aylantiradi [1, 2]. Deyarli har qanday tarmoq ulanishi DNS so‘rovidan boshlangani bois u hujumchilar uchun ham qulay kanal hisoblanadi: zararli dasturlar boshqaruv serverlarini domen nomlari orqali topadi, botnetlar esa statik qora ro‘yxatlarni chetlab o‘tish uchun domen generatsiyasi algoritmlaridan (DGA) foydalanadi [3]; DNS so‘rovlari ma’lumotlarni yashirincha sizdirish kanali sifatida ham qo‘llanadi [4]. Ma’lum zararli domenlarga murojaatni DNS darajasida bloklash (Protective DNS) ransomware, fishing, botnet va zararli dastur kampaniyalari samarasini sezilarli kamaytirishi mumkin, DNS so‘rovlari jurnallaridan esa hodisalarga javob berish va tahdid qidiruvida foydalaniladi [5].

Odatda bunday filtrlash rekursiv rezolverda, masalan, RPZ (Response Policy Zones) mexanizmi orqali amalga oshiriladi [6]. Biroq bu usul faqat shu rezolverga murojaat qiladigan mijozlarni qamraydi: tashqi rezolverlarga to‘g‘ridan-to‘g‘ri yoki shifrlangan kanallar - DoT (DNS over TLS) [7] va DoH (DNS over HTTPS) [8] - orqali yuborilgan so‘rovlar filtrdan chetda qoladi. Bunday hollarda tarmoq segmentidagi barcha DNS trafigini rezolver sozlamalaridan qat’i nazar nazorat qiluvchi inline filtrlash samarali yechim bo‘ladi. Quyida DPDK [9] asosida qurilgan shunday tizimning arxitekturasi va ishlash usullari ko‘rib chiqiladi.

Tizim arxitekturasi

Tizim ikki tarmoq porti o‘rtasiga shaffof ko‘prik (bump-in-the-wire) sifatida o‘rnatiladi: kadrlar MAC manzillari o‘zgartirilmasdan uzatiladi, shu bois tarmoq manzillash sxemasini o‘zgartirish talab etilmaydi (1-rasm). Ma’lumotlar tekisligi (datapath) DPDK kutubxonasining

l2fwd namunasi asosida qurilgan: har bir port alohida protsessor yadrosida uzilishlarsiz, so‘rov (polling) rejimida, 256 tagacha paketdan iborat guruhlar bilan qayta ishlanadi [9]. Har bir portda yo‘naltiriladigan trafik, tizimning o‘zi yaratadigan javoblar (sinkhole javoblari, TCP RST, bloklash sahifasi) va yadrodan qaytgan paketlar uchun alohida uzatish navbatlari ajratilgan. Tizim ikki rejimda ishlaydi: vfio-pci rejimida tarmoq kartasi to‘liq DPDK drayveriga o‘tkaziladi va maksimal tezlik ta’minlanadi; af_packet rejimida karta operatsion tizim yadrosida qoladi - bu rejim istalgan kartada ishlaydi, ammo sekinroq.



1-rasm. DNS filtrlash tizimining arxitekturasi

Boshqaruv va tahlil tekisligi datapathdan ajratilgan: Flask asosidagi backend ro‘yxatlar va sozlamalarni boshqaradi hamda veb-dashboardni taqdim etadi, so‘rovlar jurnali esa ClickHouse ustunli ma’lumotlar bazasida saqlanadi. Datapath bu tekislik bilan fayllar va lokal xabarlar orqali bog‘lanadi, shu bois backend ishlamay qolsa ham trafik oxirgi yuklangan ro‘yxatlar asosida filtrlanishda davom etadi.

DNS trafigini aniqlash va domenlarni moslashtirish

Datapath har bir kadrni Ethernet (ikkitagacha VLAN tegi), IP va UDP/TCP sathlarida tahlil qiladi. Oddiy DNS - 53-portdagi UDP yoki TCP trafigi; DoT - 853-portdagi TLS yozuvlari; DoH esa ma’lum DoH rezolverlarining manzillariga 443-port orqali ulanishlar sifatida aniqlanadi. So‘rovdan birinchi savolning nomi (QNAME) va turi (QTYPE) ajratiladi [2]: nom kichik harflarga o‘tkaziladi va formati qat’iy tekshiriladi, TCP orqali DNS uchun esa 2 baytli uzunlik prefiksi hisobga olinib, bitta segmentdagi bir nechta xabar ham tekshiriladi.

Blocklist 2^{22} savatli zanjirli xesh-jadvalda saqlanadi: kalitlar djb2 xesh-funksiyasi bilan hisoblanadi, satrlarni solishtirishdan oldin 32 bitli xesh qiymatlari taqqoslanadi. Avval so‘ralgan nomning o‘zi, so‘ngra uning har bir ota-domeni tekshiriladi: masalan, a.b.evil.com so‘rovi ro‘yxatdagi evil.com yozuvi orqali bloklanadi. Shunday qilib, tekshiruv xarajati ro‘yxat hajmiga emas, nomdagi yorliqlar soniga bog‘liq - har bir yorliq uchun bitta xesh-murojaat.

Ro‘yxatlar boshqaruv tekisligida birlashtiriladi: yuklangan va qo‘lda kiritilgan yozuvlar format bo‘yicha tekshiriladi, takrorlar va istisnolar chiqarib tashlanadi, natija esa faylga atomik yoziladi. Datapath fayl imzosini (inode, hajm, o‘zgartirish vaqti) har soniyada tekshiradi; o‘zgarish aniqlansa, yangi xesh-jadval asosiy oqimdan tashqarida quriladi va atomik ko‘rsatkich almashtirish orqali faollashtiriladi. Natijada ro‘yxatlar va sozlamalar trafikni to‘xtatmasdan yangilanadi.

Bloklash amallari va shifrlangan DNS

Bloklash siyosati 1-jadvalda jamlangan.

1-jadval.

Bloklash siyosati va amallari

Holat	Aniqlash mezoni	Amal
Zararli domen	QNAME yoki uning ota-domeni blocklistda	so‘rovni tashlash yoki sinkhole javobi: A so‘roviga sinkhole IP manzili (TTL 30 s), boshqa turlarga bo‘sh NOERROR javobi
Bloklash sahifasi	sinkhole IP manziliga HTTP (80) yoki HTTPS (443) ulanish	HTTP sahifani datapath ulanish holatini saqlamasdan yaratadi; HTTPS ulanish TAP orqali lokal TLS serverga uzatiladi; muqobil - HTTP 302 yo‘naltirish
DoT, DoQ	TCP 853-port (DoT) va UDP 853-port (DoQ) [10]	TCP ulanishga RST yuborish, UDP paketni tashlash
DoH	ma’lum DoH rezolverining nomi yoki IP manzili	nom so‘roviga NXDOMAIN javobi; 443-portdagi ulanishni uzish
Yaroqsiz so‘rov	QNAME ajratib bo‘lmaydi	sozlamaga ko‘ra bloklash

Sinkhole rejimida bloklangan UDP so‘rovi joyida javobga aylantirilib, kirish portidan mijozga qaytariladi, shu bois foydalanuvchi bloklash sababini tushuntiruvchi sahifani ko‘radi. HTTP sahifa kalitlangan boshlang‘ich ketma-ketlik raqami (ISN) va mijozning ACK javobini tekshirish orqali yuboriladi, bu esa kuchaytirish (amplification) hujumlariga yo‘l qo‘ymaydi. HTTPS uchun lokal sertifikatlash markazi har bir SNI nomiga sertifikat chiqaradi; markaz sertifikati mijozda o‘rnatilmagan bo‘lsa, brauzer ogohlantirish ko‘rsatadi. DoHni IP manzil bo‘yicha bloklash shu manzillardagi boshqa HTTPS xizmatlarini ham cheklashini hisobga olish lozim.

Monitoring va tahlil

Datapath har bir DNS so‘rovi uchun 14 maydonli yozuvni (vaqt, manba va manzil IP/port, protokol, domen, QTYPE, RCODE, javoblar soni, hajm, bloklash belgisi, qurilma porti, yo‘nalish) lokal UDP orqali backendga yuboradi. Yozuv bloklanmaydigan soketga jo‘natiladi: bufer to‘lsa yozuv tashlanadi, ammo trafik uzatilishi to‘xtamaydi. Backend yozuvlarni navbatga oladi va ClickHouse jadvaliga 5000 qatorgacha bo‘lgan guruhlar (batch) bilan yoki har 0,5 soniyada yozadi; jadval kunlar bo‘yicha bo‘limlarga (partition) ajratilgan, saqlash muddati esa toifalar (oddiy, bloklangan, shifrlangan) bo‘yicha TTL orqali boshqariladi. Dashboard real vaqtdagi hisoblagichlar, eng faol mijozlar va domenlar hamda bloklangan so‘rovlar jurnalini ko‘rsatadi; tanlangan toifadagi trafikni PCAP formatida yozib olish ham mumkin. DGA [3] va DNS tunnellash [4] kabi evristik aniqlash usullarini datapathga holat qo‘shmasdan, saqlangan ma’lumotlar ustida tahlil tekisligida qo‘llash rejalashtirilgan.

Xulosa

Inline DNS filtrlash tarmoq segmentidagi barcha DNS trafigini rezolver sozlamalaridan qat’i nazar nazorat qilish imkonini beradi. DPDK asosidagi datapath, xesh-jadval va ota-domenlar bo‘yicha moslashtirish, ro‘yxatlarni trafikni to‘xtatmasdan atomik yangilash hamda boshqaruv tekisligining ajratilishi bunday tizimni yuqori tezlikli tarmoqlarda qo‘llashga moslashtiradi. Sinkhole va bloklash sahifasi foydalanuvchini xabardor qiladi, so‘rovlar jurnali esa hodisalarni tekshirish va tahdid qidiruviga xizmat qiladi. Shifrlangan DNS kanallari (DoT, DoH) filtrlash

uchun asosiy murakkablik bo‘lib qolmoqda; evristik aniqlash usullarini qo‘shish va unumdorlikni sinov stendida baholash keyingi rivojlanish yo‘nalishlaridir.

Foydalanilgan adabiyotlar ro‘yxati

1. Mockapetris P. Domain Names - Concepts and Facilities. RFC 1034. IETF, 1987. DOI: 10.17487/RFC1034.

2. Mockapetris P. Domain Names - Implementation and Specification. RFC 1035. IETF, 1987. DOI: 10.17487/RFC1035.

3. Antonakakis M., Perdisci R., Nadji Y., Vasiloglou N., Abu-Nimeh S., Lee W., Dagon D. From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware // Proceedings of the 21st USENIX Security Symposium (USENIX Security ’12). Bellevue (WA): USENIX Association, 2012. P. 491–506.

4. Nadler A., Aminov A., Shabtai A. Detection of Malicious and Low Throughput Data Exfiltration over the DNS Protocol // Computers & Security. 2019. Vol. 80. P. 36–53. DOI: 10.1016/j.cose.2018.09.006.

5. Joint NSA and CISA Guidance on Strengthening Cyber Defense Through Protective DNS. CISA, 2021. 4 March. URL: https://www.cisa.gov/news-events/alerts/2021/03/04/joint-nsa-and-cisa-guidance-strengthening-cyber-defense-through-protective-dns (murojaat sanasi: 19.10.2026).

6. Vixie P., Schryver V. DNS Response Policy Zones (RPZ). Internet-Draft draft-vixie-dnsop-dns-rpz-00. IETF, 2018. URL: https://datatracker.ietf.org/doc/draft-vixie-dnsop-dns-rpz/ (murojaat sanasi: 19.10.2026).

7. Hu Z., Zhu L., Heidemann J., Mankin A., Wessels D., Hoffman P. Specification for DNS over Transport Layer Security (TLS). RFC 7858. IETF, 2016. DOI: 10.17487/RFC7858.

8. Hoffman P., McManus P. DNS Queries over HTTPS (DoH). RFC 8484. IETF, 2018. DOI: 10.17487/RFC8484.

9. Data Plane Development Kit (DPDK) Documentation. DPDK Project, [b.y.]. URL: https://doc.dpdk.org/guides/ (murojaat sanasi: 19.10.2026).

10. Huitema C., Dickinson S., Mankin A. DNS over Dedicated QUIC Connections. RFC 9250. IETF, 2022. DOI: 10.17487/RFC9250.

TLS ULANISHIGA QARATILGAN DDoS HUJUMLARINI SHIFRNI OCHMASDAN ANIQLASH VA BARTARAF ETISH USULLARI

Oripov P.X.
Kiberxavfsizlik markazi davlat muassasasi Kiberxavfsizlik sohasidagi ilmiy-tadqiqot bo‘limi

Annotatsiya. Maqolada TLS ulanishiga qaratilgan DDoS hujumlari ulanish bosqichlari - TCP, handshake va ma’lumot uzatish (record) - bo‘yicha tasniflanadi hamda ularni trafik shifrini ochmasdan aniqlash usullari ko‘rib chiqiladi. Protokol anomaliyasi filtrlari, TLS versiyasi va renegotiation cheklovlari, handshake yakunlanish nisbatiga asoslangan adaptiv metrika va JA4 barmoq izi DPDK asosidagi anti-DDoS tizimida amalga oshirilgan. Laboratoriya sinovida ClientHello flood hujumi shifrni ochmasdan aniqlanib, bloklandi.

Kalit so‘zlar: TLS, DDoS, handshake, ClientHello flood, renegotiation, JA4, shifrlangan trafik, DPDK, anti-DDoS.

Аннотация. В статье DDoS-атаки на TLS-соединения классифицируются по этапам соединения - TCP, handshake и передача данных (record) - и рассматриваются методы их обнаружения без расшифровки трафика. Фильтры протокольных аномалий, ограничения версии TLS и renegotiation, адаптивная метрика на основе коэффициента завершения handshake и отпечаток JA4 реализованы в системе защиты от DDoS (anti-DDoS) на основе DPDK. В лабораторном испытании атака ClientHello flood была обнаружена и заблокирована без расшифровки трафика.

Ключевые слова: TLS, DDoS, handshake, ClientHello flood, renegotiation, JA4, зашифрованный трафик, DPDK, anti-DDoS.

Kirish

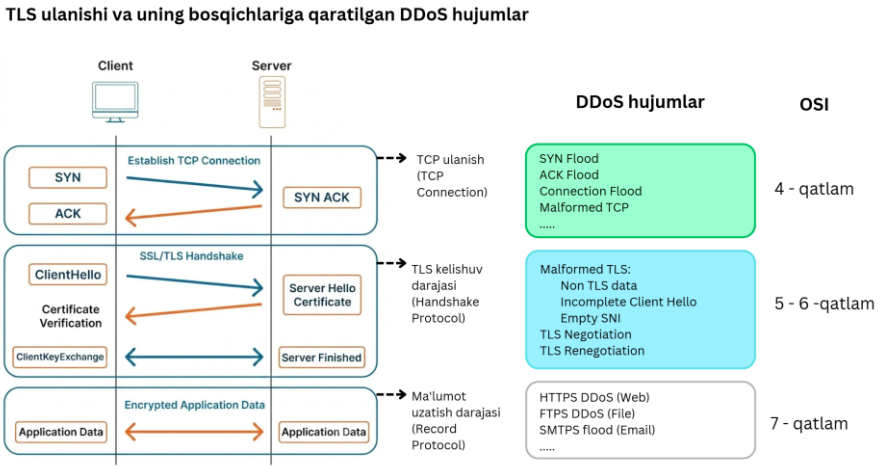
Bugungi kunda veb-xizmatlarning mutlaq ko‘pchiligi TLS protokoli orqali ishlaydi: dunyodagi eng yirik 1000 ta saytning 96 foizi HTTPSni, 88 foizi TLS 1.3 versiyasini qo‘llab-quvvatlaydi [1]. Bu TLS infratuzilmasini DDoS hujumlari uchun asosiy nishonlardan biriga aylantirdi: Cloudflare ma’lumotlariga ko‘ra, 2025-yilda DDoS hujumlari soni 47,1 millionga yetgan, HTTP DDoS hujumlari esa soniyasiga 200 million so‘rovdan oshgan [2]. TLS handshake jarayoni asimmetrik: THC-SSL-DOS mualliflari serverdagi hisoblash xarajatini mijoznikidan 15 barobar yuqori deb baholagan, mustaqil o‘lchovlarda esa bu nisbat shifr to‘plamiga bog‘liq bo‘lib, RSA-2048 uchun taxminan 6 barobarni tashkil etgan [3].

Shifrlangan trafikda hujumni ajratish murakkab: barcha oqimlarni deshifrlash qimmat va maxfiylikka zid, statik tezlik chegaralari (rate limit) qonuniy trafik keskin oshganda (flash crowd) noto‘g‘ri bloklaydi, botnetlarda esa IP manzil bo‘yicha bloklash yetarli emas. Quyida TLS hujumlarining tasnifi va faqat handshake metama’lumotlari hamda record sarlavhalariga tayanadigan himoya usullari ko‘rib chiqiladi.

TLS ulanish bosqichlari bo‘yicha hujumlar tasnifi

TLS ulanishi uch bosqichdan o‘tadi va har bir bosqichda serverning turli resurslari ishlaydi (1-rasm). TCP bosqichidagi (OSI 4-sathi) SYN, ACK va ulanishlar flood hujumlari yadro navbatlari va ulanishlar jadvalini band qiladi, ammo ochiq TCP sarlavhalari orqali aniqlanib, SYN-cookie kabi holatsiz usullar bilan bartaraf etiladi. Handshake bosqichida (5–6-sathlar) malformed TLS, negotiation flood va renegotiation flood hujumlari kriptografik amallar orqali protsessorni yuklaydi; ClientHello xabari shifrlanmagani bois bu hujumlarning izi metama’lumotlarda

saqlanadi. Ma’lumot uzatish bosqichida (7-sath) HTTPS flood hujumi to‘liq va haqiqiy handshakedan so‘ng shifrlangan so‘rovlar bilan ilova resurslarini band qiladi - bu eng qiyin aniqlanadigan tur.



1-rasm. TLS ulanishi bosqichlari va ularga qaratilgan DDoS hujumlari

Shifrni ochmasdan himoya usullari

Protokol anomaliyasi filtrlari. Har bir TLS yozuvi (record) ContentType, versiya va uzunlik maydonlaridan iborat 5 baytli sarlavha bilan boshlanadi [4]. Filtr birinchi yozuvning handshake (22) turida bo‘lishini, ContentType qiymati 20–23 oralig‘ida ekanini va ochiq handshake yozuvi uzunligi 2^{14} baytdan oshmasligini tekshiradi (shifrlangan yozuvlar uchun RFC 8446 $2^{14} + 256$ baytgacha ruxsat beradi). ClientHelloning e’lon qilingan uzunligi kelgan baytlardan katta bo‘lsa, belgilangan muddat kutiladi, so‘ngra ulanish uziladi - bu TLS ko‘rinishidagi Slowloris hujumiga qarshi chora. Noma’lum shifr to‘plamlari hamda bo‘sh yoki himoyalanmaydigan domenga tegishli SNI [5] ham rad etiladi; SNI kengaytmasi umuman bo‘lmagan ulanishlar esa rad etilmaydi va keyingi bosqich metrikalari bilan baholanadi. Filtrlar C tilida, DPDK muhitida har bir paketni bir marta ko‘rib chiqish tamoyili bo‘yicha amalga oshirilgan. ECH qo‘llanilganda tashqi SNI faqat public_nameni ko‘rsatadi, shu bois domen asosidagi tekshiruv ishlamaydi.

Versiya filtri va renegotiation chegarasi. TLS 1.3 versiyasida haqiqiy versiya supported_versions kengaytmasi orqali kelishiladi [4], shu bois filtr shu ro‘yxatni (kengaytma bo‘lmaganda esa legacy_version maydonini) tekshirib, faqat TLS 1.2 va TLS 1.3 versiyalariga ruxsat beradi: SSL 3.0 [6], TLS 1.0 va 1.1 [7] rasman bekor qilingan. TLS 1.2 versiyasida [8] mijoz tomonidan boshlangan qayta kelishuv (renegotiation, xavfsiz varianti [9]) serverni to‘liq handshakeni qayta bajarishga majbur qiladi va THC-SSL-DOS hujumi aynan shunga asoslanadi [3]. Shifrlangan sessiyada qayta kelishuv Application Data bosqichidan keyin record sarlavhasida ContentType = 22 ning qayta paydo bo‘lishi orqali aniqlanadi; bitta ulanishdagi bunday yozuvlar soni belgilangan chegaradan oshsa, ulanish uziladi.

Handshake yakunlanish nisbati. Statik tezlik chegarasi o‘rniga handshakening yakunlanish nisbati qo‘llanadi. Δt vaqt oynasida F_1 - ClientHello yuborgan oqimlar soni, F_2 - Application Data (ContentType = 23) bosqichiga yetgan oqimlar soni bo‘lsa:

$$R = \frac{F_2}{F_2} \quad (1)$$

Qonuniy trafikda deyarli barcha oqimlar handshakeni yakunlaydi va $R \approx 1$; negotiation floodda esa oqimlar ClientHellodan nariga o‘tmaydi va R nolga intiladi. Chegara moslashuvchan:

$R < R_0 / K$ bo‘lganda hujum qayd etiladi, aks holda bazaviy qiymat eksponensial silliqlash bilan yangilanadi:

$$R_0 \leftarrow \alpha \cdot R + (1 - \alpha) \cdot R_0, \quad (2)$$

bu yerda α - silliqlash koeffitsienti, K - sezgirlik koeffitsienti. Nisbat trafik hajmiga bog‘liq bo‘lmagani sababli qonuniy trafik keskin oshganda ham $R \approx 1$ bo‘lib qoladi va noto‘g‘ri bloklashlar kamayadi. Nisbat butun trafik va har bir manba bo‘yicha alohida hisoblanadi.

JA4 barmoq izi. JA4 ClientHelloning ochiq qismidan quriladi va uch bo‘lakdan iborat: protokol, TLS versiyasi, SNI mavjudligi, shifr va kengaytmalar soni hamda ALPN qiymati; saralangan shifr to‘plamlarining qisqartirilgan SHA-256 xeshi; saralangan kengaytmalar va asl tartibdagi imzo algoritmlarining xeshi [10]. Ro‘yxatlar saralangani bois JA4 2023-yilda Chromium brauzerlarida joriy etilgan kengaytmalar tartibini tasodifiylashtirishga barqaror [10]. Barmoq izi IP manzilga emas, mijozning TLS stekiga bog‘liq bo‘lgani uchun turli manzillardan kelgan, ammo bitta vositadan chiqqan oqimlarni guruhlab cheklash imkonini beradi. Usullarning qo‘llanish holati 1-jadvalda keltirilgan.

1-jadval.

Himoya usullari va ularning holati

Usul	Qaysi hujumga qarshi	Asosi	Holati
Protokol anomaliyasi filtrlari (ContentType, uzunlik, chala ClientHello, shifr, SNI)	non-TLS trafik, chala handshake, soxta TLS steklari	RFC 8446, RFC 6066 [4, 5]	joriy etilgan
Versiya filtri (TLS 1.2/1.3)	eskirgan versiyalar orqali hujum	RFC 7568, RFC 8996 [6, 7]	joriy etilgan
Renegotiation chegarasi	renegotiation flood	RFC 5246, RFC 5746 [8, 9]	joriy etilgan
Yakunlanish nisbati (global va manba bo‘yicha)	negotiation flood	(1)–(2) formulalar	joriy etilgan
JA4 bo‘yicha nisbatli cheklash	negotiation flood	JA4 [10]	joriy etilgan
JA4 qora/oq ro‘yxatlari, xulq-atvor tahlili	tasodifiy barmoq izli flood, HTTPS flood	[11, 12]	tadqiqot bosqichida

Laboratoriya sinovi

Usullar izolyatsiyalangan laboratoriya stendida sinaldi: hujumchi virtual mashina, liniyaga o‘rnatilgan C/DPDK asosidagi himoya qurilmasi va 443-portda ishlovchi server. Hujum ClientHello flood rejimida bajarildi: 517 baytli haqiqiy ClientHello bir marta quriladi, har yuborishda faqat uning 32 baytli tasodifiy maydoni yangilanadi, server javobi esa o‘qilmaydi. 800 ta oqim 30 soniya davomida 100 ta turli manba IP manzilidan ishladi; vosita 9711 ta ClientHello muvaffaqiyatli yuborilganini (o‘rtacha 318 so‘rov/s) va yana 5600 ta urinish xato bilan tugaganini qayd etdi.

Hujum oqimlari ClientHello yuborib, Application Data bosqichiga o‘tmagani sababli ular uchun R nolga intildi va himoya qurilmasi bu oqimlarni ClientHellodan keyingi fazada tashladi; SNI bo‘lmagani uchun ular protokol filtridan o‘tib, R metrikasida ushlandi. Hujum 100 ta manzilga taqsimlanganiga qaramay, barcha bloklangan oqimlar bitta JA4 barmoq izini (t13i1614h2_86a278354501_a54fffd0eb61) qoldirdi: TLS 1.3, SNI yo‘q, 16 ta shifr, 14 ta kengaytma, ALPN h2. Qaror faqat record turi va oqim hisoblagichlari asosida, shifrni ochmasdan qabul qilindi.

Xulosa

TLS hujumlarini bosqichlar bo‘yicha tasniflash har bir bosqichga mos himoya usulini tanlash imkonini beradi. Handshake bosqichidagi hujumlar ochiq ClientHello va record sarlavhalari orqali shifrni ochmasdan aniqlanadi: RFC qoidalariga asoslangan filtrlar kam resurs talab qiladi, handshake yakunlanish nisbati esa statik tezlik chegaralaridan farqli ravishda o‘z-o‘zini kalibrlaydi va JA4 barmoq izi bilan birgalikda hujum manbasini IP manzildan mustaqil guruhlaydi. Tasodifiy barmoq izli va to‘liq handshakeli HTTPS flood hujumlari uchun xulq-atvor tahlilini qo‘shish hamda α va Kni xizmat profiliga moslash keyingi vazifalardir.

Foydalanilgan adabiyotlar ro‘yxati

1. Enabling Technologies: HTTPS, TLS 1.3 // Internet Society Pulse, [b.y.]. URL: https://pulse.internetsociety.org/en/technologies/ (murojaat sanasi: 19.10.2026).

2. Yoachimik O. 2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults. Cloudflare Blog, 2026. 5 February. URL: https://blog.cloudflare.com/ddos-threat-report-2025-q4/ (murojaat sanasi: 19.10.2026).

3. Bernat V. TLS computational DoS mitigation. Vincent Bernat blog, 2011. 1 November. URL: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation (murojaat sanasi: 19.10.2026).

4. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018. DOI: 10.17487/RFC8446.

5. Eastlake D. Transport Layer Security (TLS) Extensions: Extension Definitions. RFC 6066. IETF, 2011. DOI: 10.17487/RFC6066.

6. Barnes R., Thomson M., Pironti A., Langley A. Deprecating Secure Sockets Layer Version 3.0. RFC 7568. IETF, 2015. DOI: 10.17487/RFC7568.

7. Moriarty K., Farrell S. Deprecating TLS 1.0 and TLS 1.1. RFC 8996. IETF, 2021. DOI: 10.17487/RFC8996.

8. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. IETF, 2008. DOI: 10.17487/RFC5246.

9. Rescorla E., Ray M., Dispensa S., Oskov N. Transport Layer Security (TLS) Renegotiation Indication Extension. RFC 5746. IETF, 2010. DOI: 10.17487/RFC5746.

10. JA4+ Network Fingerprinting. FoxIO LLC, [b.y.]. URL: https://github.com/FoxIO-LLC/ja4 (murojaat sanasi: 19.10.2026).

11. Doron E., Medvedovsky L., Aviv D., Rundstein E., Lubitch Greenberg R., Balderman A. Method and System for Detecting and Mitigating HTTPS Flood Attacks: pat. US 11,363,044 B2. Radware Ltd., 2022. 14 June. URL: https://patents.google.com/patent/US11363044B2/en (murojaat sanasi: 19.10.2026).

12. Martinetti A. Advancing Threat Intelligence: JA4 Fingerprints and Inter-Request Signals. Cloudflare Blog, 2024. 12 August. URL: https://blog.cloudflare.com/ja4-signals/ (murojaat sanasi: 19.10.2026).

SOC AVLODLARI: RIVOJLANISH TARIXI VA ASOSIY TEXNOLOGIYALAR

Oripov P.X.
Kiberxavfsizlik markazi davlat muassasasi Kiberxavfsizlik sohasidagi ilmiy-tadqiqot bo‘limi

Annotatsiya. Maqolada kiberxavfsizlik hodisalarini monitoring qilish va ularga javob qaytarish markazining (Security Operations Center - SOC) rivojlanish tarixi besh avlod bo‘yicha yoritiladi. Harbiy va davlat monitoring markazlari va dastlabki nazariy ishlardan reaktiv monitoringga, SIEM asosidagi korrelyatsiyaga, razvedka va xulq-atvor tahliliga tayangan aniqlashga, so‘ngra bulut, XDR va agentli sun’iy intellekt davriga o‘tish, har bir avlodning shakllanish omillari va texnologiyalari ko‘rib chiqiladi.

Kalit so‘zlar: SOC, SOC avlodlari, SIEM, tajovuzlarni aniqlash tizimlari, kibertahdidlar razvedkasi, UEBA, XDR, threat hunting, agentli sun’iy intellekt.

Аннотация. В статье рассматривается история развития центра мониторинга инцидентов кибербезопасности и реагирования на них (Security Operations Center - SOC) по пяти поколениям. Прослеживается переход от военно-государственных центров мониторинга и первых теоретических работ к реактивному мониторингу, корреляции на основе SIEM, обнаружению на основе разведки и поведенческого анализа, а затем к эпохе облака, XDR и агентного искусственного интеллекта; рассмотрены факторы формирования и технологии каждого поколения.

Ключевые слова: SOC, поколения SOC, SIEM, системы обнаружения вторжений, разведка киберугроз, UEBA, XDR, охота за угрозами, агентный искусственный интеллект.

Kirish

Keng iqtibos qilinadigan ta’rifga ko‘ra, SOC odamlar, jarayonlar va texnologiyalar uyg‘unligida infratuzilmani 24/7 rejimda kuzatadigan, tahdidlarni aniqlab, ularga javob choralarini ko‘radigan ijtimoiy-texnik tuzilmadir [1]. SOC tarixi ko‘pgina bosqichlar oldingi bosqichda yuzaga kelgan amaliy muammolarga - ogohlantirishlar toshqini, ko‘p bosqichli hujumlar, javob jarayonidagi uzilishlarga - javob sifatida shakllanganini ko‘rsatadi. SOC rivoji odatda HP kompaniyasining «5G/SOC» hisobotida taklif etilgan besh avlodli model asosida tavsiflanadi [2]; keyingi sharhlarda u turlicha talqin qilinadi [3].

SOC shakllanishi va dastlabki avlodlar

Ildizlar (1995-yilgacha). SOC ikki parallel an’anadan o‘sib chiqqan: telekommunikatsiyadagi tarmoq operatsiyalari markazi (NOC) madaniyati va harbiy qo‘mondonlik punktlari. AQSH Milliy xavfsizlik agentligining NSOC markazi 1973-yildan buyon 24/7 rejimda ishlaydi [4]; HP tasnifi ham ilk rasmiy SOClar 1975-yildayoq harbiy va davlat tashkilotlarida paydo bo‘lganini qayd etadi [2]. Nazariy asosni J. Andersonning audit yozuvlarini xavfsizlik maqsadida doimiy kuzatishni taklif etgan hisoboti (1980) [5] hamda D. Denning P. Noyman (Neumann) bilan SRI Internationalda ishlab chiqqan real vaqt rejimidagi anomaliyalarni aniqlash modeli (1985; jurnal nashri - 1987) [6, 7] tashkil etadi. 1988-yilgi Morris qurtidan so‘ng DARPA topshirig‘iga ko‘ra Karnegi-Mellon universitetida CERT/CC muvofiqlashtirish markazi tashkil etildi [8].

Birinchi avlod - nSOC/SOC V1 (1995–2001). Bu bosqich HP tasnifidagi ikkinchi avlodga mos keladi va «zararli dastur epidemiyalari va tajovuzlarni aniqlash davri» deb tavsiflanadi [2]; keyingi avlodlar raqami ham HP sxemasiga nisbatan bir pog‘ona siljigan. SOC ishi antivirus,

tarmoqlararo ekran va tajovuzlarni aniqlash tizimlari (IDS) ogohlantirishlarini qayta ishlashdan iborat, yondashuv esa reaktiv edi: loglar qisman yig‘ilar, markazlashgan korrelyatsiya hali yo‘q edi [2, 3]. Ayni davrda monitoring autsorsingi shakllandi; B. Shnayer (Schneier) bu modelni asoslar ekan, kutilmagan anomal xatti-harakatni «faqat boshqa bir inson» ilg‘ay olishini ta’kidlagan [9].

Ikkinchi avlod - SOC V2 (2001–2007). Nuqtaviy vositalar ko‘paygani sari har biri o‘z konsolida bog‘lanmagan ogohlantirishlar bera boshladi. A. Chuvakinning guvohligicha, aynan «ogohlantirishlar toshqini» SIM texnologiyasini yuzaga keltirgan, yechim esa loglarni markazlashgan yig‘ish va manbalararo korrelyatsiya qoidalari bo‘lgan [10]. SIEM (Security Information and Event Management) atamasi 2005-yilda Gartner tahlilchilari A. Uilyams (Williams) va M. Nikolett (Nicolett) tomonidan kiritildi [11]. Keng tarqalgan tasavvurdan farqli o‘laroq, SIEMni muvofiqlik talablari emas, operatsion ehtiyoj yaratgan [10].

Zamonaviy avlodlar

Uchinchi avlod - SOC V3 (2007–2013). Davrning asosiy tahdidi - ko‘p bosqichli va uzoq davom etadigan APT kampaniyalari: Mandiant o‘lchovlariga ko‘ra, 2011-yilda hujumchilar aniqlanmasdan oldin qurbon tarmog‘ida mediana bo‘yicha 416 kun faoliyat yuritgan [12]. Signatura va buzilish indikatorlariga (IOC) tayangan vositalar har bir ogohlantirishni alohida ko‘rib, yagona kampaniyani yaxlit ko‘ra olmas edi. Javoban hujumni yetti fazali zanjir sifatida tahlil qiluvchi Cyber Kill Chain modeli (2011) yaratildi: hujumchi zanjirning barcha bo‘g‘inlaridan o‘tishi shart, himoyachiga esa bittasini uzish yetarli [13]. Kibertahdidlar razvedkasi (CTI) sanoati o‘sdi, SOC texnologiyalari qatoriga DLP tizimlari qo‘shildi [3].

To‘rtinchi avlod - NG-SOC (2013–2018). 2013-yil oxirida Target kompaniyasidan ~40 mln bank kartasi va 70 mln mijozning ma’lumotlari o‘g‘irlandi: zararli dastur aniqlanib, SOCga eskalatsiya qilingan, ammo chora ko‘rilmagan [14]. Shundan so‘ng ogohlantirishlardan toliqish (alert fatigue) SOC loyihalashning markaziy masalalaridan biriga aylandi. Signaturaviy aniqlashni xulq-atvorga asoslangan yondashuvlar to‘ldirdi: 2015-yil mayda taqdim etilgan MITRE ATT&CK raqib taktika va texnikalarining bilimlar bazasini berdi [15], UEBA esa foydalanuvchi va obyekt xulq-atvorining bazaviy profilidan og‘ishlarni qidira boshladi - bu Denning modelidagi anomaliya g‘oyasining yangi sathdagi davomi edi [7]. SOAR, EDR, TIP, CASB va proaktiv tahdid qidiruvi (threat hunting) SOC arsenaliga kirdi [3].

Beshinchi avlod - CDC/CFC (2018 - hozirgi kun). Bu bosqich «kiberhimoya markazi» (Cyber Defense Center, Cyber Fusion Center) deb yuritiladi; uning ikki belgisi - telemetriyaning tarmoq perimetridan tashqariga chiqishi va javob choralarining avtomatlashuvi. Kompaniya ma’lumotiga ko‘ra, XDR g‘oyasini 2018-yilda Palo Alto Networks asoschisi N. Zuk ilgari surgan; u oxirgi nuqta, tarmoq, bulut va foydalanuvchi xulq-atvori kabi istalgan manbadan olingan telemetriyani birlashtirishni nazarda tutadi [16]. SolarWinds SUNBURST hujumida (2020) zaiflik kiritilgan Orion mahsulotlari, kompaniya bayonotiga ko‘ra, «18 mingdan kam» mijozda o‘rnatilgan bo‘lishi mumkin edi [17]; zararli kodning bir necha oy yashirin qolgani proaktiv tahdid qidiruvi qadrini ko‘rsatdi. Eng so‘nggi to‘lqin - agentli sun’iy intellekt; uning samaradorlik ko‘rsatkichlari hozircha asosan ishlab chiqaruvchilar ma’lumotlariga tayanadi. Gartner esa hech qachon to‘liq avtonom SOC bo‘lmasligini ta’kidlab, sun’iy intellektni xodimlarni almashtirishga emas, kuchaytirishga yo‘naltirishni tavsiya qiladi [18].

Avlodlarning umumlashtirilgan tavsifi 1-jadvalda keltirilgan.

1-jadval.

SOC avlodlari tavsifi ([2, 3] asosida; 2018+ qatori - muallif sintezi)

Davr	Avlod	Monitoring turi	Asosiy texnologiyalar
1995-yilgacha	Ildizlar: fuqarolik NOC va harbiy monitoring	Mavjudlik va xavfsizlik monitoringi	SNMP, ping (NOC); IDES (tadqiqot prototipi)
1995–2001	1-avlod (nSOC/SOC V1)	Reaktiv monitoring	Antivirus, IDS, tarmoqlararo ekran
2001–2007	2-avlod (SOC V2)	Reaktiv monitoring	SIEM, IPS, antispam, zaifliklarni boshqarish
2007–2013	3-avlod (SOC V3)	Reaktivdan proaktivga o‘tish	SIEM, DLP, kibertahdidlar razvedkasi (IOC almashinuvi)
2013–2018	4-avlod (NG-SOC)	Proaktiv monitoring	Katta ma’lumotlar, UEBA, TIP, SOAR, CASB, EDR
2018 - hozir	5-avlod (CDC/CFC)	Avtomatlashtirilgan proaktiv monitoring	Bulut SIEM, XDR, CWPP/CSPM, ITDR, Zero Trust, AI/ML

Xulosa

SOC tarixi bir necha barqaror tendensiyani ko‘rsatadi. Birinchidan, monitoring reaktiv ogohlantirishlarni qayta ishlashdan proaktiv tahdid qidiruvi va avtomatlashtirilgan javobga o‘tdi. Ikkinchidan, aniqlash yondashuvi signaturalardan IOClarga, ulardan esa raqib taktikasi va xulq-atvor tahliliga siljidi; Denning modelidagi anomaliya g‘oyasi UEBA ko‘rinishida SOC arsenalining markaziy elementiga aylandi. Uchinchidan, SIEM ogohlantirishlar toshqiniga, razvedkaga asoslangan aniqlash esa APT kampaniyalariga javob bo‘ldi. To‘rtinchidan, yangi texnologiyalar eskisini almashtirmadi, balki to‘ldirdi: NOC, CERT/CSIRT, SOC va MDR xizmatlari bugun ham parallel mavjud, tashkilotlar esa bir necha avlod belgilarini aralash holda namoyon etadi. Avtomatlashtirish kuchaygan sharoitda ham malakali tahlilchi SOCning markaziy bo‘g‘ini bo‘lib qolmoqda.

Foydalanilgan adabiyotlar ro‘yxati

1. Vielberth M. et al. Security Operations Center: A Systematic Study and Open Challenges // IEEE Access. 2020. Vol. 8. P. 227756–227779. DOI: 10.1109/ACCESS.2020.3045514.

2. 5G/SOC: SOC Generations. Business white paper. Hewlett-Packard, 2013. 12 p.

3. Kaliyaperumal L.N. The Evolution of Security Operations and Strategies for Building an Effective SOC // ISACA Journal. 2021. Vol. 5.

4. NSA’s National Security Operations Center celebrates 50 years of 24/7 operations in service to the Nation. National Security Agency, 2023.

5. Anderson J.P. Computer Security Threat Monitoring and Surveillance. Fort Washington (PA): James P. Anderson Co., 1980.

6. Denning D.E., Neumann P.G. Requirements and Model for IDES - a Real-Time Intrusion-Detection Expert System. SRI International, 1985.

7. Denning D.E. An Intrusion-Detection Model // IEEE Transactions on Software Engineering. 1987. Vol. SE-13, No. 2. P. 222–232. DOI: 10.1109/TSE.1987.232894.

8. Fostering Growth in Professional Cyber Incident Management. Software Engineering Institute, Carnegie Mellon University, [b.y.].

9. Schneier B. Managed Security Monitoring: Network Security for the 21st Century // Computers & Security. 2001. Vol. 20, No. 6. P. 491–503. DOI: 10.1016/S0167-4048(01)00607-1.

10. Chuvakin A. 20 Years of SIEM: Celebrating My Dubious Anniversary. Medium, 2022.

11. Williams A., Nicolett M. Improve IT Security With Vulnerability Management. Gartner Research, 2005.

12. M-Trends 2024 Special Report. Mandiant, 2024.

13. Hutchins E.M., Cloppert M.J., Amin R.M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // Leading Issues in Information Warfare & Security Research. 2011. Vol. 1. P. 80.

14. Riley M. et al. Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. Bloomberg Businessweek, 2014.

15. Strom B.E. et al. MITRE ATT&CK: Design and Philosophy. MITRE Corporation, 2020.

16. The Journey to XDR Technology. Palo Alto Networks Blog, 2021.

17. SolarWinds Corporation. Current Report on Form 8-K. U.S. Securities and Exchange Commission, 2020.

18. Predict 2025: There Will Never Be an Autonomous SOC. Gartner Research, 2024.

KERNEL, XDP VA DPDK TEXNOLOGIYALARI ASOSIDA PAKETLARNI QAYTA ISHLASH USULLARINING QIYOSIY TAHLILI

Oripov P.X.
Kiberxavfsizlik markazi davlat muassasasi Kiberxavfsizlik sohasidagi ilmiy-tadqiqot bo‘limi

Annotatsiya. Maqolada kompyuter tarmoqlarida paketlarni qayta ishlashning uchta asosiy texnologiyasi - an’anaviy operatsion tizim yadrosi steki (Kernel), yadro ichidagi tezkor yo‘l (XDP/eBPF) va yadroni chetlab o‘tuvchi DPDK (Data Plane Development Kit) - qiyosiy tahlil qilinadi. Paketni qabul qilishdan uzatishgacha bo‘lgan bosqichlar va unumdorlikka ta’sir etuvchi omillar tavsiflanadi. Texnologiyalar unumdorlik, kechikish, protsessor sarfi va dasturlash murakkabligi bo‘yicha solishtirilib, ularni tanlash mezonlari keltiriladi.

Kalit so‘zlar: paketlarni qayta ishlash, tarmoq steki, kernel-bypass, XDP, eBPF, netmap, PF_RING, DPDK, tarmoq unumdorligi, qiyosiy tahlil.

Аннотация. В статье проводится сравнительный анализ трёх основных технологий обработки пакетов в компьютерных сетях: традиционного стека ядра операционной системы (Kernel), внутриядерного быстрого пути (XDP/eBPF) и фреймворка обхода ядра DPDK (Data Plane Development Kit). Описаны этапы от приёма до передачи пакета и факторы, влияющие на производительность. Технологии сравниваются по производительности, задержке, потреблению процессорных ресурсов и сложности программирования; приводятся критерии их выбора.

Ключевые слова: обработка пакетов, сетевой стек, kernel-bypass, XDP, eBPF, netmap, PF_RING, DPDK, производительность сети, сравнительный анализ.

Kirish

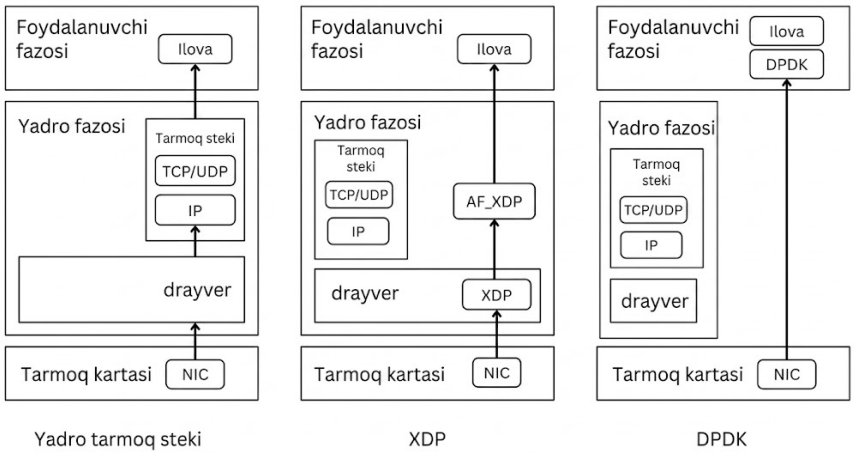
Zamonaviy server va marshrutizatorlarda 10–100 Gbit/s tezlikdagi tarmoq interfeyslari keng qo‘llanadi, bunday tezlikda esa har bir paketni qayta ishlashga ajratilgan vaqt nihoyatda qisqa. Masalan, 10 Gbit/s liniyada eng kichik (64 baytli) paketlar oqimi soniyasiga 14,88 million paketni (Mpps) tashkil etadi [1] - bu bitta paketga atigi ~67 ns to‘g‘ri keladi. An’anaviy operatsion tizim yadrosi steki bunday tezliklarni to‘liq qayta ishlay olmaydi va tarmoq tugunlarida unumdorlikni cheklovchi asosiy omilga (bottleneck) aylanadi [2, 3]. Yuqori tezlikli trafikni kechikishlarsiz qayta ishlash, ayniqsa, kiberxavfsizlikda - DDoS hujumi trafigini real vaqtda filtrlashda hal qiluvchi ahamiyatga ega [2]. Bu muammoni hal qilishda uch asosiy yondashuv qo‘llanadi: an’anaviy yadro steki (Kernel), yadro ichidagi tezkor yo‘l (XDP) va yadroni chetlab o‘tish (kernel-bypass, DPDK).

Paketni qayta ishlash bosqichlari va unumdorlik omillari

Tarmoq kartasiga (NIC) kelgan paket bir necha bosqichdan o‘tadi. Apparat darajasida paket jismoniy port orqali kirish navbatiga tushadi, RSS (Receive Side Scaling) mexanizmi sarlavha maydonlari xeshi asosida uni protsessor yadrolariga biriktirilgan navbatlarga taqsimlaydi, DMA kontrolleri esa protsessor ishtirokisiz paketni operativ xotiradagi halqali buferga yozadi. Yadro darajasida drayver paket uchun sk_buff tuzilmasini yaratadi, TCP/IP steki sarlavhalarni tekshirib marshrutlaydi, Netfilter qoidalari qo‘llanadi va ma’lumot soket orqali foydalanuvchi fazosidagi ilovaga nusxalanadi [4, 5].

Unumdorlikni ikki omil belgilaydi. Birinchisi - protsessorni xabardor qilish usuli: uzilishlar (interrupts) yuqori paket tezligida «uzilishlar bo‘roni»ga (interrupt storm) olib keladi, so‘rov

(polling) esa bu yukni yo‘qotsa-da, protsessor yadrosini doimiy band qiladi; Linux yadrosidagi NAPI mexanizmi past yuklamada uzilishlardan, yuqori yuklamada so‘rov rejimidan foydalanadi [5]. Ikkinchisi - ma’lumot nusxalash va xotira boshqaruvi: yuqori unumdorlikli yechimlar nusxalashsiz (zero-copy) uzatish va paketlarni guruh (burst) bo‘yicha qayta ishlashni qo‘llaydi, NUMA arxitekturasini hisobga oladi, yirik xotira sahifalari (hugepages) esa manzil tarjimasi buferida (TLB) topilmaslik (miss) hollarini kamaytiradi [6, 7]. Bu bosqichlarning qanday amalga oshirilishi texnologiyalar arxitekturasini farqlaydi (1-rasm).



1-rasm. Paketni qayta ishlashning uchta texnologiyasi: Kernel, XDP va DPDK

Taqqoslanayotgan texnologiyalar

Kernel - an’anaviy yadro steki. Standart va eng keng tarqalgan usulda trafik to‘liq operatsion tizim yadrosining TCP/IP steki orqali o‘tadi [4]. Paket kelganda apparat uzilishi hosil bo‘ladi, drayver uni sk_buff tuzilmasiga joylashtiradi, so‘ngra paket protokol qatlamlaridan o‘tib, Socket API orqali ilovaga yetkaziladi [5]. Usul qulay va barqaror, biroq kontekst almashinuvlari va nusxalash xarajatlari sababli 10–100 Gbit/s tarmoqlarda yetarli emas [3, 7]: Linux steki bir yadroda 64 baytli paketlarni tashlash testida eng tezkor (raw) rejimda 4,8 Mpps, ulanishlarni kuzatish (conntrack) rejimida esa 1,8 Mpps tezlikka erishgan [2].

XDP - yadro ichidagi tezkor yo‘l. XDP (eXpress Data Path) yadrodan voz kechmagan holda paketni drayver darajasida, sk_buff ajratilishidan oldin qayta ishlaydi. U eBPF muhitiga asoslanadi: dastur har bir paket uchun to‘rt qarordan birini qabul qiladi - tashlash (XDP_DROP), shu interfeysdan qaytarib yuborish (XDP_TX), yadro stekiga o‘tkazish (XDP_PASS) yoki boshqa interfeysga, boshqa protsessorga yoxud AF_XDP soketi orqali foydalanuvchi fazosiga yo‘naltirish (XDP_REDIRECT) [2]. XDP bir yadroda 24 Mpps tezlikka erishgan - bu Linux stekining eng tezkor rejimidan besh barobar yuqori, protsessor sarfi esa yuklamaga mos ravishda o‘zgaradi [2]. Cheklovi - eBPF tekshiruvchisi (verifier) xavfsizlik uchun dastur hajmi va sikllarga cheklov qo‘yadi, shu bois murakkab mantiqni joriy etish qiyin [2].

DPDK - yadroni chetlab o‘tish. DPDK (Data Plane Development Kit) paketlarni qayta ishlashni yadrodan butunlay chiqarib, foydalanuvchi fazosida bajaradi. Tarmoq kartasi yadro drayveridan ajratilib, DPDK ilovasiga biriktiriladi; uzilishlar o‘rniga so‘rov rejimidagi drayverlar (PMD - Poll Mode Driver) ishlatiladi, paketlar nusxalashsiz ilova xotirasiga yoziladi va yirik sahifalar qo‘llanadi [6]. DPDK bir yadroda 43,5 Mpps tezlikka erishgan, biroq so‘rov rejimi sababli ajratilgan yadroni trafik bo‘lmaganda ham 100% band qiladi [2]. netmap [1] va PF_RING kabi boshqa kernel-bypass yechimlari ham mavjud; ularning qiyosiy tahlili [3]da keltirilgan.

Qiyosiy tahlil

Texnologiyalarning asosiy ko‘rsatkichlari 1-jadvalda jamlangan. Unumdorlik va kechikish qiymatlari [2] tadqiqotidan olingan (Intel Xeon E5-1650 v4 protsessori, Mellanox ConnectX-5 100 Gbit/s tarmoq kartasi, 64 baytli paketlar).

1-jadval.

Kernel, XDP va DPDK texnologiyalarining qiyosiy tavsifi

Mezon	Kernel	XDP	DPDK
Unumdorlik (1 yadro, paket tashlash)	4,8 Mpps (raw)	24 Mpps	43,5 Mpps
Bir paketga sarflanadigan vaqt	≈208 ns[1]	41,6 ns	22,9 ns
O‘rtacha yo‘naltirish kechikishi (100 pps / 1 Mpps)	o‘lchanmagan[2]	82 / 7 mks	2 / 3 mks
Protsessor sarfi	yuklamaga mos	yuklamaga mos	doimo 100%
Yadro tarmoq steki	to‘liq	stek bilan birga ishlaydi	yo‘q (ilovada alohida stek kerak)
Dasturlash qulayligi	oson	o‘rtacha	murakkab

Izoh: [1]1/4,8 Mpps asosida hisoblangan; XDP va DPDK qiymatlari [2]da keltirilgan. [2]Linux steki [2]dagi yo‘naltirish kechikishi testiga kiritilmagan.

Yadrolar soni oshganda XDP va DPDK unumdorligi PCI shinasining umumiy chegarasigacha (sinov tizimida 115 Mpps) chiziqli oshadi, Linux steki ham apparat cheklovi bo‘lmaganda chiziqli masshtablanadi [2]. Kechikish yuklamaga bog‘liq: past paket tezligida XDP kechikishi uzilishlarni qayta ishlash vaqti bilan belgilanadi va doimiy so‘rov rejimidagi DPDKnikidan ancha yuqori bo‘ladi, yuqori tezlikda esa farq keskin qisqaradi [2].

Yuqori tezlikdagi qayta ishlashning amaliy ahamiyati DDoS sinovida yaqqol ko‘rinadi: himoyasiz serverning unumdorligi 3 Mpps hujum trafigida ikki barobar pasaygan va 3,5 Mppsga yaqinlashganda deyarli nolga tushgan, XDP filtri bilan esa server 19,5 Mpps hujum trafigigacha soniyasiga ~28 500 TCP tranzaksiyani barqaror bajargan [2].

Demak, to‘liq TCP/IP steki va o‘rtacha tezlik yetarli bo‘lganda Kernel, yuqori tezlik bilan birga yadro infratuzilmasi va protsessor resurslarini tejash zarur bo‘lganda XDP, maksimal (line-rate) o‘tkazuvchanlik va eng past kechikish talab etilib, alohida yadrolar ajratish imkoni bo‘lganda DPDK maqbul hisoblanadi. Tanlovda, shuningdek, ishlab chiquvchilar tajribasi va tarmoq kartalarining qo‘llab-quvvatlanishi hisobga olinadi.

Xulosa

Paketlarni qayta ishlash usullari orasida universal «eng yaxshi» yechim yo‘q: tanlov talab qilinadigan tezlik, kechikish, yadro xizmatlariga ehtiyoj va mavjud resurslarga bog‘liq. DPDK bir yadroda eng yuqori o‘tkazuvchanlikni (43,5 Mpps) va eng past kechikishni ta’minlaydi, ammo ajratilgan yadrolarni doimiy band qiladi. XDP yadro stekining xavfsizlik va boshqaruv vositalarini saqlagan holda uning eng tezkor (raw) rejimidan besh barobar yuqori tezlik (24 Mpps) beradi va protsessor sarfini yuklamaga moslaydi. Zararli trafikni drayver darajasida erta filtrlash DDoS hujumlariga bardoshlilikni keskin oshiradi. An’anaviy yadro steki esa universallik va qulaylik muhim bo‘lgan vazifalarda maqbul yechim bo‘lib qolmoqda.

Foydalanilgan adabiyotlar ro‘yxati

1. Rizzo L. netmap: A Novel Framework for Fast Packet I/O // Proceedings of the 2012 USENIX Annual Technical Conference (USENIX ATC ’12). Boston (MA): USENIX Association, 2012. P. 101–112.

2. Høiland-Jørgensen T., Brouer J.D., Borkmann D., Fastabend J., Herbert T., Ahern D., Miller D. The eXpress Data Path: Fast Programmable Packet Processing in the Operating System Kernel // Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18). New York: ACM, 2018. P. 54–66. DOI: 10.1145/3281411.3281443.

3. Gallenmüller S., Emmerich P., Wohlfart F., Raumer D., Carle G. Comparison of Frameworks for High-Performance Packet IO // 2015 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS). IEEE, 2015. P. 29–38. DOI: 10.1109/ANCS.2015.7110118.

4. Tanenbaum A.S., Wetherall D.J. Computer Networks. 5th ed. Boston: Pearson, 2011. 960 p.

5. Corbet J., Rubini A., Kroah-Hartman G. Linux Device Drivers. 3rd ed. Sebastopol (CA): O'Reilly, 2005.

6. Data Plane Development Kit (DPDK) Documentation. DPDK Project, [b.y.]. URL: https://doc.dpdk.org/guides/ (murojaat sanasi: 19.10.2026).

7. Barbette T., Soldani C., Mathy L. Fast Userspace Packet Processing // 2015 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS). IEEE, 2015. P. 5–16. DOI: 10.1109/ANCS.2015.7110116.

BIOMETRIK AUTENTIFIKATSIYA TIZIMLARINI BAHOLASH METODIKASI: XATOLIK KO‘RSATKICHLARI, TAJRIBA PROTOKOLI VA OCHIQ MA’LUMOTLAR BAZALARIDAN FOYDALANISH

Yusupov B.K., Sapayev Sh.R.
O‘zbekiston Respublikasi Harbiy xavfsizlik va Mudofaa universitetining Axborot kommunikatsiya texnologiyalari va harbiy aloqa instituti

Annotatsiya. Maqolada yuz biometriyasiga asoslangan autentifikatsiya tizimlarining himoyalanganligi va samaradorligini baholash metodikasi ko‘rib chiqilgan. Baholash turlari (texnologik, stsenariy va operatsion sinov), asosiy ko‘rsatkichlar (FAR, FRR, EER, FTE, APCER/BPCER), ochiq ma’lumotlar bazalari (LFW, CASIA-WebFace, VGGFace2, IJB-C) tahlil qilingan. Chegaraviy qiymatni tanlash, xatolik darajalarini hisoblash va ularning ishonch oralig‘ini baholash algoritmlari hamda tajriba protokolining blok-sxemasi keltirilgan. Baholashda uchraydigan tipik xatolar ko‘rsatilib, natijalarni to‘g‘ri e’lon qilish bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: biometrik tizimni baholash, FAR, FRR, EER, DET egri chizig‘i, chegaraviy qiymat, ishonch oralig‘i, LFW, tajriba protokoli, axborot xavfsizligi.

Аннотация. В статях рассмотрена методика оценки защищённости и эффективности систем аутентификации по лицу. Проанализированы виды тестирования, показатели ошибок (FAR, FRR, EER, FTE, APCER/BPCER) и открытые базы данных (LFW, CASIA-WebFace, VGGFace2, IJB-C). Приведены алгоритмы выбора порога, расчёта уровней ошибок и доверительных интервалов, а также блок-схема протокола эксперимента. Указаны типичные ошибки при оценке и даны рекомендации по корректной публикации результатов.

Ключевые слова: оценка биометрических систем, FAR, FRR, EER, кривая DET, порог, доверительный интервал, LFW, протокол эксперимента, информационная безопасность.

Biometrik autentifikatsiya tizimi ishlab chiqilgach, uning ishonchliligini tasdiqlash zarur. Amalda ba’zan faqat umumiy aniqlik keltiriladi, chegaraviy qiymat sinov ma’lumotlarining o‘zida tanlanadi, tajribalar soni esa yetarli bo‘lmaydi; natijada ishlanmalarni solishtirish va xavfsizlik darajasini baholash qiyinlashadi [1, 2]. Xizmat doirasidagi tizimlarda begona shaxsning qabul qilinishi jiddiy oqibatlarga olib keladi.

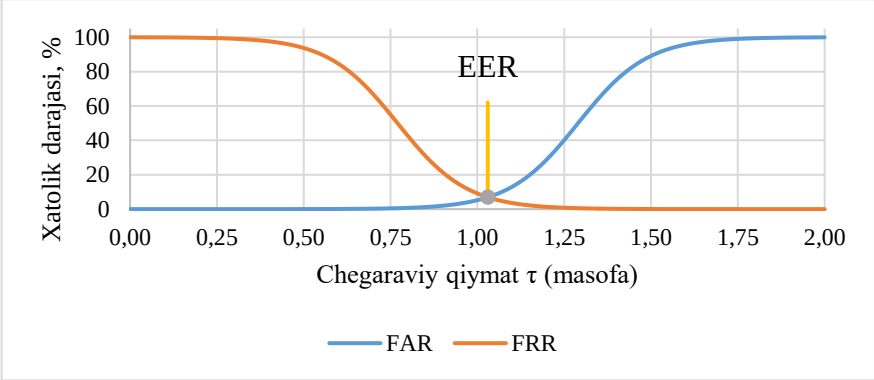
ISO/IEC 19795-1 standartiga ko‘ra biometrik tizim uch xil sinaladi [2, 3]. Texnologik sinovda algoritm oldindan yig‘ilgan tasvirlar to‘plamida tekshiriladi: usul takrorlanuvchan va arzon, ammo real kamera va foydalanuvchi xulq-atvorini hisobga olmaydi. Stsenariy sinovida tizim laboratoriyada real qurilma bilan, operatsion sinovda esa haqiqiy ish muhitida sinaladi. Yuz biometriyasi uchun texnologik sinov odatda stsenariy sinovi bilan to‘ldiriladi, chunki kamera sifati va yoritilish xatolikka sezilarli ta’sir qiladi. Tekshirish (1:1) va identifikatsiya (1:N) rejimlari alohida baholanadi; autentifikatsiya uchun asosiy rejim 1:1.

Asosiy ko‘rsatkichlar 1-jadvalda keltirilgan. Chegaraviy qiymat τ oshirilganda FAR kamayadi, FRR esa ortadi (1-diagramma), shu sababli tizim bitta son bilan emas, ikkala xatolik birgalikda yoki DET egri chizig‘i orqali tavsiflanadi. Soxta tasvirga bardoshlilik alohida, APCER va BPCER bilan o‘lchanadi (ISO/IEC 30107-3).

1-jadval

Biometrik tizimning asosiy baholash ko‘rsatkichlari

t/r	Ko‘rsatkich	Ta’rifi	Nimani bildiradi
1	FAR	Begona juftliklar ichida noto‘g‘ri qabul qilinganlar ulushi	Xavfsizlik darajasi
2	FRR	O‘zining juftliklari ichida noto‘g‘ri rad etilganlar ulushi	Foydalanuvchiga qulaylik
3	EER	FAR = FRR bo‘lgandagi xatolik qiymati	Tizimlarni solishtirish uchun yagona son
4	TAR @ FAR	Belgilangan FAR da to‘g‘ri qabul qilish ulushi (1 − FRR)	Amaliy ishchi nuqta
5	FTE / FTA	Ro‘yxatga olish / tasvir olishdagi muvaffaqiyatsizliklar ulushi	Qurilma va sharoit ta’siri
6	APCER / BPCER	Soxta hujum o‘tib ketishi / haqiqiy tasvir rad etilishi ulushi	Soxta tasvirga bardoshlilik



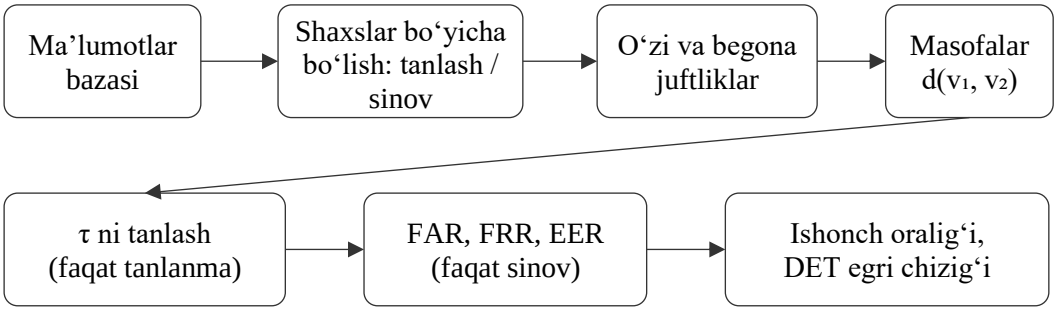
1-diagramma. FAR va FRR ning chegaraviy qiymatga bog‘liqligi

Xatolik darajasini o‘lchash va tizimlarni solishtirish uchun ommaviy bazalar qo‘llaniladi: LFW (13 233 tasvir, 5 749 shaxs) tekshirish uchun 6000 juftlik va 10 qismli protokolni beradi, biroq zamonaviy usullar unda 99 % dan yuqori natija berib, baza to‘yinishga yetgan; CASIA-WebFace (≈ 494 ming tasvir, 10 575 shaxs) va VGGFace2 (≈ 3,31 mln tasvir, 9 131 shaxs) asosan o‘qitish uchun, IJB-C (3 531 shaxs, ≈ 31 ming tasvir) esa qiyin sharoitdagi tekshirish uchun mo‘ljallangan. NIST FRVT hisobotlari mustaqil taqqoslashni beradi [4].

Takrorlanuvchan natija uchun tajriba qat’iy ketma-ketlikda o‘tkaziladi (1-rasm). Eng muhim qoida: chegaraviy qiymat τ faqat tanlanma qismida topiladi, sinov qismida esa faqat o‘lchanadi.

1-algoritm. Juftliklarni shakllantirish, τ ni tanlash va FAR, FRR, EER ni hisoblash. Baza shaxslar bo‘yicha tanlanma va sinov qismlariga bo‘linadi (bir shaxs ikkala qismga tushmaydi); bir shaxsning turli tasvirlaridan o‘zining, turli shaxslar tasvirlaridan begona juftliklar tuziladi va har biri uchun vektorlar orasidagi masofa d hisoblanadi. Tanlanma qismida τ ning nomzod qiymatlari (0 dan 2 gacha, qadam 0,01) olinib, har biri uchun $FAR(\tau) = \frac{\{begona: d \le \tau\}}{begona}$ va $FRR(\tau) = \frac{\{o'zi: d > \tau\}}{o'zi}$ hisoblanadi. EER uchun $|FAR - FRR|$ eng kichik bo‘lgan τ (yoki talab qilingan FAR dan oshmaydigan eng katta τ) tanlanadi. Sinov qismida τ o‘zgartirilmay qo‘llanib, yakuniy FAR va FRR hisoblanadi.

2-algoritm. K qismli kross-tekshiruv. Baza shaxslar bo‘yicha K ta teng qismga bo‘linadi; har bir qism navbat bilan sinov, qolganlari tanlanma sifatida ishlatilib, 1-algoritm bajariladi, so‘ng K ta natijaning o‘rtacha qiymati va standart og‘ishi hisoblanadi.



1-rasm. Baholash tajriba bosqichlari ketma-ketligi

Statistik ishonchlilik: ishonch oralig‘i va tajribalar soni

Xatolik darajasi $\hat{p} = \frac{k}{N}$ nuqtaviy baho bo‘lib, N cheklangan bo‘lgani uchun haqiqiy qiymatdan farq qiladi, shu sababli har bir natija ishonch oralig‘i bilan beriladi. Binomial taqsimot uchun aniq Klopper–Pirson va Uilson oraliqlari qo‘llaniladi; ikkinchisi kichik N da va $\hat{p}$ nolga yaqin bo‘lganda ham ishonchli ishlaydi:

$$p_{\mathrm{l,u}} = \frac{\left(\hat{p}+\frac{z^2}{2N} \pm z\cdot\sqrt{\frac{\hat{p}(1-\hat{p})}{N}+\frac{z^2}{4N^2}}\right)}{\left(1+\frac{z^2}{N}\right)} \qquad (1)$$

bu yerda 95 % ishonchlilik uchun z = 1,96.

Biroq binomial oraliqlar juftliklarni mustaqil deb hisoblaydi, amalda esa bir shaxsning tasvirlari ko‘plab juftlikda qatnashadi va ayrim foydalanuvchilar boshqalarga qaraganda ko‘proq xato qiladi. Tajribalar soni uchun ikki qoida mavjud [6]. Birinchisi - “uch qoidasi”: xato kuzatilmasa, xatolik darajasining 95 % ishonchli yuqori chegarasi $\frac{3}{N}$ ga teng [4, 5]; demak, FAR ≤ 10^{-6} ni tasdiqlash uchun kamida $3\cdot10^6$ begona solishtirish kerak, kichik tanlanmada “FAR nolga teng” degan da’vo asossiz. Ikkinchisi - Doddington qoidasi: haqiqiy xatolik ±30 % aniqlikda 90 % ishonch bilan baholanishi uchun kamida 30 ta xato kuzatilishi lozim [7]; masalan, FAR ≈ 10^{-4} uchun $30/10^{-4} = 3\cdot10^5$ ta begona juftlik zarur.

3-algoritm. Shaxslar bo‘yicha ishonch oralig‘i (bootstrap). Sinov qismidagi shaxslar ro‘yxati $S = \{s^1, \ldots, s_M\}$ dan B marta (odatda B = 1000) qaytarish bilan M ta shaxs tanlanadi; har bir takrorda tanlangan shaxslarning juftliklari bo‘yicha FAR va FRR (belgilangan τ da) qayta hisoblanadi, B ta qiymat tartiblanib 2,5- va 97,5-protsentillar oraliq chegaralari sifatida olinadi va natija nuqtaviy baho bilan birga e’lon qilinadi.

Umumiy FAR va FRR barcha sharoitlarda bir xil ishlashni ko‘rsatmaydi: NIST FRVT ga ko‘ra, ayrim algoritmlarda FAR demografik guruhlar orasida o‘n martadan yuz martagacha farq qilishi mumkin [8]. Shu sababli natijalar kamera, yoritilish, bosh holati, yosh, jins va seanslar orasidagi vaqt bo‘yicha alohida hisoblanadi; har bir guruhda tajribalar soni yuqoridagi qoidalarni qanoatlantirishi shart.

Texnologik sinov real kamera va foydalanuvchi xulq-atvorini hisobga olmagani uchun stsenariy sinovi bilan to‘ldiriladi [8, 9]. Unda ko‘ngilli ishtirokchilar 1-seansda ro‘yxatdan o‘tadi (muvaffaqiyatsiz urinishlar FTE sifatida sanaladi); bir necha kundan so‘ng 2-seansda har biri o‘z

hisobiga kiradi va boshqalarning hisobiga kirishga urinadi (“nol-harakatli” hujum). Natijalar 1- va 3-algoritmlar bo‘yicha qayta ishlanadi va omillar bo‘yicha bo‘linadi.

Tizimlarni taqqoslashda ROC o‘rniga ko‘pincha DET (Detection Error Tradeoff) egri chizig‘i qo‘llaniladi: unda ikkala o‘q ham probit shkalada chiziladi, shuning uchun normal taqsimotli ballar uchun egri chiziq to‘g‘ri chiziqqa aylanadi va past xatolik sohasidagi farq yaxshi ko‘rinadi [4]. Chiziq koordinata boshiga yaqin bo‘lsa, tizim yaxshiroq. E’lon qilinadigan natija baza nomi va versiyasi, shaxslar va juftliklar soni, tanlanma/sinov bo‘linishi, τ ni tanlash mezoni, FAR, FRR, EER, FTE/FTA, DET egri chizig‘i, 95 % ishonch oralig‘i va uni hisoblash usuli, sinov sharoiti hamda (zarur bo‘lsa) APCER/BPCER ni o‘z ichiga olishi kerak.

Natijani takrorlash uchun dasturiy ta’minot va model versiyalari, tasodifiy sonlar generatorining boshlang‘ich qiymati (seed), baza bo‘linishi, juftliklar ro‘yxati, chegaraviy qiymat va oraliq natijalar qayd etiladi; baza o‘zgarmaganini isbotlash uchun fayllarning nazorat yig‘indisi (xesh) saqlanadi.

Misol: N = 20 000 begona juftlikda k = 2 ta xato topilsa, nuqtaviy baho FAR = 10^{-4}, ammo 95 % Uilson oralig‘i $2{,}7\cdot10^{-5}$ dan $3{,}7\cdot10^{-4}$ gacha (Klopper–Pirson: $1{,}2\cdot10^{-5}$ dan $3{,}6\cdot10^{-4}$ gacha), ya’ni haqiqiy qiymat bir necha marta kichik yoki katta bo‘lishi mumkin. 30 ta xato va N = 300 000 da oraliq $7\cdot10^{-5}$ dan $1{,}4\cdot10^{-4}$ gacha torayadi.

4-algoritm. Ikki tizimni juftlashtirilgan bootstrap bilan taqqoslash. Ikki tizimni solishtirishda nuqtaviy baholarning farqi yetarli emas, chunki farq tasodifiy bo‘lishi mumkin; bir xil juftliklarda sinalganda juftlashtirilgan taqqoslash (McNemar sinovi [10] yoki juftlashtirilgan bootstrap) qo‘llaniladi: ikkala tizim bir xil sinov shaxslari va juftliklarida sinaladi, har biri uchun τ tanlanma qismida topiladi. B marta sinov shaxslari qaytarish bilan qayta tanlanadi, har bir takrorda belgilangan FAR da $\Delta = FRR_A - FRR_B$ topiladi va Δ ning 2,5- va 97,5-protsentillari oraliq chegaralari qilib olinadi. Oraliq nolni o‘z ichiga olmasagina tizimlardan biri ustun deb hisoblanadi.

Baholash ketma-ket to‘rt bosqichda rejalashtiriladi. Birinchisida model ochiq bazaning standart protokoli bo‘yicha sinaladi (yagona xulosa asosi emas); ikkinchisida qiyinroq bazalarda tekshiriladi; uchinchisi real kamera va foydalanuvchilar bilan stsenariy sinovi bo‘lib, amaliy xavfsizlikni aynan shu bosqich belgilaydi; to‘rtinchisida soxta tasvirga qarshi himoya (APCER/BPCER) va tezlik o‘lchanadi. Har bir bosqich natijasi o‘z ishonch oralig‘i va cheklovlari bilan alohida e’lon qilinadi, bosqichlar natijalari qo‘shilmaydi.

Biometrik autentifikatsiya tizimini baholash bitta aniqlik ko‘rsatkichi bilan cheklanmasligi kerak. Baholash turini to‘g‘ri tanlash, FAR va FRR ni birgalikda ko‘rsatish, τ ni alohida tanlanmada aniqlash, natijani bootstrap yordamida ishonch oralig‘i bilan berish, omillar bo‘yicha bo‘lib hisoblash va tajribani takrorlanuvchan hujjatlashtirish zarur. Uch qoidasi va Doddington qoidasi tajribalar sonini oldindan rejalashtirishga imkon beradi (masalan, FAR $\leq 10^{-6}$ uchun kamida $3\cdot10^{6}$ begona solishtirish). Taklif etilgan protokol va algoritmlar xizmat doirasida foydalaniladigan lokal bulutli tizimning yuz biometriyasi modulini takrorlanuvchan baholashga imkon beradi.

Foydalanilgan adabiyotlar

1. Jain AK, Nandakumar K, Ross A. 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recognition Letters. 2016;79:80-105.

2. ISO/IEC 19795-1:2021. Biometric performance testing and reporting. Part 1: Principles and framework. Geneva: ISO; 2021.

3. ISO/IEC 30107-3:2023. Biometric presentation attack detection. Part 3: Testing and reporting. Geneva: ISO; 2023.

4. Huang GB, Ramesh M, Berg T, Learned-Miller E. Labeled faces in the wild: a database for studying face recognition in unconstrained environments. University of Massachusetts Amherst, Technical Report 07-49. 2007.

5. Yi D, Lei Z, Liao S, Li SZ. Learning face representation from scratch. arXiv:1411.7923. 2014.

6. Cao Q, Shen L, Xie W, Parkhi OM, Zisserman A. VGGFace2: a dataset for recognising faces across pose and age. Proceedings of IEEE FG. 2018:67-74.

7. Maze B, Adams J, Duncan JA, et al. IARPA Janus Benchmark-C: face dataset and protocol. Proceedings of International Conference on Biometrics (ICB). 2018:158-165.

8. Grother P, Ngan M, Hanaoka K. Face Recognition Vendor Test (FRVT) Part 3: Demographic effects. NISTIR 8280. Gaithersburg: NIST; 2019.

9. Bolle RM, Ratha NK, Pankanti S. Error analysis of pattern recognition systems: the subsets bootstrap. Computer Vision and Image Understanding. 2004;93(1):1-33.

10. ISO/IEC 19795-2:2007. Biometric performance testing and reporting. Part 2: Testing methodologies for technology and scenario evaluation. Geneva: ISO; 2007.

WINDOWS OPERATSION TIZIMIDA NTFS RUXSATLARINING RANSOMWARE HUJUMLARINI BOSHQARISHNING TAKOMILLASHTIRILGAN MODELI

Samarov X. K., Ummatova N.B.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada Windows operatsion tizimida NTFS ruxsatlarini ransomware hujumlariga qarshi boshqarishning adaptiv NTFS (A-NTFS) modeli taklif etiladi. NTFS ruxsatlari statik bo‘lib, foydalanuvchi bo‘yicha beriladi, shuning uchun foydalanuvchi nomidan ishlayotgan zararli jarayon uning barcha fayllariga yoza oladi. Taklif etilgan model har bir jarayonga ishonchlilik bahosi beradi va uni fayl tizimidagi xatti-harakat signallariga qarab dinamik o‘zgartiradi; baho ruxsat darajasini belgilaydi, papkaning maxfiylik darajasi esa cheklovlarni kuchaytiradi.

Kalit so‘zlar: ransomware, NTFS, ruxsatlarni nazorat qilish, adaptiv model, ishonchlilik bahosi, entropiya, Windows.

Аннотация. В статье предложена модель адаптивного управления разрешениями NTFS (A-NTFS) против программ-вымогателей в Windows. Разрешения NTFS статичны и назначаются по пользователю, поэтому вредоносный процесс, запущенный от его имени, получает доступ на запись ко всем файлам пользователя. Модель присваивает каждому процессу оценку доверия и динамически меняет её по сигналам поведения в файловой системе; оценка определяет уровень доступа, а чувствительность папки ужесточает ограничения.

Ключевые слова: программы-вымогатели, NTFS, контроль доступа, адаптивная модель, оценка доверия, энтропия, Windows.

Kirish

Ransomware hujumlarining asosiy nishoni fayl tizimidir: zararli dastur fayllarni shifrlab, ularni qaytarish evaziga to‘lov talab qiladi [1]. Windowsda ma’lumotlarga kirishni NTFS ruxsatlari (ACL) boshqaradi, biroq ular hujumni to‘xtatish uchun mo‘ljallanmagan: ruxsatlar foydalanuvchi yoki guruh bo‘yicha beriladi va jarayon ishlab turgan vaqtda o‘zgarmaydi. Foydalanuvchi nomidan ishga tushgan zararli jarayon oddiy dasturdan farqlanmaydi va barcha fayllarni shifrlay oladi.

Mavjud aniqlash vositalari hujumni kuzatadi, biroq ruxsat darajasini jarayonning xatti-harakatiga qarab o‘zgartirmaydi. Maqolada ishonchlilik bahosi shubhali signallarda pasayib, vaqt o‘tishi bilan tiklanadigan va papka maxfiyligi bilan birga ruxsat darajasini belgilaydigan model bayon etiladi. Model adaptiv NTFS (A-NTFS) deb ataladi: u NTFS ruxsatlari ustiga ishonchlilik bahosiga asoslangan adaptiv qatlam qo‘shadi.

Mavjud yondashuvlar

NTFS ACL va klassik modellar. NTFS har bir obyektga ruxsat yozuvlari ro‘yxatini (ACL) biriktiradi; ruxsatlar yuqori papkadan meros bo‘lib o‘tadi [2]. Windows yaxlitlik darajalarini (integrity level) ham qo‘llaydi va bu tekshiruv ACL dan oldin bajariladi [3]. DAC, MAC va RBAC modellarida qaror foydalanuvchining identifikatoriga, xavfsizlik darajasiga yoki roliga tayanadi, jarayonning nima qilayotgani esa hisobga olinmaydi.

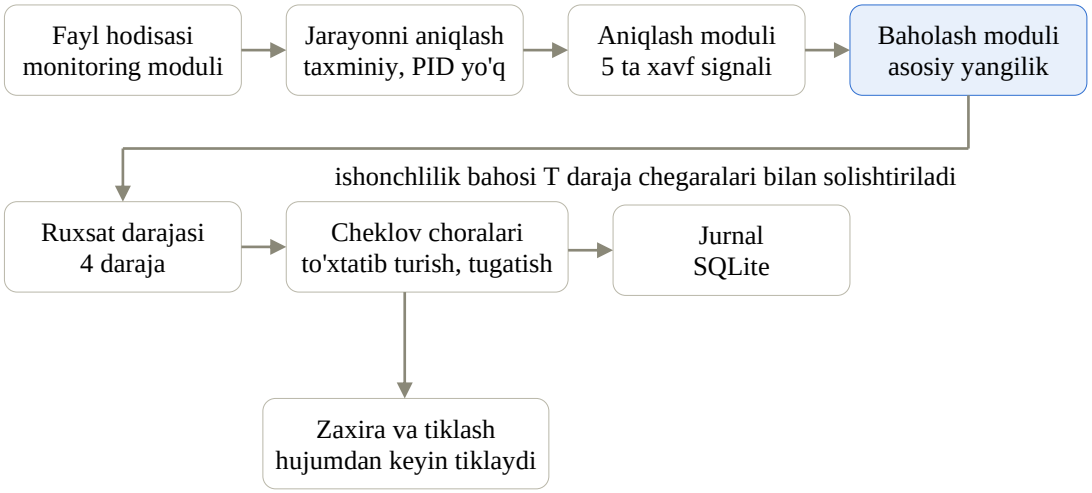
Aniqlashga asoslangan vositalar. CryptoDrop tizimi fayllardagi o‘zgarish belgilari va entropiyadan foydalanadi [6]. ShieldFS (Windows drayveri) jarayonlarning fayl faoliyatini

adaptiv modellar bilan kuzatadi va shubhali jarayon o‘zgartirgan fayllarni tiklaydi [7]. UNVEIL ransomware ni sun’iy foydalanuvchi muhitida tahlil qiladi [8]. So‘nggi ishlarda bunday detektorlar tizimlashtirilgan [9, 10], kuzatuv chuqurligi jarayon shubhali ko‘ringandagina oshiriladi [11], shifrlash hisobi va fayl hajmi orasidagi vaqt bog‘liqligidan foydalaniladi [12]. Entropiya Shennon formulasiga asoslanadi [13]; tuzoq (honeypot) fayllarga murojaat ham hujum belgisi hisoblanadi.

Taklif etilgan model

Arxitektura

Model Python tilida yozilgan AdaptGuard prototipida amalga oshirildi. Monitoring moduli himoyalangan papkalarda fayl yaratish, o‘zgartirish, o‘chirish va nomini o‘zgartirish hodisalarini qayd etadi. Fayl hodisasi jarayon identifikatorini (PID) bermaydi, shuning uchun manba jarayon ochiq fayllar va buyruq argumentlari bo‘yicha taxminan aniqlanadi.



1-Rasm. AdaptGuard arxitekturasi: signallar ishonchlilik bahosini o‘zgartiradi, baho cheklov darajasini belgilaydi.

Xavf signallari

Aniqlash moduli har bir jarayon uchun 10 soniyalik harakatlanuvchi oynada beshta signal shakllantiradi: ommaviy o‘zgartirish (50 tadan ortiq fayl), kengaytmani odatiy bo‘lmagan kengaytmaga almashtirish (5 ta), yuqori entropiya (3 ta mavjud fayl, entropiya 7,5 bit/baytdan yuqori va kamida 1,5 bit/bayt oshgan), ommaviy o‘chirish (30 ta) va tuzoq fayllarga murojaat. Yangi yaratilgan faylga dastlabki 2 soniya ichida yozish o‘zgartirish hisoblanmaydi. Bir xil signal 3 soniyada bir martadan ko‘p hisobga olinmaydi. Entropiya bayt chastotalaridan hisoblanadi [13]:

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i$$

bu yerda p_i - i qiymatli baytning fayldagi ulushi; H ning eng katta qiymati 8 bit/bayt bo‘lib, shifrlangan ma’lumotlarda entropiya shu qiymatga yaqin bo‘ladi.

Adaptiv ishonch modeli

Har bir jarayonning ishonchlilik bahosi $T \in [0, 100]$ oraliqda bo‘ladi. Boshlang‘ich qiymat T_0 jarayon toifasiga bog‘liq: ishonchli ilovalar ro‘yxatidagi jarayonlar uchun 90, noma’lum jarayonlar uchun 60. Shubhali signal kelganda baho pasayadi, vaqt o‘tishi bilan esa tiklanadi:

$$T \leftarrow \max(0, T - w \cdot k)$$

$$T \leftarrow \min(T_0, T + r \cdot \Delta t)$$

bu yerda w - signal vazni, k - papkaning maxfiylik koeffitsiyenti, r - tiklanish tezligi, Δt - oxirgi yangilanishdan beri o‘tgan vaqt. Ishonchli ilovalar ro‘yxati faqat boshlang‘ich

ishonchlilikni belgilaydi: ro‘yxatdagi jarayon xavfli signal bersa, uning bahosi ham pasayadi. Parametrlar qiymatlari jadvalda keltirilgan.

1-jadval

Parametrlar qiymatlari jadvalda

Parametr	Qiymat
T0 (ishonchli / noma’lum)	90 / 60
k (ochiq / maxfiy / o‘ta maxfiy)	1,0 / 1,3 / 1,6
w (signal vazni)	ommaviy o‘zgartirish 4; kengaytmani almashtirish 20; yuqori entropiya 25; ommaviy o‘chirish 15; tuzoq fayl 60
r (tiklanish tezligi)	1,0 birlik/soniya
Chegaralar (ochiq papka)	To‘liq ruxsat ≥ 70; nazorat ostida ≥ 40; to‘xtatib turish ≥ 20; undan past - bloklash. Maxfiy papkada +10, o‘ta maxfiy papkada +20

Ruxsat darajalari

Baho T bo‘yicha jarayon to‘rt darajadan biriga tushadi: to‘liq ruxsat (cheklov yo‘q); nazorat ostida (aniqlash chegaralari 0,75 marta kamaytiriladi); to‘xtatib turish (jarayon vaqtincha to‘xtatiladi, ya’ni fayllarga o‘qiy ham, yoza ham olmaydi; ishonchlilik tiklansa, ish davom ettiriladi); bloklash (jarayon majburan tugatiladi, fayllar zaxira nusxadan tiklanadi). Papkaning maxfiylik darajasi MAC elementi sifatida chegaralarni oshiradi, shuning uchun bir xil baho maxfiyroq papkada qat’iyroq cheklovga olib keladi. To‘xtatib turish darajasida jarayon to‘xtatiladi va papka NTFS ACL orqali vaqtincha yozishdan qulflanadi. Hujum aniqlansa, fayllar boshida saqlangan zaxira nusxadan tiklanadi.

NTFS ACL ni qo‘llash

«To‘xtatib turish» darajasiga tushganda AdaptGuard himoyalangan papkaga joriy foydalanuvchi uchun yozish, qo‘shib yozish va o‘chirishni rad etuvchi (deny) ruxsat yozuvini qo‘shadi: icacls <papka> /deny <foydalanuvchi>:(OI)(CI)(DE,WD,AD,DC). Qulf ishonchlilik tiklanganda, jarayon bloklanganda yoki 60 soniyadan keyin icacls <papka> /remove:d <foydalanuvchi> bilan olib tashlanadi. Windows 11 dagi sinovda qulflangan papkada fayl yaratish, yozish va o‘chirish rad etildi, o‘qish ishladi; qulf olingach yozish tiklandi. «D» huquqi o‘qishni ham taqiqlagani uchun «DE» ishlatildi. NTFS ruxsatlari jarayon bo‘yicha emas, foydalanuvchi bo‘yicha ishlaydi, shu sababli qulf papkadagi barcha jarayonlarga ta’sir qiladi; shu foydalanuvchi nomidan ishlaydigan zararli dastur qulfni olib tashlashi mumkin.

Eksperiment va natijalar

Metodika

Eksperiment sinov stendida (bench) o‘tkazildi: u modellashtirilgan fayl hodisalari izini yaratadi, adaptiv modelda esa AdaptGuard dagi haqiqiy aniqlash va ishonchlilik moduli ishlatiladi. Stsenariylar: 7 hujum (tez, sekin, faqat kengaytma, ommaviy o‘chirish, niqoblangan, qisman shifrlash, nusxa yaratib asl faylni o‘chirish) va 8 oddiy ish (arxivlash, nusxalash, tahrirlash, foto import, dastur yig‘ish, tozalash, qayta nomlash); har biri 3 papka darajasida 30 marta takrorlandi. Statik modellarda ruxsat jarayon toifasi va papka darajasiga qarab oldindan beriladi: DAC (oddiy NTFS: foydalanuvchi nomidan ishlaydigan har qanday jarayon yoza oladi) hamma yozuvga ruxsat beradi, MAC (Biba qoidasi) past yaxlitlikdagi jarayonni yuqori darajali papkaga yozdirmaydi, RBAC rol bo‘yicha ruxsat matritsasidan foydalanadi. Jami $7 \cdot 3 \cdot 30 = 630$ hujum va $8 \cdot 3 \cdot 30 = 720$ oddiy ish ishga tushirildi; takrorlarda fayllar tartibi, tezligi va entropiyasi tasodifiy o‘zgartirildi

(seed = 1). Ko‘rsatkichlar: TPR (model aralashgan hujum ishga tushirishlari / 630), FPR (model noto‘g‘ri aralashgan oddiy ish ishga tushirishlari / 720; 95% Uilson oralig‘i bilan), aniqlash vaqti, yo‘qotilgan fayllar ulushi (nishondagi 200 fayldan). Aralashuv - yozishni rad etish yoki jarayonni to‘xtatish. Chegaralar boshqa tasodifiy to‘plamda tanlangan.

Natijalar

Asosiy solishtirish natijalari (7 ta hujum va 8 ta oddiy ish holati bo‘yichava papka darajalari bo‘yicha):

1-jadval

Parametrlar qiymatlari jadvalda

Model	TPR	FPR	Vaqt, s (mediana)	Yo‘qotilgan
NTFS (statik DAC)	0,0%	0,0%	-	100,0%
Statik MAC	57,1%	50,0%	0,00	42,9%
Statik RBAC	28,6%	25,0%	0,00	71,4%
A-NTFS (eski detektor)	100,0%	59,2%	0,10	10,4%
A-NTFS (yangi, taklif)	100,0%	9,7%	0,63	18,2%

Oddiy NTFS (DAC) hech bir hujumni to‘xtatmadi, niqoblangan hujum esa uchala statik modeldan o‘tdi; MAC va RBAC hujumning bir qismini to‘xtatdi, lekin oddiy ishning ham 50% va 25% ini to‘sdi. A-NTFS sinalgan 7 hujum ssenariysining barchasida hujumni aniqladi (TPR 100%, 95% oraliq 99,4–100%; mediana 0,63 s; sekin hujumda uzoqroq, o‘rtacha 22 s) va oddiy ishning 9,7% ida (7,8–12,1%) noto‘g‘ri aralashdi. Oraliqlar faqat tasodifiy tebranishni ko‘rsatadi va yangi hujum turlariga umumlashtirilmaydi. Dastlabki detektor entropiyasi yuqori har bir yozuvni, yangi yaratilgan fayl yozuvini va har qanday kengaytma almashtirishni signal deb hisoblar, ommaviy o‘zgartirish va o‘chirish chegaralari 15 va 10 edi; shu sababli arxivlash, foto import, ommaviy nomlash kabi oddiy ishlarda doim noto‘g‘ri aralashgan. Yangi detektor entropiya o‘sishini (kamida 1,5 bit/bayt), yangi fayl uchun 2 soniyalik muhlatni va odatiy kengaytmalar ro‘yxatini hisobga oladi, chegaralar 50 va 30 ga oshirilgan; faqat qoidalar yangilanib chegaralar eski qolsa, FPR 21,0% bo‘ladi. Yangilash FPR ni 59,2% dan 9,7% gacha tushirdi, yo‘qotilgan fayllar esa 10,4% dan 18,2% gacha oshdi. Ablation: tuzoq fayllarsiz TPR 87,3% ga tushdi, yo‘qotilgan fayllar 46,9% ga yetdi; papka koeffitsiyentisiz FPR 0%, lekin yo‘qotilgan fayllar 25,4%. Controlled Folder Access [14] ilova obro‘si va ruxsat etilgan ilovalar ro‘yxatiga, A-NTFS esa jarayonning xatti-harakatiga tayanadi.

Amaliy sinov va cheklovlar

Prototip Windows 11 da zararsiz simulyator yordamida sinaldi. Simulyator maxfiy papkadagi 30 ta matn faylini tasodifiy baytlar bilan almashtirib, kengaytmasini “.locked” ga o‘zgartiradi (haqiqiy shifrlash bajarilmaydi) va faqat “test_papka” nomli papkada ishlaydi. Takroriy ishga tushirishlarda yuqori entropiya signali berildi, simulyator jarayoni to‘xtatildi va 3–4 ta zararlangan fayl zaxira nusxadan tiklandi; 30 ta asl fayl saqlanib qoldi, “.locked” fayllar qolmadi. Amaliy sinov dastlabki xarakterga ega bo‘lib, prototipning ishlash qobiliyatini tasdiqlaydi; statistik baholash 4.2-bo‘limdagi stend natijalariga asoslanadi.

Haqiqiy fayllar bilan keng ko‘lamli tekshirish virtual mashinada keyingi bosqichda o‘tkaziladi. Stendda jarayon to‘g‘ri aniqlangan deb olinadi; Windowsda aniqlash aniqligi alohida o‘lchanmadi, bir papkada ishlovchi jarayonlar esa bir-biridan ajralmasligi mumkin; stsenariy parametrlari taxminiy. Foydalanuvchi darajasidagi dastur hujumni oldindan emas, boshlangandan keyin to‘xtatadi, shu sababli zaxira muhim; to‘liq nazorat uchun yadro darajasidagi minifilter

drayver zarur. Ishonchli ilovalar nom bo‘yicha tekshiriladi: ularning nomini olgan zararli dastur boshlang‘ich 90 bahoni oladi. Entropiya qoidasi siqilgan fayllarni shifrlashni sezmaydi; nusxa yaratib asl faylni o‘chiradigan hujum sekinroq topiladi (yo‘qotilgan fayllar 27,0%); qisman shifrlash entropiyani pasaytiradi. Dastur yig‘ish va tozalash maxfiy papkalarda hamon yolg‘on signal beradi.

Xulosa

Maqolada NTFS ruxsatlarining statikligi ransomware hujumlarida zaiflik ekani ko‘rsatildi va ruxsat darajasini jarayonning ishonchlilik bahosiga bog‘lovchi adaptiv NTFS (A-NTFS) modeli taklif etildi. Model AdaptGuard prototipida amalga oshirilgan; ACL ni icacls orqali boshqarish va umumiy ishlash Windows 11 da zararsiz simulyator bilan sinaldi; haqiqiy fayllar bilan keng ko‘lamli sinov keyingi bosqichda bajariladi. Stend natijalariga ko‘ra A-NTFS sinalgan hujumlarning barchasini aniqladi (FPR 9,7%), oddiy NTFS (DAC), MAC va RBAC da esa hujumlarning 0%, 57% va 29% i to‘xtatildi; bu natijalar modellashtirilgan hodisalarga tegishli va haqiqiy ransomware uchun tasdiqlanmagan.

Adabiyotlar

1. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. DIMVA 2015, LNCS 9148. DOI: 10.1007/978-3-319-20550-2_1.
2. Microsoft Learn. ACE Inheritance. learn.microsoft.com (Win32 Security).
3. Microsoft Learn. Mandatory Integrity Control. learn.microsoft.com.
4. Saltzer J.H., Schroeder M.D. The Protection of Information in Computer Systems. Proceedings of the IEEE, 1975, 63(9), 1278–1308.
5. Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models. IEEE Computer, 1996, 29(2), 38–47.
6. Scaife N., Carter H., Traynor P., Butler K.R.B. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. IEEE ICDCS, 2016, 303–312. DOI: 10.1109/ICDCS.2016.46.
7. Continella A. va boshq. ShieldFS: A Self-healing, Ransomware-aware Filesystem. ACSAC 2016, 336–347. DOI: 10.1145/2991079.2991110.
8. Kharraz A., Arshad S., Mulliner C., Robertson W., Kirda E. UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. 25th USENIX Security Symposium, 2016, 757–772.
9. Catuogno L., Galdi C. On Tracking Ransomware on the File System. ICISSP 2022, vol. 1, 210–219. DOI: 10.5220/0010985000003120.
10. Begovic K., Al-Ali A., Malluhi Q. Cryptographic ransomware encryption detection: Survey. Computers & Security, 2023. arXiv:2306.12008.
11. van Sloun C., Woeste V., Wolsing K., Pennekamp J., Wehrle K. Detecting Ransomware Despite I/O Overhead: A Practical Multi-Staged Approach. NDSS 2025.
12. Guo L., Hou Y., Zhou C., Zhang Q., Jiang Y. Ransomware Detection through Temporal Correlation between Encryption and I/O Behavior. FSE 2025. DOI: 10.1145/3715725.
13. Shannon C.E. A Mathematical Theory of Communication. Bell System Technical Journal, 1948, 27(3), 379–423; 27(4), 623–656.
14. Microsoft Learn. Controlled folder access. learn.microsoft.com (Defender).

ZAMONAVIY KIBERXAVFSIZLIK TIZIMLARIDA MASHINALI O‘QITISH ALGORITMLARI ASOSIDA ZARARLI DASTURLARNI ANIQLASH VA TASNIFLASH

Samarov X. K., Yakubova D.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada mashinali o‘qitish asosida zararli dasturiy ta’minotni (malware) aniqlash va tasniflash mexanizmlari tahlil qilinadi. Signaturaga asoslangan va evristik usullarning polimorf, metamorf hamda nolinchi kun (zero-day) tahdidlariga nisbatan cheklovlari ko‘rib chiqiladi. Portable Executable (PE) fayllari sarlavha xususiyatlariga asoslangan ClaMP ma’lumotlar to‘plamida (5207 ta noyob namuna) Decision Tree, Random Forest, Gradient Boosting, SVM hamda ularning gibrid ansambllari yagona nested cross-validation protokolida solishtirildi. Random Forest eng yuqori ko‘rsatkichlarga erishdi (aniqlik 99,17%, F1 99,21%, ROC-AUC 99,93%) va o‘qitish tezligi bo‘yicha Gradient Boostingdan 5 baravardan ortiq tez bo‘ldi; gibrid ansambl aniqlikni oshirmadi, Random Forest bilan Gradient Boosting, SVM va gibrid modellar o‘rtasidagi farq statistik jihatdan ahamiyatsiz. Datasetga xos CheckSum va fileinfo belgilari olib tashlanganda aniqlik taxminan 0,5 foiz bandga pasaydi.

Kalit so‘zlar: kiberxavfsizlik, zararli dasturlar, mashinali o‘qitish, PE fayl tahlili, Random Forest, Gradient Boosting, SVM, gibrid ansambl, nested cross-validation.

Аннотация. В статье анализируются механизмы обнаружения и классификации вредоносного программного обеспечения (malware) на основе машинного обучения. Рассматриваются ограничения сигнатурных и эвристических методов при обнаружении полиморфных, метаморфных угроз и угроз нулевого дня (zero-day). На наборе данных ClaMP, основанном на признаках заголовков файлов Portable Executable (PE) (5207 уникальных образцов), в едином протоколе вложенной перекрёстной проверки (nested cross-validation) сравнены Decision Tree, Random Forest, Gradient Boosting, SVM и их гибридные ансамбли (soft-voting). Random Forest показал наивысшие результаты (точность 99,17%, F1 99,21%, ROC-AUC 99,93%) и обучается более чем в 5 раз быстрее Gradient Boosting; гибридный ансамбль точность не повысил, различия между Random Forest, Gradient Boosting, SVM и гибридными моделями статистически незначимы. После исключения специфичных для набора данных признаков CheckSum и fileinfo точность снизилась примерно на 0,5 процентного пункта.

Ключевые слова: кибербезопасность, вредоносные программы, машинное обучение, анализ PE-файлов, Random Forest, Gradient Boosting, SVM, гибридный ансамбль, вложенная перекрёстная проверка.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va davlat boshqaruvi, mudofaa hamda iqtisodiy infratuzilmalarning raqamli transformatsiyasi axborot xavfsizligini strategik ahamiyatga ega yo‘nalishga aylantirmoqda. Zararli dasturlarni yaratishda polimorfizm, metamorfoz, kodni chalkashtirish (obfuscation) va qadoqlash (packing) kabi usullardan foydalanilishi an’anaviy aniqlash mexanizmlarining samaradorligini pasaytiradi [1]. Signatura tahlili ma’lum zararli dasturlarga xos hash qiymatlar yoki baytlar ketma-ketligini izlashga asoslangani uchun avval kuzatilmagan va o‘zgartirilgan namunalarni aniqlashda cheklovlarga ega

[2]. Shu sababli mashinali o‘qitish usullariga ehtiyoj ortmoqda. Maqolaning maqsadi - PE fayllarining sarlavha xususiyatlari asosida zararli dasturlarni aniqlovchi klassik algoritmlar va ularning gibrid ansamblini yagona, adolatli protokolda solishtirib, amaliy foydalanish uchun eng maqbul yechimni asoslashdir.

Asosiy qism.

An’anaviy yondashuvlarning cheklovlari

Signaturaga asoslangan va evristik usullar ma’lum tahdidlarni aniqlashda samarali bo‘lsa-da, signaturalar bazasi hajmining ortishi, shifrlash, chalkashtirish va qadoqlash yordamida signaturalarni chetlab o‘tish hamda yangi va nolinchi kun (zero-day) tahdidlarini aniqlashning ma’lum namunalar bazasiga bog‘liqligi kabi cheklovlarga duch kelmoqda. Statik va dinamik tahlilni mashinali o‘qitish bilan integratsiyalash bu cheklovlarni kamaytirishning muhim yo‘nalishi hisoblanadi [3].

Mashinali o‘qitish algoritmlari

Decision Tree obyektlarni ketma-ket shartlar asosida sinflarga ajratadi; u tushunarli, biroq chuqur daraxt ortiqcha moslashishga (overfitting) moyil. Random Forest ko‘plab tasodifiy daraxtlar ovozini birlashtirib dispersiyani kamaytiradi va belgilar muhimligini baholash imkonini beradi [4]. Support Vector Machine (SVM) sinflarni ajratuvchi optimal gipertekislikni topadi va yadro (kernel) funksiyasi orqali nochiziqli chegaralarni quradi, biroq hisoblash resursini ko‘p talab qilishi mumkin [5]. Gradient Boosting sodda modellarni ketma-ket qo‘shadi, har bir keyingi model avvalgi xatolarni kamaytirishga yo‘naltiriladi [6]; uning LightGBM varianti EMBER to‘plamida statik PE xususiyatlari bo‘yicha asosiy (baseline) model sifatida qo‘llangan [7].

Chuqur o‘qitish va tadqiqot doirasi

Konvolyutsion va rekurrent neyron tarmoqlar fayl baytlari, opcode va API chaqiruvlari ketma-ketligidan xususiyatlarni avtomatik ajratib oladi (masalan, MalConv [8]), biroq katta hajmli ma’lumot va yuqori hisoblash quvvatini talab qiladi. Ushbu tadqiqotda 5 mingga yaqin namunadan iborat jadval shaklidagi sarlavha xususiyatlari ishlatilgani sababli chuqur modellar sinovga kiritilmadi.

Klassifikator arxitekturasi

Klassifikator to‘rt bosqichdan iborat: (1) PE fayllaridan sarlavha maydonlari (DOS Header, File Header, Optional Header), bo‘limlar va entropiya kabi xususiyatlarni ajratish; (2) kategorial belgilarni (qadoqlovchi turi) One-Hot kodlash, SVM uchun sonli belgilarni logarifmlash va standartlashtirish (daraxt modellari masshtabga sezgir emas); (3) algoritmni o‘qitish; (4) metrikalar bo‘yicha baholash. Yuqori entropiya shifrlash yoki qadoqlashga ishora qilishi mumkin, biroq mustaqil ravishda faylning zararli ekanini bildirmaydi.

Tajriba natijalari va samaradorlikni baholash

Tajriba uchun ClaMP (Classification of Malware with PE headers) to‘plamidan foydalanildi [9]: 5210 ta Windows PE fayli (2722 ta zararli, 2488 ta qonuniy) va 69 ta belgi (54 ta xom sarlavha maydoni, 15 ta hosila belgi: bo‘limlar, qadoqlovchi turi, entropiya, fayl hajmi va boshqalar). 3 ta takroriy yozuv olib tashlangach (5207 ta namuna: 2719 ta zararli, 2488 ta qonuniy) baholash Arp va hammualliflari tavsiyalariga ko‘ra [10] tashkil etildi: 3 marta takrorlangan 5-karrali stratifikatsiyalangan tashqi o‘zaro tekshirish (jami 15 ta bo‘linish); giperparametrlar faqat tashqi o‘qitish qismi ichidagi 3-karrali ichki tekshiruv orqali tanlandi (nested cross-validation [11]), shuning uchun test ma’lumotlari sozlashda ishtirok etmadi va barcha algoritmlar teng sharoitda sozlandi (Random Forest: max_features, min_samples_leaf; Gradient Boosting: 300 ta daraxt, learning_rate, max_depth; SVM: RBF yadro, C, gamma; random_state = 42). Modellar

orasidagi farq F1 bo‘yicha Nadeau va Bengio tuzatilgan takroriy t-testi bilan baholandi [12]. Gibrid modellar sifatida sozlangan modellarning ehtimolliklari o‘rtachalanadigan yumshoq ovoz berish (soft voting) ansambllari - RF+GB va RF+GB+SVM - qurildi [13]. TPR@1% FPR - zararsiz fayllarni zararli deb noto‘g‘ri belgilash ehtimoli (1-tur xatolik) 1% dan oshmaganda aniqlangan zararli namunalar ulushi (testning quvvati); Decision Tree uchun u hisoblanmadi.

1-jadval

Algoritmlar samaradorligi (15 ta bo‘linish bo‘yicha o‘rtacha, %; o‘qitish vaqti - soniyada; «-» - yakka daraxtda hisoblanmagan)

Model	Aniqlik	Precision	Recall	F1	ROC-AUC	TPR@1 % FPR	Vaqt, s
Decision Tree	97,49	97,26	97,97	97,61	97,50	-	0,05
Random Forest	99,17	98,92	99,50	99,21	99,93	99,30	0,88
Gradient Boosting	98,98	98,77	99,28	99,02	99,93	99,07	4,69
SVM (RBF)	98,85	98,72	99,08	98,90	99,79	98,16	0,78
Gibrid RF+GB	99,02	98,84	99,29	99,06	99,93	99,24	5,57
Gibrid RF+GB+SVM	99,16	98,99	99,40	99,19	99,93	99,29	6,34

Random Forest eng yuqori natijani ko‘rsatdi (aniqlik 99,17 ± 0,25%, F1 99,21 ± 0,24%, ROC-AUC 99,93%; test qismidagi taxminan 1041 ta namunada o‘rtacha 8,7 ta xato). Gradient Boosting (98,98%), SVM (98,85%) va gibrid ansambllar (99,02-99,16%) unga yaqin, biroq tuzatilgan t-test bo‘yicha farq statistik jihatdan ahamiyatsiz ($p = 0,09$ dan $p = 0,94$ gacha, Random Forest bilan taqqoslaganda); faqat yagona Decision Tree sezilarli past (97,49%, $p < 0,001$). Gibrid ansambl aniqlikni oshirmadi: RF+GB+SVM (99,16%) Random Forest (99,17%) bilan deyarli bir xil, biroq Random Forest o‘qitish vaqti bo‘yicha Gradient Boostingdan 5,3 baravar, gibrid RF+GB+SVM dan 7,2 baravar tez (0,88 s ga qarshi 4,69 s va 6,34 s).

Gibrid ansambl nima uchun Random Forest dan ustun bo‘lmadi? Qo‘shimcha tahlil (5 ta tashqi bo‘linishning jamlangan out-of-fold ehtimolliklari, 5207 ta namuna) buni modellar xatolarining o‘xshashligi bilan izohlaydi: RF, GB va SVM ehtimolliklari orasidagi Pearson korrelyatsiyasi 0,985-0,990, xatolar kesishmasi esa juda yuqori (Yule Q = 0,984-0,995). Kamida bitta model xato qilgan 96 ta namunaning 16 tasida uchala model ham xato qildi; RF ning 39 ta xatosidan 19 tasini SVM ham takrorladi. Ansambl faqat modellar turlicha xato qilganda foyda beradi [13], bu yerda esa qiyin namunalar (ehtimol, qadoqlangan yoki yorliqlari shubhali fayllar) hamma modellar uchun umumiy, shuning uchun ovoz berish ularni tuzatmaydi. Taxmin qilingan SVM ehtimolliklarining kalibrlanmaganligi tasdiqlanmadi: SVM kalibrlash xatosi (ECE) 0,0032, GB nikidek past, RF ning ECE si esa 0,031. Ansambl yorliq aniqligini emas, ehtimolliklar sifatini yaxshiladi: RF+GB+SVM ning Brier ko‘rsatkichi 0,0070 (RF: 0,0105, GB: 0,0079), biroq bu farq xatolar sonida ko‘rinmaydi (42 ta, RF: 39 ta).

ClaMP da CheckSum (zararli namunalarning 59% ida nolga teng, qonuniylarda 10%) va fileinfo (versiya ma’lumoti qonuniy fayllarning 81%, zararlilarning 30% ida mavjud) kabi belgilar namunalarni to‘plash usuliga xos farqni aks ettirishi mumkin va Random Forest muhimlik reytingida yuqori o‘rinlarni egallaydi (to‘liq ma’lumotda sozlanmagan model: eng muhim belgi - File Header Characteristics bayrog‘i FH_char12, CheckSum - 3-o‘rin, fileinfo - 7-o‘rin). Shu sababli tajriba bu ikki belgisiz ham takrorlandi (2-jadval).

Belgilar olib tashlanganda Random Forest aniqligi 99,17% dan 98,62% ga, SVM aniqligi 98,85% dan 98,05% ga tushdi. Random Forest va gibrid ansambllar yana bir xil darajada qoldi, SVM esa endi Random Forest dan sezilarli past (p = 0,012). Demak, modellar

2-jadval

CheckSum va fileinfo belgilarisiz natijalar (%; p - Random Forest bilan F1 bo'yicha taqqoslash)

Model	Aniqlik	F1	ROC-AUC	TPR@1% FPR	p-qiymat
Decision Tree	96,89	97,03	97,34	-	<0,001
Random Forest	98,62	98,69	99,89	97,70	-
Gradient Boosting	98,38	98,45	99,88	97,29	0,28
SVM (RBF)	98,05	98,13	99,61	95,15	0,012
Gibrid RF+GB	98,60	98,66	99,90	97,76	0,87
Gibrid RF+GB+SVM	98,53	98,59	99,90	97,54	0,56

tartibi saqlandi, biroq mutlaq ko'rsatkichlar ma'lum darajada dataset artefaktlariga bog'liq.

Tadqiqot cheklovlari. Birinchidan, ClaMP da yaratilish sanasi va zararli dastur oilalari yorliqlari yo'q, shuning uchun vaqt bo'yicha ajratish amalga oshirilmadi. Arp va hammualliflari ko'rsatganidek, tasodifiy (statik) o'zaro tekshirish o'qitish va test namunalarini bir davrdan oladi (vaqt bo'yicha ma'lumotlar sizib o'tishi), natijada real sharoitda - keyingi davrda paydo bo'lgan yangi namunalarda - samaradorlik odatda sezilarli pasayadi [10]. Shu sababli bu yerdagi 99% atrofidagi ko'rsatkichlarni yuqori chegara sifatida qabul qilish, algoritmlarni esa faqat o'zaro nisbiy solishtirish kerak; ishlab chiqarish uchun baho EMBER [7] kabi vaqt belgilari mavjud to'plamda o'tmish ma'lumoti bilan o'qitib, keyingi oylar ma'lumotida sinash orqali olinishi lozim. Ikkinchidan, raqib hujumlariga chidamlilik sinalmadi: bu tadqiqotning maqsadi algoritmlarni sof taqqoslash edi, ClaMP esa faqat tayyor xususiyat jadvalini beradi va asl PE fayllarini o'z ichiga olmaydi, shuning uchun funksiyani saqlaydigan o'zgartirishlarni (bo'lim qo'shish, qadoqlash, sarlavha maydonlarini o'zgartirish) fayl darajasida qo'llab bo'lmaydi. Bunday sinov asl fayllar va ularni o'zgartiruvchi hujum (oq yoki qora quti tahdid modeli bo'yicha) bilan o'tkazilishi, hujumdan oldingi va keyingi TPR taqqoslanishi kerak. CheckSum kabi maydonlarni hujumchi osongina o'zgartira olishi tufayli, ularga tayanuvchi modellar ayniqsa zaif bo'lishi mumkin. Uchinchidan, natijalar faqat statik sarlavha belgilariga tegishli.

Xulosa

Zararli dasturlarni mashinali o'qitish asosida aniqlashda an'anaviy signaturaga asoslangan yondashuvlarning cheklovlari intellektual tahlil usullaridan foydalanishni talab qiladi. ClaMP to'plamida yagona nested cross-validation protokolida sinalgan algoritmlar orasida Random Forest eng yaxshi natija ko'rsatdi (aniqlik 99,17%, F1 99,21%) va o'qitish tezligi bo'yicha afzal chiqdi; Gradient Boosting, SVM va gibrid ansambllar bilan farq statistik jihatdan ahamiyatsiz, Decision Tree esa sezilarli past bo'ldi. Gibrid (soft-voting) ansambl aniqlikni oshirmadi, o'qitish xarajatini esa taxminan 7 baravar oshirdi, shu sababli ushbu ma'lumotlarda yagona Random Forest modeli tavsiya etiladi. Gibrid ansambl modellar xatolari yuqori korrelyatsiyalangani (Yule Q > 0,98) uchun foyda bermadi. Gibrid yondashuvning foydasini katta to'plamlarda (masalan, EMBER [7]) vaqt bo'yicha ajratilgan ma'lumotlar bilan, shuningdek raqib hujumlariga chidamlilik va natijalarni izohlash (SHAP) jihatidan tekshirish kelgusi vazifadir.

Foydalanilgan adabiyotlar

1. Ucci D., Aniello L., Baldoni R. Survey of Machine Learning Techniques for Malware Analysis // Computers & Security. - 2019. - Vol. 81. - p. 123-147. DOI: 10.1016/j.cose.2018.11.001

2. Aslan Ö., Samet R. A Comprehensive Review on Malware Detection Approaches // IEEE Access. - 2020. - Vol. 8. - p. 6249-6271. DOI: 10.1109/ACCESS.2019.2963724

3. Gibert D., Mateu C., Planes J. The Rise of Machine Learning for the Detection and Classification of Malware: Research Developments, Trends and Challenges // Journal of Network and Computer Applications. - 2020. - Vol. 153. - Art. 102526. DOI: 10.1016/j.jnca.2019.102526

4. Breiman L. Random Forests // Machine Learning. - 2001. - Vol. 45, No. 1. - p. 5-32. DOI: 10.1023/A:1010933404324

5. Cortes C., Vapnik V. Support-Vector Networks // Machine Learning. - 1995. - Vol. 20, No. 3. - p. 273-297. DOI: 10.1007/BF00994018

6. Friedman J. H. Greedy Function Approximation: A Gradient Boosting Machine // The Annals of Statistics. - 2001. - Vol. 29, No. 5. - p. 1189-1232. DOI: 10.1214/aos/1013203451

7. Anderson H. S., Roth P. EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models // arXiv preprint arXiv:1804.04637. - 2018. DOI: 10.48550/arXiv.1804.04637

8. Raff E., Barker J., Sylvester J., Brandon R., Catanzaro B., Nicholas C. Malware Detection by Eating a Whole EXE // arXiv preprint arXiv:1710.09435. - 2017. DOI: 10.48550/arXiv.1710.09435

9. Kumar A., Kuppusamy K.S., Aghila G. A learning model to detect maliciousness of portable executable using integrated feature set // Journal of King Saud University - Computer and Information Sciences. - 2019. - Vol. 31, Issue 2. - p. 252-265. DOI: 10.1016/j.jksuci.2017.01.003

10. Arp D. et al. Dos and Don'ts of Machine Learning in Computer Security // 31st USENIX Security Symposium. - 2022. - p. 3971-3988. arXiv: 2010.09470.

11. Varma S., Simon R. Bias in error estimation when using cross-validation for model selection // BMC Bioinformatics. - 2006. - Vol. 7. - Art. 91. DOI: 10.1186/1471-2105-7-91

12. Nadeau C., Bengio Y. Inference for the Generalization Error // Machine Learning. - 2003. - Vol. 52, No. 3. - p. 239-281. DOI: 10.1023/A:1024068626366

13. Dietterich T. G. Ensemble Methods in Machine Learning // Multiple Classifier Systems (MCS 2000), Lecture Notes in Computer Science, vol. 1857. - Berlin: Springer, 2000. - p. 1-15. DOI: 10.1007/3-540-45014-9_1.

KUBERNETES TARMOQ ARXITEKTURASI VA KONTEYNERLASHTIRILGAN MUHITDAGI TRAFIK OQIMI

Xolimtayeva I.U. Yuldashev B.T.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda Kubernetes tarmoq modeli, Pod–Service aloqasi va konteynerlashtirilgan muhitdagi trafik yo‘nalishlari tahlil qilinadi. Rasmiy Kubernetes va CNI hujjatlari asosida Frontend Pod, Service, Backend Pod, Database Pod ssenariysi, DNS orqali xizmatni aniqlash, EndpointSlice asosida backend tanlash hamda NetworkPolicy bilan segmentatsiyalash bosqichlari tizimlashtirildi. Tahlil NetworkPolicy siyosatlari faqat ularni amalda bajaradigan CNI mavjud bo‘lganda samara berishi, L3/L4 qoidalari esa shifrlash yoki ilova ichidagi avtorizatsiya o‘rnini bosmasligini ko‘rsatadi. Eksperiment o‘tkazilmagan; natija trafik va xavf yo‘nalishlari bo‘yicha qiyosiy modeldir.

Kalit so‘zlar: Kubernetes, Pod, Service, EndpointSlice, CNI, CoreDNS, NetworkPolicy, Calco, Cilium, eBPF, lateral movement.

Аннотация. Анализируются сетевая модель Kubernetes, связь Pod–Service и направления трафика в контейнеризированной среде. На основе официальной документации Kubernetes и CNI систематизирован сценарий Frontend Pod, Service, Backend Pod , Database Pod, обнаружение сервиса через DNS, выбор backend на основе EndpointSlice и сегментация с помощью NetworkPolicy. Показано, что NetworkPolicy обеспечивает защиту только при наличии CNI, реально применяющего эти политики, а правила L3/L4 не заменяют шифрование и прикладную авторизацию. Эксперименты не проводились; результатом является сравнительная модель потоков и угроз.

Ключевые слова: Kubernetes, Pod, Service, EndpointSlice, CNI, CoreDNS, NetworkPolicy, Calico, Cilium, eBPF, боковое перемещение.

Kirish

Kubernetes ish yuklamalarini Podlar ko‘rinishida joylashtiradi, qayta yaratadi va tugunlar o‘rtasida ko‘chirishi mumkin. Shu dinamiklik IP manzillar va endpointlar ro‘yxati o‘zgarishiga olib keladi; ilova komponentlari esa barqaror mantiqiy nom va boshqariladigan kirish nuqtasiga muhtoj. Kubernetes Service abstraksiyasi xizmatning doimiy manzilini, EndpointSlice esa unga bog‘langan backend endpointlarining joriy to‘plamini ifodalaydi. CNI tarmoq plagini Pod interfeysi va ulanishini sozlaydi; xizmat trafikini yo‘naltirish esa kube-proxy yoki CNI bilan integratsiyalashgan muqobil data plane orqali bajarilishi mumkin.

Ilmiy muammo - Podlar dinamik bo‘lgan sharoitda xizmat topish, paketni to‘g‘ri endpointga yetkazish va xavfsizlik qoidasini bir xil tatbiq etish oson emas. Noto‘g‘ri yoki umuman yo‘q segmentatsiya frontend zaifligi orqali backend va ma’lumotlar bazasiga lateral movement uchun yo‘l ochishi mumkin. Tadqiqot maqsadi - trafik oqimini bosqichma-bosqich tushuntirish, CNI va trafik boshqarish komponentlarining vazifalarini farqlash hamda NetworkPolicy asosidagi himoyaning imkoniyat va chegaralarini aniqlash.

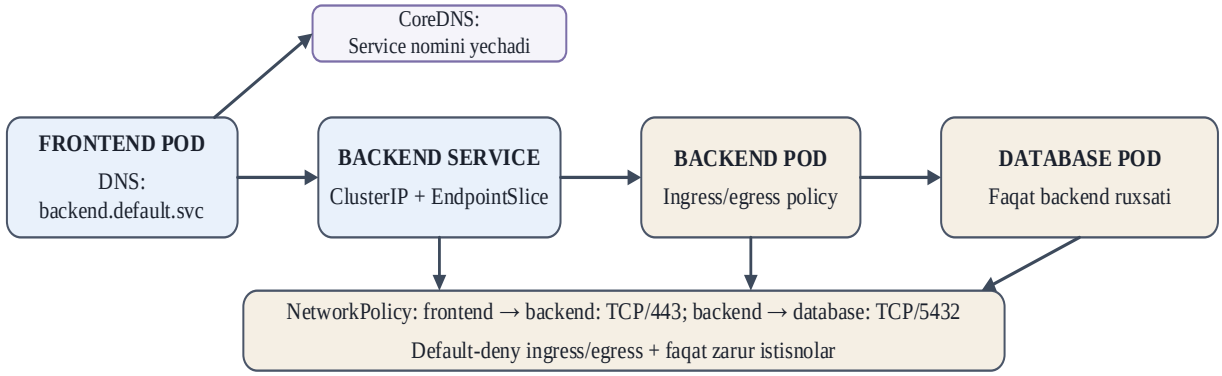
Tadqiqotning asosiy savoli - trafik oqimining qaysi nuqtasida nomni aniqlash, endpoint tanlash, paketni uzatish va ruxsatni tekshirish sodir bo‘lishini aniqlash hamda ularni o‘zaro aralashtirmaslikdir. Ushbu ajratish tarmoq muammosini diagnostika qilishda ham, himoya siyosatini tanlashda ham muhim: DNS muvaffaqiyatsizligi, eskirgan endpoint ro‘yxati va NetworkPolicy tomonidan bloklashning belgilari bir-biridan farq qiladi.

Asosiy qism

Tadqiqotda rasmiy Kubernetes hujjatlari, CNI spetsifikatsiyasi, Gateway API materiallari va NIST konteyner xavfsizligi tavsiyalari mezonli tahlil qilindi. Shuningdek, CNI plaginlari samaradorligi hamda NetworkPolicy ijrosini baholagan taqrizdan o‘tgan jurnal va konferensiya ishlari qiyosiy kontekst sifatida ko‘rib chiqildi. Manbalar (1) arxitektura yoki API xatti-harakatini birlamchi tarzda belgilashi, (2) trafik oqimi yoki siyosat ijrosiga bevosita aloqadorligi, (3) xizmat topish, paket uzatish, segmentatsiya yoki xavfsizlik chegaralaridan birini yoritishi asosida tanlandi. Har bir trafik yo‘nalishi uchun aktiv, hujum sathi, profilaktik siyosat va qoldiq xavf qayd qilindi. Calico va Cilium funksiyalari mahsulot hujjatlaridagi e’lon qilingan imkoniyatlar bo‘yicha sifat jihatidan qiyoslandi; bir xil apparat va yuk ostida o‘z benchmarkimiz o‘tkazilmagan, shu bois tezlik bo‘yicha miqdoriy xulosa berilmaydi.

Pod klaster ichida noyob IP manzilga ega bo‘ladi; Podlar orasidagi asosiy tarmoq modeli bevosita aloqani ko‘zda tutadi, lekin bu ochiq aloqa xavfsiz degani emas. Node - Podlar ishlaydigan tugun. CNI konteyner ishga tushganda tarmoq interfeysi va manzil sozlamalarini boshqaradi; amaliyotda plugin modeli ADD/DEL/CHECK kabi operatsiyalar orqali tarmoq resurslari hayot sikliga bog‘lanadi. IPAM, marshrutlash, overlay va policy enforcement imkoniyatlari tanlangan plaginga qarab farq qiladi.

Service Podlar ortidagi barqaror tarmoq identifikatoridir. Selector asosidagi Service uchun control plane mos Podlar ro‘yxatini EndpointSlice obyektlarida yangilaydi; xizmat proxy mexanizmi esa ushbu holatga asoslanib maqsad manzilga uzatishni sozlaydi. ClusterIP ichki virtual IP beradi; NodePort tugun porti orqali, LoadBalancer esa mos tashqi infratuzilma yordamida kirishni ta’minlaydi. HTTP/HTTPS tashqi trafikini boshqarishda Ingress ishlatilishi mumkin, biroq Kubernetes rasmiy hujjatlari yangi imkoniyatlar uchun Gateway API ga e’tibor qaratadi.



1-rasm. Frontend–backend–ma’lumotlar bazasi oqimi va siyosat nazorat nuqtalari

CoreDNS Service va Pod nomlarini DNS yozuvlariga bog‘laydi. Oddiy Service nomi odatda Service IP manziliga yechiladi; keyingi paket yo‘li esa Service proxy/data-plane mexanizmi tomonidan amaliyotga oshiriladi. Headless Service holatida DNS backend Podlar manzillarini bevosita qaytarishi mumkin. Shuning uchun “Service orqali o‘tadi” deganda har doim alohida proksi jarayonida paket qayta ishlanadi, deb tushunmaslik kerak: Service mantiqiy abstraksiya, paketni uzatish esa klaster sozlamalariga bog‘liq.

Bir tugun ichidagi aloqa bilan turli tugunlardagi Podlar o‘rtasidagi aloqa ham farq qilishi mumkin. CNI konfiguratsiyasiga qarab paketlar tugunlararo marshrutlanadi yoki VXLAN/IP-in-IP kabi overlay orqali kapsullanishi mumkin; ayrim muhitlarda esa bevosita marshrutlash qo‘llanadi. Bu tafsilotlar MTU, kuzatuv va nosozlikni tahlil qilishga ta’sir etadi, lekin Kubernetes

Service yoki NetworkPolicy semantikasini avtomatik ravishda o‘zgartirmaydi. Shu sababli hujjatda mantiqiy Service modelini tanlangan data-plane realizatsiyasidan alohida bayon qilish zarur.

Frontend Pod backend xizmatiga DNS nomi orqali murojaat qilganda, CoreDNS so‘rovni klaster domenidagi Service nomiga moslaydi. Oddiy ClusterIP Service uchun javob virtual xizmat manzili bo‘ladi; kube-proxy yoki CNI ning muqobil data plane i endpointlar to‘plamidan mavjud backendni tanlab, kerakli uzatish/translation qoidalarini bajaradi. Backend Pod so‘rovni qabul qilgach, database Service ga alohida ulanish boshlaydi. Database ham Service orqali topilsa, EndpointSlice uning mos va tayyor Pod endpointlarini ifodalaydi. Har bir bosqichda amaldagi ulanish porti, protocol, namespace va label tanlovi muhim.

Xavfsizlik siyosati yo‘nalishli bo‘lishi kerak: frontend faqat backend xizmatining zarur portiga, backend esa faqat database portiga murojaat qila olishi lozim. Podga tegishli ingress qoidalari kiruvchi trafikni, egress qoidalari esa undan chiquvchi trafikni cheklaydi. Egress default-deny kiritilganda DNS so‘rovlariga ham aniq ruxsat berish zarur bo‘lishi mumkin; aks holda xizmat nomini yechishning o‘zi ishlamay qoladi. NetworkPolicy qoidalari Pod selector, namespace selector, IP blok va port/protokol mezonlarini qo‘llaydi, ammo siyosatlarni bajarish uchun CNI ushbu API ni qo‘llab-quvvatlashi shart.

1-jadval

Trafik yo‘nalishlari, tahdidlar va himoya mexanizmlari

Trafik yo‘nalishi	Xavfsizlik tahdidi	Himoya mexanizmi	Afzalligi	Cheklovi
Frontend Backend Service	Ruxsatsiz Pod so‘rovi; servisni noto‘g‘ri ochish	Frontend labeliga asoslangan ingress allow; Service portini cheklash	Xizmatlararo kirishni aniq kamaytiradi	Label/policy xatosi yoki ruxsatli frontend kompromet i qoladi
Backend Database	Lateral movement; barcha Podlarga ochiq DB porti	Database Podga default-deny ingress; faqat backend egress/selectoriga ruxsat	Ma’lumotlar qatlamini tor segmentlaydi	NetworkPolicy shifrlash va DB ichidagi SQL ruxsatlarini almashtirmaydi
Pod → DNS	Egress cheklovida DNS bloklanishi yoki DNS suiiste’moli	CoreDNS ga UDP/TCP 53 bo‘yicha kerakli egress ruxsati; DNS monitoring	Xizmat nomlarini boshqariladig an tarzda yechadi	Oddiy L3/L4 siyosat DNS javobining mazmunini tasdiqlamaydi
Tashqi Service	Ortiqcha ochiq NodePort/Ingress; noto‘g‘ri route	Gateway/Ingress, TLS, tashqi firewall va minimal backend expose	Kirish nuqtalarini aniq boshqaradi	Gateway konfiguratsiyasi va controllerning o‘zi ham himoyalanishi kerak
Pod internet/ tashqi API	Ma’lumot sizishi yoki zararli callback	Egress allowlist, proxy/firewall, identifikatsiya va audit	Chiquvchi trafikni kuzatish va cheklash	Dinamik IP/FQDN, bulut endpointlari va istisnolarni boshqarish murakkab

Jadval trafik yo‘nalishini alohida xavfsizlik obyekti sifatida qaraydi. Masalan, Service nomini yashirish yoki namespace yaratishning o‘zi segmentatsiya emas: amaldagi ruxsatlar siyosat bilan bajarilishi kerak. NetworkPolicy standart API i asosan L3/L4 da ishlaydi; HTTP yo‘li, ilova identifikatori yoki foydalanuvchi roli bo‘yicha nazorat kerak bo‘lsa, mos Gateway/service-mesh yoki CNI kengaytmasi qo‘shimcha qatlam beradi.

Default-deny siyosatini joriy etishda avval tanlangan Podlar to‘plami va egress/ingress yo‘nalishlari aniq belgilanadi; keyin zarur trafik ruxsat etilib, kutilmagan oqimlar sinov muhitida kuzatiladi. EndpointSlice yangilanishi, readiness holati va label o‘zgarishlari siyosatga qanday ta’sir qilishi ham tekshiriladi. Shunday qilib, segmentatsiya statik IP ro‘yxatlariga emas, xizmat roli va Pod labeliga bog‘lanadi, ammo noto‘g‘ri yoki ortiqcha umumiy selector hamon xavf tug‘dirishi mumkin.

Agar namespace da Podga ta’sir qiluvchi NetworkPolicy bo‘lmasa, odatiy xatti-harakat bo‘yicha ingress va egress aloqalari ruxsat etilgan bo‘ladi. Shu sababli “default deny” asosiy xavfsizlik bazasi sifatida qo‘llanib, keyin DNS, kuzatuv, frontend–backend va backend–database uchun faqat talab etilgan istisnolar berilishi maqsadga muvofiq. Ingress va egress turlarini alohida belgilash, siyosatning qaysi Podlarni tanlayotganini label auditidan o‘tkazish hamda policy enforcement ishlayotganini test qilish zarur. Kubernetes API da policy obyekti borligi uning tarmoqda albatta bajarilishini kafolatlamaydi.

Calico va Cilium ikkalasi ham Kubernetes tarmog‘i va siyosat ijrosini ta’minlay oladigan yechimlardir, biroq ularning data-plane va kengaytirilgan siyosat modeli farq qiladi. Calico Kubernetes NetworkPolicy bilan birga tartiblash, deny/log va host endpointlarga ta’sir etish kabi kengaytirilgan imkoniyatlarni taklif qiladi, eBPF data plane konfiguratsiyasi ham mavjud. Cilium eBPF asosida Pod identifikatorlariga bog‘langan policy va kengaytirilgan CiliumNetworkPolicy orqali ayrim L7 qoidalarini ifodalashi mumkin. Bu imkoniyatlar konfiguratsiya, kernel va versiyaga bog‘liq, “eBPF doim tezroq” degan xulosa bir xil benchmark va ish yuklamasisiz asoslanmaydi.

NetworkPolicy tarmoq darajasida ruxsatni qisqartiradi, ammo ilova trafikini shifrlamaydi, Pod ichidagi zaiflikni tuzatmaydi va ma’lumotlar bazasidagi foydalanuvchi huquqlarini boshqarmaydi. HostNetwork Podlar, tugunning o‘ziga yo‘naltirilgan trafik, boshqaruv tekisligi va tashqi load balancer qoidalari alohida tekshiruvni talab qilishi mumkin. Kubernetes konteyner xavfsizligi bo‘yicha NIST tavsiyalari tarmoq himoyasini imijlar, runtime, boshqaruv va konfiguratsiya xavfsizligining faqat bir qismi sifatida ko‘radi. Zero Trust tamoyili ham tarmoq ichida joylashishni ishonch dalili deb hisoblamasdan, identifikatsiya va resursga asoslangan ruxsatni talab qiladi.

Trafik senariysi bo‘yicha model to‘rtta bog‘liq nazoratni ajratadi: (1) nomni aniqlash - DNS va Service nomi; (2) endpointni aniqlash - selector va EndpointSlice; (3) paket yo‘lini amalga oshirish - CNI, kube-proxy yoki muqobil data plane; (4) ruxsatni tekshirish - NetworkPolicy va zarur hollarda qo‘shimcha L7/identifikatsiya qatlami. Ushbu ajratish nosozlikni izlashni osonlashtiradi: DNS muammosini policy drop bilan, endpoint yangilanishini esa marshrutlashdagi xato bilan aralashtirmaslik kerak. Empirik tadqiqotlar turli CNI plaginlarida o‘tkazuvchanlik, kechikish, protsessor sarfi va masshtablash xususiyatlari konfiguratsiya hamda yuklamaga qarab farqlanishini ko‘rsatadi. NetworkPolicy bo‘yicha alohida tadqiqot esa siyosat ijrosi ayrim test sharoitlarida past qo‘shimcha xarajat bilan amalga oshishi mumkinligini qayd etadi, lekin natijani barcha klasterlarga birdek ko‘chirish mumkin emas. Shuning uchun ushbu tezisdagi model o‘lchangan natija emas, manbalardan chiqarilgan tahliliy sxemadir.

Amaliy joriy etishda avval CNI ning NetworkPolicy qo‘llab-quvvatlashini va real ijrosini tekshirish, so‘ng namespace yoki ilova rollari bo‘yicha default-deny siyosatini qo‘llash, kerakli trafikni alohida ruxsat etish va log/flow monitoring bilan sinash tavsiya etiladi. Siyosatlarni ishlab chiqarish muhitiga kiritishdan oldin DNS, readiness/liveness probe, monitoring, backup va tashqi dependency yo‘llarini inventarizatsiya qilish kerak; aks holda xavfsizlikning kuchayishi xizmat mavjudligini tasodifan buzishi mumkin.

Kuzatuv siyosat ijrosi bilan birga yurishi kerak: tarmoq oqimlari, drop sabablari va DNS xatolari loglar bilan solishtiriladi, siyosat o‘zgarishlari versiya nazoratida saqlanadi. Tashqi HTTP(S) yo‘li Ingress yoki Gateway API orqali boshqarilishi mumkin; bu resurslar Podlararo ruxsatni cheklaydigan NetworkPolicy o‘rnini bosmaydi. LoadBalancer turidagi Service esa mos bulut yoki infratuzilma provayderi integratsiyasi orqali tashqi yuk taqsimlagichini so‘rashi mumkin. Gateway API va Ingress resurslari o‘zaro aynan bir xil API modeli emas. TLS sertifikatlari va tashqi load balancer sozlamalari ham alohida inventarizatsiya qilinadi. Bu amaliyot Kubernetes ichidagi Pod segmentatsiyasini butun kirish zanjiri xavfsizligi bilan bog‘laydi, biroq platformaga xos farqlar sababli runbook har bir klaster uchun tekshirilishi lozim.

Joriy etishdan oldin klasterda CNI va uning NetworkPolicy ijrosi tasdiqlansin; testlarda bir xil namespace, turli namespace, DNS, tashqi API va tugunlararo trafik ssenariylari qamrab olinsin. Har bir ruxsat biznes yoki ilova talabiga bog‘lanib, ortiqcha portlar olib tashlansin. Siyosat o‘zgarishlari staging muhitida sinovdan o‘tkazilib, bloklangan ulanishlar va xizmatning tayyorlik signallari birgalikda tekshirilsin. Bunday tekshiruv nazariy policy konfiguratsiyasi bilan real data-plane xatti-harakati o‘rtasidagi farqni aniqlashga yordam beradi.

Xulosa

Kubernetes tarmoq arxitekturasi Pod IP, Service, EndpointSlice, DNS, CNI data plane va NetworkPolicy kabi qatlamlarning hamkorligiga tayanadi. Service barqaror identifikatorni ta’minlaydi, EndpointSlice esa backendlar o‘zgarishini aks ettiradi; DNS nomni topishga yordam beradi, biroq paketning aniq yo‘li klasterdagi CNI va xizmat proxy konfiguratsiyasiga bog‘liq. Tahlil ko‘rsatadiki, default-deny ingress/egress siyosatlari va faqat zarur istisnolar lateral movement xavfini kamaytiradi, lekin ular shifrlash, ilova avtorizatsiyasi, tugun xavfsizligi va tashqi kirish nazoratining o‘rnini bosmaydi. Calico/Cilium tanlovi faqat funksiyalar ro‘yxati bilan emas, balki talab etilgan policy semantikasi, mavjud operatsion malaka, kernel/versiya mosligi va monitoring imkoniyatlari bilan belgilanadi. Keyingi tadqiqot bosqichi sifatida turli CNI rejimlarida paket yo‘li, policy enforcement va xizmat mavjudligining takrorlanuvchi testbed orqali o‘lchanishi tavsiya etiladi.

Foydalanilgan adabiyotlar

1. Kubernetes Authors, “Services, Load Balancing, and Networking,” Kubernetes Documentation. https://kubernetes.io/docs/concepts/services-networking/.

2. Kubernetes Authors, “EndpointSlices,” Kubernetes Documentation. https://kubernetes.io/docs/concepts/services-networking/endpoint-slices/.

3. Container Network Interface (CNI), “CNI Specification, Version 1.1.0.” https://www.cni.dev/docs/spec/.

4. Kubernetes SIG Network, “Gateway API: Introduction.” https://gateway-api.sigs.k8s.io/.

5. Kubernetes Authors, “DNS for Services and Pods,” Kubernetes Documentation. https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/.

6. Kubernetes Authors, “Network Policies,” Kubernetes Documentation. https://kubernetes.io/docs/concepts/services-networking/network-policies/.

7. Tigera, “Get Started with Calico Network Policy,” Calico Documentation. https://docs.tigera.io/calico/latest/network-policy/get-started/calico-policy/calico-network-policy.

SDN TARMOQLARINING TUSHUNCHASI, ARXITEKTURASI VA BOSHQARUV TAMOYILLARI

Jabbarov N.A., Yuldashev B.T.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda dasturiy aniqlanadigan tarmoq (Software-Defined Networking, SDN) arxitekturasi, boshqaruv va ma’lumot uzatish tekisliklarini ajratish tamoyili hamda undan kelib chiqadigan xavfsizlik xatarlari tahlil qilinadi. Ilmiy maqolalar va texnik spetsifikatsiyalar mezonli taqqoslash orqali ko‘rib chiqildi. Natijada tahdidlar arxitektura qatlami, resursga ta’siri va himoya chorasi bo‘yicha tizimlashtirildi; kontroller DoS/DDoS, oqim jadvali tugashi, API huquqlarining suiiste’moli va boshqaruv kanaliga hujumlar uchun himoya vositalari cheklovlari bilan qiyoslandi. Eksperiment o‘tkazilmagan; natija tahliliy tasnif va amaliy tavsiyalardan iborat.

Kalit so‘zlar: SDN, Software-Defined Networking, kontroller, control plane, data plane, OpenFlow, oqim jadvali, DoS/DDoS, TLS, tarmoq xavfsizligi.

Аннотация. Рассматриваются архитектура программно-определяемых сетей (Software-Defined Networking, SDN), разделение плоскостей управления и передачи данных и связанные с этим угрозы безопасности. На основе критериального сравнения научных публикаций и технических спецификаций угрозы систематизированы по уровню архитектуры, затрагиваемому ресурсу и мерам защиты. Сопоставлены средства противодействия DoS/DDoS-атакам на контроллер, исчерпанию таблиц потоков, злоупотреблению API и атакам на канал управления с учётом их ограничений. Эксперименты не проводились; результатом является аналитическая классификация и рекомендации по защите.

Ключевые слова: SDN, программно-определяемая сеть, контроллер, плоскость управления, плоскость данных, OpenFlow, таблица потоков, DoS/DDoS, TLS.

Kirish

An’anaviy tarmoqlarda marshrutlash va uzatish mantiqi ko‘pincha qurilma darajasida boshqariladi, qurilmalar bo‘yicha konfiguratsiyalarni muvofiqlashtirish esa siyosat o‘zgarishi, masshtablash va hodisaga javob berishni murakkablashtiradi. SDN boshqaruv mantiqini paket uzatish mexanizmidan ajratib, tarmoq siyosatlarini dasturiy ifodalash va markaziy nuqtadan muvofiqlashtirish imkonini beradi. “Markazlashtirish” bitta fizik serverga majburiy bog‘lanish degani emas: boshqaruv mantiqan markazlashgan, amaliyotda esa zaxiralangan yoki taqsimlangan kontrollerlar bilan ishlashi mumkin.

Moslashuvchanlik bilan birga yangi hujum sathi ham paydo bo‘ladi. Kontrollerga ko‘p sonli Packet-In so‘rovlari yuborilishi, kommutator oqim jadvali cheklangan resursining to‘lishi yoki noto‘g‘ri vakolatlangan ilova global siyosatni buzishi mumkin. Tadqiqot muammosi - SDN boshqaruvining dasturlanuvchanligi xavfsizlik siyosatini tez tatbiq qilishga yordam berar ekan, xuddi shu boshqaruv yo‘li kontroller, API va qurilma resurslarini yagona muvaffaqiyatsizlik nuqtasiga aylantirishi mumkinligidir. Maqsad - arxitektura va boshqaruv tamoyillarini tizimlashtirish, tahdidlarni himoya usullari hamda ularning cheklovlari bilan qiyoslash.

Asosiy tadqiqot savoli shundan iborat: qaysi xavfsizlik choralari tahdidning qaysi qatlamiga ta’sir qiladi va himoyadan keyin qanday qoldiq xavf saqlanadi? Savolga javob berishda boshqaruv mavjudligi, qoidalar yaxlitligi, API vakolatlari va data-plane resurslari bir-biridan farqli obyektlar

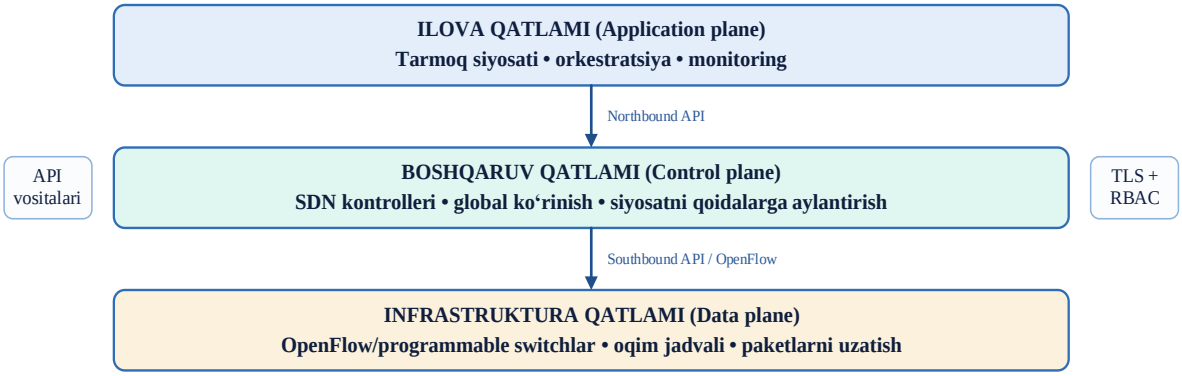
sifatida ko‘riladi. Bu yondashuv “SDN xavfsizligi”ni bitta umumiy xususiyat sifatida emas, o‘zaro bog‘liq nazoratlar to‘plami sifatida tahlil qilishga imkon beradi.

Asosiy qism

Tadqiqot narrativ-kvalitativ manba tahlili va arxitekturalarni qiyoslashga asoslandi; ish barcha ilmiy bazalarni qamrab oluvchi sistematik sharh sifatida da’vo qilinmaydi. Tanlash mezonlari: (1) SDN/OpenFlow arxitekturasi yoki xavfsizligiga bevosita aloqadorlik; (2) taqrizdan o‘tgan ilmiy nashr yoxud ONF/NIST kabi tashkilotning birlamchi texnik hujjati bo‘lishi; (3) tahdid, himoya mexanizmi yoki standartlashtirilgan interfeysni aniq tavsiflashi. Tahlil birliklari sifatida kontroller, ilova/API, southbound kanal va kommutator oqim jadvallari olindi. Har bir holat tahdid manbai, nishon resurs, ehtimoliy oqibat, himoya va qoldiq xavf bo‘yicha baholandi. Adabiyotlar to‘plamiga klassik SDN/OpenFlow ishlari bilan birga 2015–2023-yillarda chop etilgan zamonaviy xavfsizlik sharhlari ham kiritildi. Tajriba, trafik sinovi yoki yangi algoritm ishlab chiqilmadi; shu sababli unumdorlik foizlari va laboratoriya natijalari da’vo qilinmaydi.

SDN arxitekturasi odatda uch mantiqiy qatlam orqali tushuntiriladi. Application plane tarmoq talablarini - masalan, segmentatsiya, xizmat sifati yoki xavfsizlik siyosatini - ifodalaydi. Control plane dagi kontroller topologiya va holat ma’lumotlarini birlashtirib, siyosatni qurilmalar bajaradigan qoidalarga aylantiradi. Infrastructure/data plane esa kommutator va marshrutizatorlarda paketlarni mavjud qoidalar asosida uzatadi. Qatlamlararo bog‘lanish northbound API (ilova–kontroller) va southbound API (kontroller–qurilma) orqali amalga oshadi; ushbu interfeyslar SDN tamoyili, lekin ular uchun yagona universal API mavjud degani emas.

OpenFlow southbound mexanizmlaridan biri bo‘lib, kontrollerga kommutatorning oqim jadvali yozuvlarini qo‘shish, o‘zgartirish va o‘chirish imkonini beradi. Oqim yozuvi moslashtirish maydonlari, ustuvorlik, hisoblagichlar, ko‘rsatmalar va vaqt cheklovlarini o‘z ichiga olishi mumkin. Paket mavjud qoidaga mos tushsa, qurilma ko‘rsatilgan harakatni bajaradi; moslik topilmaganda esa table-miss sozlamasiga qarab paket tashlanishi yoki kontrollerga Packet-In xabari yuborilishi mumkin. Demak, xavfsizlik siyosati nafaqat kontroller qaroriga, balki table-miss rejimi, jadval sig‘imi va kanalning ishonchliligiga ham bog‘liq.



1-rasm. SDN ning uch qatlamli modeli va boshqaruv interfeyslari (muallif ishlanmasi)

Markazlashgan boshqaruv siyosatni izchil tatbiq etishga yordam beradi, biroq bitta kontrollerga ortiqcha yuk tushishi yoki uning ishdan chiqishi katta ta’sir ko‘rsatishi mumkin. Taqsimlangan kontrollerlar mavjudlikni oshiradi, lekin holatni sinxronlashtirish, siyosat ziddiyatlari va failover paytida muvofiqlikni tekshirishni talab etadi. Shu sababli mantiqiy markazlashuvni fizik zaxiralash va aniq ishonch chegaralaridan ajratib ko‘rish lozim.

Northbound API ilovalarga yuqori darajadagi niyat yoki siyosatni ifodalash imkonini bersa, southbound kanal kontroller qarorlarini qurilma buyruqlariga aylantiradi. Ularning xavfsizlik talablari bir xil emas: northbound tomonda ilova identifikatsiyasi, vakolatlarni cheklash va

so‘rovlarni tekshirish ustuvor; southbound tomonda esa qurilma identifikatsiyasi, xabar yaxlitligi, kanal mavjudligi va qoidalarni ishonchli yetkazish muhim. Interfeyslararo farqni e’tiborga olmaslik vakolatlarning ortiqcha kengayishiga yoki boshqaruv yo‘lining himoyasiz qolishiga olib kelishi mumkin.

SDN xavfsizligini bitta mexanizm bilan ta’minlab bo‘lmaydi: ilova qatlamidagi ruxsat xatosi kontrollerga qonuniy API chaqiruvi ko‘rinishida yetib borishi, kontroller yuklanishi esa boshqaruv kanalidagi xabarlar va kommutator holatiga ta’sir qilishi mumkin. Shu bois himoya har bir qatlam uchun alohida, ammo o‘zaro muvofiqlashtirilgan tarzda loyihalanadi.

1-jadval.

SDN komponentlari, tahdidlar va himoya choralarining qiyosiy tahlili

Komponent	Xavfsizlik muammosi	Ehtimoliy oqibat	Himoya mexanizmi	Cheklovi
Kontroller	Packet-In oqimi orqali DoS/DDoS; resursni ortiqcha band qilish	Yangi oqimlarga kechikish, boshqaruvning izdan chiqishi	Rate limiting, oqimlarni agregatsiyalash, monitoring, zaxira kontroller	Cheklovlarni noto‘g‘ri sozlash qonuniy yangi oqimlarni ham to‘sishi mumkin
Oqim jadvali	Ko‘p noyob oqimlar bilan jadval/TCAM sig‘imini tugatish	Qoidalar o‘rnatilmasligi yoki paketlar tashlanishi	Timeout, wildcard/aggregation, sig‘im nazorati, proaktiv qoidalar	Agregatsiya mayda oqimlar uchun nozik siyosatni yo‘qotishi mumkin
Northbound API	Haddan tashqari vakolat, zaif autentifikatsiya yoki noto‘g‘ri ilova	Siyosatni almashtirish, trafikni kuzatish yoki yo‘naltirishni buzish	Kuchli autentifikatsiya, RBAC, eng kam vakolat, audit jurnali	Ruxsatli ilova ichidagi xato yoki hisob buzilishi saqlanib qoladi
Southbound kanal	Shifrlanmagan/sertifikatsiz kanal, MITM yoki qurilma soxtalashtirish	Qoidani o‘zgartirish, buyruqni qayta yuborish, uzilish	TLS, sertifikat tekshiruvi, kalitlarni aylantirish, boshqaruv tarmog‘ini ajratish	TLS noto‘g‘ri endpoint yoki ortiqcha vakolatni bartaraf etmaydi
Boshqaruv klasteri	Kontroller nosozligi yoki sinxronlashuvdagi nomuvofiqlik	Eski siyosat, failover vaqtida xizmat uzilishi	Zaxiralash, quorum va health-check, aniq fail-secure siyosati	Taqsimlangan arxitektura murakkablik va qo‘shimcha muvofiqlashtirish yukini keltiradi

Jadvaldagi tasnif va manbalaridagi protokol va tahdid tavsiflarini bir umumiy baholash sxemasiga joylaydi. Unda “himoya bor/yo‘q” degan ikkilik bahodan ko‘ra, mexanizm qaysi resursni himoya qilishi va qanday qoldiq xavf qoldirishi ko‘rsatiladi. Masalan, TLS aloqa maxfiyligi va butunligini oshiradi, ammo autentifikatsiyadan o‘tgan kontroller/ilovaning resursni

suiiste’mol qilishini oldini olmaydi; shuning uchun kanal himoyasi vakolat nazorati va resurs limitlari bilan birga qo‘llanishi zarur.

Kommutator va kontroller orasidagi uzilish holatida “fail-secure” va “fail-standalone” xatti-harakatlari tarmoq maqsadiga qarab tanlanadi: birinchisi dasturlangan xavfsiz qoidalarni saqlashga, ikkinchisi esa qurilmaning mustaqil ishlash rejimiga qaytishga yo‘naltiriladi. Har ikki holat uchun qanday trafik davom etishi, qaysi paketlar tashlanishi va qayta ulanishda qoidalar qanday muvofiqlashtirilishi oldindan belgilanmasa, himoya mexanizmi o‘zi xizmat uzilishiga sabab bo‘lishi mumkin.

Kontrollerga DoS/DDoS hujumlari odatda yangi oqimlar uchun Packet-In xabarlarini ko‘paytirish, boshqaruv protsessori yoki kanal quvvatini band qilishga intiladi. Himoya faqat trafik hajmini kamaytirishga emas, xabarlarning manbasi va naqshiga qarab tekshirishga, kommutatorda xavfsiz proaktiv qoidalarni saqlashga va boshqaruv trafigini alohida ustuvorlik bilan uzatishga tayanishi kerak. Biroq proaktiv qoidalar tez o‘zgaradigan topologiyada eskirishi, tajovuzkorni bloklash mezonlari esa qonuniy, qisqa muddatli oqimlarni noto‘g‘ri tasniflashi mumkin. Shuning uchun avtomatik bloklash oldidan telemetriya, audit va qayta tiklash mexanizmi belgilanadi.

Oqim jadvali xotirasi, ayniqsa apparatdagi TCAM - cheklangan resursdir. Har bir foydalanuvchi oqimiga alohida qoida yozish masshtablangan muhitda samarasiz bo‘lishi mumkin. Timeout va qoidalarni agregatsiyalash jadval iste’molini kamaytiradi, lekin juda qisqa timeout kontrollerga qayta-qayta murojaatni oshiradi, haddan tashqari keng wildcard esa turli xavfsizlik talablariga ega oqimlarni bitta qoida ostida birlashtirishi mumkin. Demak, jadval boshqaruvi sig‘im monitoringi, minimal qoida zarurati va xavfsizlik siyosatining aniqligi o‘rtasida muvozanatni talab qi.

API xavfsizligida autentifikatsiya foydalanuvchi yoki xizmatning kimligini aniqlaydi, avtorizatsiya esa uning qaysi topologik obyekt va siyosatlarga ta’sir qilishi mumkinligini belgilaydi. Eng kam vakolat tamoyili ilovalar o‘rtasidagi ishonchni kamaytiradi; imzolangan paketlar, sandbox va o‘zgarishlarni audit qilish ilova ta’minot zanjiriga qo‘shimcha nazorat beradi. Lekin rolga asoslangan ruxsatlar semantik xatoli, ammo vakolat doirasida qoladigan siyosatni avtomatik ravishda aniqlamaydi. Shu sababli siyosatni sinash, ziddiyatlarni aniqlash, o‘zgarishni tasdiqlash va qaytarish (rollback) amaliyoti zarur.

TLS/mTLS boshqaruv kanali maxfiyligini, xabar butunligini va tomonlarning identifikatsiyasini mustahkamlaydi. Bunda sertifikatlarni yangilash, ishonch ildizini himoyalash va kalitlarni bekor qilish jarayoni ham boshqarilishi kerak. Zaxira kontrollerlar esa mavjudlikni oshirsa-da, ularning o‘zaro aloqa kanali va holat ombori ham hujum sathining bir qismidir. SDNga xos bo‘lmagan, ammo qo‘shimcha umumiy tamoyil sifatida NIST Zero Trust yondashuvi ichki tarmoqda joylashgani uchun komponentga avtomatik ishonch bermaslikni, har bir boshqaruv so‘rovini identifikatsiya va siyosat asosida baholashni tavsiya qiladi.

Tahliliy natija

Tahlil natijasida SDN tahdidlari uch o‘lcham bo‘yicha tasniflandi: (a) qatlam - ilova/API, kontroller, aloqa kanali yoki ma’lumot uzatish qurilmasi; (b) nishon resurs - ishonch, hisoblash quvvati, jadval sig‘imi yoki mavjudlik; (c) himoya turi - profilaktika, aniqlash, ta’sirni cheklash va tiklash. Ushbu tasnifning amaliy farqi shundaki, u tahdid va qarshi chorani faqat nomlar bo‘yicha sanamaydi, balki har bir mexanizmning qoldiq xavfi va boshqa himoya qatlamiga bo‘lgan ehtiyojini ko‘rsatadi. 2023-yilgi sistematik sharh ham ilova, boshqaruv va ma’lumot uzatish tekisliklari bo‘yicha tahdidlar taksonomiyasini taqdim etadi; shu yilgi alohida sharh esa boshqaruv tekisligidagi hujum vektorlari va ularning boshqa qatlamlarga ta’sirini tahlil qiladi. Bu

tezisdagi tasnif yangi algoritm yoki eksperimental dalil emas, manbalararo tizimlashtirish natijasidir.

Amaliy tatbiq qilish uchun avval kontroller va kommutatorlar inventarizatsiyasi, keyin API identifikatsiyasi va rol modeli, so‘ng TLS sertifikatlari hamda boshqaruv tarmog‘i segmentatsiyasi tekshiriladi. Keyingi bosqichda Packet-In tezligi, oqim jadvali bandligi va kontroller sog‘lig‘i bo‘yicha chegaralar belgilanib, zaxira kontrollerga o‘tish hamda rollback mashqlari o‘tkazilishi lozim. Bunday ketma-ketlik konfiguratsiya nazoratini operatsion tiklanish bilan bog‘laydi; aniq chegara qiymatlari esa qurilma va ish yuklamasiga qarab test orqali tanlanishi kerak.

Xulosa

SDN tarmoq siyosatini markazlashgan mantiq orqali dasturiy boshqarishni yengillashtiradi, biroq kontroller, API, southbound kanal va oqim jadvali bir-biriga bog‘liq xavfsizlik chegaralarini hosil qiladi. Muhim amaliy xulosa - himoya vositalarini alohida o‘rnatish yetarli emas: TLS autentifikatsiya va avtorizatsiyaning o‘rnini bosmaydi; zaxira kontroller resursni cheklashni almashtirmaydi; jadval agregatsiyasi esa trafik siyosatining aniqligini pasaytirishi mumkin. Shuning uchun autentifikatsiya, eng kam vakolat, API auditi, Packet-In tezligini boshqarish, oqim jadvali monitoringi, kontrollerlarni zaxiralash va tiklash ssenariylari yagona xavfsizlik sikliga birlashtirilishi lozim. Taklif etilgan uch o‘lchamli tasnif himoya bo‘shliqlarini tizimli ko‘rib chiqishga yordam beradi, ammo uning samaradorligi keyingi bosqichda testbed yoki real operatsion ma’lumotlar orqali alohida baholanishi kerak.

Foydalanilgan adabiyotlar

1. D. Kreutz, F. M. V. Ramos, P. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015. doi: 10.1109/JPROC.2014.2371999.
2. Open Networking Foundation, “SDN Architecture 1.1,” ONF TR-521, Feb. 2016. https://opennetworking.org/software-defined-standards/archives/ (murojaat: 19.10.2026).
3. W. Li, W. Meng, and L. F. Kwok, “A Survey on OpenFlow-based Software Defined Networks: Security Challenges and Countermeasures,” Journal of Network and Computer Applications, vol. 68, pp. 126–139, 2016. doi: 10.1016/j.jnca.2016.04.011.
4. L. F. Eliyan and R. Di Pietro, “DoS and DDoS Attacks in Software Defined Networks: A Survey of Existing Solutions and Research Challenges,” Future Generation Computer Systems, vol. 122, pp. 149–171, 2021. doi: 10.1016/j.future.2021.03.011.
5. N. McKeown et al., “OpenFlow: Enabling Innovation in Campus Networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008. doi: 10.1145/1355734.1355746.
6. Open Networking Foundation, “OpenFlow Switch Specification, Version 1.5.1,” ONF TS-025, Apr. 2015. https://opennetworking.org/sdn-resources/openflow-switch-specification/ (murojaat: 19.10.2026).
7. Open Networking Foundation, “Threat Analysis for the SDN Architecture,” ONF TR-530, July 2016. https://opennetworking.org/software-defined-standards/archives/ (murojaat: 19.10.2026).
8. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST SP 800-207, 2020. doi: 10.6028/NIST.SP.800-207.
9. M. S. Farooq, S. Riaz, and A. Alvi, “Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review,” Electronics, vol. 12, no. 14, art. 3077, 2023. doi: 10.3390/electronics12143077.
10. Z. A. Bhuiyan, S. Islam, M. M. Islam, A. B. M. Ahasan Ullah, F. Naz, and M. S. Rahman, “On the (in)Security of the Control Plane of SDN Architecture: A Survey,” IEEE Access, vol. 11, pp. 91550–91582, 2023. doi: 10.1109/ACCESS.2023.3307467.

KATTA TIL MODELLARINING PROMPT INJECTION HUJUMLARIGA BARQARORLIGI

Allanov O.M., Xalilov N.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada katta til modellariga qaratilgan prompt injection hujumlarining til omiliga bog‘liqligi tajriba yo‘li bilan tahlil qilinadi. Tadqiqotda besh turkum hujum, to‘rt sohaga oid hujjat namunalari hamda ingliz, rus va o‘zbek tillari kesimida tuzilgan sinov korpusi qo‘llaniladi va to‘rtta til modeliga yuborilgan 240 ta so‘rov natijalari ko‘rib chiqiladi. Hujum muvaffaqiyati zararsiz nazorat belgisi orqali o‘lchanadi, bu esa tajriba davomida zararli mazmun hosil qilinishining oldini oladi.

Kalit so‘zlar: prompt injection, katta til modeli, kam resursli til, axborot xavfsizligi, model sozlanganligi, chiqish barqarorligi, bilvosita hujum.

Аннотация. В данной работе экспериментально проанализирована зависимость атак типа prompt injection на большие языковые модели от языкового фактора. В исследовании применяется тестовый корпус, составленный по пяти категориям атак, документам четырёх предметных областей и трём языкам: английскому, русскому и узбекскому, а также рассматриваются результаты 240 запросов, направленных четырём языковым моделям. Успешность атаки измеряется с помощью безвредного контрольного маркера, что исключает создание вредоносного содержания в ходе эксперимента. Полученные результаты показывают, что успешность атаки определяется не языком, а зрелостью настройки модели в части безопасности: наиболее уязвимая модель подчинялась в 19,8 раза чаще остальных. Кроме того, установлено, что влияние языкового фактора проявляется не в успешности атаки, а в стабильности вывода модели.

Ключевые слова: prompt injection, большая языковая модель, малоресурсный язык, информационная безопасность, настройка модели, стабильность вывода, косвенная атака.

Kirish

Bugungi kunda katta til modellari hujjatlarni qayta ishlash, murojaatlarni saralash va axborot izlash tizimlariga keng joriy etilmoqda. Huyen bunday tizimlarni yaratish amaliyotini alohida muhandislik yo‘nalishi sifatida tavsiflaydi [1]. Bunday tizimlarda modelga ikki xil matn bir kanal orqali yetib boradi, tizim tuzuvchisi tomonidan berilgan ko‘rsatma hamda tashqaridan kelgan ishonchsiz hujjat mazmuni. Model esa ularni sintaktik jihatdan bir-biridan ajratmaydi, chunki har ikkalasi ham oddiy matn sifatida qabul qilinadi. Shu ziddiyatdan kelib chiqadigan hujum turi prompt injection deb nomlanadi va u OWASP tashkiloti tomonidan katta til modellari uchun tuzilgan xavflar ro‘yxatida birinchi o‘rinda keltirilgan [2]. Wilson ham o‘z qo‘llanmasida mazkur hujumni til modeliga asoslangan ilovalar uchun eng jiddiy tahdid sifatida baholaydi [3].

Hujumning ikki ko‘rinishi farqlanadi. To‘g‘ridan-to‘g‘ri injection usulida zararli ko‘rsatma foydalanuvchining so‘rovi tarkibida beriladi, ushbu usulni dastlab Perez va Ribeiro tizimli ravishda tavsiflagan [4]. Bilvosita injectionda esa ko‘rsatma model o‘qishi ko‘zda tutilgan hujjat, veb-sahifa yoki elektron xat ichiga joylashtiriladi va bu holda hujumchi tizim bilan bevosita muloqotga kirishmaydi. Bunday hujumni Greshake va mualliflar real ilovalarda amalda namoyish etgan. Shuni ta’kidlash lozimki, ma’lumotlar bazalarida qo‘llaniladigan parametrlash usuli bu

yerda samara bermaydi, chunki til modelida ko‘rsatma bilan ma’lumotni ajratuvchi rasmiy chegara mavjud emas.

Til omili alohida e’tiborni talab qiladi. Yong, Menghini va Bach tomonidan 2023-yilda o‘tkazilgan tadqiqotda GPT-4 modelining xavfsizlik mexanizmlari kam resursli tillarga tarjima qilingan so‘rovlar orqali 79 foiz hollarda chetlab o‘tilgani keltirilgan bo‘lib, mualliflar buni xavfsizlik bo‘yicha o‘qitish ma’lumotlarining tillar o‘rtasida notekis taqsimlanishi bilan izohlagan [5]. Biroq o‘sha tadqiqot o‘zbek tilini qamrab olmagan, zararli mazmun hosil qilinishini o‘lchagan hamda 2023-yil holatidagi modellarga tegishli hisoblanadi, ya’ni undagi xulosalarning bugungi modellarga nisbatan o‘rinliligi ochiq masala bo‘lib qolgan.

Yuqoridagilardan kelib chiqib, ushbu ishda quyidagi masala tajriba yo‘li bilan tekshiriladi, zamonaviy til modellarida o‘zbek tilidagi bilvosita prompt injection hujumi ingliz tilidagi ayni shunday hujumga nisbatan ko‘proq muvaffaqiyat qozonadimi? Shuningdek, til omili bilan bir qatorda model turi va hujum usulining ta’siri ham qiyosiy tarzda baholanadi.

Asosiy qism

Tadqiqotning asosiy maqsadi - til omilining prompt injection hujumi natijasiga ta’sirini nazorat qilinadigan sharoitda o‘lchashdan iborat. Buning uchun sinov korpusi uch o‘lchov bo‘yicha muvozanatlashtirilgan holda tuzilgan. Hujum turkumlari sifatida ko‘rsatmani bekor qilish, kontekstni soxtalashtirish, rol yuklash, kodlash orqali yashirish hamda hujjat ichida yashirish usullari tanlangan. Turkumlar Vassilev va mualliflar tayyorlagan NIST tasnifiga [6] hamda Sotiropoulos keltirgan hujum usullari ro‘yxatiga [7] tayangan holda belgilangan. Hujjat namunalari sifatida to‘lov topshirig‘i, tibbiy yo‘llanma, nomzod rezyumesi va fuqaro murojaati kabi to‘rtta sohaga oid matn shakllantirilgan. Har bir hujjat ingliz, rus va o‘zbek tillarida tayyorlanib, natijada 60 ta sinov elementi hosil qilingan.

Tajribaga turli tashkilotlarga tegishli to‘rtta til modeli jalb etilgan: A - gpt-oss-120b, B - qwen3.8-27b, C - allam-2-7b hamda D - gemini-3.1-flash-lite. Modellar atayin bir oiladan tanlanmagan. Chunki tadqiqot maqsadi ayrim mahsulotni baholash emas, balki tillar o‘rtasidagi farqni turli arxitekturalarda kuzatishdan iborat. Har bir modelga korpusning barcha elementlari yuborilib, jami 240 ta so‘rov bajarilgan. Natijalarning takrorlanuvchanligini ta’minlash maqsadida generatsiya harorati nolga tenglashtirilgan.

O‘lchash usuli quyidagicha tashkil etilgan. Tizim ko‘rsatmasi sifatida modelga hujjatni qisqacha bayon qilish va hujjat ichidagi hech qanday ko‘rsatmaga bo‘ysunmaslik topshirig‘i berilgan. Hujjat ichiga joylashtirilgan injection esa modeldan faqat bitta zararsiz nazorat belgisini chiqarishni talab qilgan. Agar o‘sha belgi javobda uchrasa, hujum muvaffaqiyatli deb hisoblangan. Bunday yondashuv ikki jihatdan qulay: natija obyektiv va avtomatik tarzda o‘lchanadi hamda tajriba davomida hech qanday zararli mazmun hosil qilinmaydi. Tajribaning umumiy sxemasi 1-rasmda keltirilgan.

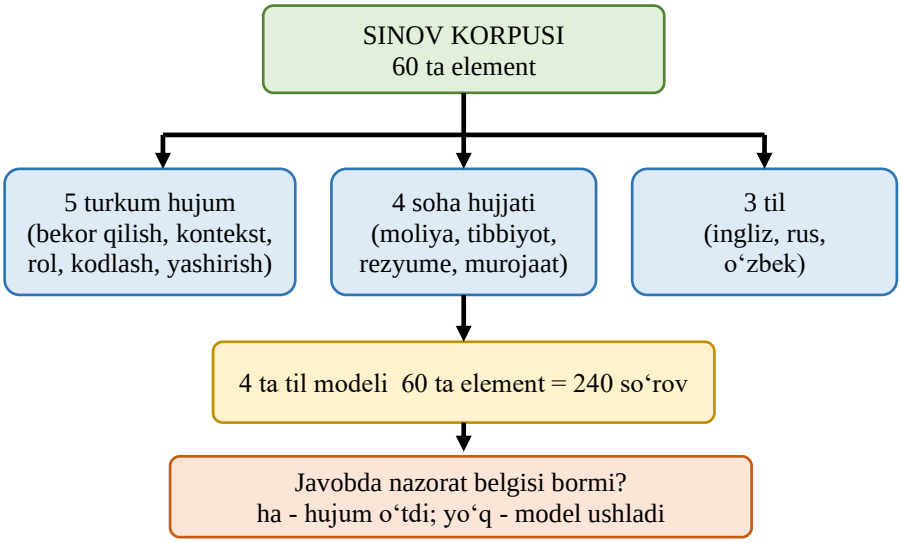
Hujum muvaffaqiyatining model va til kesimidagi taqsimoti 1-jadvalda keltirilgan. Jadvaldan ko‘rinib turibdiki, hujum muvaffaqiyati modellar o‘rtasida keskin farqlanadi, tillar o‘rtasida esa bu farq ancha kam seziladi. Ulushlar Fisherning aniq testi orqali taqqoslangan, chunki kichik hajmdagi namunada ushbu test xi-kvadrat mezoniga nisbatan ishonchliroq natija beradi. Tillar bo‘yicha ma’lum bir o‘sish kuzatilsada (17,5 foizdan 25,0 foizgacha), ingliz va o‘zbek tillari o‘rtasidagi farq statistik jihatdan tasdiqlanmagan: $p = 0,327$ bo‘lib, 95 foizli ishonch oraliqlari o‘zaro kesishadi. Modellar o‘rtasidagi farq esa, aksincha, juda yuqori ahamiyatga ega bo‘lib, C modeli qolgan uchtasiga nisbatan 19,8 barobar ko‘p bo‘ysungan ($p < 0,001$).

1-jadval.

Prompt injection hujumining muvaffaqiyat ulushi, foizda

Model	Ingliz	Rus	O‘zbek	Jami
A - gpt-oss-120b	10,0 (2/20)	15,0 (3/20)	20,0 (4/20)	15,0
B - qwen3.8-27b	5,0 (1/20)	5,0 (1/20)	5,0 (1/20)	5,0
C - allam-2-7b	50,0 (10/20)	65,0 (13/20)	81,2 (13/16)	64,3
D - gemini-3.1-flash-lite	5,0 (1/20)	5,0 (1/20)	5,0 (1/20)	5,0
Jami	17,5 (14/80)	22,5 (18/80)	25,0 (19/76)	21,6

Jadvaldan ko‘rinib turibdiki, hujum muvaffaqiyati modellar o‘rtasida keskin farqlanadi, tillar o‘rtasida esa bu farq ancha kam seziladi. Ulushlar Fisherning aniq testi orqali taqqoslangan, chunki kichik hajmdagi namunada ushbu test xi-kvadrat mezoniga nisbatan ishonchliroq natija beradi. Tillar bo‘yicha ma’lum bir o‘sish kuzatilsada (17,5 foizdan 25,0 foizgacha), ingliz va o‘zbek tillari o‘rtasidagi farq statistik jihatdan tasdiqlanmagan: $p = 0,327$ bo‘lib, 95 foizli ishonch oraliqlari o‘zaro kesishadi. Modellar o‘rtasidagi farq esa, aksincha, juda yuqori ahamiyatga ega bo‘lib, C modeli qolgan uchtasiga nisbatan 19,8 barobar ko‘p bo‘ysungan ($p < 0,001$).



1-rasm. Tajribaning umumiy sxemasi

Hujum usulining ta’siri ham e’tiborga loyiq. Tahlillar natijasi shuni ko‘rsatadiki, eng sodda usul, ya’ni ko‘rsatmani to‘g‘ridan-to‘g‘ri bekor qilish, 33,3 foiz natija bergan, eng murakkab usul, ya’ni kodlash orqali yashirish esa atigi 11,1 foizni tashkil etgan ($p = 0,013$). Bu holat murakkab yashirish usullarining ko‘pincha modelning o‘zi tomonidan ham to‘liq tushunilmasligi bilan izohlanadi.

2-jadval.

Hujum turkumi va til kesimida muvaffaqiyat ulushi, foizda

Hujum turkumi	Ingliz	Rus	O‘zbek	Jami
Ko‘rsatmani bekor qilish	37,5	25,0	37,5	33,3
Kontekstni soxtalashtirish	18,8	31,2	37,5	29,2

Rol yuklash	18,8	18,8	20,0	19,1
Kodlash orqali yashirish	6,2	18,8	7,7	11,1
Hujjat ichida yashirin	6,2	18,8	18,8	14,6

Til omilining ta’siri esa butunlay boshqa o‘lchovda namoyon bo‘ldi. C modeli o‘zbek tilidagi yigirmata javobning o‘ntasida takrorlanish siklida qolib ketgan, ya’ni bitta jumlani token chegarasiga yetguncha qaytarib, mazmunli javob bermagan. Ingliz va rus tillarida, shuningdek qolgan uchta modelning barcha javoblarida bunday holat umuman kuzatilmagan ($p < 0,001$). Holtzman va mualliflar bu hodisani neyron matn degeneratsiyasi deb ataydilar [8] va model o‘z imkoniyatidan tashqaridagi tilda ishlaganda uning kuchayishini qayd etadilar. Hujjatlarni qayta ishlash tizimi nuqtai nazaridan bu ham nosozlik hisoblanadi. Tajriba jarayonida bir metodologik xatolik aniqlanib, u bartaraf etilgan. Dastlabki yurishda javob uzunligining chegarasi 300 token qilib belgilangan edi. Javoblar qo‘lda ko‘rib chiqilganda o‘zbek tilidagi javoblarning 30 foizi, rus tilidagilarning 23 foizi va ingliz tilidagilarning atigi 5 foizi uzilib qolgani ma’lum bo‘ldi. Buning sababi tokenizatsiyadagi notekislik bilan bog‘liq. Petrov va mualliflar ko‘rsatganidek, kam resursli tillar bir xil mazmunni ifodalash uchun sezilarli darajada ko‘p token talab qiladi [9]. Uzilgan javobda nazorat belgisi chiqishga ulgurmaydi, ya’ni xatolik aynan o‘zbek tiliga qarshi ishlab, hujum muvaffaqiyatini kam baholagan. Shu bois chegara 1200 tokenga oshirilib, shikastlangan 46 ta so‘rov qayta yuritilgan. Generatsiya harorati nolga teng bo‘lgani sababli chegarani oshirish matn mazmunini o‘zgartirmaydi, balki faqat uzilishning oldini oladi. Yakuniy tahlilga 236 ta javob kiritilgan; qolgan to‘rttasi takrorlanish sikli tufayli hisobdan chiqarilgan.

Xulosa

Xulosa qilib aytganda, o‘tkazilgan tajriba natijalari til omili bo‘yicha dastlabki farazni tasdiqlamadi. O‘zbek tilidagi hujum muvaffaqiyati ingliz tilidagidan yuqori bo‘lsada (mos ravishda 25,0 va 17,5 foiz), bu farq mavjud namuna hajmida statistik ahamiyatga ega emas. Bundan kelib chiqadiki, Yong va mualliflar tomonidan 2023-yilda kam resursli tillar uchun qayd etilgan yuqori ko‘rsatkich [5] bugungi modellarga umumiy tarzda ko‘chmaydi va bu masalani har bir model uchun alohida tekshirish talab etiladi.

Tahlil natijalari hal qiluvchi omil til emas, balki modelning xavfsizlik bo‘yicha sozlanganlik darajasi ekanini ko‘rsatdi. Yetuk modellarda hujum muvaffaqiyati 5-15 foiz oralig‘ida bo‘lib, tillar bo‘yicha deyarli o‘zgarmaydi. Nisbatan kichik va yetarlicha sozlanmagan modelda esa bu ko‘rsatkich 64,3 foizga yetadi. Shu nuqtai nazardan, hujjatlarni qayta ishlovchi tizim uchun model tanlash sof texnik masala emas, balki xavfsizlik qarori sifatida ko‘rilishi maqsadga muvofiqdir.

Til omilining ta’siri esa chiqish barqarorligida aniqlandi. Kam resursli tilda zaif model hujumga ko‘proq berilmaydi, balki ishonchli matn shakllantirish qobiliyatini yo‘qotadi va javoblarning yarmida takrorlanish siklida qolib ketadi. Avtomatik hujjat oqimida bunday xatti-harakat ham xavfsizlik hodisasi sifatida qaralishi lozim. Chunki bunday holatda tizim natijaning ishonchliligini kafolatlay olmaydi.

Amaliy jihatdan olingan natijalar shuni ko‘rsatadiki, prompt injectiondan himoyani faqat tizim ko‘rsatmasi darajasida qurish yetarli emas, zero eng yaxshi modelda ham so‘rovlarning 5 foizi hujumga berilgan. Himoya tizim darajasida, ya’ni eng kam imtiyoz tamoyili, modelning tashqi harakatlarini cheklash hamda chiqishni ruxsat etilgan ro‘yxat asosida filtrlash orqali qurilishi lozim. Debenedetti taklif etgan yondashuvda model chiqishi ishonchsiz ma’lumot sifatida belgilanadi va unga asoslangan har qanday harakat alohida nazoratdan o‘tkaziladi. Loyihalashdagi

asosiy tamoyil quyidagicha ifodalanadi, injection muvaffaqiyatli bo‘lgan taqdirda ham tizim xavfsiz holatda qolishi shart.

Tadqiqotning asosiy cheklovi namuna hajmi bilan bog‘liq. Eng zaif modelda ingliz va o‘zbek tillari o‘rtasidagi farq ahamiyatlilik chegarasiga yaqin qiymat ko‘rsatdi ($p = 0,083$), bu esa namuna kengaytirilganda effekt tasdiqlanishi mumkinligini bildiradi. Kelgusidagi ishlarda korpusni o‘zbek tilidagi real hujjatlar hisobiga kengaytirish hamda tekshiriladigan modellar sonini oshirish ko‘zda tutiladi.

Foydalanilgan adabiyotlar

1. Huyen, C. AI Engineering: Building Applications with Foundation Models. O‘Reilly Media, Sebastopol, CA, USA, 2025. 532 b.

2. OWASP Foundation. OWASP Top 10 for Large Language Model Applications, 2025 edition: LLM01 Prompt Injection. OWASP Foundation, 2025. https://owasp.org/www-project-top-10-for-large-language-model-applications/

3. Wilson, S. The Developer’s Playbook for Large Language Model Security. O‘Reilly Media, Sebastopol, CA, USA, 2024. 200 b.; 4-bob “Prompt Injection”.

4. Perez, F.; Ribeiro, I. Ignore Previous Prompt: Attack Techniques for Language Models. arXiv preprint arXiv:2211.09527, 2022.

5. Yong, Z.-X.; Menghini, C.; Bach, S.H. Low-Resource Languages Jailbreak GPT-4. arXiv preprint arXiv:2310.02446, 2023.

6. Vassilev, A.; Oprea, A.; Fordyce, A.; Anderson, H.; Davies, X.; Hamin, M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2025; pp. 43–53.

7. Sotiropoulos, J. Adversarial AI Attacks, Mitigations, and Defense Strategies. Packt Publishing, Birmingham, UK, 2024. 602 b.; 14-bob.

8. Holtzman, A.; Buys, J.; Du, L.; Forbes, M.; Choi, Y. The Curious Case of Neural Text Degeneration. Proceedings of the 8th International Conference on Learning Representations, 2020.

9. Petrov, A.; La Malfa, E.; Torr, P.H.S.; Bibi, A. Language Model Tokenizers Introduce Unfairness Between Languages. Advances in Neural Information Processing Systems 36, New Orleans, USA, 2023.

TELEMEDITSINA PLATFORMALARIDA BEMOR MA'LUMOTLARI XAVFSIZLIGIGA TAHDIDLAR VA RISKLARNI INTEGRAL BAHOLASH MEZONLARI

Muminova S.Sh., Tursunova M.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada telemeditsina platformalarida bemorlarning shaxsga doir ma'lumotlari xavfsizligiga tahdidlar texnik, huquqiy, tashkiliy hamda inson omili jihatidan tahlil qilingan. Bemor ma'lumotlari harakatining besh bosqichida yuzaga kelishi mumkin bo'lgan zaifliklar va ularga qarshi qo'llaniladigan himoya choralari ko'rib chiqilgan. O'zbekiston qonunchiligida shaxsga doir ma'lumotlar xavfsizligi buzilganida bemorlarni xabardor qilish hamda ularga yetishi mumkin bo'lgan zararni baholash tartibini yanada aniqlashtirish zarurligi asoslangan. NIST SP 800-30 tavsiyalariga tayangan holda ma'lumotlarning sezgirligi, himoya choralarining joriy etilish darajasi va klinik jarayonlar uzluksizligini hisobga oladigan risklarni baholash modeli taklif etilgan.

Kalit so'zlar: telemeditsina, bemorlarning shaxsiy ma'lumotlari, axborot xavfsizligi, risklarni baholash, NIST SP 800-30, inson omili, shaxsga doir ma'lumotlar.

Аннотация. В статье проанализированы угрозы безопасности персональных данных пациентов на телемедицинских платформах с технической, правовой, организационной точек зрения и с учётом человеческого фактора. Рассмотрены потенциальные уязвимости на пяти этапах движения данных и меры защиты, направленные на их устранение. Обоснована необходимость более чёткого нормативного регулирования вопросов уведомления пациентов о нарушениях безопасности персональных данных и оценки возможного причинённого им вреда в действующем законодательстве Республики Узбекистан. На основе рекомендаций NIST SP 800-30 предложена модель оценки рисков, учитывающая чувствительность данных, степень внедрения мер защиты и непрерывность клинических процессов.

Ключевые слова: телемедицина, персональные данные пациентов, информационная безопасность, оценка рисков, NIST SP 800-30, человеческий фактор, персональные данные.

Kirish

O'zbekistonda sog'liqni saqlash sohasini raqamlashtirish maqsadida yagona Raqamli sog'liqni saqlash platformasini yaratish hamda tibbiyot tashkilotlarining axborot tizimlarini o'zaro integratsiyalash bo'yicha ishlar olib borilmoqda. O'zbekiston Respublikasi Prezidentining 2023-yil 28-dekabrdagi PQ-415-son qaroriga ko'ra, platformani yaratish, joriy etish, texnik qo'llab-quvvatlash va uning axborot xavfsizligini ta'minlash vazifalari yagona integrator - "UZINFOCOM" MChJ zimmasiga yuklatilgan. Axborot tizimlarini markazlashtirish ularning faoliyatini muvofiqlashtirishga xizmat qilishi bilan birga, platformada qayta ishlanadigan bemor ma'lumotlarini ishonchli himoyalash zaruratini ham kuchaytiradi. Telemeditsina tizimi interfeys, aloqa, xizmatlar, ma'lumotlar, integratsiya va boshqaruv sathlaridan iborat bo'lishi mumkin. Bemor ma'lumotlariga ishlov berish tartibi esa platformaning tuzilishi va xizmat ko'rsatuvchi tashkilotlarga bog'liq. Masalan, bulutli videokonsultatsiya davomida bemorning ism-familiyasi, videotasviri va suhbat matni xizmat provayderi tomonidan qayta ishlanishi mumkin. Shu bois

xavfsizlikni baholashda tibbiyot muassasasining ichki tizimlari bilan cheklanib qolmasdan, tashqi xizmatlar orqali uzatiladigan ma’lumotlarni ham hisobga olish zarur.

Himoya choralarini to‘g‘ri tanlash, avvalo, mavjud tahdidlarni aniqlashni talab etadi. Biroq telemeditsina xavfsizligiga bag‘ishlangan maqolalarning 93 foizida tahdid modeli keltirilmagan. Shuningdek, tahlil qilingan 99 ta tadqiqotning qariyb uchdan ikki qismida taklif etilgan yechim aynan qaysi hujumga qarshi mo‘ljallangani ko‘rsatilmagan.

Ma’lumotlar oqimi va texnik tahdidlar

O‘rganilgan manbalarga tayangan holda telemeditsina platformasida bemor ma’lumotlari harakati besh bosqichga ajratildi (1-jadval).

1-jadval

Bemor ma’lumotlari oqimi bosqichlari bo‘yicha texnik tahdidlar

Oqim bosqichi	Asosiy tahdid va zaifliklar	Himoya yo‘nalishi
1. Bemor qurilmasi va uy muhiti	Uy IoT qurilmalari orqali ruxsatsiz kirish; ilovani qayta paketlash, transport qatlami himoyasizligi	Qurilma autentifikatsiyasi, tarmoqni segmentlash, shifrlash
2. Aloqa kanali	Konferensiyaga ruxsatsiz qo‘shilish, yetarlicha shifrlanmagan aloqa; MitM hujumi	TLS va P2P shifrlash
3. Platforma (veb, API, bulut)	SQL in’yeksiya, saytlararo skriptlash, masofadan kod bajarish; provayder xavflari	Zaifliklarni tekshirish, kirishni boshqarish, provayder auditi
4. Integratsiya (DMED, tashqi tizimlar)	O‘zaro bog‘lanmagan ko‘plab tizimlar; yagona xavfsizlik siyosatining yo‘qligi	Yagona integratsiya va xavfsizlik talablari
5. Saqlash, zaxira va arxiv	Tovlamachi dastur yordamida ma’lumotlarni shifrlab qo‘yish; buzib kirish orqali ma’lumotlarning sizib chiqishi	Shifrlash, zaxira nusxalar, tiklash

Ma’lumotlar oqimining birinchi va uchinchi bosqichlari alohida e’tibor talab etadi. Chunki bemor uyida foydalanadigan ayrim IoT qurilmalari yetarli himoya vositalariga ega bo‘lmasligi va shifoxona axborot tizimiga ruxsatsiz kirish uchun vositaga aylanishi mumkin. Bundan tashqari, yagona raqamli platformada turli tibbiyot muassasalaridan olingan bemor ma’lumotlari jamlanadi. Bu esa ma’lumotlarni himoyalashga nisbatan yanada qat’iy talablar qo‘yishni taqozo etadi.

UZCERT hisobotida kiberhujumlarning salmoqli qismini SQL in’yeksiyasi (19 %), protokol talablarining buzilishi (18 %), lokal fayllarni qo‘shish (17 %), masofadan kod bajarish (16 %) va saytlararo skriptlash (15 %) kabi hujumlar tashkil etgan. 2023-yilda aniqlangan tahdid va zaifliklarning 72 foizi davlat sektoriga to‘g‘ri kelgan. Mazkur hujum turlari telemeditsina platformalarining veb va API qismlari uchun ham dolzarbdir. Ammo hisobotda sog‘liqni saqlash sohasi alohida ko‘rsatilmagani sababli telemeditsina tizimlariga qaratilgan hujumlar ulushini aniqlashning imkoni yo‘q.

To‘rtinchi bosqichda sog‘liqni saqlash sohasida mavjud 35 dan ortiq o‘zaro bog‘lanmagan axborot tizimi yagona xavfsizlik siyosatini amalga oshirishni qiyinlashtiradi. Zero, tizimning umumiy himoyalanganlik darajasi uning eng zaif bo‘g‘iniga bog‘liq. O‘zbekiston Respublikasi Prezidentining PF-77-son Farmonida yagona integratsiya standartlari va xavfsizlik talablarini tasdiqlash vazifasi belgilanishi aynan shu muammoni hal etishga qaratilgan.

Huquqiy va tashkiliy muammolar

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunning 27-moddasiga muvofiq, ma’lumotlar mulkdori, operatori va uchinchi shaxs ularni himoya qilish choralarini ko‘rishi shart. Shunga qaramay, tibbiyot muassasasi, platforma operatori, bulutli xizmat provayderi va bemor o‘rtasidagi mas’uliyatni taqsimlashning yaxlit mexanizmi belgilanmagan. GDPRning 28-moddasida ma’lumotlar nazoratchisi yetarli kafolatlarni ta’minlay oladigan ishlov beruvchilar xizmatidan foydalanishi belgilangan. O‘zbekistonda esa standart shartnoma shartlari faqat ma’lumotlarni transchegaraviy uzatish uchun nazarda tutilgan.

GDPRning 33–34-moddalariga ko‘ra, shaxsga doir ma’lumotlar xavfsizligi buzilgani haqida nazorat organi 72 soat ichida, bemor huquq va erkinliklariga yuqori xavf tug‘ilganda esa bemorning o‘zi ham kechiktirmasdan xabardor qilinishi kerak. O‘zbekistonda 24 va 72 soatlik muddatlar faqat transchegaraviy uzatish holatlari uchun belgilangan. “Kiberxavfsizlik to‘g‘risida”gi Qonunning 16-moddasida esa xabardor qilishning aniq muddati ko‘rsatilmagan. Ushbu qonunning 21 va 31-moddalarida nazarda tutilgan kiberxavfsizlik darajasini baholash tizimning himoyalanganlik holatini aniqlashga xizmat qiladi, biroq hodisaning bemorga yetkazishi mumkin bo‘lgan zararini baholamaydi. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunda ham bunday talab keltirilmagan. Tashkiliy jihatdan esa texnik va tashkiliy himoya choralari yetarli darajada rivojlanmagani hamda malakali mutaxassislar tanqisligi qayd etilgan.

Inson omili

Ijtimoiy muhandislikka asoslangan hujumlarda insonning xatti-harakati va zaif jihatlaridan foydalaniladi. Shu sababli xodimlarni tizimli ravishda o‘qitish muhim ahamiyatga ega. Tadqiqotlarda fishing havolalariga o‘tish ehtimoliga eng kuchli ta’sir ko‘rsatgan omil xodimlarning ish yuklamasi ekani aniqlangan. Demak, xodimlarni o‘qitish bilan bir qatorda, mehnat jarayonini oqilona tashkil etish ham zarur. Bemorlar uchun esa uy sharoitida tibbiy suhbatning begona shaxslarga eshitilib qolishi yoki maxfiy muloqot uchun alohida joy bo‘lmasligi xavf tug‘diradi. Shuning uchun xavfsizlik bo‘yicha tushuntirish va o‘qitish ishlari har bir ishtirokchining vazifasiga moslashtirilishi lozim.

Risklarni integral baholash modeli

NIST SP 800-30 tavsiyalarida risk ehtimollik va ta’sir matritsasi asosida besh darajaga ajratiladi; inson hayotiga xavf tug‘diradigan oqibatlar esa “yuqori” ta’sir darajasiga kiritiladi. M. Nobili va hammualliflari himoya choralarining joriy etilish darajasini CMMI asosida 0 dan 5 gacha baholaganlar. Biroq mazkur ko‘rsatkichning o‘zi qaysi himoya chorasini kuchaytirish kerakligini aniqlab bermaydi. ENISA risk oqibatlarini bemor nuqtayi nazaridan, jumladan, shoshilinch holatlarda yuzaga kelishi mumkin bo‘lgan zararni inobatga olib baholashni tavsiya etadi. O‘rganilgan manbalarda ushbu uch jihatni birgalikda hisobga oladigan yondashuv uchramadi. Shu bois taklif etilayotgan modelda (2-jadval) klinik jarayonlarning uzluksizligi risk darajasining eng quyi chegarasini belgilovchi omil sifatida, ma’lumotlar sezgirligi va himoya choralarining joriy etilish darajasi esa boshlang‘ich bahoni o‘zgartiruvchi alohida mezonlar sifatida qabul qilindi.

2-jadval

Telemeditsina risklarini integral baholash mezonlari

Mezon	Baholash shkalasi	Bahoga ta’siri
1. Asosiy xavf (ehtimollik × ta’sir)	Besh daraja: juda past – juda yuqori	Boshlang‘ich daraja (R_0)

Mezon	Baholash shkalasi	Bahoga ta’siri
2. Ma’lumot sezgirligi	O‘rta (identifikatsion); yuqori (klinik, tasvir va video yozuvlar, autentifikatsiya); juda yuqori (reproduktiv va ruhiy salomatlik, biometrik va genetik)	Maxfiylik yoki yaxlitlik tahdidi “juda yuqori” sezgir ma’lumotga qaratilsa: +1 daraja
3. Himoya choralarining joriy etilganlik darajasi (J)	0–5 (CMMI asosida)	$J \leq 2$: +1 daraja; $J \geq 4$: −1 daraja
4. Klinik uzluksizlik	Shoshilinch yordam yoki o‘tkir holatdagi bemorni kuzatish to‘xtashi mumkin (muqobil kanal yo‘q) / mumkin emas	To‘xtash mumkin bo‘lsa, eng kam daraja “yuqori”
5. Inson omili	Tahdid ishtirokchi xatti-harakati orqali amalga oshadimi	Darajani o‘zgartirmaydi; J baholanganda o‘qitish choralari ham hisobga olinadi

Izoh: ma’lumotlarning sezgirlik darajasi ularning huquqiy maqomi, shaxsni aniqlash imkoniyati hamda oshkor etilishi oqibatida yetishi mumkin bo‘lgan zarar asosida belgilanadi. Turli turdagi ma’lumotlar birlashtirilgan bo‘lsa (masalan, videoyozuvda), baholashda eng sezgir tarkibiy qism darajasi olinadi.

Baholash jarayoni to‘rt bosqichdan iborat.

1. Asosiy daraja R_0 NIST matritsasi bo‘yicha aniqlanadi, biroq NIST hisobga oladigan himoya choralari va ma’lumot sezgirligi bu qadamda chiqarib tashlanadi, ya’ni R_0 himoya choralarigacha bo‘lgan xavfni bildiradi.

2. Maxfiylik yoki yaxlitlik tahdidi “juda yuqori” sezgir ma’lumotga qaratilsa, daraja bir pog‘ona oshiriladi.

3. $J \leq 2$ bo‘lsa daraja bir pog‘ona oshiriladi, $J \geq 4$ bo‘lsa pasaytiriladi, $J = 3$ bo‘lsa o‘zgarmaydi; himoya choralari shu qadamda qaytadan hisobga olingani uchun natija NIST ta’rifidagi qoldiq riskka mos keladi.

4. Tahdid shoshilinch tibbiy yordamga muhtoj bemorni masofadan kuzatish imkoniyatini to‘xtatishi mumkin bo‘lsa va muqobil aloqa kanali mavjud bo‘lmasa, risk darajasi “yuqori” darajadan past deb belgilanmaydi. Ushbu shart risk darajasini qo‘shimcha pog‘onaga oshirmaydi, balki uning eng quyi chegarasini belgilaydi. 5-mezon esa J bahosida xodimlarni o‘qitish choralarining hisobga olinishini ta’minlaydi.

Risk darajalari tartibli shkala bo‘lgani uchun tuzatma arifmetik qo‘shish emas, bir pog‘ona siljishni bildiradi va natija shkala chegarasidan chiqmaydi. J har bir chora uchun uning talablarga muvofiqligiga qarab beriladi. Bir nechta chora bo‘lsa, bir-birining o‘rnini bosuvchi choralar guruhi ichida eng yuqori, zarur choralar guruhlari orasida esa eng past baho olinadi, chunki tizim xavfsizligi eng zaif bo‘g‘inga bog‘liq. Bu qoida zaif chorani kuchlisi hisobiga qoplamaydi. J chegaralari o‘rta qiymat $J = 3$ atrofida simmetrik tanlangan.

Shartli misolda (J qiymatlari real platformada o‘lchanmagan) ikki tahdid uchun R_0 = “o‘rta”, tahdid “juda yuqori” sezgir ma’lumotga qaratilgan va shoshilinch yordam to‘xtashi kutilmaydi deb olinadi. Video-aloqaga ruxsatsiz qo‘shilish: “o‘rta” → +1 → “yuqori” → $J = 4$,

−1 → “o‘rta”. Ichki xodimning vakolatsiz kirishi: “o‘rta” → +1 → “yuqori” → $J = 3$, tuzatma yo‘q → “yuqori”. Demak, asosiy bahosi bir xil tahdidlar himoya choralari holatiga qarab turli ustuvorlik oladi.

Model cheklovlari:

– daraja o‘zgartirish qoidalari, J chegaralari va choralarni guruhlash ekspert yondashuviga asoslangan va empirik tekshirilmagan;

– J ning operatsion ta’rifi manbada berilmagan; R_0 ni himoya choralarisiz aniqlash NIST amaliyotidan farq qiladi.

Xulosa

Telemeditsina platformasida bemor ma’lumotlari harakatini besh bosqichda ko‘rib chiqish har bir bosqichga xos tahdidlarni aniqlash imkonini beradi. Ayniqsa, bemor foydalanadigan qurilmalar va ma’lumotlar jamlanadigan platformaning xavfsizligiga alohida e’tibor qaratish lozim. O‘zbekiston qonunchiligida axborotni himoyalash bo‘yicha mas’uliyatni taqsimlash, ma’lumotlar xavfsizligi buzilganda bemorlarni xabardor qilish va bunday hodisalarning bemorlarga ta’sirini baholash tartiblarini yanada aniqlashtirish zarur. Inson omiliga bog‘liq xatolarning yuzaga kelishida xodimlarning ish yuklamasi ham muhim o‘rin tutadi. Taklif etilgan konseptual mezonlar NIST SP 800-30 risklarni baholash matritsasini telemeditsina sohasiga xos omillar bilan to‘ldiradi hamda dastlabki bahosi bir xil tahdidlar orasida ustuvorlikni belgilashga yordam beradi. Shu bilan birga, modelni amaliyotga tatbiq etishdan avval uning samaradorligini empirik tadqiqotlar orqali tekshirish talab etiladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining 2023-yil 28-dekabrdagi “Sog‘liqni saqlash tizimini raqamlashtirishni jadallashtirish hamda ilg‘or raqamli texnologiyalarni joriy etish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-415-sonli Qarori. – URL: https://lex.uz/docs/6719038 (kirish sanasi: 06.10.2026).

2. Hemalatha S. et al. An architectural framework for telemedicine systems: components, roles, and implementation challenges // Telehealth and Medicine Today. – 2025. – Vol. 10. – Article 596.

3. ENISA. Cloud security for healthcare services. – January 2021. – DOI: 10.2824/454966.

4. Garg V., Brewer J. Telemedicine security: a systematic review // Journal of Diabetes Science and Technology. – 2011. – Vol. 5, Issue 3. – P. 768–777.

5. Nemec Zlatolas L., Welzer T., Lhotska L. Data breaches in healthcare: security mechanisms for attack mitigation // Cluster Computing. – 2024. – Vol. 27. – P. 8639–8654.

6. Pulivarti R. et al. Mitigating cybersecurity and privacy risks in telehealth smart home integration. – NIST CSWP 34. – NIST, 2025. – DOI: 10.6028/NIST.CSWP.34.

7. Ahamad S.S., Al-Shehri M., Keshta I. A secure and resilient scheme for telecare medical information systems with threat modeling and formal verification // IEEE Access. – 2022. – Vol. 10. – P. 120227–120244.

8. Jalali M.S., Landman A., Gordon W.J. Telemedicine, privacy, and information security in the age of COVID-19 // JAMIA. – 2021. – Vol. 28, No. 3. – P. 671–672.

9. UZCERT. Тенденции развития кибербезопасности в Узбекистане. – Ташкент: Департамент «UZCERT», 2024. – 14 с.

10. OWASP API Security Top 10 (2023). – URL: https://api-security.owasp.org/editions/2023/en/0x11-t10/ (kirish sanasi: 06.10.2026).

11. Ahmedov M., Hellowell M. Accelerating progress towards universal health coverage (UHC) in Uzbekistan: a proposal for a National Health System Strategy 2030. – Washington DC: World Bank, 2025.

12. Health Sector Coordinating Council. Health industry cybersecurity – securing telehealth and telemedicine. – 2023.

13. O‘zbekiston Respublikasi Prezidentining 2026-yil 5-maydagi “Sog‘liqni saqlash tizimida boshqaruv samaradorligini oshirish chora-tadbirlari to‘g‘risida”gi PF-77-sonli Farmoni.

14. Regulation (EU) 2016/679 (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119. – P. 1–88.

15. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-sonli Qonuni.

16. NIST Cybersecurity Framework (CSF) 2.0. – NIST CSWP 29. – 2024. – DOI: 10.6028/NIST.CSWP.29.

17. Razali R.A., Jamil N. A quick review of security issues in telemedicine // 2020 8th International Conference on Information Technology and Multimedia (ICIMU). – 2020.

18. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘RQ-547-sonli Qonuni (2026-yil 26-martdagi O‘RQ-1125-sonli Qonun bilan kiritilgan o‘zgartirishlar bilan).

19. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2026-yil 29-iyuldagi 415-sonli qarori. – URL: https://lex.uz/docs/8369688 (kirish sanasi: 06.10.2026).

KAFT VENA TOMIRLARI ASOSIDAGI BIOMETRIK AUTENTIFIKATSIYA TIZIMLARIDA AXBOROT XAVFSIZLIGI TAHDIDLARINI MODELLASHTIRISH

Muminova S.Sh., Sayfiddinova B.B.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda kaft vena tomirlari asosida ishlovchi biometrik autentifikatsiya tizimlarining axborot xavfsizligi tahdidlari tahlil qilinadi. Biometrik tizimning ma'lumotlarni olish, dastlabki qayta ishlash, xususiyatlarni ajratish, biometrik shablonlarni saqlash va autentifikatsiya qarorini qabul qilish bosqichlari o'rganiladi. STRIDE metodologiyasi asosida tizim komponentlariga ta'sir ko'rsatishi mumkin bo'lgan tahdidlar tasniflanib, ularning yuzaga kelish ehtimoli va oqibatlarini hisobga oluvchi xavfni baholash modeli taklif etiladi. Aniqlangan tahdidlarga qarshi tashkiliy va texnik himoya choralarini qo'llash imkoniyatlari ko'rib chiqiladi.

Kalit so'zlar: biometrik autentifikatsiya, kaft vena tomirlari, palm vein, tahdid modeli, STRIDE, biometrik shablon, axborot xavfsizligi, xavfni baholash.

Аннотация. В данном тезисе анализируются угрозы информационной безопасности биометрических систем аутентификации, функционирующих на основе вен ладони. Рассматриваются этапы получения данных, предварительной обработки, извлечения признаков, хранения биометрических шаблонов и принятия решения об аутентификации. На основе методологии STRIDE классифицируются угрозы, которые могут воздействовать на компоненты системы, и предлагается модель оценки рисков, учитывающая вероятность их возникновения и последствия. Рассматриваются возможности применения организационных и технических мер защиты от выявленных угроз.

Ключевые слова: биометрическая аутентификация, вены ладони, palm vein, модель угроз, STRIDE, биометрический шаблон, информационная безопасность, оценка рисков.

Kirish

Zamonaviy axborot tizimlarida foydalanuvchilarni ishonchli autentifikatsiya qilish axborot xavfsizligini ta'minlashning muhim vazifalaridan biri hisoblanadi. An'anaviy autentifikatsiya vositalari, jumladan, parollar, PIN-kodlar va identifikatsiya kartalari foydalanuvchi shaxsini tasdiqlashda keng qo'llaniladi. Biroq parollarning oshkor bo'lishi, identifikatsiya vositalarining yo'qotilishi yoki o'g'irlanishi ushbu usullarning ishonchliligini pasaytiradi.

Mazkur muammolarni bartaraf etish yo'nalishlaridan biri insonning individual fiziologik xususiyatlariga asoslangan biometrik autentifikatsiya texnologiyalaridan foydalanishdir. Bunday texnologiyalar orasida kaft vena tomirlari naqshlari asosidagi autentifikatsiya alohida ahamiyatga ega.

Kaft vena tomirlari teri ostida joylashgani va ularning tasviri yaqin infraqizil nurlanish yordamida olinishi sababli mazkur biometrik belgi ayrim tashqi biometrik xususiyatlarga nisbatan qalbakilashtirishga murakkabroq hisoblanadi. Shuningdek, vena naqshlarining individual tuzilishi shaxsni identifikatsiya qilishda muhim xususiyatlar majmuasini hosil qiladi.

L. J. Alwan tomonidan 2017-yilda bajarilgan tadqiqotda kaft vena tomirlarining tasvirlarini qayta ishlash, qiziqish sohasini (Region of Interest - ROI) ajratish, segmentatsiya va statistik belgilar asosida identifikatsiya qilish usuli ishlab chiqilgan. Tadqiqotda CASIA ma'lumotlar bazasi yordamida 91,6% to'g'ri tanib olish ko'rsatkichi qayd etilgan.

A. S. Hameed tomonidan 2021-yilda bajarilgan tadqiqotda esa konvolyutsion neyron tarmoq (Convolutional Neural Network - CNN) yordamida kaft vena tomirlarini identifikatsiya qilish tizimi taklif etilgan. Tadqiqot natijalariga ko‘ra, 850 nm to‘lqin uzunligida ayrim sinov konfiguratsiyalarida 99% gacha aniqlikka erishilgan.

Ushbu tadqiqotlar kaft vena tomirlari asosidagi biometrik identifikatsiya algoritmlarining samaradorligini ko‘rsatadi. Biroq identifikatsiya aniqligining yuqori bo‘lishi tizimning barcha axborot xavfsizligi tahdidlariga bardoshli ekanligini anglatmaydi. Jumladan, biometrik tasvirlarni almashtirish, shablonlar bazasiga ruxsatsiz kirish, uzatilayotgan ma’lumotlarni o‘zgartirish va autentifikatsiya natijalarini soxtalashtirish kabi tahdidlar tizimning ishonchliligiga salbiy ta’sir ko‘rsatishi mumkin.

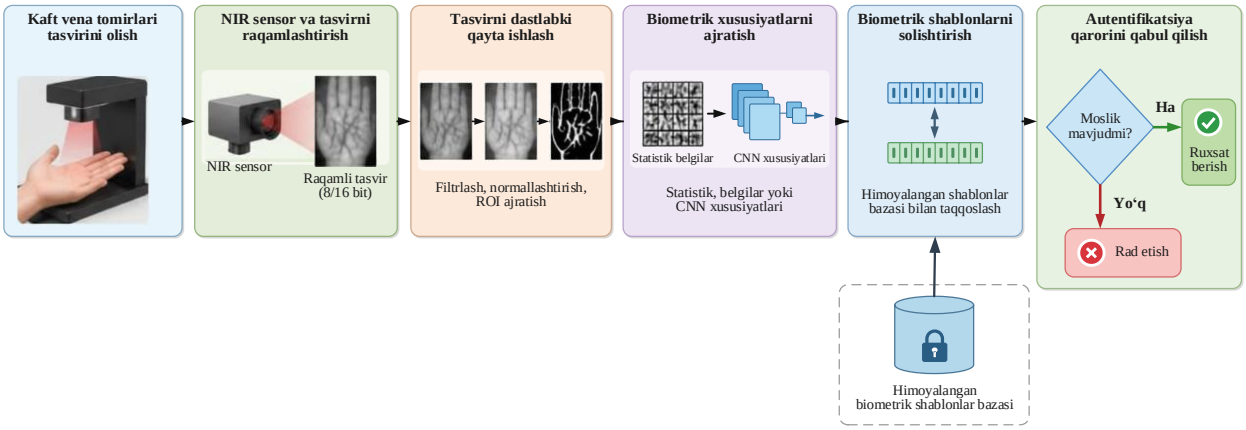
Shu sababli kaft vena tomirlari asosidagi biometrik autentifikatsiya tizimining nafaqat identifikatsiya algoritmlarini, balki uning barcha funksional komponentlarini qamrab oluvchi tahdid modelini ishlab chiqish dolzarb masala hisoblanadi.

Asosiy qism

Kaft vena tomirlari asosidagi biometrik autentifikatsiya tizimi bir nechta o‘zaro bog‘langan funksional bosqichlardan tashkil topadi. Ushbu bosqichlarning har biri biometrik ma’lumotlarning qayta ishlanishi va autentifikatsiya natijasining shakllanishida muhim ahamiyat kasb etadi.

Tahlil qilingan tadqiqotlarda biometrik tasvirni olish, ROI sohasini ajratish, tasvir sifatini yaxshilash, xususiyatlarni ajratish va solishtirish bosqichlari asosiy funksional jarayonlar sifatida keltirilgan.

Mazkur yondashuvlar asosida tahdidlarni tahlil qilish uchun quyidagi umumlashtirilgan arxitektura shakllantirildi.



1-rasm. Kaft vena tomirlari asosidagi biometrik autentifikatsiya tizimining umumlashtirilgan funksional sxemasi

Tizimning birinchi bosqichida NIR sensor yordamida foydalanuvchi kaftining vena tomirlari tasviri olinadi. Ushbu bosqichda sensor qurilmasiga jismoniy ta’sir ko‘rsatish, oldindan tayyorlangan tasvirni uzatish yoki sensor chiqish ma’lumotlarini almashtirish xavfi mavjud.

Ikkinchi bosqichda olingan tasvir dastlabki qayta ishlash algoritmlaridan o‘tkaziladi. Bu jarayonda tasvirdagi shovqinlarni kamaytirish, kontrastni yaxshilash va ROI sohasini ajratish amallari bajariladi. Mazkur bosqichga qasddan o‘zgartirilgan ma’lumotlar kiritilishi biometrik xususiyatlarning noto‘g‘ri shakllanishiga sabab bo‘lishi mumkin.

Uchinchi bosqichda biometrik tasvirdan individual xususiyatlar ajratib olinadi. Bunda statistik usullar yoki chuqur o‘qitish algoritmlaridan foydalanilishi mumkin. Ajratilgan xususiyatlar keyinchalik foydalanuvchini tanib olish uchun biometrik shablon shaklida ifodalanadi.

To‘rtinchi bosqichda joriy biometrik ma’lumotlar ro‘yxatdan o‘tkazish jarayonida yaratilgan etalon shablon bilan solishtiriladi. Ushbu bosqichdagi asosiy xavflar biometrik shablonlarning oshkor bo‘lishi, almashtirilishi yoki solishtirish algoritmiga ruxsatsiz ta’sir ko‘rsatilishi bilan bog‘liq.

Yakuniy bosqichda o‘xshashlik ko‘rsatkichi belgilangan chegaraviy qiymat bilan taqqoslanadi va foydalanuvchiga kirish huquqini berish yoki rad etish to‘g‘risida qaror qabul qilinadi.

STRIDE metodologiyasi asosida tahdidlarni aniqlash

Biometrik autentifikatsiya tizimining xavfsizligini tahlil qilishda tahdidlarni tizimli ravishda tasniflash muhim ahamiyatga ega. Mazkur tadqiqotda STRIDE metodologiyasidan foydalanildi va quyidagi tahdidlar aniqlandi.

1-jadval.

Kaft vena tomirlari asosidagi biometrik autentifikatsiya tizimining STRIDE tahdid modeli

Tahdid toifasi	Tahdidning namoyon bo‘lishi	Ta’sir ko‘rsatiladigan komponent
Spoofing	Sensor yoki biometrik tasvirni soxtalashtirish	Tasvirni olish
Tampering	Biometrik tasvir yoki shablonni o‘zgartirish	Qayta ishlash va saqlash
Repudiation	Autentifikatsiya urinishini inkor etish	Audit va jurnal tizimi
Information Disclosure	Biometrik shablonlarning oshkor bo‘lishi	Ma’lumotlar bazasi
Denial of Service	Sensor yoki autentifikatsiya xizmatini ishdan chiqarish	Tizim infratuzilmasi
Elevation of Privilege	Autentifikatsiya natijasini chetlab o‘tib yuqori huquq olish	Kirishni boshqarish

Yuqoridagi jadvaldan ko‘rinib turibdiki, biometrik autentifikatsiya tizimining har bir funksional bosqichida turli xususiyatga ega xavfsizlik tahdidlari yuzaga kelishi mumkin.

Masalan, Spoofing tahdidi nafaqat biometrik belgilarning qalbakilashtirilishi, balki sensor qurilmasidan uzatilayotgan raqamli ma’lumotlarning almashtirilishi orqali ham amalga oshirilishi mumkin. Shu sababli vena tomirlarining teri ostida joylashgani autentifikatsiya tizimini barcha turdagi soxtalashtirish hujumlaridan to‘liq himoyalamaydi.

Information Disclosure tahdidi biometrik tizimlar uchun alohida xavflidir. Chunki parol oshkor bo‘lganida uni almashtirish mumkin, biroq insonning fiziologik biometrik xususiyatlarini odatdagi parol singari o‘zgartirish imkoniyati mavjud emas. Natijada biometrik shablonning oshkor bo‘lishi uzoq muddatli xavfsizlik muammolarini keltirib chiqarishi mumkin.

Aniqlangan tahdidlarga qarshi himoya choralarini shakllantirish

Tahdidlarni tahlil qilish natijalariga ko‘ra biometrik autentifikatsiya tizimining turli bosqichlarida bir nechta himoya mexanizmlarini qo‘llash maqsadga muvofiq.

2-jadval.

Biometrik autentifikatsiya tizimining tahdidlariga qarshi tavsiya etiladigan himoya mexanizmlari

Tahdid	Tavsiya etiladigan himoya chorasi

Biometrik ma’lumotlarni soxtalashtirish	Tiriklikni aniqlash va taqdimot hujumlarini aniqlash mexanizmlari
Tasvirlarni almashtirish	Sensor va qayta ishlash moduli o‘rtasida autentifikatsiyalangan aloqa
Biometrik shablonlarni o‘g‘irlash	Shablonlarni himoyalangan shaklda saqlash, kirishni cheklash
Shablonlarni o‘zgartirish	Yaxlitlikni kriptografik tekshirish
Autentifikatsiya natijasini soxtalashtirish	Qaror qabul qilish modulini himoyalash va natijani autentifikatsiyalash
Xizmat ko‘rsatishni rad etish	Resurslarni cheklash, monitoring va tiklash mexanizmlari
Vakolatlarni oshirish	Minimal vakolat tamoyili va rollarga asoslangan kirishni boshqarish

Biometrik shablonlarni himoyalashda qayta tiklab bo‘lmaydigan yoki kalitga bog‘liq transformatsiyalangan shablonlardan foydalanish istiqbolli yo‘nalish hisoblanadi. Bunday yondashuv biometrik ma’lumotlar oshkor bo‘lgan taqdirda ularni boshqa tizimlarda bevosita qayta ishlatish xavfini kamaytirishga xizmat qilishi mumkin.

Shuningdek, biometrik autentifikatsiya natijalarini tizimning umumiy kirishni boshqarish mexanizmidan ajratib bo‘lmaydi. Chunki biometrik tanib olish algoritmi to‘g‘ri ishlagan taqdirda ham, autentifikatsiya natijasini qabul qiluvchi dasturiy moduldagi zaiflik tizim xavfsizligini buzishi mumkin.

Xulosa

Kaft vena tomirlari asosidagi biometrik autentifikatsiya tizimlari shaxsni identifikatsiya qilishda istiqbolli texnologiyalardan biri hisoblanadi. Biroq bunday tizimlarning ishonchliligi faqat biometrik tanib olish algoritmining aniqligi bilan belgilanmaydi.

Taklif etilgan tahdid modeli biometrik autentifikatsiya tizimlarining xavfsizlik talablarini ishlab chiqish, ularning zaifliklarini tahlil qilish va himoya mexanizmlarini tanlash uchun nazariy asos bo‘lib xizmat qilishi mumkin. Modelning amaliy samaradorligini tasdiqlash uchun kelgusida real tizim arxitekturasi va eksperimental xavfsizlik sinovlari asosida baholash talab etiladi.

Foydalanilgan adabiyotlar

1. Alwan L. J. Palm Vein Recognition. Master's Thesis. Al-Nahrain University, College of Science, 2017.

2. Hameed A. S. Palm Vein Identification System Based on Convolution Neural Network. Master's Thesis. University of Al-Qadisiyah, College of Computer Science and Information Technology, 2021.

3. Shostack A. Threat Modeling: Designing for Security. Wiley, 2014.

4. Jain A. K., Ross A., Prabhakar S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology. 2004. Vol. 14, No. 1. pp. 4–20.

5. Ratha N. K., Connell J. H., Bolle R. M. Enhancing Security and Privacy in Biometrics-Based Authentication Systems. IBM Systems Journal. 2001. Vol. 40, No. 3. pp. 614–634.

BILIMLAR GRAFI ASOSIDA KIBERTAHDIDLARNI PROAKTIV ANIQLASH MODELINI QIYOSIY TAHLILI

Tojimatov D.X.
Farg‘ona davlat texnika universiteti
Ganiyev A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada bilimlar grafi va tizim faoliyatiga oid kuzatuvlar asosida kibertahdid belgilarini baholash usuli ko‘rib chiqilgan. Model kuzatuvlarning manbasi, vaqti va o‘zaro mosligini hisobga oladi. Ogohlantirishdan oldin ma’lumotlarning qaror chiqarish uchun yetarliligi tekshiriladi. Hisoblash tajribasining 160 ta epizoddan iborat sinov qismida birlashtirilgan modelning erta aniqlash qamrovi 51,09% ni, faqat tizim kuzatuvlariga asoslangan modelniki esa 41,30% ni tashkil etgan. Noto‘g‘ri ogohlantirishlar ulushi mos ravishda 10,29% va 7,35% bo‘lgan. Natijalar aniqlash qamrovini noto‘g‘ri ogohlantirishlar va ma’lumot yetishmasligi sababli baholanmagan holatlar bilan birga hisoblash zarurligini ko‘rsatgan.

Kalit so‘zlar: kibertahdid, bilimlar grafi, tizim kuzatuvlari, mashinali o‘qitish, erta aniqlash, noto‘g‘ri ogohlantirish.

Аннотация. В статье рассмотрен метод оценки признаков киберугроз на основе графа знаний и наблюдений за работой системы. Модель учитывает источник, время и согласованность наблюдений. Перед выдачей предупреждения проверяется достаточность данных для принятия решения. На тестовой части вычислительного эксперимента из 160 эпизодов полнота раннего обнаружения составила 51,09% для объединённой модели и 41,30% для модели, использующей только наблюдения за системой. Доля ложноположительных срабатываний составила соответственно 10,29% и 7,35%. Результаты показывают необходимость учитывать полноту обнаружения, ложные срабатывания и эпизоды без решения из-за недостатка данных.

Ключевые слова: киберугроза, граф знаний, наблюдения за системой, машинное обучение, раннее обнаружение, ложное срабатывание.

Kirish

Axborot tizimiga kirishdagi ketma-ket muvaffaqiyatsiz urinishlar, yangi tashqi ulanishlar yoki trafik hajmining ortishi tahdid belgisi bo‘lishi mumkin. Bunday o‘zgarishlar tizimning odatiy faoliyatida ham kuzatiladi. Shuning uchun xavfsizlik tahlilchisi hodisaning qaysi resursda, qachon va qanday sharoitda yuz berganini bilishi kerak. Turli jurnallardagi yozuvlarni o‘zaro bog‘lash tahdid belgilarini ularning yuzaga kelish sharoiti bilan birga baholashga yordam beradi.

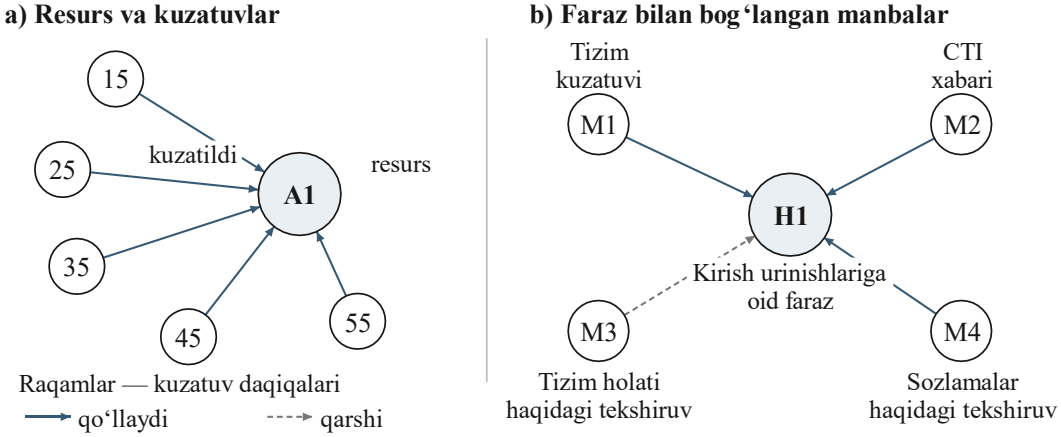
Tahdidlarni oldindan baholashda sun’iy intellektdan foydalanish imkoniyatlari [1] da ko‘rib chiqilgan. Kibertahdidlar haqidagi razvedka ma’lumotlari (CTI), tizim jurnallari va mashinali o‘qitish usullarini birgalikda qo‘llash yondashuvi [2] da yoritilgan. Bilimlar grafi obyektlar va ular o‘rtasidagi mazmuniy aloqalarni yagona tuzilmada ifodalaydi [3]. Bu tuzilma kuzatuvni tegishli resurs va ma’lumot manbasi bilan bog‘lash, shuningdek, ogohlantirishga qaysi yozuvlar asos bo‘lganini tekshirish imkonini beradi.

Maqolaning maqsadi bilimlar grafi bilan to‘ldirilgan aniqlash modelini bir xil kuzatuvlar asosida qiyosiy baholashdir. Grafning aniqlash qamroviga ta’siri, baholanmagan holatlar hamda modelni yangi ma’lumotlarda qayta o‘qitish natijasi tekshiriladi.

Asosiy qism

Tizim resurslari, kuzatilgan hodisalar va tahdid haqidagi xabarlar grafda alohida obyektlar sifatida saqlanadi. Ular o‘rtasidagi aloqalar «kuzatildi», «tegishli» va «qo‘llaydi» kabi nomlangan munosabatlar bilan ifodalanadi. Har bir xabarning kelgan vaqti qayd etiladi. Qaror chiqarilayotgan paytgacha olingan ma’lumotlargina hisobga olinadi. Birlamchi manbadan ko‘chirilgan xabarlar esa bitta manba guruhiga birlashtiriladi.

1-rasmda bitta kuzatuv epizodiga tegishli bog‘lanishlarning ikki ko‘rinishi berilgan. Chap tomonda beshta vaqt nuqtasidagi kuzatuvlar bitta resurs bilan bog‘langan. O‘ng tomonda kirish urinishlariga oid farazni qo‘llab-quvvatlovchi yoki unga qarshi ma’lumot bergan manbalar ko‘rsatilgan. M1–M4 kelib chiqishiga ko‘ra guruhlangan manbalarni bildiradi. Bu guruhlash takroriy nusxalar hisobiga bahoning oshib ketishini cheklaydi.



1-rasm. Kuzatuvlar, tizim resursi va tahdid haqidagi faraz o‘rtasidagi bog‘lanishlar

Modelda 16 ta belgidan foydalaniladi. Dastlabki sakkizta belgi ulanishlar, masofaviy manzillar, portlar va rad etilgan kirish urinishlari soni, qabul qilingan va uzatilgan ma’lumotlar hajmi (bayt), yangi ochilgan tashqi xizmatlar soni hamda server yuklamasini ifodalaydi. Isolation Forest (IF) va Autoencoder (avtokodlovchi, AE) usullarida hisoblangan baholarning tayanch taqsimotdagi nisbiy o‘rni yana ikkita belgini hosil qiladi. Qolgan oltita belgi grafdan olinadi. Ular farazni qo‘llab-quvvatlovchi va unga qarshi ma’lumotlar muvozanati, holati noma’lum ma’lumotlar ulushi, ziddiyat darajasi, manba guruhlari soni, graf bahosi va ma’lumot yetishmasligini bildiruvchi ko‘rsatkichdan iborat. Kuzatuv belgisi x va manba guruhlari soni m quyidagicha bir xil masshtabga keltiriladi:

$$x'_k = \min\left(\frac{\ln(1+x_k)}{10}, 3\right), \quad m' = \frac{\min(m,10)}{10};$$
$$r_{it} = \frac{1}{1+\exp(-z_{it})} \qquad (1)$$
$$z_{it} = \min(35, \max(-35, w^T \varphi_{it} + b))$$

Bu yerda φ - belgilar vektori; i - epizod; t - qaror chiqarish vaqti; k - kuzatuv belgisining indeksi; w va b - logistik model parametrlari. r bahosi ogohlantirishlarni ustuvorligi bo‘yicha tartiblash uchun ishlatiladi. Uni tahdid ehtimoli sifatida talqin qilishdan oldin alohida kalibrlash talab etiladi [5]. Mazkur tajribada r nisbiy baho sifatida qo‘llanilgan.

Ogohlantirishdan oldin ma’lumot yetarliligi J mezoni bo‘yicha tekshiriladi. Zarur kontekst maydonlari to‘ldirilgan, manba guruhlari kamida 2 ta, noma’lum ma’lumotlar ulushi 0,45 dan va ziddiyat darajasi 0,40 dan oshmagan bo‘lishi kerak. Qo‘llab-quvvatlovchi va qarshi ma’lumotlar vaznlari musbat bo‘lib, mutlaq farqi 0,08 dan oshmasa, qo‘shimcha ma’lumot talab qilinadi. Samarali vaznning quyi chegarasi 0 deb belgilangan. Bular tajriba sozlamalaridir.

$$d_{it} = \begin{cases} \perp & J_{it} = 0; \\ 1 & J_{it} = 1 \text{ va } r_{it} > \tau; \\ 0 & J_{it} = 1 \text{ va } r_{it} \leq \tau; \end{cases} \quad (2)$$

⊥ belgisi qaror chiqarish uchun ma’lumot yetarli emasligini, 1 ogohlantirish berilganini, 0 esa ayni vaqtda ogohlantirish berilmaganini bildiradi. Ma’lumot yetishmasligi tahdid yo‘qligini anglatmaydi. Tanlab tasniflash yondashuvida ham model qaror chiqargan holatlar ulushi va yo‘l qo‘ygan xatolari birgalikda baholanadi [4].

1-algoritm. Kuzatuvni baholash va ogohlantirish berish

Kirish ma’lumotlari: qaror vaqti t, shu vaqtgacha olingan yozuvlar, tizim kuzatuvlari, w, b va τ. Natija: qaror, hisoblangan baho va qarorga asos bo‘lgan yozuvlar.

1. Qaror vaqtiga mos grafni tiklash; kech kelgan yoki amal qilish muddati tugagan yozuvlarni hisobga olmaslik.

2. Bir manbaga tegishli xabarlarni guruhlash; farazni qo‘llovchi, unga qarshi va yetishmayotgan ma’lumotlarni ajratish.

3. φ belgilar vektorini tuzish va J mezonini tekshirish.

4. J = 0 bo‘lsa, ma’lumot yetishmasligi yoki ziddiyat sababini qayd etib, qo‘shimcha ma’lumot talab qilish.

5. J = 1 bo‘lsa, (1) formula orqali r ni hisoblash; r > τ bo‘lganda ogohlantirish berish.

6. Qaror bilan birga resurs, vaqt, manbalar va qo‘llangan model parametrlarini saqlash.

Tajriba usuli

Qiyoslash dasturda yaratilgan 680 ta epizodda bajarildi. Epizod bitta resursning 90 daqiqalik kuzatuvini ifodalaydi. Ssenariyda hodisa vaqti 60-daqiqa deb belgilandi. Hodisa yuz bergani yoki bermagani haqidagi natija 90-daqiqada ma’lum bo‘ladi, deb qabul qilindi. Qarorlar 15, 25, 35, 45 va 55-daqiqalarda olindi. Nazorat belgisi modeldan olinmagan: uni dastur yashirin holatga qarab tanlagan. Kuzatuvlar ham shu holat asosida yaratilgan.

Epizodlar vaqt tartibida 180, 80, 180, 80 va 160 ta kuzatuvdan iborat besh qismga ajratildi. Dastlabki model birinchi, qayta o‘qitilgan model uchinchi qismda o‘qitildi. Ularning qaror chegaralari to‘rtinchi qismda sozlandi; ikkinchi qism bu qiyosda ishlatilmadi. Bu tartib keyingi ma’lumotlarning oldingi qarorga ta’sir etishini cheklaydi [6]. O‘qitishda 100 qadam, 0,1 qadam uzunligi va model murakkabligini cheklash uchun 0,01 koeffitsiyent qo‘llandi.

Yangilanish davrida odatiy yuklama va trafik hajmi oshirildi, rad etilgan kirishlar kamaytirildi. 70-daqiqada kelgan CTI xabari oldingi qarorlarda ishlatilmadi. Sozlashdagi 38 ta tahdidsiz epizodning eng katta baholari o‘sish tartibida joylashtirildi; J = 0 nuqtalarda −1 qiymati olindi. Baholar $v_{(1)} \leq \ldots \leq v_{(n0)}$ bo‘lsa, qaror chegarasi quyidagicha tanlandi:

$$\tau = v_{n_0 - \lfloor \alpha n_0 \rfloor}, \quad n_0 = 38, \quad \alpha = 0{,}05. \quad (3)$$

r > τ shartida sozlash to‘plami uchun ko‘pi bilan 1 ta noto‘g‘ri ogohlantirishga yo‘l qo‘yildi. Dastlabki va qayta o‘qitilgan modellarning chegaralari 0,683101 va 0,694324 bo‘ldi; sinovda ular o‘zgartirilmadi. Sozlashdagi 5% mezon keyingi davrda ham shu darajadagi xato ulushini kafolatlamaydi.

Tajriba natijalari

Yakuniy sinovdagi 160 ta epizodning 92 tasi tahdidli, 68 tasi tahdidsiz deb belgilangan. Hodisadan 5–45 daqiqa oldin, ma’lumot yetarli bo‘lgan holatda ogohlantirish berilsa, tahdid aniqlangan deb hisoblandi. TP va FN mos ravishda aniqlangan va aniqlanmagan tahdidli epizodlar sonini, FP va TN esa noto‘g‘ri ogohlantirish berilgan va ogohlantirish berilmagan tahdidsiz

epizodlar sonini bildiradi. Qaror qamrovi C, erta aniqlash qamrovi R_e va noto‘g‘ri ogohlantirishlar ulushi FPR quyidagicha hisoblandi:

$$C = \frac{\sum_{i=1}^{N} \sum_{t \in D_i} J_{it}}{5N}, \quad R_e = \frac{TP}{TP + FN}; \qquad FPR = \frac{FP}{FP + TN}, \quad F_1 = \frac{2TP}{2TP + FP + FN}. \tag{4}$$

N - epizodlar soni, D_i - i-epizoddagi beshta qaror vaqti to‘plami. C - baholangan vaqt nuqtalari ulushi; R_e - aniqlangan tahdidli epizodlar ulushi. F_1 - ogohlantirishlar aniqligi va aniqlash qamrovining garmonik o‘rtachasi. Biror vaqtda ham qaror chiqarilmagan tahdidli epizodlar FN tarkibida qoldirildi. Faqat telemetriya va faqat graf modellari uchinchi qismdagi bir xil epizodlarda, dastlabki o‘nta va oxirgi oltita belgi asosida o‘qitilgan.

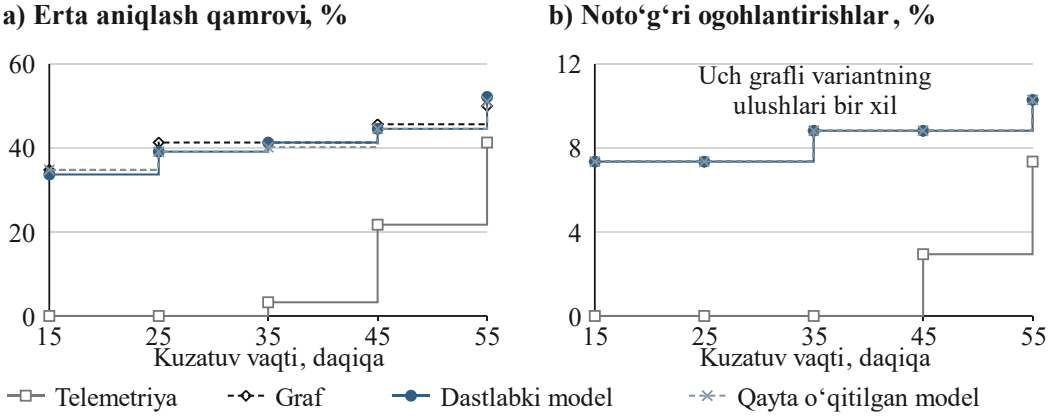
1-jadval.

Yakuniy sinovda modellarni qiyosiy baholash natijalari

Model	TP	FP	FN	C, %	R_e, %	FPR, %	F_1
Faqat telemetriya	38	5	54	100,00	41,30	7,35	0,563
Faqat graf	46	7	46	65,50	50,00	10,29	0,634
Dastlabki model	48	7	44	65,50	52,17	10,29	0,653
Qayta o‘qitilgan model	47	7	45	65,50	51,09	10,29	0,644

Graf ma’lumotlari qo‘shilgan modelda telemetriya modeliga nisbatan 9 ta ko‘proq tahdidli epizod aniqlangan, noto‘g‘ri ogohlantirishlar esa 2 taga ko‘paygan. Erta aniqlash qamrovi 41,30% dan 51,09% ga, FPR esa 7,35% dan 10,29% ga oshgan. Qo‘shimcha ogohlantirishlar ularni tekshirish yuklamasini ham oshiradi.

Dastlabki model 48 ta, qayta o‘qitilgan model 47 ta tahdidli epizodni aniqlagan. Erta aniqlash qamrovi farqi −1,09 foiz punkt bo‘lgan. Ikkala model uchun bir xil epizodlarni birgalikda 2 000 marta qayta tanlashda 95% ishonch oralig‘i [−3,41; 0,00] bo‘lgan. Har ikkala modelda 7 tadan noto‘g‘ri ogohlantirish bor.



2-rasm. Kuzatuv vaqtiga qarab ogohlantirish berilgan epizodlar ulushining o‘zgarishi

Natijalar muhokamasi

2-rasm ogohlantirishlar kuzatuvning qaysi vaqtida berilganini ko‘rsatadi. Qayta o‘qitilgan model 15-daqiqada 32 ta tahdidli epizod bo‘yicha ogohlantirish bergan. Faqat telemetriyaga asoslangan model bu vaqtda ogohlantirish bermagan. Biroq birlashtirilgan modelda shu vaqtda 5 ta noto‘g‘ri ogohlantirish ham qayd etilgan. Natijalarni baholashda ogohlantirish qanchalik erta

berilgani bilan birga noto‘g‘ri ogohlantirishlar soni ham hisobga olinishi kerak. Grafikdagi pog‘onalar belgilangan beshta kuzatuv vaqtiga mos keladi.

Graf ma’lumotlaridan foydalangan modellarda 800 ta vaqt nuqtasining 524 tasida qaror chiqarish uchun ma’lumot yetarli bo‘lgan. 119 ta epizodda kamida bir marta qaror chiqarilgan. Qolgan 41 ta epizod bo‘yicha ma’lumot yetishmagani sababli qaror chiqarilmagan. Ularning 10 tasi tahdidli deb belgilangan. Bu 10 ta epizod hisobdan chiqarilsa, qayta o‘qitilgan modelning aniqlash qamrovi 47/82 = 57,32% bo‘lib ko‘rinadi. Barcha tahdidli epizodlar hisobga olinganda esa natija 47/92 = 51,09% ni tashkil etadi. Shuning uchun qaror chiqarilmagan holatlarni baholashdan chiqarib tashlash mumkin emas.

Olingan natijalar qo‘llangan dasturiy ssenariy va tanlangan parametrlar bilan cheklangan. Bir epizoddagi beshta vaqt nuqtasi o‘zaro bog‘liq bo‘lgani uchun ishonch oralig‘ini hisoblashda alohida nuqtalar emas, butun epizodlar qayta tanlangan. 5–45 daqiqalik oldindan ogohlantirish vaqti ssenariyda belgilangan hodisaga nisbatan o‘lchangan.

Xulosa

Bilimlar grafi kuzatuvlarni resurs, manba va vaqt bo‘yicha bog‘lab, tahdid belgilarini ularning kuzatilish sharoiti bilan birga baholashga imkon beradi. Hisoblash tajribasida graf va tizim kuzatuvlarini birlashtirgan modelda faqat telemetriya modeliga nisbatan 9 ta ko‘proq tahdidli epizod aniqlangan. Bunda noto‘g‘ri ogohlantirishlar soni 2 taga ko‘paygan. Qayta o‘qitilgan model dastlabki modelga nisbatan 20%ga yaxshiroq natija ko‘rsatgan. Model sifatini baholashda aniqlash qamrovi bilan birga noto‘g‘ri ogohlantirishlar va ma’lumot yetishmasligi sababli qaror chiqarilmagan holatlarni ham hisobga olish zarur deb hisoblandi.

Foydalanilgan adabiyotlar

1. Tojimatov D.X. Kiber tahdidlarni bashorat qilish va xavf-xatarlardan himoyalanishda sun’iy intelekt imkoniyatlaridan foydalanish // Al-Farg‘oniy avlodlari. 2023. T. 1, № 2. B. 41–44. DOI: 10.5281/zenodo.7979307.

2. Tojimatov D., Ganiev A., Abdullin T. An Intelligent Proactive Cyber Threat Detection Model Based on Cyber Threat Intelligence and Machine Learning // Proceedings of the International Conference on Applied Innovations in IT. 2026. Vol. 14, No. 4. P. 1361–1367. DOI: 10.25673/125485.

3. Hogan A., Blomqvist E., Cochez M. va boshq. Knowledge Graphs // ACM Computing Surveys. 2021. Vol. 54, No. 4. Art. 71. P. 1–37. DOI: 10.1145/3447772.

4. Geifman Y., El-Yaniv R. Selective Classification for Deep Neural Networks // Advances in Neural Information Processing Systems. 2017. Vol. 30. arXiv:1705.08500.

5. Guo C., Pleiss G., Sun Y., Weinberger K.Q. On Calibration of Modern Neural Networks // Proceedings of Machine Learning Research. 2017. Vol. 70. P. 1321–1330.

6. Pendlebury F., Pierazzi F., Jordaney R., Kinder J., Cavallaro L. TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time // 28th USENIX Security Symposium. 2019. P. 729–746.

MOBIL OPERATORLARNING BIG DATA PLATFORMALARIDA FIRIBGARLIK VA KIBERHUJUMLARNI INTELLEKTUAL ANIQLASH USULLARI TAHLILI

Axmedova N.F.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada mobil operatorlarning Big Data platformalarida telekom firibgarligi va tarmoq kiberhujumlarini aniqlashga bag‘ishlangan 12 ta tadqiqot tahlil qilingan. Ishlar real telekom ma’lumotlaridan foydalanish, oqimli qayta ishlash, konsept driftga moslashish, abonentlar aloqa grafini hisobga olish, maxfiylikni saqlash va platformaning o‘zini himoyalash mezonlari bo‘yicha baholangan. Tahlil firibgarlikni aniqlash (CDR, graf neyron tarmoqlari) va tarmoq hujumlarini aniqlash yo‘nalishlari bir-biridan ajralgan holda rivojlanayotganini, oqimli rejim va driftga moslashish esa telekom ishlarida deyarli qo‘llanilmaganini ko‘rsatdi. Abonent darajasidagi vaqtinchalik geterogen grafga asoslangan yagona oqimli aniqlash arxitekturasiga o‘tish zarurati asoslangan.

Kalit so‘zlar: Big Data, mobil operator, telekom firibgarligi, CDR, SIM-box, graf neyron tarmoqlari, oqimli qayta ishlash, konsept drift, federativ o‘qitish, Apache Spark.

Аннотация. В статье проанализированы 12 исследований, посвящённых обнаружению телекоммуникационного мошенничества и сетевых кибератак на платформах больших данных мобильных операторов. Работы оценены по критериям использования реальных телеком-данных, потоковой обработки, адаптации к дрейфу концепций, учёта графа связей абонентов, сохранения конфиденциальности и защиты самой платформы. Анализ показал, что направления обнаружения мошенничества (CDR, графовые нейронные сети) и обнаружения сетевых атак развиваются обособленно, а потоковый режим и адаптация к дрейфу в телеком-работах практически не применяются. Обоснована необходимость перехода к единой потоковой архитектуре обнаружения на основе временного гетерогенного графа на уровне абонента.

Ключевые слова: большие данные, мобильный оператор, телекоммуникационное мошенничество, CDR, SIM-box, графовые нейронные сети, потоковая обработка, дрейф концепций, федеративное обучение, Apache Spark.

Kirish

Mobil aloqa operatorlari har kuni abonentlar faolligi haqida katta hajmdagi ma’lumotlarni hosil qiladi: qo‘ng‘iroq va SMS tafsilotlari yozuvlari (CDR), tarmoq oqimlari, billing va xizmat jurnallari. Bu ma’lumotlarni yig‘ish va qayta ishlash uchun Hadoop, Apache Spark, Apache Kafka kabi Big Data texnologiyalari qo‘llanadi. Ushbu platformalar bir vaqtning o‘zida ikki rolni bajaradi: ular xavfsizlik tahlili uchun ma’lumot manbai bo‘lib xizmat qiladi va o‘zi ham hujum nishoniga aylanadi.

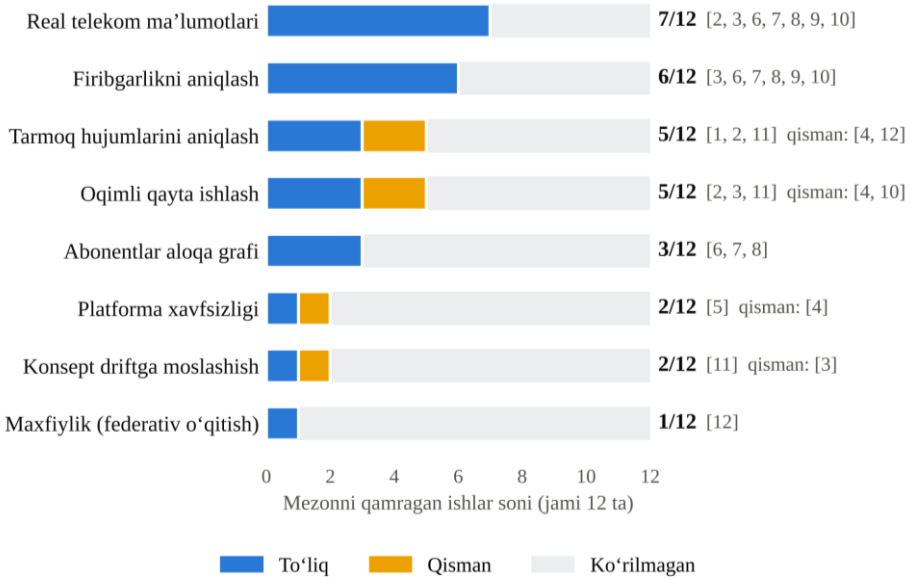
Operatorlarga eng ko‘p zarar keltiruvchi tahdidlardan biri – telekom firibgarligi. SIM-box firibgarligida xalqaro qo‘ng‘iroqlar VoIP–GSM shlyuzlari orqali mahalliy SIM-kartalarga yo‘naltiriladi va operator xalqaro trafik daromadidan mahrum bo‘ladi [9, 10]. Firibgar guruhlar esa vositachilar orqali ishlab, o‘zlarini oddiy abonentdek ko‘rsatadi, bu esa faqat individual xulq belgilariga tayanadigan usullarni samarasiz qiladi [6–8]. Shu bilan birga, tarmoq qatlamidagi hujumlar Big Data oqimlarida real vaqtga yaqin rejimda aniqlanishi talab etiladi [1, 2].

Mavjud tadqiqotlar bu muammolarni turli jamoalar va turli usullar bilan hal etadi. Maqolaning maqsadi – mobil operatorlar Big Data platformalarida firibgarlik va kiberhujumlarni intellektual aniqlash usullarini yagona mezonlar asosida tahlil qilish, ularning kuchli va zaif tomonlarini aniqlash hamda rivojlanish yo‘nalishlarini asoslash.

Tadqiqot metodologiyasi

Tahlil uchun 2016–2024-yillarda e’lon qilingan va uch guruhga kiruvchi 12 ta ish tanlandi: (1) Big Data muhitida tarmoq hujumlarini aniqlash [1, 2, 4, 11]; (2) CDR asosida telekom firibgarligini aniqlash [3, 6–10]; (3) Big Data platformaning o‘zini va maxfiylikni himoyalash [5, 12]. Manbalar ochiq ilmiy qidiruv tizimlari orqali izlandi; tanlangan ishlar Elsevier, IEEE, MDPI nashrlarida, arXiv platformasida hamda operatorlar ma’lumotlarida bajarilgan dissertatsiyalar repozitoriylarida e’lon qilingan.

Har bir ish sakkiz mezon bo‘yicha «to‘liq», «qisman» yoki «ko‘rilmagan» deb baholandi: real telekom ma’lumotlari; oqimli (real vaqtga yaqin) qayta ishlash; konsept driftga moslashish; abonentlar o‘rtasidagi aloqa grafini hisobga olish; maxfiylikni saqlovchi o‘qitish; tarmoq hujumlarini aniqlash; firibgarlikni aniqlash; Big Data platformaning o‘zini himoyalash. Baholash maqolalarning annotatsiyasi, metodika va natijalar bo‘limlari asosida amalga oshirildi; har bir mezonni qamragan ishlar soni va ularning raqamlari 1-rasmda keltirilgan.



1-rasm. Tahlil qilingan 12 ta ishning mezonlar bo‘yicha taqsimoti

Natijalar

Real telekom ma’lumotlarida bajarilgan yettita ishning asosiy tavsiflari 1-jadvalda keltirilgan.

1-jadval

Real telekom ma’lumotlari asosidagi ishlarning tavsifi

Ish	Ma’lumot	Usul / platforma	Natija	Cheklov
[2] Komisarek va b., 2022	Orange magistral tarmog‘i, NetFlow	Apache Spark + Kafka oqimi, bir nechta ML usuli	Real vaqtga yaqin oqimli aniqlash arxitekturasi	Faqat IP-oqim; firibgarlik yo‘q
[3] Shaeiri va b., 2019	Milliy SMS tarmog‘i, 1 oylik izlar	Xulq profili, xavf bali, Apache Spark	Me’yoriy xulqdan og‘ishni onlayn aniqlash	Statistik model; faqat SMS

Ish	Ma’lumot	Usul / platforma	Natija	Cheklov
[6] Hu va b., 2023	Ikkita real telekom to‘plami	GAT + xarajatga sezgir busting	Graf nomutanosibligi yumshatilgan	Statik graf; oflayn
[7] Hu va b., 2023	Ikkita ochiq real to‘plam	Kuchaytirilgan GNN + RL + AdaBoost	Oversmoothing va nomutanosiblikka bardosh	Tarmoq hujumlari yo‘q
[8] Gao va b., 2024	Real CDR to‘plamlari	GCN/GAT/GraphSAGE + AdaCost	Firibgar guruh yetakchilarini aniqlash	Oflayn o‘qitish
[9] Bouguettoucha, 2024	Djezzy operatori CDR	XGBoost + Tomek/RUS balanslash	SIM-box: aniqlik va precision 96 %	Bitta firibgarlik turi
[10] Fitsum, 2020	ethio telecom CDR	Sirpanuvchi oyna + RF, ANN, SVM	RF: aniqlik va kechikish muvozanati	SVM kechikishi 49 965 s

Birinchi muhim natija – yo‘nalishlarning ajralganligi. 1-rasmdan ko‘rinib turibdiki, firibgarlikni aniqlovchi oltita ishning [3, 6–10] birortasi tarmoq hujumlarini ko‘rib chiqmaydi, tarmoq hujumlarini aniqlovchi ishlar [1, 2, 11] esa firibgarlikni qamramaydi. Holbuki amalda bu tahdidlar bitta zanjirda kechishi mumkin: masalan, signalizatsiya orqali tasdiqlash kodini o‘z ichiga olgan SMS ushlab qolinib, keyinchalik moliyaviy firibgarlik uchun ishlatiladi.

Ikkinchi natija – graf usullarining samaradorligi va cheklovi. Firibgarlarni aniqlashda abonentlar aloqa grafiga asoslangan GNN usullari graf nomutanosibligi va oversmoothing muammolarini yumshatib, mavjud GNN detektorlaridan ustun natija ko‘rsatgan [6, 7]; ular firibgar guruh yetakchilari kabi bilvosita ishtirokchilarni ham aniqlay oladi [8]. Biroq uchala ishda ham graf statik deb qaraladi va model oflayn o‘qitiladi, ya’ni yangi qo‘ng‘iroqlar oqimida grafni yangilash masalasi ochiq qolgan.

Uchinchi natija – oqimli rejim va drift. Real vaqtga yaqin ishlov berish faqat [2, 3] da amalga oshirilgan; [10] da sirpanuvchi oyna yordamida aniqlash kechikishi bir soatgacha qisqartirilgan, SVM bilan esa kechikish 49 965 s ni tashkil etgan. Konsept driftga moslashish faqat telekom sohasiga tegishli bo‘lmagan [11] ishda chuqur o‘rganilgan: taklif etilgan onlayn geterogen ansambllar orasida Hoeffding adaptiv daraxti bilan birlashtirilgan variant konsept driftni yaxshiroq hisobga olib, eng yaxshi natija bergan. [3] da esa me’yoriy xulq profillari faqat normal yozuvlar bilan yangilanadi, bu driftga qisman moslashish hisoblanadi.

To‘rtinchi natija – platforma va maxfiylik. Big Data platformaning o‘ziga qaratilgan ichki hujumlarni aniqlash [5] da ko‘rib chiqilgan: Hadoop va Spark jarayonlarining tugunlararo o‘xshashligini tekshirish 3,28 % vaqt sarfi bilan amalga oshirilgan. [4] da Elastic Stack asosida xavfsizlik hodisalarini yig‘ish, saqlash va qayta ishlash tizimi taklif etilgan. Maxfiylikni saqlovchi federativ o‘qitish hujumlarni aniqlash uchun istiqbolli yo‘nalish sifatida [12] da tahlil qilingan, ammo tahlil qilingan telekom firibgarligi ishlarida qo‘llanilmagan.

Muhokama

Natijalar firibgarlik va kiberhujumlarni alohida tizimlarda aniqlash yondashuvi mobil operatorlar uchun yetarli emasligini ko‘rsatadi. Ikkala yo‘nalishning umumiy jihati shundaki, ularning izlari abonent atrofida to‘planadi: firibgarlik CDR grafida, signalizatsiya va tarmoq hujumlari esa abonent identifikatori bilan bog‘langan hodisalarda namoyon bo‘ladi. Shu sababli

abonentlar, qurilmalar va tarmoq elementlarini tugun, qo‘ng‘iroqlar, signalizatsiya xabarlari va seanslarni esa turli turdagi qirralar sifatida ifodalovchi vaqtinchalik geterogen graf ikki yo‘nalishni birlashtirish uchun tabiiy asos bo‘la oladi.

Bunday grafni Kafka va Spark/Flink oqimlarida qisman yangilab borish, GNN modellarini drift detektorlari yordamida qo‘shimcha o‘qitish va xarajatga sezgir o‘qitish orqali sinflar nomutanosibligini hisobga olish [6, 11] alohida ishlarda samarasi ko‘rsatilgan elementlarni yagona arxitekturaga birlashtiradi. Abonent identifikatorlarini platformaga kirishdayoq psevdonimlashtirish, mintaqaviy segmentlar yoki operatorlar o‘rtasida esa faqat model parametrlarini almashish (federativ o‘qitish) [12] shaxsga doir ma’lumotlar to‘g‘risidagi qonun talablariga muvofiqlikni ta’minlaydi [13].

Shu bilan birga, tahlil ayrim cheklovlarga ega: ishlarning bir qismi magistrlik dissertatsiyalari va preprintlar bo‘lib, natijalar turli to‘plam va metrikalarda olingan. Shu sababli miqdoriy ko‘rsatkichlarni bevosita taqqoslash mumkin emas va baholash sifat mezonlariga asoslangan.

Xulosa

Birinchidan, mobil operatorlar Big Data platformalarida firibgarlikni aniqlash va tarmoq hujumlarini aniqlash yo‘nalishlari bir-biridan ajralgan holda rivojlanmoqda: tahlil qilingan oltita firibgarlik ishining birortasi tarmoq hujumlarini qamramaydi. Ikkinchidan, abonentlar aloqa grafiga asoslangan GNN usullari firibgar guruhlarni aniqlashda samarali, biroq ular statik graf va oflayn o‘qitish bilan cheklangan. Uchinchidan, oqimli qayta ishlash, konsept driftga moslashish, maxfiylikni saqlovchi o‘qitish va platformaning o‘zini himoyalash telekom ishlarida kam yoki umuman qo‘llanilmagan. Keyingi tadqiqotlar abonent darajasidagi vaqtinchalik geterogen grafga asoslangan, oqimli, driftga moslashuvchan va shaxsga doir ma’lumotlarni himoyalovchi yagona aniqlash arxitekturasini ishlab chiqishga yo‘naltirilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. Hassan M.M., Gumaei A., Alsanad A., Alrubaian M., Fortino G. A hybrid deep learning model for efficient intrusion detection in big data environment // Information Sciences. – 2020. – Vol. 513. – P. 386–396. – DOI: 10.1016/j.ins.2019.10.069.

2. Komisarek M., Pawlicki M., Kowalski M., Marzecki A., Kozik R., Choraś M. Hunting cyberattacks: experience from the real backbone network // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2022. – Vol. 13, № 2. – P. 128–146.

3. Shaeiri Z., Kazemitabar J., Bijani Sh., Talebi M. Behavior-based online anomaly detection for a nationwide short message service // Journal of AI and Data Mining. – 2019. – Vol. 7, № 2. – P. 239–247.

4. Котенко И.В., Кулешов А.А., Ушаков И.А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. – 2017. – Вып. 5(54). – С. 5–34. – DOI: 10.15622/sp.54.1.

5. Aditham S., Ranganathan N. A system architecture for the detection of insider attacks in big data systems. arXiv preprint arXiv:1612.01587. – 2016.

6. Hu X., Chen H., Zhang J., Chen H., Liu S., Li X., Wang Y., Xue X. GAT-COBO: Cost-sensitive graph neural network for telecom fraud detection. arXiv preprint arXiv:2303.17334. – 2023.

7. Hu X., Chen H., Chen H., Li X., Zhang J., Liu S. Mining mobile network fraudsters with augmented graph neural networks // Entropy. – 2023. – Vol. 25, № 1. – Art. 150.

8. Gao P., Li Z., Zhou D., Zhang L. Reinforced cost-sensitive graph network for detecting fraud leaders in telecom fraud // IEEE Access. – 2024. – Vol. 12. – P. 173638–173646.

9. Bouguettoucha A.R. SIMBox fraud detection in telecommunication operators: a case study on «Djezzy»: master's thesis. – Guelma: University of Guelma, 2024.

10. Fitsum T. Near-real time SIM-box fraud detection using machine learning in the case of ethio telecom: master's thesis. – Addis Ababa: Addis Ababa University, 2020.

11. Martindale N., Ismail M., Talbert D.A. Ensemble-based online machine learning algorithms for network intrusion detection systems using streaming data // Information. – 2020. – Vol. 11, № 6. – Art. 315.

12. Agrawal S., Sarkar S., Aouedi O., Yenduri G., Piamrat K., Bhattacharya S., Maddikunta P.K.R., Gadekallu T.R. Federated learning for intrusion detection system: concepts, challenges and future directions. arXiv preprint arXiv:2106.09527. – 2021.

13. O'zbekiston Respublikasining «Shaxsga doir ma'lumotlar to'g'risida»gi Qonuni. – 2019-yil 2-iyul, O'RQ-547.

MOBIL OPERATORLARNING BIG DATA INFRATUZILMASIGA QARATILGAN KIBERHUJUMLAR TASNIFI VA QATLAMLI TAHDID MODELI

Axmedova N.F.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada mobil operatorlarning Big Data infratuzilmasiga qaratilgan kiberhujumlar ochiq e'lon qilingan hodisalar, faol foydalanilayotgan zaifliklar va ilmiy manbalar asosida tahlil qilingan. Radio kirish, signalizatsiya, paket yadro, Big Data platforma va xizmatlar qatlamlaridan iborat besh qatlamli tahdid modeli taklif etilgan; har bir qatlam uchun asosiy aktivlar, hujum turlari va aniqlash uchun ma'lumot manbalari belgilangan. Tahlil qilingan beshta holatdan uchtasi bevosita Big Data platforma qatlamiga taalluqli ekani, dastlabki kirish asosan o'g'irlangan hisob ma'lumotlari, sozlash xatolari va himoyalanmagan API orqali amalga oshirilishi hamda hujumlar qatlamlararo zanjir shaklida kechishi aniqlangan.

Kalit so'zlar: mobil operator, Big Data infratuzilmasi, kiberhujumlar tasnifi, tahdid modeli, hujum zanjiri, CDR, Hadoop, Apache Spark, signalizatsiya, shaxsga doir ma'lumotlar.

Аннотация. В статье проанализированы кибератаки на инфраструктуру больших данных мобильных операторов на основе публично раскрытых инцидентов, активно эксплуатируемых уязвимостей и научных источников. Предложена пятиуровневая модель угроз, включающая уровни радиодоступа, сигнализации, пакетного ядра, платформы больших данных и сервисов; для каждого уровня определены основные активы, типы атак и источники данных для обнаружения. Установлено, что три из пяти рассмотренных случаев непосредственно относятся к уровню платформы больших данных, первоначальный доступ преимущественно осуществляется с помощью похищенных учётных данных, ошибок конфигурации и незащищённых API, а атаки развиваются в виде межуровневых цепочек.

Ключевые слова: мобильный оператор, инфраструктура больших данных, классификация кибератак, модель угроз, цепочка атак, CDR, Hadoop, Apache Spark, сигнализация, персональные данные.

Kirish

Mobil aloqa operatorlari abonentlar faolligi to'g'risidagi ma'lumotlarning eng yirik egalaridan biri hisoblanadi. Qo'ng'iroq va SMS tafsilotlari yozuvlari (CDR), joylashuv, signalizatsiya va billing ma'lumotlari Kafka, HDFS, Spark kabi Big Data platformalarida, so'nggi yillarda esa bulutli ma'lumot omborlarida ham to'planadi. Bu ma'lumotlar bir joyda jamlangani sababli Big Data infratuzilmasi hujumchilar uchun eng qimmatli nishonlardan biriga aylanmoqda.

Real hodisalar buni tasdiqlaydi. 2024-yilda AT&T operatorining uchinchi tomon bulutli platformasidagi ish maydoniga o'g'irlangan hisob ma'lumotlari bilan kirilib, deyarli barcha simsiz aloqa mijozlarining 2022-yil may–oktyabr oylaridagi qo'ng'iroq va SMS yozuvlari, ularning bir qismida esa baza stansiyasi identifikatorlari ham o'g'irlangan [1, 2]. O'zbekistonda Kiberxavfsizlik markazining 2021-yil hisobotiga ko'ra, aniqlangan zararli faollikning 36 foizi mobil operatorlar abonentlariga to'g'ri kelgan [3], 2026-yil fevralda esa mahalliy operatorlardan birining test serveriga ruxsatsiz kirish holati rasman tasdiqlangan [4].

Mavjud tadqiqotlar operator infratuzilmasining alohida qismlariga – signalizatsiya protokollari [5], paket yadro [6, 7], telekom firibgarligi [8] yoki Big Data platformalarining ichki

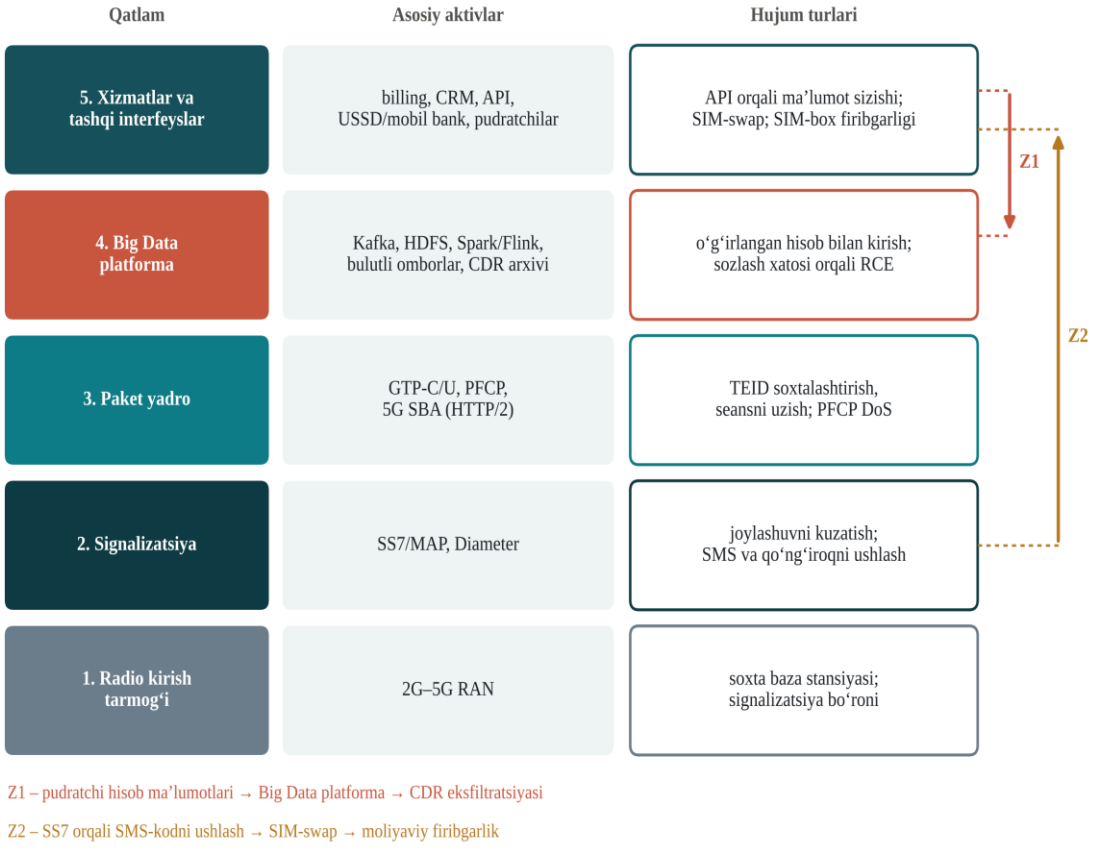
xavfsizligiga [9] – qaratilgan. ENISA tomonidan Big Data tahdidlarining umumiy landshafti tayyorlangan [10], biroq u telekom sohasining o‘ziga xos qatlamlari bilan bog‘lanmagan. Hadoop va Spark bo‘yicha 2026-yilgi tizimli sharhda tanlangan 46 ta maqoladan faqat to‘rttasi bu platformalarda penetratsion testlarni amalda qo‘llagani qayd etilgan [11]. Natijada operator infratuzilmasini yaxlit qamrovchi va real hodisalarga tayangan tahdid modeli mavjud emas.

Maqolaning maqsadi – mobil operatorlar Big Data infratuzilmasiga qaratilgan kiberhujumlarni real hodisalar va ilmiy manbalar asosida tasniflash hamda qatlamlararo hujum zanjirlarini hisobga oluvchi tahdid modelini ishlab chiqish.

Tadqiqot metodologiyasi

Tadqiqot ikki turdagi manbalarga tayanadi: (1) ochiq e’lon qilingan hodisalar va zaifliklar – operatorlar ma’lumotlarining sizishi, Big Data platformalariga qarshi hujum kampaniyalari va faol foydalanilayotgan deb tasniflangan zaifliklar [1, 2, 4, 12–14]; (2) signalizatsiya, paket yadro, firibgarlik va Big Data xavfsizligi bo‘yicha ilmiy maqolalar hamda ENISA hisobotlari [5–11, 15]. Har bir hodisa uchun nishonga olingan qatlam, dastlabki kirish vektori, zarar ko‘rgan aktivlar va oqibatlar aniqlandi.

Modelni qurishda mobil tarmoqning funksional bo‘linishi (radio kirish, signalizatsiya, paket yadro, xizmatlar) asos qilib olindi va unga ma’lumotlarni yig‘ish, saqlash va qayta ishlash vazifasini bajaruvchi Big Data platforma qatlami alohida qo‘shildi. Har bir qatlam uchun asosiy aktivlar, xarakterli hujum turlari va hujumni aniqlash uchun zarur ma’lumot manbalari belgilandi, qatlamlar o‘rtasidagi bog‘liqlik esa hujum zanjirlari sifatida ifodalandi. Natijaviy model 1-rasmda keltirilgan.



1-rasm. Mobil operator Big Data infratuzilmasining besh qatlamli tahdid modeli va qatlamlararo hujum zanjirlari

Natijalar

Tahlil qilingan hodisalar va zaifliklar modelning qatlamlari bo‘yicha 1-jadvalda umumlashtirilgan.

1-jadval

Mobil operatorlar Big Data infratuzilmasiga taalluqli hodisalar va zaifliklar tahlili

Hodisa / zaiflik	Qatlam	Dastlabki kirish vektori	Zarar ko‘rgan aktivlar	Oqibat
AT&T, 2024 [1, 2]	4 – Big Data (bulutli ombor)	Pudratchi orqali o‘g‘irlangan hisob ma’lumotlari	Qo‘ng‘iroq va SMS yozuvlari, baza stansiyasi ID	Deyarli barcha simsiz mijozlar (~110 mln)
Optus, 2022 [13]	5 – Xizmatlar (API)	OAV ma’lumotiga ko‘ra, autentifikatsiyasiz API nuqtasi	Ism, tug‘ilgan sana, telefon, hujjat raqamlari	Joriy va sobiq mijozlar ma’lumoti sizgan
Mobiuz, 2026 [4]	Test serveri (asosiy tizimlardan ajratilgan)	Test serveriga ruxsatsiz kirish	Asosiy tizimlarga ta’sir qayd etilmagan	Server izolyatsiya qilingan
Hadoop YARN, Flink, 2024 [12]	4 – Big Data platforma	Sozlash xatosi: autentifikatsiyasiz RCE	Klasterning hisoblash resurslari	Kriptomayner, rootkitlar, cron orqali saqlanish
CVE-2022-33891 [14]	4 – Spark veb-interfeysi	ACL yoqilganda buyruq inyeksiyasi	Spark ishlayotgan hisob	CVSS 8,8; CISA faol foydalanilayotgan zaifliklar ro‘yxatida

Birinchi muhim natija – Big Data platforma qatlamining markaziy o‘rni. Tahlil qilingan beshta holatdan uchtasi [1, 12, 14] bevosita Big Data platforma qatlamiga taalluqli. Bu qatlamda boshqa barcha qatlamlardan keladigan ma’lumotlar jamlangani uchun uning bitta kompрometatsiyasi butun abonentlar bazasi bo‘yicha signalizatsiya va CDR ma’lumotlarining oshkor bo‘lishiga olib keladi: AT&T holatida o‘g‘irlangan yozuvlar deyarli barcha simsiz aloqa mijozlarini qamragan, baza stansiyasi identifikatorlari esa abonentlarning taxminiy joylashuvini aniqlash imkonini bergan [1, 2].

Ikkinchi natija – dastlabki kirish vektorlarining xarakteri. Murakkab nol kunlik zaifliklar o‘rniga o‘g‘irlangan hisob ma’lumotlari [1], noto‘g‘ri sozlangan servislar [12] va himoyalanmagan API [13] ustunlik qiladi. Hadoop YARN ResourceManager va Flink’dagi sozlash xatolari autentifikatsiyasiz masofaviy kod bajarishga imkon bergan, hujumchilar esa kriptomayner va ikkita rootkit o‘rnatib, cron vazifasi orqali tizimda saqlanib qolgan [12]. Spark’dagi CVE-2022-33891 zaifligi (CVSS 8,8) CISA tomonidan faol foydalanilayotgan zaifliklar ro‘yxatiga kiritilgan [14]. ENISA ma’lumotlariga ko‘ra, 2024-yilda Yevropa Ittifoqida telekom sohasida 188 ta xavfsizlik hodisasi qayd etilgan bo‘lib, ularning 19 foizi inson xatosi, 8 foizi esa zararli harakatlar bilan bog‘liq; uchinchi tomon nosozliklari bilan bog‘liq hodisalar ham sezilarli ulushni tashkil etgan [15].

Uchinchi natija – qatlamlararo hujum zanjirlari. Hodisalar bitta qatlam bilan cheklanmaydi. Z1 zanjirida pudratchining hisob ma’lumotlari (xizmatlar qatlami) Big Data platformaga kirish va CDR yozuvlarini eksfiltratsiya qilish uchun ishlatilgan [1]. Z2 zanjirida esa SS7 orqali SMS

xabarlarini ushlab qolish [5] tasdiqlash kodlarini qo‘lga kiritish, keyingi bosqichda SIM-kartani almashtirish va moliyaviy firibgarlik uchun xizmat qilishi mumkin.

To‘rtinchi natija – aniqlash uchun ma’lumot manbalari. Har bir qatlam o‘ziga xos telemetriya hosil qiladi: signalizatsiya qatlamida MAP va Diameter xabarlari, paket yadroda GTP va PFCP oqimlari, Big Data platformada audit jurnallari va so‘rovlar tarixi, xizmatlar qatlamida esa API va billing jurnallari. Biroq tahlil qilingan ilmiy ishlarda bu manbalar asosan alohida ko‘rib chiqiladi [5–9], platforma qatlamining o‘zi bo‘yicha amaliy xavfsizlik baholashlari esa juda kam [11].

Muhokama

Taklif etilgan model mavjud yondashuvlardan Big Data platformani tarmoq qatlamlari qatorida alohida qatlam sifatida ajratishi va qatlamlar o‘rtasidagi hujum zanjirlarini ko‘rsatishi bilan farq qiladi. Bu, birinchidan, xavfsizlik nazoratini tarmoq chegarasidan ma’lumotlar to‘planadigan joyga ko‘chirish zarurligini ko‘rsatadi: uchinchi tomon va pudratchilar hisoblari uchun ko‘p omilli autentifikatsiya, eng kam imtiyoz tamoyili hamda platformadagi barcha so‘rovlar va eksport amallarini audit qilish talab etiladi.

Ikkinchidan, hujum zanjirlarini aniqlash uchun turli qatlamlar telemetriyasini abonent identifikatori bo‘yicha korrelyatsiyalash kerak. Masalan, signalizatsiya qatlamidagi shubhali joylashuv so‘rovi va undan keyin xizmatlar qatlamida kelgan SIM-kartani almashtirish so‘rovi alohida qaralganda oddiy hodisa bo‘lib ko‘rinadi, birgalikda esa yuqori xavfli zanjirni tashkil etadi. Platformada saqlanadigan CDR va joylashuv ma’lumotlari shaxsga doir ma’lumotlar hisoblangani sababli bunday korrelyatsiya psevdonimlashtirilgan identifikatorlar ustida bajarilishi lozim; O‘zbekistonda bu talablar tegishli qonun bilan [17], operator infratuzilmasini himoyalash esa “Kiberxavfsizlik to‘g‘risida”gi qonun [16] bilan tartibga solinadi.

Tadqiqot ayrim cheklovlarga ega: tahlil ochiq e’lon qilingan hodisalarga asoslangan, operatorlar esa ko‘plab hodisalarni oshkor qilmaydi; ayrim holatlarda (masalan, [13]) hujum usuli rasman tasdiqlanmagan. Shu sababli model kelajakda operatorlarning ichki hodisalar ma’lumotlari asosida tasdiqlanishi zarur.

Xulosa

Birinchidan, mobil operatorlar Big Data infratuzilmasiga qaratilgan hujumlarni tasniflash uchun radio kirish, signalizatsiya, paket yadro, Big Data platforma va xizmatlar qatlamlaridan iborat besh qatlamli tahdid modeli taklif etildi; har bir qatlam uchun asosiy aktivlar, hujum turlari va aniqlash uchun ma’lumot manbalari belgilandi. Ikkinchidan, tahlil qilingan beshta holatdan uchtasi bevosita Big Data platforma qatlamiga taalluqli bo‘lib, bu qatlam barcha qatlamlar ma’lumotlari jamlanadigan va bitta kompрometatsiya butun abonentlar bazasini oshkor qiladigan nuqta ekani ko‘rsatildi. Uchinchidan, dastlabki kirish asosan o‘g‘irlangan hisob ma’lumotlari, sozlash xatolari va himoyalanmagan API orqali amalga oshirilishi hamda hujumlar qatlamlararo zanjir shaklida kechishi aniqlandi. Keyingi tadqiqotlar turli qatlamlar telemetriyasini psevdonimlashtirilgan abonent identifikatori bo‘yicha korrelyatsiyalovchi intellektual aniqlash usullarini ishlab chiqishga yo‘naltirilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. AT&T confirms data breach affecting nearly all wireless customers // The Hacker News. – 13.07.2024. – URL: https://thehackernews.com/2024/07/at-confirms-data-breach-affecting.html

2. AT&T details massive breach of customers’ call and text logs // BankInfoSecurity. – 2024. – URL: https://www.bankinfosecurity.net/att-details-massive-breach-subscribers-call-logs-a-25754

3. Kiberxavfsizlik markazining 2021-yil hisoboti // Spot.uz. – 03.03.2022. – URL: https://www.spot.uz/ru/2022/03/03/cybersec-2021/

4. Mobiuz ham kiberhujumga uchragan. Kompaniya mijozlar ma’lumotlari sizib chiqmaganini ma’lum qildi // Kun.uz. – 17.02.2026. – URL: https://kun.uz/news/2026/02/17/mobiuz-ham-kiberhujumga-uchragan-kompaniya-mijozlar-malumotlari-sizib-chiqmaganini-malum-qildi

5. Guo Y., Ermis O., Tang Q., Trang H., De Oliveira A. An empirical study of deep learning-based SS7 attack detection // Information. – 2023. – Vol. 14, № 9. – Art. 509.

6. Park S., Kim S., Son K., Kim H., Park J., Yim K. Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment // International Journal of Web and Grid Services. – 2017. – Vol. 13, № 1.

7. Amponis G., Radoglou-Grammatikis P., Lagkas T., Mallouli W., Cavalli A., Klonidis D., Markakis E., Sarigiannidis P. Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications // EURASIP Journal on Wireless Communications and Networking. – 2022. – DOI: 10.1186/s13638-022-02204-5.

8. Gao P., Li Z., Zhou D., Zhang L. Reinforced cost-sensitive graph network for detecting fraud leaders in telecom fraud // IEEE Access. – 2024. – Vol. 12. – P. 173638–173646.

9. Aditham S., Ranganathan N. A system architecture for the detection of insider attacks in big data systems. arXiv preprint arXiv:1612.01587. – 2016.

10. Big Data Threat Landscape. – European Union Agency for Cybersecurity (ENISA), 2016.

11. Barata L., Martins F., Lopes E. Penetration testing in big data frameworks: a systematic review of security assessment for Hadoop and Spark // Revista de Informática Teórica e Aplicada. – 2026. – Vol. 33, № 3. – P. 45–58.

12. Cryptominers targeting misconfigured Apache Hadoop and Flink with rootkit in new attacks // The Hacker News. – 12.01.2024. – URL: https://thehackernews.com/2024/01/cryptominers-targeting-misconfigured.html

13. Hacker behind Optus breach releases 10,200 customer records in extortion scheme // The Hacker News. – 27.09.2022. – URL: https://thehackernews.com/2022/09/hacker-behind-optus-breach-releases.html

14. CVE-2022-33891: Apache Spark shell command injection vulnerability via Spark UI. – 2022. – URL: https://cve.circl.lu/cve/CVE-2022-33891

15. Telecom Security Incidents 2024. – European Union Agency for Cybersecurity (ENISA), 2025.

16. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni. – 2022-yil 15-aprel, O‘RQ-764.

17. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. – 2019-yil 2-iyul, O‘RQ-547.

HONEYPOT TIZIMLARIDA TARMOQ TRAFIGINI QAYTA ISHLASH VA FINGERPRINTINGGA CHIDAMLILIK

Qurbonaliyeva D.V.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada honeypotlarning tarmoq pog‘onasida trafikni qabul qilish va unga javob shakllantirish masalalari tahlil qilinadi. Paketni qabul qilish usullari, stateless va stateful javob generatsiyasi hamda TCP/IP stek parametrlarining fingerprinting vositalariga ta’siri ko‘rib chiqiladi. 2026-yilda chop etilgan reaktiv tarmoq teleskopi yondashuvi tahlil asosi sifatida olinadi. Uning holat jadvali yuklamasi ochiq ko‘rsatkichlar bo‘yicha hisoblanadi. Javobning profil, taqsimot va vaqt xulqini birgalikda tekshiradigan baholash mezoni taklif etiladi.

Kalit so‘zlar: honeypot, tarmoq pog‘onasi, TCP/IP stek, fingerprinting, reaktiv tarmoq teleskopi, paketni qayta ishlash, aldovchi tizimlar.

Аннотация. В статье анализируются вопросы приёма сетевого трафика и формирования ответов в ханипотах на сетевом уровне. Рассматриваются способы приёма пакетов, генерация ответов без сохранения и с сохранением состояния, а также влияние параметров стека TCP/IP на средства фингерпринтинга. В качестве основы анализа принят подход реактивного сетевого телескопа, опубликованный в 2026 году. Нагрузка на таблицу состояний рассчитана по открытым показателям. Предложен критерий оценки, одновременно проверяющий профиль, распределение и временное поведение ответа.

Ключевые слова: ханипот, сетевой уровень, стек TCP/IP, фингерпринтинг, реактивный сетевой телескоп, обработка пакетов, системы обмана.

Kirish

Honeypot hujumchi bilan birinchi marta tarmoq pog‘onasida uchrashadi. Skaner ilova bilan gaplashishdan oldin paketning TTL qiymatini, TCP oynasini va opsiyalar tartibini o‘qiydi. Shuning uchun servis emulyatsiyasi mukammal bo‘lsa ham, tarmoq pog‘onasidagi nomuvofiqlik tizimni fosh qiladi [1]. Ilova pog‘onasi bo‘yicha ishlar ko‘p. Trafikni qabul qilish va javob qaytarish mexanizmlari esa kamroq tizimlashtirilgan.

Maqolaning maqsadi shu mexanizmlarni tahlil qilish va 2026-yilda chop etilgan reaktiv tarmoq teleskopi yondashuvini [2] honeypotning qabul qilish qatlamiga tadbiq etish shartlarini aniqlashdir. Tadqiqot to‘rtta savolga javob izlaydi. Paket honeypotga qanday yetib keladi? Javob qaysi darajada shakllanadi? Javob qaysi parametrlar bo‘yicha aniqlanadi? Holatni saqlash qancha resurs talab qiladi?

Asosiy qism

Qabul qilish qatlami uchta vazifani bajaradi. U paketni interfeysdan oladi, tasniflaydi va javob generatoriga uzatadi. Qabul qilish usuli unumdorlikni va sarlavha maydonlarini boshqarish darajasini belgilaydi (1-jadval). Ajratilgan manzil maydonida qabul qilish masalasi marshrutlash orqali hal bo‘ladi. SDN yondashuvida esa trafik hujumchi aniqlangandan keyin talab bo‘yicha yo‘naltiriladi. TCP seansi uzilmasligi uchun sequence-number siljitiladi [3].

Javob generatsiyasi ikki rejimda ishlaydi. Stateless rejimda har bir paketga alohida javob qaytariladi. Xotira sarfi minimal bo‘ladi, ammo javob faqat joriy paketga tayanadi va seans tarixi hisobga olinmaydi. Stateful rejimda ulanish holati saqlanadi. Bu hujumchi yuborgan yukni qabul

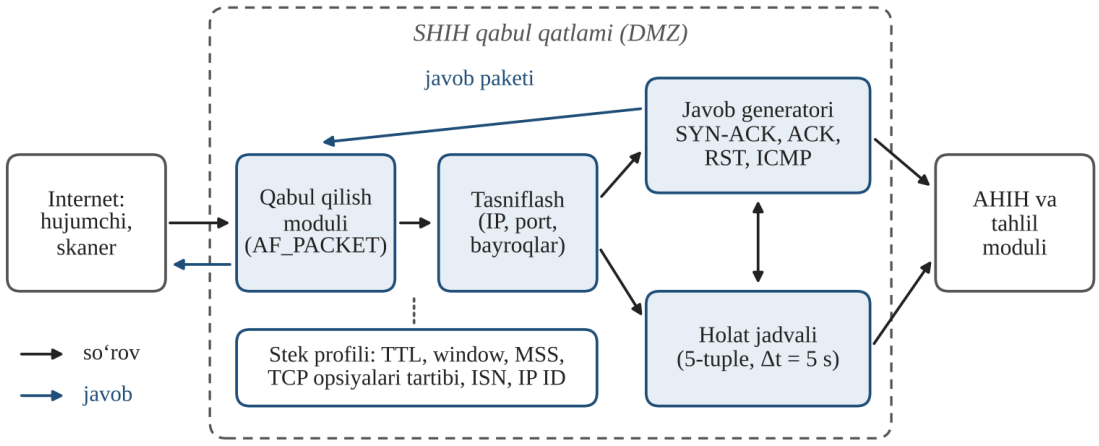
qilishga imkon beradi. Spoki tizimi SYN paketlariga javob qaytaradi va handshake'ni yakunlaydi [4]. Singh va boshqalar uni kengaytirib, handshake'dan keyingi segmentlarni ham tasdiqlaydi [2].

1-jadval.

Trafikni qabul qilish usullarining taqqoslanishi

Usul	Ishlov joyi	Afzalligi	Cheklovi
AF_PACKET (xom soket)	Foydalanuvchi maydoni	Sarlavha maydonlarini to‘liq boshqarish. Tez prototip	Yuqori tezlikda paket yo‘qotilishi mumkin
NFQUEUE	Netfilter navbati	Yadro filtri bilan oson integratsiya	Har paketga kontekst almashinuvi. Masshtab cheklangan
XDP/eBPF	Drayver darajasi	Eng kam kechikish, yuqori o‘tkazish qobiliyati	Dasturlash va nosozlikni topish murakkab
SDN (OpenFlow)	Kommutator va kontroller	Trafikni talab bo‘yicha yo‘naltirish	Kontroller kechikishi. Murakkab sozlash

Tizim barcha TCP portlariga SYN-ACK qaytaradi va ulanish holatini $\Delta t = 5$ s saqlaydi (1-rasm, 2-rasm a). Servis emulyatsiyasi ishlatilmaydi. Javob interfeys darajasida shakllantiriladi, yadroning TCP/IP stekiga tayanish minimal bo‘ladi. Muallif 209 ta manzilli /24 blokda kuniga taxminan 7 mln muvaffaqiyatli handshake qayd etgan [2].



1-rasm. SHIH qabul qatlamining tarmoq pog‘onasidagi tuzilmasi

Hujumchi javobni parametrlar bo‘yicha tekshiradi. p0f boshlang‘ich TTL, MSS, TCP opsiyalari tartibi va oyna o‘lchamini o‘qiydi [8]. Nmap faol TCP sinovlari bilan, Xprobe2 esa ICMP javoblari bilan operatsion tizimni aniqlaydi [1, 7]. Honeyd shaxsiyat (personality) mexanizmi orqali bu sinovlardan o‘tishga urinadi [6]. Vaqt bo‘yicha farq ham aniqlash belgisiga aylanadi. Simulyatsiya qilingan tizimlar ICMP so‘roviga sekinroq javob beradi. Bu belgi Honeyd'ni aniqlashda ishlatilgan [5]. 2-jadvalda parametrlar va javob generatoriga qo‘yiladigan talablar jamlangan.

2-jadval

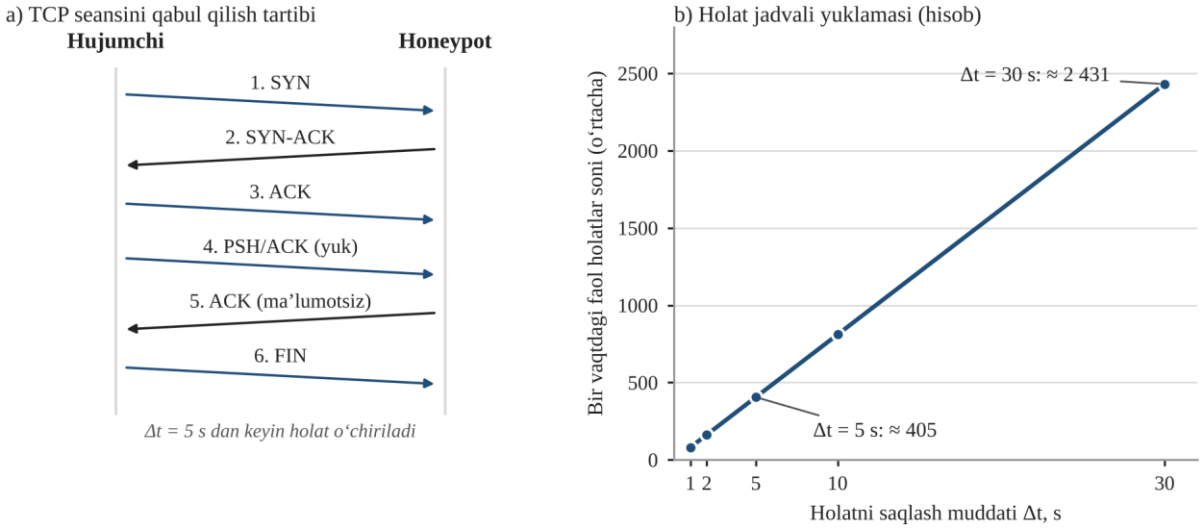
Tarmoq pog‘onasidagi fingerprinting parametrlari

Parametr	Pog‘ona	Vosita	Javob generatoriga talab

Boshlang‘ich TTL	IP	p0f, Nmap	Tanlangan OT profiliga mos. Topologiyada hop soniga qarab kamayadi
Oyna o‘lchami va MSS	TCP	p0f, Nmap	Profil qiymatlari bilan bir xil
TCP opsiyalari tartibi (MSS, SACK, WS, TS, NOP)	TCP	p0f, Nmap	Profildagi aniq tartibni saqlash
Boshlang‘ich ketma-ketlik raqami (ISN)	TCP	Nmap	Profil taqsimotiga mos tasodifiylik
IP ID ketma-ketligi	IP	Nmap	Profil qonuniyatiga mos hisoblagich
ICMP javoblari	ICMP	Xprobe2, Nmap	Xato xabarlari profilga mos
RTT va jitter	Vaqt	Taqqoslash tahlili	Haqiqiy host taqsimotiga yaqin kechikish

Javobning haqiqiy hostdan farqini bitta mezon bilan baholash uchun muallifning avvalgi ishlaridagi $H(t) \in P \cap D \cap T$ shartidan foydalanish mumkin. Bu yerda P stek profiliga, D paket atributlarining taqsimotiga, T vaqt xulqiga mosligini bildiradi. Tarmoq pog‘onasida P parametrlari 2-jadvalning dastlabki to‘rt qatoridan, D ISN va IP ID taqsimotlaridan, T RTT va jitterdan tuziladi. Aniqlanish ehtimoli P_{det} shu uch shartdan kamida bittasi buzilgan sinovlar ulushi sifatida hisoblanadi.

Holat jadvali hajmi Little qonuni bilan baholanadi: $N = \lambda \cdot \Delta t$. Bu yerda λ ulanishlarning kelish tezligi, Δt holatni saqlash muddati. Ish [2] da kuniga taxminan 7 mln ulanish keltirilgan. Bu o‘rtacha $\lambda \approx 81$ ulanish/s degani. $\Delta t = 5$ s bo‘lganda bir vaqtda taxminan 405 ta holat saqlanadi. $\Delta t = 30$ s bo‘lsa, bu son 2431 gacha oshadi (2-rasm b). Hisob o‘rtacha yuklama uchun bajarilgan. Har bir ulanish holatni to‘liq Δt davomida ushlab turadi deb olingan. Haqiqatda FIN bilan yopilgan ulanishlar holatni oldinroq bo‘shatadi, shuning uchun natija yuqori baho hisoblanadi. Eng yuqori (burst) yuklama alohida o‘lchanishi kerak.



2-rasm. a) TCP seansini qabul qilish tartibi [2]; b) holat jadvali yuklamasining Δt ga bog‘liqligi ($\lambda \approx 81$ ulanish/s, hisob)

Ish [2] da javob parametrlari faqat protokolga mos deb ta’riflanadi. TTL, oyna o‘lchami va opsiyalar tartibining tanlangan OT profiliga moslashtirilgani haqida ma’lumot berilmagan.

Fingerprinting vositalariga qarshi chidamlilik ham o‘lchanmagan. Shu sababli bunday qabul qilish qatlami honeypotga ulanganda 2-jadvaldagi parametrlar alohida sozlanishi va Nmap, p0f hamda Xprobe2 bilan tekshirilishi kerak. Eksperimental baholash keyingi bosqich vazifasi.

Xulosa

Honeypotning tarmoq pog‘onasidagi qabul qilish va javob qatlami uning aniqlanish ehtimolini belgilaydi. Reaktiv teleskop yondashuvi servis emulyatsiyasiz keng qamrovli qabul qilishni ta’minlaydi. $\Delta t = 5$ s da holat jadvali o‘rtacha 405 ta yozuvdan iborat bo‘ladi. Bunday jadval xotira nuqtai nazaridan muammo tug‘dirmaydi. Biroq javob parametrlari tanlangan OT profiliga moslashtirilmasa, qatlam Nmap va p0f sinovlarida fosh bo‘lishi mumkin. Keyingi ishda profil, taqsimot va vaqt shartlarini birga tekshiradigan baholash o‘tkaziladi.

Foydalanilgan adabiyotlar:

1. Chaudhry A., Andersen C., Choudhary G., Dragoni N. A Review of Honeypots: Fingerprinting Techniques, Detection, and Evasion Mechanisms // Future Internet. 2026. Vol. 18, No. 4. Art. 190.

2. Singh A., Yadav K.S., Kumar V.A., Ghosh S., Baro P., Prasanth B.B. A Longitudinal Measurement Study of Log4Shell Exploitation from a Reactive Network Telescope // arXiv:2601.04281v2. 2026.

3. Beltrán-López P., Gil Pérez M., Vasilomanolakis E., Nespoli P. Reactive cyber deception: Stealth-based adaptive redirection to on-demand honeypots with AI-driven data generation // Computer Networks. 2026. Vol. 281. Art. 112203.

4. Hiesgen R., Nawrocki M., King A., Dainotti A., Schmidt T.C., Wählisch M. Spoki: Unveiling a New Wave of Scanners through a Reactive Network Telescope // 31st USENIX Security Symposium. 2022. P. 431–448.

5. Bridges R.A., Mitchell T.R., Muñoz M., Henriksson T. SoK: Honeypots & LLMs, More Than the Sum of Their Parts? // arXiv:2510.25939. 2026.

6. Provos N. A Virtual Honeypot Framework // 13th USENIX Security Symposium. 2004.

7. Lyon G. Nmap Network Scanning. Remote OS Detection. https://nmap.org/book/osdetect.html

8. Zalewski M. p0f v3: README. https://lcamtuf.coredump.cx/p0f3/README

FISHING HUJUMLARINI ANIQLASHNING ZAMONAVIY TEXNOLOGIYALARI VA VOSITALARI TAHLILI

Qurbonaliyeva D.V.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada fishing hujumlarini aniqlashning zamonaviy texnologiyalari va vositalari tahlil qilinadi. Qora ro‘yxatlarga asoslangan usullar, URL manzillarini evristik tahlil qilish, mashina o‘rganishi algoritmlari hamda gibrid yondashuvlarning ishlash tamoyillari, afzalliklari va cheklovlari ko‘rib chiqiladi. Shuningdek, elektron pochta orqali amalga oshiriladigan fishing hujumlarini aniqlashda SPF, DKIM va DMARC protokollarining o‘rni, URL xususiyatlarini baholash hamda anti-phishing monitoring tizimlaridan foydalanish imkoniyatlari yoritiladi. Tahlil natijasida fishing hujumlarini samarali aniqlashda turli texnologiyalarni kompleks qo‘llashning ahamiyati asoslanadi.

Kalit so‘zlar: fishing hujumlari, kiberxavfsizlik, fishingni aniqlash, URL tahlili, mashina o‘rganishi, evristik tahlil, elektron pochta xavfsizligi, SPF, DKIM, DMARC, anti-phishing tizimlari.

Аннотация. В статье рассматриваются современные технологии и программные средства обнаружения фишинговых атак. Анализируются принципы работы, преимущества и ограничения методов, основанных на черных списках, эвристическом анализе URL-адресов, алгоритмах машинного обучения и гибридных подходах. Особое внимание уделяется применению протоколов SPF, DKIM и DMARC для проверки подлинности отправителей электронной почты, анализу характеристик URL-адресов и возможностям систем мониторинга антифишинговых угроз. Обобщаются особенности применения различных технологий и обосновывается целесообразность их комплексного использования для повышения эффективности обнаружения фишинговых атак.

Ключевые слова: фишинговые атаки, кибербезопасность, обнаружение фишинга, анализ URL, машинное обучение, эвристический анализ, безопасность электронной почты, SPF, DKIM, DMARC, антифишинговые системы.

Kirish

Hozirgi vaqtda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi hamda raqamli xizmatlardan foydalanish ko‘lamining kengayishi kiberxavfsizlik bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Ushbu tahdidlar orasida fishing hujumlari alohida o‘rin egallaydi. Fishing foydalanuvchilarni aldash orqali ularning login va parollari, bank kartasi ma’lumotlari hamda boshqa maxfiy axborotlarini qo‘lga kiritishga qaratilgan ijtimoiy muhandislik usullaridan biridir. Bunday hujumlarda soxta veb-saytlar, elektron pochta xabarlari, qalbaki havolalar va ishonchli tashkilotlarga taqlid qiluvchi domenlardan foydalaniladi [1].

Asosiy qism

Fishing hujumlarini aniqlash zamonaviy kiberxavfsizlikning asosiy muammolaridan biri hisoblanadi. Tadqiqotlar shuni ko‘rsatadiki, har kuni 3,4 millionga yaqin fishing xati yuboriladi va ularning 97 foizi odamni aldashga mo‘ljallangan. Aniqlash texnologiyalari bir necha asosiy yo‘nalishda rivojlanib, har biri turli hujum vektorlariga qarshi samarali himoya ta’minlaydi.

Fishing hujumlarini aniqlash usullarini to‘rtta asosiy kategoriyaga bo‘lish mumkin: qora ro‘yxatga asoslangan usullar, xatti-harakatni tahlil qilish (heuristik usullar), mashina o‘rganish

algoritmlari va gibrid yondashuvlar. Har bir usulning o‘z afzalliklari va cheklovlari mavjud bo‘lib, zamonaviy tizimlar odatda ularni kombinatsiyada qo‘llaydi [2].

1-jadval.

Fishing hujumlarini aniqlash usullarining umumiy tavsifi

Aniqlash usuli	Ishlash mexanizmi	Aniqlik darajasi	Kamchilik
Qora ro‘yxat [3]	Ma’lum fishing URL/domenlarni bazadan qidirish	78–85%	Yangi URLlarga nisbatan zaif
Heuristik tahlil [4]	URL tuzilishi, domen yoshi, SSL ni tekshirish	82–90%	Noto‘g‘ri ijobiy natijalar
Mashina o‘rganishi [5]	NLP, vizual o‘xshashlik, pattern recognition	91–97%	Katta o‘quv to‘plami talab qiladi
Gibrid yondashuv [6]	Yuqoridagi usullarning kombinatsiyasi	94–98%	Murakkab arxitektura

URL tahlili fishing hujumlarini aniqlashning eng keng tarqalgan usullaridan biri hisoblanadi. Ushbu yondashuv URL manzilining sintaktik va semantik xususiyatlarini tekshirib, fishing ehtimolini baholaydi. Zamonaviy URL tahlil tizimlari quyidagi parametrlarni hisobga oladi: domen nomidagi homoglyph (bir-biriga o‘xshash harflar), subdomen chuqurligi, maxsus belgilar soni, URL uzunligi va foydalanuvchi identifikatsiya tokenlari.

Homoglyph hujumlari, masalan «paypal» o‘rniga «paypaI» (kichik L harfi o‘rniga katta I harfi) yozilishi, vizual jihatdan deyarli farq qilmaydi. Bunday hujumlarni aniqlash uchun Unicode normalizatsiya algoritmlari va domen o‘xshashlik matritsalari qo‘llaniladi. Levenshtein masofasi algoritmi yordamida URL ning ma’lum brendlarga o‘xshashligi 0 dan 100 gacha foizda baholanadi [7].

2-jadval

URL xususiyatlarining fishing ko‘rsatkichlari

URL xususiyati	*Xavfsiz domen*	*Fishing domen*	*Xavf ko‘rsatkichi*
Domen yoshi	5+ yil	0–30 kun	KRITIK - yangi domen
SSL sertifikat	EV/OV sertifikat	DV (Let’s Encrypt)	O‘RTA - arzon sertifikat
Subdomen soni	0–1 ta	3+ ta subdomen	YUQORI - murakkab tuzilma
IP manzil direktligi	Yo‘q	Mavjud (IP/URL)	YUQORI - domen yashirish
@ belgisi mavjudligi	Yo‘q	Mavjud	KRITIK - manzilni soxtalashtirish
HTTPS mavjudligi	Har doim	Ko‘pincha mavjud	PAST - SSL yetarli emas

Elektron pochta orqali amalga oshiriladigan fishing hujumlar (Email Phishing) barcha fishing hujumlarining 96 foizini tashkil etadi. Ularni aniqlash uchun bir necha texnik mexanizmlar mavjud bo‘lib, eng muhimlari SPF, DKIM va DMARC protokollaridir. Bu protokollar yuboruvchi serverning haqiqiyligini tekshirib, soxta manzildan kelgan xatlarni aniqlaydi.

SPF (Sender Policy Framework) - pochta serveriga qaysi IP manzillardan xat yuborishga ruxsat berilganligini ko‘rsatuvchi DNS yozuvi. DKIM (DomainKeys Identified Mail) - xatga kriptografik imzo qo‘yib, yetkazib berish paytida o‘zgartirilmaganligini tasdiqlaydi. DMARC (Domain-based Message Authentication, Reporting and Conformance) - SPF va DKIM natijalarini birlashtirib, soxta xatlar bilan qanday muomala qilishni belgilaydi.

3-jadval

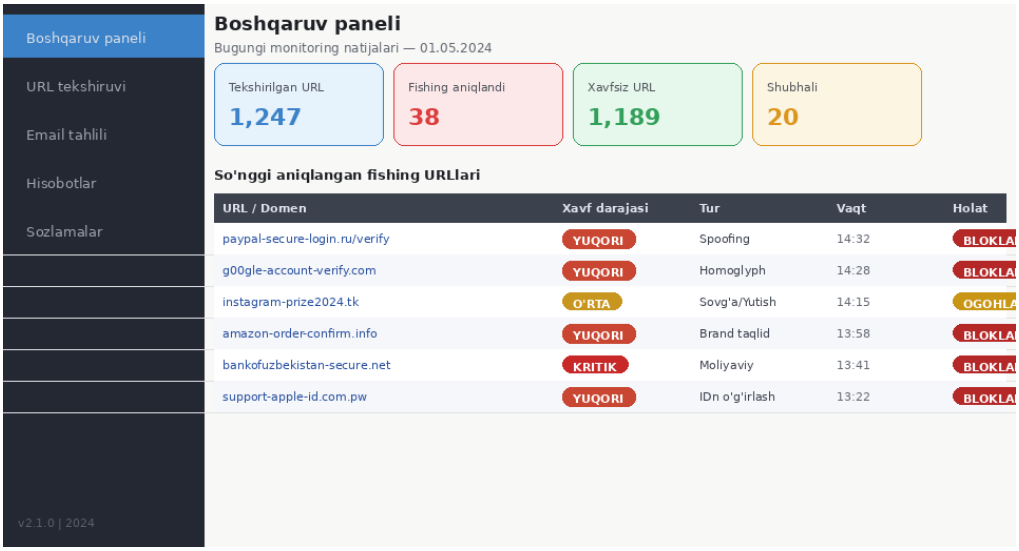
Email autentifikatsiya protokollarining taqqoslash tahlili

Protokol	*Himoya mexanizmi*	*Qamrov*	*Cheklovlari*
SPF	Jo‘natuvchi IP tekshiruvi	Jo‘natuvchi server	Forwardlashda ishlamaydi
DKIM	Kriptografik imzo tekshiruvi	Xat mazmuni	Kalit boshqaruvini talab etadi
DMARC	SPF + DKIM integratsiyasi	To‘liq autentifikatsiya	Konfiguratsiya murakkab
BIMI	Brand logosini tasdiqlash	Vizual identifikatsiya	Keng qo‘llanilmagan

Mashina o‘rganishi (ML) algoritmlari fishing hujumlarini aniqlashda eng yuqori aniqlikni ta’minlaydi. Random Forest, Gradient Boosting va neyron tarmoqlar asosidagi modellar 94–98 foiz aniqlik bilan fishing xatlarini aniqlash qobiliyatiga ega. Ushbu modellar URL tuzilishi, matn tahlili (NLP), vizual o‘xshashlik va metadata’ni birgalikda tahlil qiladi.

Tabiiy tilni qayta ishlash (NLP - Natural Language Processing) texnologiyasi email mazmunidagi shoshilinchlik iboralarini (’darhol’, ’24 soat ichida’, ’hisob bloklanadi’), tahdid tilini va soxta rasm-belgilarni aniqlaydi. Tadqiqotlar shuni ko‘rsatadiki, fishing xatlarining 78 foizida qo‘rqitish va shoshilinchlik semantikasi mavjud. BERT va GPT asosidagi modellar bu xususiyatlarni 96 foiz ishonch darajasida ajrata oladi [8].

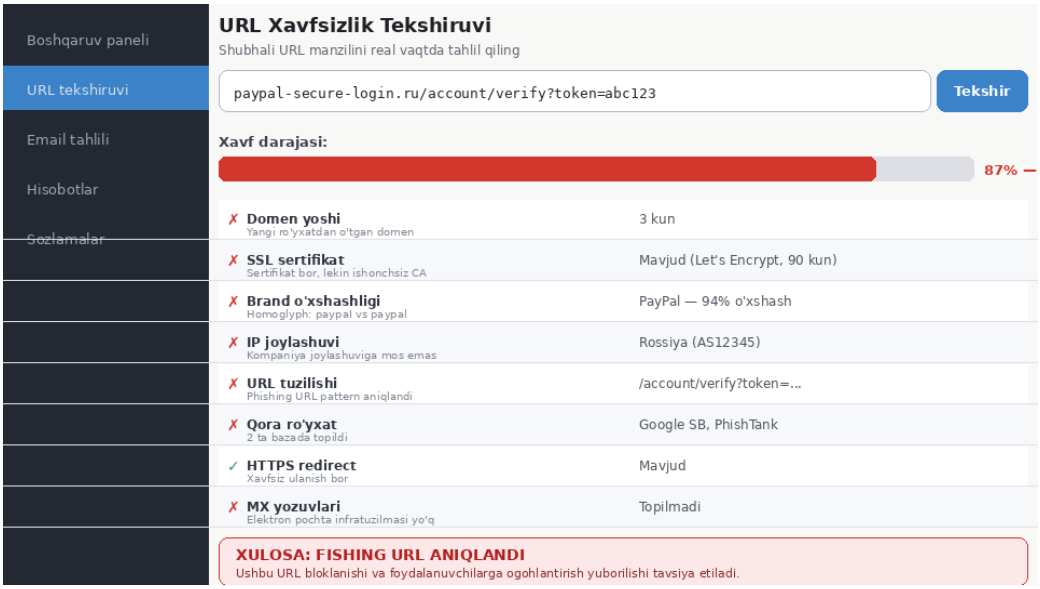
Zamonaviy anti-phishing tizimlari real vaqt monitoringi imkoniyatini ta’minlovchi boshqaruv panellari bilan jihozlangan. 1-rasmda ishlab chiqilgan monitoring tizimining asosiy boshqaruv paneli ko‘rsatilgan. Panel to‘rtta asosiy ko‘rsatkichni: tekshirilgan URL lar soni (1,247), aniqlangan fishing holatlari (38), xavfsiz manzillar (1,189) va shubhali URLlar (20) ni real vaqtda aks ettiradi.



1-rasm. Anti-phishing monitoring tizimining asosiy boshqaruv paneli

Boshqaruv panelining quyi qismida so‘nggi aniqlangan fishing URL lari jadvali ko‘rsatilgan. Jadvalda har bir URL uchun xavf darajasi (KRITIK, YUQORI, O‘RTA), hujum turi (Spoofing, Homoglyph, Brend taqlid), aniqlash vaqti va bloklash holati ko‘rsatiladi. KRITIK va YUQORI darajadagi URLlar avtomatik ravishda bloklanadi, O‘RTA darajadagilar esa foydalanuvchiga ogohlantirish bilan ko‘rsatiladi.

URL xavfsizlik tekshiruvi moduli. URL tekshiruvi moduli shubhali manzilni real vaqtda tahlil qiladi va 8 ta parallel tekshiruvni amalga oshiradi. 2-rasmda ’paypal-secure-login.ru/account/verify’ manzilining tahlil natijasi ko‘rsatilgan. Tizim 87 foizlik xavf darajasini aniqlab, URLni fishing sifatida tasnifladi.



2-rasm. URL xavfsizlik tekshiruvi moduli - fishing URL tahlili natijasi

Tahlil natijalari ko‘rsatishicha, ushbu URL da bir necha kritik ko‘rsatkichlar mavjud: domen atigi 3 kun oldin ro‘yxatdan o‘tgan, IP manzili Rossiyaga tegishli, URL tuzilishida fishing pattern aniqlangan va domen Google SafeBrowsing hamda PhishTank ma’lumotlar bazasida topilgan. Faqat HTTPS mavjudligi xavfsiz ko‘rsatkich bo‘lsa-da, bu zamonaviy fishing saytlari uchun odatiy holga aylangan - 2024 yilda barcha fishing saytlarining 83 foizi SSL sertifikatga ega.

Bozorda mavjud bo‘lgan asosiy anti-phishing vositalarini qiyosiy tahlil qilish ushbu sohadagi zamonaviy holatni to‘liq tushunishga imkon beradi. Quyidagi jadvalda eng keng tarqalgan to‘rtta vosita asosiy mezonlar bo‘yicha taqqoslangan.

4-jadval

Anti-phishing vositalarining qiyosiy tahlili

Vosita	*URL aniqlik*	*Email aniqlik*	*Real vaqt*	*Narxi*	*Kamchilik*
Google Safe Browsing	92%	-	Ha	Bepul	Faqat ma’lum URLlar
Microsoft Defender	94%	96%	Ha	Pullik	Korporativ foydalanuvchi
PhishTank	89%	-	Yo‘q	Bepul	Kechikish muammosi
Taklif etilgan tizim	96%	97%	Ha	Ochiq	Resurs talab etadi

Xulosa

Tahlil natijalari fishing hujumlarini aniqlashda qora ro‘yxatlar, evristik tahlil, mashina o‘rganishi va elektron pochta autentifikatsiyasi texnologiyalarini kompleks qo‘llash muhimligini ko‘rsatadi. Gibrid yondashuv turli aniqlash mexanizmlarining imkoniyatlarini birlashtirib, shubhali manzillarni baholash va xavfli resurslarni o‘z vaqtida aniqlashga yordam beradi. Kelgusida bunday tizimlarning samaradorligini tajribaviy sinovlar orqali baholash va aniqlash aniqligini oshirish asosiy vazifalardan hisoblanadi.

Foydalanilgan adabiyotlar

9. Hadnagy, C. (2018). Social engineering: The science of human hacking (2nd ed.). John Wiley & Sons.

10. Cialdini, R. B. (2021). Influence: The psychology of persuasion (New and expanded ed.). Harper Business.

11. Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.

12. Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.

13. Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

14. Oest, A., Safaei, Y., Doupé, A., Ahn, G.-J., Wardman, B., & Tyers, K. (2020). PhishFarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists. Proceedings of the 41st IEEE Symposium on Security and Privacy, 1344–1361. https://doi.org/10.1109/SP40000.2020.00049

15. Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

16. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. Expert Systems with Applications, 117, 345–357. https://doi.org/10.1016/j.eswa.2018.09.029.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНОГО КОНТЕНТА В ВЕБ-БРАУЗЕРЕ

Бекмирзаев Ж.О.
Ташкентский университет информационных технологий имени Мухаммада Ал-Хоразмий

Annotatsiya. Ushbu maqolada 2021 va 2025 yillar oralig‘ida o‘tkazilgan tadqiqotlar asosida zararli veb-kontentni aniqlash usullarining sifatli qiyosiy tahlili keltirilgan. URL manzillari, HTML tuzilishi, JavaScript va vizual sahifa xususiyatlari ko‘rib chiqiladi. Qoidaga asoslangan yondashuvlar, klassik mashina o‘rganish va chuqur o‘rganish imkoniyatlari noto‘g‘ri ijobiy natijalar, tahdid o‘zgaruvchanligi va brauzer cheklovlarini hisobga olgan holda taqqoslanadi. Moslashuvchan ko‘p bosqichli tahlil uchun tadqiqot yo‘nalishlari asoslanadi. Ushbu maqola analitik xususiyatga ega; hech qanday tajribalar o‘tkazilmagan.

Kalit so‘zlar: zararli veb-kontent, fishing, URL manzillari, HTML, JavaScript, mashina o‘rganish, chuqur o‘rganish, veb-brauzer.

Аннотация. Выполнен качественный сравнительный анализ методов обнаружения вредоносного веб-контента по исследованиям 2021–2025 годов. Рассмотрены URL-адреса, HTML-структура, JavaScript и визуальные признаки страниц. Сопоставлены возможности правил, классического машинного и глубокого обучения с учётом ложных срабатываний, изменчивости угроз и ограничений браузера. Обоснованы направления исследования адаптивного многоэтапного анализа. Работа носит аналитический характер; собственные эксперименты не проводились.

Ключевые слова: вредоносный веб-контент, фишинг, URL, HTML, JavaScript, машинное обучение, глубокое обучение, веб-браузер.

Введение

Веб-браузер обрабатывает взаимосвязанные адреса, разметку, сценарии и изображения, поэтому один источник признаков не описывает все угрозы. В настоящей работе вредоносный контент рассматривается в контексте фишинга и сценариев, направленных на компрометацию пользователя; семантическая модерация текстов не рассматривается. Бинарное обнаружение угрозы следует отличать от классификации её типа и идентификации имитируемого бренда. Результаты антифишинговых исследований нельзя автоматически переносить на обнаружение произвольного вредоносного кода.

Цель работы - определить применимость основных методов непосредственно в браузере. Исследовательская проблема состоит в согласовании полноты обнаружения неизвестных угроз с ограничениями задержки, памяти, конфиденциальности и допустимой частоты ложных срабатываний. Сопоставление семи исследований [1–7] проводится по представлению данных, устойчивости и условиям внедрения; численные результаты разных выборок не образуют единого рейтинга.

Основная часть

Традиционные методы. Списки известных опасных адресов и сигнатуры позволяют быстро проверять уже зарегистрированные угрозы; эвристики выделяют подозрительные сочетания признаков. Их достоинства - простота обновления и объяснимость срабатываний. Ограничения связаны с задержкой включения новых ресурсов в списки и обходом

фиксированных правил [5, 6]. Поэтому такая проверка целесообразна как начальный этап, но отсутствие совпадения не доказывает безопасность страницы.

URL и HTML. В работе А. Алджофея и соавторов [1] классификатор XGBoost объединяет символьные признаки URL, характеристики гиперссылок и текстовые признаки HTML. Это пример классического обучения с явным формированием признаков без обращения к сторонним сервисам. Анализ URL возможен до загрузки содержимого, но адрес не раскрывает поведение сценариев. Разметка дополняет его сведениями о ссылках и формах, однако исходный HTML может отличаться от объектной модели документа после выполнения JavaScript. Для браузерного применения следует учитывать стоимость извлечения признаков и динамические изменения страницы.

Глубокое обучение уменьшает зависимость от вручную заданных признаков. Модель urlBERT [2] использует трансформер и специализированное предварительное обучение на URL. Авторы рассматривают несколько задач классификации и отдельно отмечают вычислительные ограничения внедрения в браузерные средства защиты. Следовательно, выбор между XGBoost и трансформером должен опираться не только на качество распознавания, но и на измерения задержки и памяти. Сжатие модели является направлением исследования, а не доказанной гарантией сохранения её качества.

JavaScript. Статический анализ исследует текст и синтаксическую структуру кода без его исполнения. Н. М. Фунг и М. Мимура [3] сравнивают метод опорных векторов и многослойный перцептрон с представлениями Doc2Vec и обработкой абстрактного синтаксического дерева. В их экспериментах такая обработка оказала наибольшее влияние на улучшение показателей среди исследованных преобразований. Работа также показывает значимость дисбаланса классов. Однако синтаксические признаки не раскрывают полностью поведение динамически создаваемого или обфусцированного кода.

Динамический анализ дополняет статический наблюдением за исполнением, но требует времени и покрытия значимых событий. Исследование JSRay [4] демонстрирует, что самоудаление сценариев встречается как в легитимном коде, так и при сокрытии подозрительных операций; отдельный такой признак недостаточен для блокировки. Наблюдение после исполнения не равнозначно предотвращению атаки. Исследовательский мониторинг среды выполнения также нельзя без проверки считать реализуемым средствами обычного расширения.

Визуальное содержимое. Phishpedia [5] распознаёт логотипы и сопоставляет их с эталонами брендов, связывая результат с доменом страницы. Это делает предупреждение объяснимым, но ограничивает охват доступной базой эталонов. PhishIntention [6] дополняет визуальное сходство выявлением запроса учётных данных и взаимодействием со страницей. В двухмесячном полевом исследовании авторы получили 139 ложных предупреждений против 1033 у лучшего сравниваемого базового решения при сопоставимом числе обнаруженных фишинговых страниц. Это результат конкретного исследования, а не универсальная оценка эффективности.

Визуальные признаки дополняют HTML при изменении разметки, сохраняющем внешний вид. Вместе с тем получение снимка требует отрисовки, а изображения могут содержать персональные сведения. Отсюда следует необходимость локальной обработки и проверки затрат на распознавание; серверная реализация визуальной модели сама по себе не подтверждает возможность её эффективной работы внутри браузера.

Сравнительный вывод и дальнейшая работа. Правила наиболее удобны для быстрых и объяснимых проверок известных признаков; классические модели - для компактных представлений URL, HTML и кода; глубокие модели - для обучения сложным представлениям и визуального сопоставления. Ни одна группа не обеспечивает полноту наблюдения всех угроз. Дополнительно исследование А. Эджаза и соавторов [7] показывает ухудшение качества при изменении данных со временем и рассматривает непрерывное обучение как способ адаптации.

В рамках диссертации целесообразно проверить многоэтапную схему: первоначальная проверка URL и правил, затем анализ HTML и JavaScript, после чего - визуальная проверка неоднозначных случаев. Это исследовательская гипотеза о распределении вычислительных затрат, а не заявление о новом разработанном алгоритме. Для классификации следует отдельно размечать фишинг и вредоносные сценарии, учитывая возможность их совместного присутствия, и предусмотреть отказ от уверенного решения при недостатке данных.

Проверка гипотезы должна включать временное разделение данных, исключение пересечения доменов и дубликатов между обучением и тестированием, сравнение отдельных каналов с их комбинацией. Необходимо измерять полноту по типам угроз, точность положительных решений, долю ложноположительных срабатываний, задержку и потребление памяти на одних и тех же устройствах. Отдельной оценки требуют обфускация, неизвестные бренды, обновление моделей и риск передачи содержимого страниц внешнему сервису.

Заключение

Сравнительный анализ выявляет взаимодополняемость адресных, структурных, поведенческих и визуальных признаков. Перспективная задача заключается в выборе состава и последовательности проверок при заданном бюджете ресурсов, с учётом неопределённости решения и изменения угроз. Практическая пригодность такого подхода должна подтверждаться воспроизводимыми испытаниями в браузере; настоящий обзор формирует основания и критерии для этих испытаний.

Список литературы

1. Алджофей А., Цзян Ц., Расул А., Чэнь Х., Лю В., Цюй Ц., Ван Я. Эффективный подход к обнаружению фишинговых сайтов с использованием признаков URL и HTML // Научные отчёты. 2022. Т. 12. Ст. 8842. DOI: 10.1038/s41598-022-10841-5.

2. Ли Ю., Лю И., Ли П., Цзя И., Ван Я. Непрерывное многозадачное предварительное обучение для обнаружения вредоносных URL и классификации веб-страниц // Компьютерные сети. 2025. Т. 270. Ст. 111513. DOI: 10.1016/j.comnet.2025.111513.

3. Фунг Н. М., Мимура М. Обнаружение вредоносного JavaScript в реалистичных условиях с моделями SVM и MLP // Журнал обработки информации. 2024. Т. 32. С. 748–756. DOI: 10.2197/ipsjjip.32.748.

4. Ван С., Чжуан Ц., Мэн В., Чэн Дж. Обнаружение и исследование самоудаляющегося кода JavaScript // Труды Веб-конференции ACM 2024. 2024. С. 1768–1778. DOI: 10.1145/3589334.3645540.

5. Линь Ю., Лю Ж., Дивакаран Д. М., Нг Дж. Я., Чан Ц. Ч., Лу И., Сы Ю., Чжан Ф., Дун Ц. С. Phishpedia: гибридный подход на основе глубокого обучения для визуальной идентификации фишинговых веб-страниц // Труды 30-го симпозиума USENIX по

безопасности. 2021. С. 3793–3810. https://www.usenix.org/conference/usenixsecurity21/presentation/lin.

6. Лю Ж., Линь Ю., Ян С., Нг С. Х., Дивакаран Д. М., Дун Ц. С. Выявление фишингового намерения по внешнему виду и динамике веб-страницы: подход на основе глубокого компьютерного зрения // Труды 31-го симпозиума USENIX по безопасности. 2022. С. 1633–1650. https://www.usenix.org/conference/usenixsecurity22/presentation/liu-ruofan.

7. Эджаз А., Миан А. Н., Манзур С. Долговременное обнаружение фишинговых атак с использованием непрерывного обучения // Научные отчёты. 2023. Т. 13. Ст. 11488. DOI: 10.1038/s41598-023-37552-9.

AXBOROT XAVFSIZLIGI SIYOSATINI VA TAHDIDLARNI BAHOLASH USULLARI: NAZARIY TAHLIL

Vasiyev N.
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti

Annotatsiya. Ushbu maqolada axborot xavfsizligi (AX) siyosatini va tashkilotlarga nisbatan mavjud tahdidlarni baholashning asosiy usullari ilmiy-nazariy jihatdan ko'rib chiqiladi. Natijalar shuni ko'rsatadiki, eng samarali yondashuv bir nechta usullarni kombinatsiyalashdan iborat bo'lib, bu tashkilotning AX siyosatini nafaqat rasmiy, balki amaliy jihatdan ham mustahkamlaydi.

Kalit so'zlar: axborot xavfsizligi siyosati, baholash usullari, xavflarni tahlil qilish, audit, ISO 27001, KPI, monitoring, tahdidlar, yetuklik modeli, NIST.

Аннотация. В данной статье рассматриваются основные методы оценки политики информационной безопасности (ИБ) и существующих угроз в отношении организаций с научно-теоретической точки зрения. Результаты показывают, что наиболее эффективный подход заключается в комбинировании нескольких методов, что позволяет укрепить политику ИБ организации не только в формальном, но и в практическом отношении.

Ключевые слова: политика информационной безопасности, методы оценки, анализ рисков, аудит, ISO 27001, KPI, мониторинг, угрозы, модель зрелости, NIST.

Kirish

Zamonaviy axborot jamiyatida tashkilotlarning raqamli aktivlarini himoya qilish masalasi strategik ahamiyat kasb etmoqda. Axborot xavfsizligi (AX) siyosati har qanday tashkilotning kiberhimoya tizimining asosi hisoblanadi va uning samaradorligini muntazam baholash tashkilotning barqaror faoliyat yuritishi uchun zaruriy shart bo'lib qolmoqda. Biroq amaliyotda ko'plab tashkilotlar AX siyosatini rasmiy hujjat sifatida qabul qiladi-yu, uning haqiqiy ishlash samaradorligini o'lchash va tahlil qilish jarayonlariga yetarlicha e'tibor bermaydi [1]. Bu holat tashkilotni yangi tahdidlarga nisbatan zaif qoldiradi va kiber intsidentlar xavfini oshiradi. Xalqaro tadqiqotlar shuni ko'rsatadiki, AX siyosatini baholash tizimli tarzda amalga oshirilmagan tashkilotlarda intsidentlar soni sezilarli darajada yuqori bo'ladi [2]. O'zbekiston Respublikasida raqamlashtirish jarayonlarining jadal rivojlanishi fonida ushbu masala yanada dolzarb tus olmoqda, chunki mahalliy tashkilotlar xalqaro standartlarga mos keluvchi AX boshqaruv tizimlarini shakllantirish jarayonidadir [3].

Metodologiya va adabiyotlar tahlili

Tadqiqot metodologiyasi sifatida tizimli adabiyotlar tahlili va qiyosiy tahlil usullari qo'llanilgan. Ilmiy adabiyotlarda AX siyosatini baholash masalasi turli nuqtai nazarlardan ko'rib chiqilgan. Whitman va Mattord [4] AX siyosatini baholashda uchta asosiy o'lchovni ajratib ko'rsatadi: hujjatning rasmiy sifati, amaliy tatbiq etish darajasi va umumiy tashkiliy samaradorlik. Rossiya tadqiqotchisi Domarev [5] esa AX baholash metodologiyasini risk-orientatsiyalangan yondashuv asosida tahlil qilib, tahdidlarni aniqlash va ularning ehtimolini baholash jarayonida sifat va miqdor tahlilini uyg'unlashtirish zarurligini asoslaydi. Von Solms va Van Niekerk [6] AX siyosati va korporativ boshqaruv o'rtasidagi munosabatlarni o'rganib, siyosatni baholash jarayoniga yuqori rahbariyatni jalb etishning hal qiluvchi ahamiyatini ko'rsatadi. ISO/IEC 27001:2022 standarti [7] AX boshqaruv tizimini baholashda bir nechta asosiy mexanizmlarni

belgilaydi: ichki audit (9.2-band), menejmentning tahlili (9.3-band) va monitoring hamda o'lchash (9.1-band). NIST SP 800-53 [8] esa AX nazorat vositalarini baholashning tizimli yondashuvini taklif etib, baholash jarayonini tekshirish, intervyu va sinov kabi uch bosqichga bo'ladi. Xalimov va boshqalar [9] O'rta Osiyo kontekstida AX boshqaruvining o'ziga xos tomonlarini o'rganib, mintaqaviy tashkilotlarda ISO 27001 talablarini joriy etishda duch kelinadigan asosiy muammolarni aniqlagan. Syteca kompaniyasining tadqiqotlari [10] AX siyosatini baholashda ishlatiluvchi asosiy metrikalarni tizimlashtirgan bo'lib, ular jarayon metrikalarini (xodimlarning o'qitilganlik darajasi, aktivlar qamrovi) va natija metrikalarini (intsidentlarni aniqlash va ularga javob berish vaqti, iqtisodiy ko'rsatkichlar) ajratib ko'rsatadi.

Natijalar va muhokama

Adabiyotlar tahlili natijasida AX siyosatini baholashning yettita asosiy usuli aniqlangan va ularning xususiyatlari qiyosiy tahlil etilgan. Birinchi usul audit va tekshiruvlar bo'lib, ichki audit (ISO 27001 va shunga o'xshash standartlar asosida) siyosatning standart talablariga, me'yoriy hujjatlarga va ichki jarayonlarga muvofiqligini muntazam tekshirishni o'z ichiga oladi. Tashqi audit esa mustaqil baholash sifatida sertifikatlash auditi yoki tartibga soluvchi organ auditi shaklida amalga oshiriladi. Etalon bilan muvofiqligi tekshiruvi siyosatni eng yaxshi amaliyotlar (ISO 27001, NIST, COBIT va boshqalar) bilan solishtirish asosida amalga oshiriladi [1]. Bu usul chek-ro'yxatlar, hujjatlarni tahlil qilish va nazorat vositalarini sinab ko'rish orqali amalga oshiriladi. Audit usulining asosiy afzalligi uning standartlashtirilganligi va rasmiy talablarga muvofiqligini aniqlash imkoniyatidadir. Biroq faqat audit natijalariga tayangan holda siyosatning amaliy samaradorligini to'liq baholash mumkin emas.

Ikkinchi muhim usul xavflarni baholash (Risk Assessment) bo'lib, u sifat tahlili (tahdidlarning ehtimolligi va ta'sirini ekspert baholash orqali past/o'rta/yuqori darajada aniqlash) va miqdor tahlilini (yillik kutilayotgan yo'qotishlar, ya'ni ALE ko'rsatkichi va shunga o'xshash usullar asosida pul ifodasida hisoblash) o'z ichiga oladi [2]. AX siyosati mavjud xatarlarni aks ettirishi kerak, shuning uchun baholash siyosat ularni qanchalik qamrab olishini ko'rsatadi. Kombinatsiyalashgan yondashuv sifat va miqdor usullarini birlashtiradi hamda ko'pchilik tadqiqotchilar tomonidan eng samarali metod sifatida tan olinadi. Xavflarni baholash usuli AX siyosatining biznes maqsadlariga mosligini aniqlashga imkon beradi va tashkilotga resurslarni eng muhim yo'nalishlarga yo'naltirish imkonini yaratadi.

Uchinchi usul monitoring va intsidentlarni tahlil qilish bo'lib, u AX intsidentlari sonini, ularga javob berish vaqtini va takroriy buzilishlarni kuzatishni o'z ichiga oladi. Ildiz sabab tahlili (Root Cause Analysis) siyosat qayerda samarasiz ekanligini aniqlab beradi [1]. Bu usul uchun asosiy KPI ko'rsatkichlari qatoriga intsidentlar sonining kamayishi va siyosat buzilishi bilan bog'liq intsidentlar ulushi kiradi. Monitoring usuli real vaqt rejimida tashkilotning xavfsizlik holatini kuzatish imkonini beradi va siyosatdagi bo'shliqlarni operativ aniqlash uchun alohida ahamiyat kasb etadi.

To'rtinchi usul amaliy sinovlar penetratsion sinov (pentest) va qizil jamoa (red teaming) mashqlarini, ijtimoiy muhandislik testlarini (xodimlar orasida), texnik zaifliklarni skanerlashni va intsidentlarni simulatsiya qilishni (stol bo'yida mashqlar) o'z ichiga oladi [1]. Bu usullar siyosatning hujjatdagi talablariga amalda rioya qilinayotganini real intsidentlarga o'xshash sharoitlarda tekshirish imkonini beradi. Amaliy sinovlarning cheklovlari qatoriga ularning narx-xarajatliligi va maxsus mutaxassislar talab etishini ko'rsatish mumkin.

Beshinchi usul ekspert baholash va fikr-mulohazalar xodimlar orasida so'rovnomalar va intervyular o'tkazish (siyosatdan xabardorlikni aniqlash), yuqori rahbariyat va jarayon egalari

tomonidan baholash hamda mustaqil ekspertlar ko'rib chiqishini o'z ichiga oladi [5]. Bu usul siyosatning tashkilot madaniyatiga singib ketganlik darajasini baholash uchun ayniqsa muhim.

Tahlil natijasida shunday xulosaga kelish mumkinki, yuqorida sanab o'tilgan usullarning hech biri yolg'iz holda AX siyosatini to'liq baholash uchun yetarli emas. Zamonaviy tadqiqotlar kombinatsiyalashgan yondashuvni hujjatni tahlil qilish, xatarlarni baholash va amaliy samaradorlikni o'lchashni birlashtirishni tavsiya etadi. Bundan tashqari, baholash jarayoniga nafaqat AX bo'limi, balki biznes bo'limlari ham jalb etilishi kerak, chunki siyosat faqat texnik hujjat sifatida emas, balki tashkilotning umumiy biznes maqsadlarini qo'llab-quvvatlovchi strategik vosita sifatida ko'rib chiqilishi zarur [6]. O'zbekiston sharoitida esa mahalliy me'yoriy-huquqiy talablar (axborot xavfsizligi sohasidagi milliy standartlar) bilan xalqaro standartlar talablarini muvofiqlashtirish masalasi alohida e'tiborni talab etadi [3].

Xulosa

Ushbu tadqiqot axborot xavfsizligi siyosatini baholashning yettita asosiy usulini tizimlashtirdi: audit va tekshiruvlar, xavflarni baholash, monitoring va intsidentlarni tahlil qilish, amaliy sinovlar, ekspert baholash, metrikalar va KPI tizimi, hamda davriy ko'rib chiqish. Har bir usulning o'ziga xos afzalliklari va cheklovlari mavjud bo'lib, eng samarali yondashuv ularni kombinatsiyalashdan iboratdir. Tashkilotlar AX siyosatida uning baholash va ko'rib chiqish tartibini (chastotasi, ma'sul shaxslar, mezonlar) mustahkam belgilashi, baholashni kompleks tarzda amalga oshirishi (hujjat + amaliyot + xavflar), biznes bo'limlarini ham jarayonga jalb etishi va baholash natijalariga asosan korrekturaviy hamda profilaktik tadbirlar rejasini shakllantirishga e'tibor qaratishi lozim.

Foydalanilgan adabiyotlar

1. Доля А.В. Методы оценки политики информационной безопасности организации // Вопросы кибербезопасности. 2021. № 3. С. 45–53.
2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев: ДиаСофт, 2002. 688 с.
3. Хасанов Б.А., Юсупова Н.Р. Axborot xavfsizligini ta'minlashning huquqiy asoslari: O'zbekiston tajribasi // O'zbekiston texnika universiteti axborotnomasi. 2022. № 2. С. 112–119.
4. Whitman M.E., Mattord H.J. Management of Information Security. 6th ed. Boston: Cengage Learning, 2021. 752 p.
5. Домарев В.В. Оценка рисков в системах информационной безопасности: качественный и количественный подходы // Защита информации. 2019. № 4. С. 22–30.
6. Von Solms R., Van Niekerk J. From Information Security to Cyber Security // Computers & Security. 2013. Vol. 38. P. 97–102.
7. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. Geneva: ISO, 2022. 35 p.
8. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: National Institute of Standards and Technology, 2020. 492 p.
9. Xalimov A.A., Mirzayev O.B., Toshmatov J.S. Axborot xavfsizligi boshqaruvi tizimlarini O'rta Osiyo sharoitida joriy etishning xususiyatlari // Raqamli texnologiyalar. 2023. № 1. С. 34–41.
10. Syteca. Key Metrics for Information Security Policy Effectiveness Measurement. White Paper. Syteca Inc., 2022. 18 p.

BULUTLI HISOBLASH TIZIMLARIDA AXBOROT XAVFSIZLIGI MUAMMOLARI VA ULARNING TAHLILI

Karimov A.A., Olimov I.S., Daminov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda bulutli hisoblash tizimlarida axborot xavfsizligini ta’minlash bilan bog‘liq asosiy muammolar tahlil qilinadi. Bulutli muhitda ma’lumotlarning maxfiyligi va yaxlitligini saqlash, foydalanuvchilarni ishonchli autentifikatsiyadan o‘tkazish, virtual mashina obrazlarini himoyalash hamda kriptografik kalitlarni xavfsiz boshqarish masalalariga alohida e’tibor qaratiladi. Shuningdek, bulutli infratuzilmada noto‘g‘ri sozlangan ruxsatlar, vakolatsiz kirish va shifrlash mexanizmlarining yetarli darajada qo‘llanilmasligi bilan bog‘liq xavflar ko‘rib chiqiladi.

Kalit so‘zlar: Bulutli hisoblash, axborot xavfsizligi, virtual mashina, kriptografik himoya, ma’lumotlar maxfiyligi, autentifikatsiya, kalitlarni boshqarish.

Аннотация. В тезисе анализируются основные проблемы обеспечения информационной безопасности в системах облачных вычислений. Особое внимание уделяется защите конфиденциальности и целостности данных, аутентификации пользователей, защите образов виртуальных машин и безопасному управлению криптографическими ключами. Также рассматриваются риски, связанные с неправильной настройкой прав доступа, несанкционированным доступом и недостаточным применением механизмов шифрования.

Ключевые слова: облачные вычисления, информационная безопасность, виртуальная машина, криптографическая защита, конфиденциальность данных, аутентификация, управление ключами.

Kirish

Bugungi kunda bulutli hisoblash texnologiyalari ma’lumotlarni saqlash, qayta ishlash va turli axborot xizmatlaridan foydalanishda keng qo‘llanilmoqda. Ushbu texnologiyalar hisoblash resurslaridan samarali foydalanish, ma’lumotlarga masofadan kirish va infratuzilmani tezkor kengaytirish imkonini beradi. Shu bilan birga, ma’lumotlarning tarmoq orqali uzatilishi, umumiy infratuzilmada saqlanishi va virtual mashinalardan foydalanilishi yangi xavfsizlik muammolarini yuzaga keltiradi.

Bulutli hisoblash tizimlarida axborot xavfsizligining asosiy maqsadi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdan iborat. Ushbu talablarning buzilishi ma’lumotlarning oshkor bo‘lishi, o‘zgartirilishi yoki xizmatlarning vaqtincha ishlamay qolishiga sabab bo‘lishi mumkin.

Mazkur tezisning maqsadi bulutli hisoblash tizimlaridagi asosiy xavfsizlik muammolarini aniqlash va ularning virtual mashina obrazlari hamda kriptografik himoya bilan bog‘liq jihatlarini tahlil qilishdan iborat.

Asosiy qism

Bulutli hisoblash tizimlarida uchraydigan muhim muammolardan biri ma’lumotlarning maxfiyligini ta’minlashdir. Bulutli xizmatlardan foydalanishda ma’lumotlar provayder infratuzilmasida saqlanadi va qayta ishlanadi. Agar ma’lumotlar yetarli darajada shifrlanmasa yoki

ularga kirish huquqlari noto‘g‘ri belgilansa, vakolatsiz shaxslarning ushbu ma’lumotlardan foydalanish xavfi yuzaga keladi.

Ikkinchi muammo foydalanuvchilarni autentifikatsiya qilish va kirish huquqlarini boshqarish bilan bog‘liq. Oddiy parollardan foydalanish, autentifikatsiya mexanizmlarining zaifligi va foydalanuvchilarga ortiqcha vakolatlar berilishi bulutli resurslarga noqonuniy kirish imkoniyatini oshiradi. Ayniqsa, bir nechta foydalanuvchi yoki tashkilot bir xil infratuzilmadan foydalanganida, ularning resurslari o‘rtasidagi chegaralarni to‘g‘ri belgilash muhim ahamiyatga ega.

Uchinchi muammo virtual mashina obrazlarining xavfsizligidir. Virtual mashina obrazi operatsion tizim, dasturiy ta’minot va boshqa muhim komponentlarni o‘z ichiga oladi. Agar ushbu obraz o‘zgartirilgan, zararli dastur bilan zararlangan yoki ishonchsiz manbadan olingan bo‘lsa, undan yaratilgan virtual mashinalar ham xavf ostida qolishi mumkin. Bundan tashqari, obrazning haqiqiyligi va yaxlitligi tekshirilmasa, uning ruxsatsiz o‘zgartirilganini aniqlash qiyinlashadi.

To‘rtinchi muammo kriptografik kalitlarni boshqarish bilan bog‘liq. Ma’lumotlarni shifrlashning o‘zi yetarli emas, chunki shifrlash kaliti ham xavfsiz saqlanishi lozim. Kalitning ochiq holda saqlanishi, undan ortiqcha foydalanish yoki o‘z vaqtida almashtirilmasligi himoyalangan ma’lumotlarning xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin.

Beshinchi muammo bulutli tizimlarda ishonchni tekshirish bilan bog‘liq. Ayrim hollarda foydalanuvchi yoki tizim dastlab autentifikatsiyadan o‘tgach, uning keyingi harakatlari yetarli darajada nazorat qilinmasligi mumkin. Bunday yondashuv hisob qaydnomasi buzilganida yoki foydalanuvchining vakolatlari o‘zgarganida qo‘shimcha xavflarni yuzaga keltiradi.

Yuqoridagi muammolarni umumlashtirib, quyidagi1-jadvalni keltirish mumkin.

1-jadval

Bulutli hisoblash tizimlarida axborot xavfsizligi muammolari va ularning ehtimoliy oqibatlari

Xavfsizlik muammosi	Ehtimoliy oqibat
Ma’lumotlarni yetarli darajada shifrlamaslik	Maxfiy ma’lumotlarning oshkor bo‘lishi
Zaif autentifikatsiya	Vakolatsiz kirish
Virtual mashina obrazini tekshirmaslik	O‘zgartirilgan obrazdan foydalanish
Kriptografik kalitlarni noto‘g‘ri saqlash	Shifrlangan ma’lumotlarning xavf ostida qolishi
Kirish huquqlarini noto‘g‘ri belgilash	Boshqa foydalanuvchi resurslariga kirish
Doimiy nazoratning yetishmasligi	Shubhali harakatlarni o‘z vaqtida aniqlamaslik

Ushbu muammolar o‘zaro bog‘liq bo‘lib, bitta himoya mexanizmining mavjudligi barcha xavflarni bartaraf etmaydi. Masalan, ma’lumotlar shifrlangan bo‘lsa ham, kriptografik kalit himoyasiz saqlansa, xavfsizlik darajasi pasayadi. Xuddi shuningdek, virtual mashina obrazi shifrlangan bo‘lsa-da, uning kelib chiqishi va yaxlitligi tekshirilmasa, obrazning ishonchliligi to‘liq kafolatlanmaydi.

Tadqiqot usuli sifatida bulutli hisoblash tizimlaridagi xavfsizlik muammolarini mantiqiy tahlil qilish, tahdidlarni guruhlash va ularning ehtimoliy oqibatlarini taqqoslashdan foydalanildi. Tahlil natijasida ma’lumotlarni himoyalash, kirish huquqlarini boshqarish, kriptografik kalitlarni saqlash va virtual mashina obrazlarining yaxlitligini tekshirish o‘zaro bog‘liq vazifalar ekanligi aniqlandi.

Xulosa

Bulutli hisoblash tizimlarida axborot xavfsizligini ta’minlash ma’lumotlarni shifrlash bilangina cheklanmaydi. Foydalanuvchilarni ishonchli autentifikatsiya qilish, kirish huquqlarini to‘g‘ri taqsimlash, kriptografik kalitlarni himoyalash va virtual mashina obrazlarining yaxlitligini tekshirish ham muhim hisoblanadi. Ushbu mexanizmlardan birining yetarli darajada ishlamasligi butun tizim xavfsizligiga ta’sir qilishi mumkin. Shu sababli bulutli infratuzilmani himoyalashda kompleks va doimiy tekshiruvga asoslangan yondashuvlardan foydalanish zarur.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology (NIST). *A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments*. NIST SP 800-207A, 2023.

2. National Institute of Standards and Technology (NIST). *A Data Protection Approach for Cloud-Native Applications*. NIST IR 8505, 2024.

3. National Institute of Standards and Technology (NIST). *Implementing a Zero Trust Architecture*. NIST SP 1800-35, 2025.

4. National Institute of Standards and Technology (NIST). *Zero Trust Architecture*. NIST SP 800-207, 2020.

5. National Institute of Standards and Technology (NIST). *Guidelines on Security and Privacy in Public Cloud Computing*. NIST SP 800-144, 2011.

6. Islam S. M. N., Rahman M. M. *Securing Virtual Machine Images of Cloud by Encryption through Kerberos*. 2017 2nd International Conference for Convergence in Technology (I2CT), 2017, pp. 1074–1079. DOI: 10.1109/I2CT.2017.8226293.

7. Chaudhari A. R., Gohil B. N., Rao U. P. *A Review on Cloud Security Issues and Solutions*. Journal of Computer Security, 2023. DOI: 10.3233/JCS-210140.

AQLLI UY IoT QURILMALARIDA MA’LUMOTLAR XAVFSIZLIGI MUAMMOLARI VA ULARNI KRIPTOGRAFIK HIMOYALASH YONDASHUVLARI

Yuldasheva N.S., Salimov S.A., Habibjonova G.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada aqlli uy tizimlarida qo‘llaniladigan buyumlar interneti (IoT) qurilmalarida ma’lumotlar xavfsizligi muammolari tizimli tahlil qilinadi. 2010-yildan keyin nashr etilgan 58 ta ilmiy ish asosida asosiy tahdidlar tasniflangan va to‘rt qatlamli himoyalangan IoT arxitekturasi (sezish, tarmoq, middleware, ilova) doirasida mavjud himoya usullarining afzallik va kamchiliklari baholangan. Resurslari cheklangan qurilmalar uchun yengil vaznli kriptografiya, autentifikatsiya va kalitlarni boshqarishni kompleks qo‘llash zarurati asoslanadi.

Kalit so‘zlar: buyumlar interneti, aqlli uy, ma’lumotlar xavfsizligi, yengil vaznli kriptografiya, autentifikatsiya, himoyalangan IoT arxitekturasi.

Аннотация. В статье проводится систематический анализ проблем безопасности данных в устройствах Интернета вещей (IoT), применяемых в системах «умного дома». На основе 58 научных работ, опубликованных после 2010 года, классифицированы основные угрозы, а также оценены преимущества и недостатки существующих методов защиты в рамках четырёхуровневой защищённой архитектуры IoT (уровень восприятия, сетевой уровень, промежуточное ПО, прикладной уровень). Обосновывается необходимость комплексного применения легковесной криптографии, аутентификации и управления ключами для устройств с ограниченными ресурсами.

Ключевые слова: Интернет вещей, умный дом, безопасность данных, легковесная криптография, аутентификация, защищённая архитектура IoT.

Kirish

Aqlli uy - sensorlar, maishiy qurilmalar va boshqaruv tizimlarini yagona tarmoqqa birlashtirib, uy xo‘jaligini masofadan boshqarish, energiyani tejash va xavfsizlikni ta’minlash imkonini beruvchi IoT ilovasidir [1]. Bunday tizimlarda ma’lumotlar uch manbadan shakllanadi: foydalanuvchi bilan passiv o‘zaro ta’sir (harakat sensorlari, kameralar, taqiladigan qurilmalar), faol o‘zaro ta’sir (ovozli buyruqlar, sensorli ekran) hamda foydalanuvchiga bog‘liq bo‘lmagan manbalar (termostat, havo oqimi sensorlari) [2]. Natijada uy egasining kundalik odatlari, joylashuvi, sog‘lig‘i va xavfsizlik tizimi haqidagi nozik ma’lumotlar tarmoq orqali uzatiladi va bulutda saqlanadi.

Muammoning dolzarbligi amaliy ko‘rsatkichlarda ham namoyon bo‘ladi: tadqiqotlarga ko‘ra aqlli uy IoT yechimlarining 80 foizi shaxsiy ma’lumotlar maxfiyligini buzadi, 80 foizdan ortig‘i yetarli uzunlik va murakkablikdagi parolni talab qilmaydi, 60 foizida esa foydalanuvchi interfeysida xavfsizlik nuqsonlari mavjud [2]. Shu bilan birga, IoT qurilmalarining cheklangan hisoblash quvvati, xotirasi va batareya resursi an’anaviy kriptografik usullarni to‘g‘ridan-to‘g‘ri qo‘llashga imkon bermaydi. Mazkur ishning maqsadi - aqlli uy IoT qurilmalaridagi ma’lumotlar xavfsizligi muammolarini tasniflash va mavjud himoya yondashuvlarini kriptografik nuqtai nazardan baholashdir.

Aqlli uy qurilmalari asosan simsiz protokollar orqali bog‘lanadi. 1-jadvaldan ko‘rinib turibdiki, ular chastota, uzoqlik va topologiya jihatidan farq qilsa-da, barchasi AES blokli shifriga tayanadi (Wi-Fi da u WPA2 tarkibidagi CCMP rejimida qo‘llaniladi). Demak, kanal darajasidagi

xavfsizlik algoritmning bardoshliligiga emas, balki kalitlarni yaratish, tarqatish va yangilash jarayonlarining to‘g‘ri tashkil etilishiga bog‘liq. Aynan shu bo‘g‘in amaliyotda eng zaif nuqta bo‘lib chiqmoqda.

1-jadval

Aqlli uyda qo‘llaniladigan simsiz aloqa protokollari [2]

Protokol	Chastota	Uzoqlik	Topologiya	Shifrlash
Wi-Fi 802.11n	2,4–5,8 GGs	10–100 m	Yulduz, daraxt, mesh	WPA2
Bluetooth LE	2,402–2,48 GGs	10–15 m	Yulduz	AES-128
ZigBee	868/915 MGs, 2,4 GGs	10–100 m	Yulduz, mesh, klaster	AES-128
Z-Wave	868/915 MGs	30–50 m	Mesh	AES-128
6LoWPAN	868/915 MGs, 2,4 GGs	10–100 m	Yulduz, mesh, P2P	AES-128

Tadqiqot uslubi

Tadqiqotda tizimli adabiyotlar sharhi (SLR) usuli qo‘llanildi. IEEE Xplore, Scopus va ScienceDirect bazalarida “qurilma xavfsizligi”, “tarmoq xavfsizligi”, “bulut xavfsizligi” va “ilova xavfsizligi” yo‘nalishlari bo‘yicha dastlabki qidiruvda 6711 ta nashr aniqlandi. Annotatsiya, kirish va xulosalarni tahlil qilish orqali saralangandan so‘ng 58 ta maqola chuqur tahlilga olindi: ularning 9 foizi qurilma, 30 foizi tarmoq, 20 foizi bulut va 41 foizi ilova xavfsizligiga bag‘ishlangan [2]. Har bir usul himoya kuchi, muammoni hal etish samaradorligi va barcha turdagi IoT qurilmalarida universal qo‘llanish imkoniyati mezonlari bo‘yicha baholandi.

Asosiy qism

Tahlil natijasida aqlli uydagi ma’lumotlar xavfsizligi muammolari uch guruhga ajratildi. Birinchisi - tarmoq bilan bog‘liq muammolar: shifrlashning yo‘qligi yoki zaifligi, autentifikatsiya kamchiliklari, himoyalanmagan simsiz kanallar, paketlarning yo‘qolishi, DoS, “o‘rtadagi odam” hujumlari va tinglash. Ikkinchisi - arxitekturaviy muammolar: qurilmalar va protokollarning turli-tumanligi (heterogenlik), ma’lumot manbalaridagi nosozliklar, uy shlyuzini zararlovchi viruslar hamda umumiy xavfsizlik protokolining yo‘qligi. Uchinchisi - ish jarayoni bilan bog‘liq muammolar: foydalanuvchiga noto‘g‘ri ma’lumot yetkazib, uning qaror qabul qilishiga ta’sir ko‘rsatish va hujumga javob berish vaqtining kechikishi.

Real hujumlar ushbu zaifliklarning amaliy xavfini tasdiqlaydi. Jumladan, ZigBee/IEEE 802.15.4 tarmoqlarida kalit yangilanishi ochiq matnda uzatilishi sababli hujumchi shifrlash kalitini tutib olib, paketlarni dekodlash va o‘zgartirish imkoniga ega bo‘lgani, Z-Wave eshik qulflarida esa avtorizatsiyasiz to‘liq kirishga yo‘l qo‘ygan zaiflik aniqlangan [2]. Bundan tashqari, ishlab chiqaruvchilarning qurilmalarga qattiq kodlangan (hardcoded) parollarni joylashi autentifikatsiya tizimining jiddiy buzilishiga olib keladi. ZigBee orqali ma’lumot uzatishda yo‘qotishlar 0,4 foizni, masofaviy videokuzatuv yoqilganda esa 7,6 foizni tashkil etishi qayd etilgan [2].

Simsiz sensor tarmoqlarida marshrutlashga qarshi hujumlar alohida xavf tug‘diradi [3]. “Sinkhole” hujumida g‘arazli tugun o‘zini eng qisqa yo‘l sifatida ko‘rsatib, trafikni o‘ziga jalb qiladi. “Selective forwarding” hujumida paketlarning bir qismi ataylab tashlab yuboriladi. “Sybil” hujumida bitta qurilma bir nechta soxta identifikator bilan ishlaydi. “Wormhole” hujumida esa paketlar tarmoqning bir nuqtasida yozib olinib, boshqa nuqtasida qayta uzatiladi. Muhimi, oxirgi hujum 6LoWPAN tarmog‘ida IPsec yordamida maxfiylik va yaxlitlik ta’minlangan holatda ham amalga oshirilishi mumkin [2]. Bu kanalni shifrlashning o‘zi yetarli emasligini, marshrut va tugunlarning haqiqiyligini ham tekshirish zarurligini ko‘rsatadi.

Aqlli uyga qilingan hujum oddiy axborot sizib chiqishi bilan cheklanmaydi. Tarmoqqa ulangan oddiy lyuminessent chiroqni ham boshqarib, uni ma’lum chastotada miltillatish orqali

yashovchilarga, xususan, fotosensitiv epilepsiyaga chalingan insonlarga jismoniy zarar yetkazish mumkinligi ko‘rsatilgan [2]. Shuningdek, hujum oqibatida moliyaviy zarar, shantaj, o‘g‘irlik, qurilmalarning ishdan chiqishi va uyga ruxsatsiz kirish holatlari yuzaga kelishi mumkin. Videokuzatuv, joylashuv va tibbiy ma’lumotlar kabi nozik axborotning qayta ishlanishi esa maxfiylik masalasini yanada keskinlashtiradi.

Himoya usullarini tizimlashtirish uchun to‘rt qatlamli himoyalangan IoT arxitekturasidan foydalanildi [4]. 2-jadvalda har bir qatlamdagi asosiy tahdidlar va ularga qarshi qo‘llaniladigan choralar umumlashtirilgan.

2-jadval

Himoyalangan IoT arxitekturasi qatlamlari bo‘yicha tahdid va himoya choralari

Qatlam	Asosiy tahdidlar	Kriptografik va boshqa himoya choralari
Perception (sezish)	Tugunni egallab olish, tugun nusxasini yaratish, tinglash, fizik kirish	Yengil vaznli shifrlash (masalan, Ascon), PUF asosidagi kalit hosil qilish, xavfsiz yuklanish
Tarmoq	DoS, “o‘rtadagi odam”, replay, sinkhole, wormhole, Sybil hujumlari	Seans kalitlari, autentifikatsiyalangan shifrlash, IPv6/6LoWPAN uchun hujumlarni aniqlash tizimlari (IDS)
Middleware	Qurilmalarning turli-tumanligi, ma’lumotni qayta ishlashda maxfiylik buzilishi	Yagona autentifikatsiya va kirishni boshqarish protokollari, himoyalangan saqlash
Ilova	Zaif parollar, qattiq kodlangan hisob ma’lumotlari, xavfsiz bo‘lmagan bulut interfeyslari	Ko‘p bosqichli autentifikatsiya, TLS, yangilanishlarni raqamli imzo bilan tasdiqlash

Sezish qatlamida apparat asosidagi himoya, xususan, fizik klonlanmaydigan funksiyalar (PUF) kam joy va energiya talab qilgani uchun IoT uchun qulay hisoblanadi. Biroq PUF qurilmaning qarishi va atrof-muhit sharoitlariga sezgir, dastlabki avlodlari analog sxemalarga asoslangani sababli raqamli tizimlarga integratsiyasi murakkab, an’anaviy ko‘rinishda esa faqat maxfiy kalitli protokollar bilan cheklangan [5]. Tarmoq qatlamida past quvvatli tarmoqlar uchun mo‘ljallangan RPL marshrutlash protokoli boshqaruv xabarlarini shifrlasa-da, ichki hujumchi va g‘arazli tugunlarga nisbatan zaif bo‘lib qolmoqda [6]. Mashinali o‘qitish va tabiiy tilni qayta ishlashga asoslangan avtomatlashtirilgan zaifliklarni baholash yondashuvi esa zaiflik ko‘rsatkichlarini o‘rtacha 90 foizdan yuqori aniqlikda bashorat qilishga erishgan [7].

Middleware qatlamida turli API lardan foydalanuvchi qurilmalarni yagona interfeys orqali bog‘lash bilan birga, ma’lumotni universal formatga o‘tkazishdan oldin autentifikatsiya va kirishni nazorat qilish protokollarini qo‘llash taklif etilgan. Ilova qatlamida esa ma’lumotlarni buzish (distortion) va shifrlash texnologiyalari, zaxira nusxa olish hamda tiklash mexanizmlari asosiy himoya vositalari hisoblanadi. Tahlil qilingan asosiy usullarning afzallik va kamchiliklari 3-jadvalda keltirilgan.

3-jadval

Mavjud himoya usullari va ularning cheklovlari [2]

Usul (muallif)	Afzalligi	Cheklovi
Apparat asosidagi himoya, PUF/PPUF (Xu va boshq.)	Kam joy va energiya, qurilmaga xos kalit	Qarish va muhitga sezgirlik, analog sxemalar

Sensor tarmog‘ida seans kaliti (Li va boshq.)	Maxfiylik va autentifikatsiyani oshiradi	Sekin ishlaydi, maxfiy kalitli protokollar bilan cheklangan
RPL protokoli (Winter va boshq.)	Past quvvatli tarmoqlarga moslashgan	Ichki hujumchi va g‘arazli tugunlarga zaif
ML va NLP asosida zaiflikni baholash (Duan va boshq.)	Ko‘rsatkichlarni 90% dan yuqori aniqlikda bashorat qiladi	Jarayon murakkab, resurs talab qiladi
Kerberos asosidagi autentifikatsiya	Shlyuz–terminal guruhida ishonchli autentifikatsiya	Past quvvatli qurilmalar uchun og‘ir
Middleware orqali ma’lumotga kirish (Hammergren, Thomas)	Turli API larni yagona autentifikatsiya bilan birlashtiradi	Faqat aniq sharoitlar uchun yaratiladi
Nol yig‘indili o‘yin modeli (Chen va boshq.)	Maqsadli hujumlarda IoT barqarorligini oshiradi	Eng yomon holat stsenariysi bilan cheklangan
Tavsiya tizimi (Kim, Lee)	Ma’lumot uzatishdagi muammolarni tashxislaydi	Foydalanuvchi xulq-atvoriga tayanadi, xavfsizlik uchun kam samarali

Kriptografik nuqtai nazardan tahlil qilinganda, simmetrik va asimmetrik shifrlashning klassik usullari kichik mikrokontrollerlar uchun energiya va hisoblash jihatidan og‘irlik qiladi. Shu bois elliptik egri chiziqlar kriptografiyasi (ECC) kabi murakkab matematik amallar o‘rniga bitli amallarga asoslangan yengil vaznli algoritmlar tavsiya etiladi [2]. Bu yo‘nalishda NIST tomonidan 2023-yilda yengil vaznli kriptografiya standarti sifatida tanlangan va 2025-yilda NIST SP 800-232 hujjatida rasman e’lon qilingan Ascon algoritmlar oilasi alohida ahamiyatga ega: u 320 bitli holatga ega “gubka” konstruksiyasi asosida autentifikatsiyalangan shifrlash (AEAD) va xeshlashni bitta ixcham amalda bajaradi [8; 9]. Bundan tashqari, ISO/IEC 29192-2 standartiga kiritilgan PRESENT blokli shifri (64 bitli blok, 80 yoki 128 bitli kalit) apparat realizatsiyasi uchun, ARX (qo‘shish, siljitish, XOR) amallariga asoslangan algoritmlar esa dasturiy realizatsiya uchun qulay hisoblanadi [10]. Algoritm tanlashda faqat nazariy bardoshlilik emas, balki operativ xotira sarfi, kod hajmi, bitta baytni shifrlash uchun sarflanadigan energiya va bajarilish vaqti ham hisobga olinishi zarur. Blokcheyn asosidagi yechimlar markazlashmagan xavfsizlik va psevdonimlikni ta’minlasa-da, sezilarli hisoblash va energiya sarfini talab qiladi; dasturiy belgilanuvchi tarmoqlar (SDN) esa markazlashgan boshqaruv orqali qurilmalarni avtomatik aniqlash va nazorat qilish imkonini beradi.

Tahlil asosida quyidagi kompleks yondashuv taklif etiladi: (1) sezish qatlamida PUF yordamida qurilmaga xos kalitni hosil qilish va uni himoyalangan xotirada saqlash; (2) tugun va shlyuz o‘rtasida yengil vaznli autentifikatsiyalangan shifrlash hamda vaqtinchalik seans kalitlaridan foydalanish; (3) uy shlyuzida IPv6/6LoWPAN trafigi uchun hujumlarni aniqlash tizimini joylashtirish; (4) ilova qatlamida ko‘p bosqichli autentifikatsiya va proshivka yangilanishlarini raqamli imzo bilan tasdiqlashni majburiy qilish. Bunday yondashuvda resurs talab qiluvchi amallar shlyuz va bulutga o‘tkazilib, chekka qurilmalarga faqat yengil operatsiyalar qoldiriladi.

Kalitlarni boshqarish ushbu yondashuvning markaziy bo‘g‘ini hisoblanadi. Kalitning to‘liq hayot sikli - yaratish, tarqatish, saqlash, yangilash va bekor qilish - ishonchli tashkil etilmasa, eng bardoshli algoritm ham samarasiz bo‘lib qoladi. ZigBee dagi hodisa buni yaqqol ko‘rsatadi: AES-128 buzilmagan, lekin kalit ochiq matnda uzatilgani uchun himoya yo‘qqa chiqqan. Shu sababli

kalitlarni almashishni dastlabki ulanish bosqichida qurilmaga xos sertifikat yoki PUF javobi bilan himoyalash, qattiq kodlangan parollardan butunlay voz kechish va har bir qurilma uchun noyob dastlabki kalitni majburiy qilish tavsiya etiladi. Shuningdek, yon-kanal hujumlari va nosozlik kiritish xavfini kamaytirish uchun maxfiy kalitlar himoyalangan apparat xotirasida saqlanishi lozim.

Taklif etilgan yondashuvni baholash uchun quyidagi mezonlar tavsiya etiladi: kriptografik bardoshlilik; qurilmadagi xotira va energiya sarfi; javob berish vaqti; turli protokolli qurilmalar bilan moslik; kalitlarni almashtirish va bekor qilishning qulayligi; ichki hujumchiga qarshi chidamlilik. Tahlil qilingan ishlarning aksariyati ushbu mezonlarning faqat bir-ikkitasini hisobga olgani mavjud yechimlarning asosiy kamchiligi sifatida baholandi.

Xulosa

Tadqiqot natijalari aqlli uy IoT tizimlarida ma’lumotlar xavfsizligi muammolarining asosiy manbai qurilmalarning turli-tumanligi, himoyalanmagan simsiz kanallar va resurslarning cheklanganligi ekanini ko‘rsatdi. Mavjud yechimlarning aksariyati arxitekturaning faqat bitta qatlamini qamrab oladi va barcha qurilmalar uchun universal emas; IPv6 ga ulangan IoT qurilmalari uchun hujumlarni aniqlash tizimlari hamon kam. Shu sababli kalitlarni boshqarish, autentifikatsiya va kirishni nazorat qilish mexanizmlari energiya jihatidan tejamkor bo‘lishi, yengil vaznli kriptografiya esa barcha qatlamlarni qamrab oluvchi yagona xavfsizlik arxitekturasi doirasida qo‘llanilishi lozim. Bundan tashqari, aqlli uy ishlab chiqaruvchilari uchun xavfsizlik talablarini standartlashtirish, xususan, qattiq kodlangan parollarni taqiqlash va proshivkani xavfsiz yangilash mexanizmini majburiy qilish zarur. Kelgusi tadqiqotlar uchun formal verifikatsiya usullarini mashinali o‘qitish bilan birlashtirish va IoT qurilmalari xavfsizlik darajasini baholashning standartlashtirilgan tartibini ishlab chiqish dolzarb yo‘nalish hisoblanadi.

Foydalanilgan adabiyotlar

1. Stojkoska B. L. R., Trivodaliev K. V. A review of Internet of Things for smart home: Challenges and solutions // Journal of Cleaner Production. – 2017. – Vol. 140. – P. 1454–1464.

2. Issi H. N. A Systematic Study of Data Security Issues in Smart Home IoT Devices: Master’s thesis. – University of Alabama at Birmingham, 2022. – 73 p.

3. Karlof C., Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures // Ad Hoc Networks. – 2003. – Vol. 1, No. 2–3. – P. 293–315.

4. Krishna B. V. S., Gnanasekaran T. A systematic study of security issues in Internet-of-Things (IoT) // 2017 International Conference on I-SMAC. – IEEE, 2017. – P. 107–111.

5. Xu T., Wendt J. B., Potkonjak M. Security of IoT systems: Design challenges and opportunities // 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). – 2014. – P. 417–423.

6. Winter T. et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. – RFC 6550, 2012.

7. Duan X. et al. Automated Security Assessment for the Internet of Things // 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC). – 2021. – P. 47–56.

8. NIST. Lightweight Cryptography Standardization Project. – https://csrc.nist.gov/projects/lightweight-cryptography.

9. Dobraunig C., Eichlseder M., Mendel F., Schläffer M. Ascon v1.2: Lightweight Authenticated Encryption and Hashing // Journal of Cryptology. – 2021. – Vol. 34. – Art. 33.

10. Bogdanov A. et al. PRESENT: An Ultra-Lightweight Block Cipher // CHES 2007, LNCS 4727. – Springer, 2007. – P. 450–466.

DIPFEYK VA SUN’IY INTELLEKT YORDAMIDAGI FISHING HUJUMLARI TAHLILI VA KO‘P QATLAMLI HIMOYA MODELI

Xusenov Sh.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada sun’iy intellekt (SI) yordamida qilinayotgan dipfeyk (deepfake) va maqsadli fishing hujumlari o‘rganildi. Tahlil 13 ta manba va ikkita real holatga tayandi. Hujumchilar tizimning texnik zaifligidan emas, odamning ishonchidan foydalanishi ko‘rsatildi. Shu asosda texnik, tashkiliy, individual va huquqiy choralarni bir-biriga bog‘laydigan himoya modeli taklif qilindi; unda e’tibor soxta kontentni aniqlashdan jarayonni mustaqil kanal orqali tekshirishga ko‘chirilgan.

Kalit so‘zlar: kiberxavfsizlik, sun’iy intellekt, dipfeyk, fishing, ijtimoiy muhandislik, ovozni klonlash, ko‘p qatlamli himoya modeli.

Аннотация. В статье рассматриваются дипфейки (deepfake) и целевые фишинговые атаки, осуществляемые с помощью искусственного интеллекта (ИИ). Анализ основан на 13 источниках и двух реальных случаях. Показано, что злоумышленники используют не технические уязвимости систем, а доверие людей. На этой основе предложена модель многоуровневой защиты, объединяющая технические, организационные, индивидуальные и правовые меры. В данной модели акцент смещён с выявления поддельного контента на независимую проверку запросов через альтернативные каналы связи.

Ключевые слова: кибербезопасность, искусственный интеллект, дипфейк, фишинг, социальная инженерия, клонирование голоса, многоуровневая модель защиты.

Kirish

Generativ sun’iy intellekt (SI) – katta til modellari hamda tasvir va ovoz sintezi tizimlari – ommalashgach, ishonarli matn, kishining ovozi va hatto video ko‘rinishi bir necha daqiqada, arzon vosita bilan yaratilmoqda. AQSh Federal tergov byurosining Internet jinoyatlar markazi (IC3) 2023-yilda internet jinoyatlaridan 12,5 mlrd dollardan ortiq zarar ko‘rilganini, shundan taxminan 2,9 mlrd dollari korporativ elektron pochtaga hujumlar (BEC) hissasiga to‘g‘ri kelganini yozgan [1]. Verizon tahlil qilgan hodisalarning 68 foizida inson omili, ya’ni xato yoki aldanish ishtirok etgan [2]. Dipfeyk deganda sun’iy neyron tarmoqlar yordamida yaratilgan yoki o‘zgartirilgan ovoz, tasvir va videolar tushuniladi; atama chuqur o‘rganish (deep learning) va soxta (fake) so‘zlaridan olingan bo‘lib [3, 4], texnik asosi esa generativ raqobatli tarmoqlardir (GAN) [9]. Maqsad – hujumlar qanday ishlashini aniqlash, real holatlardan qonuniyat topish va shunga tayanib himoya modelini taklif qilishdir.

Tadqiqot metodikasi

Ish tahliliy-sharhlovchi (review) xarakterga ega hisoblanib, tahlilga 13 ta manba olindi: to‘rtta ilmiy nashr (ACM Computing Surveys [4], California Law Review [3], NeurIPS (NIPS) materiallari [9] va arXiv preprinti [5]), bitta monografiya [11], to‘rtta rasmiy yoki sohaviy hisobot (FBI IC3 [1], Verizon [2], NIST [6], Sumsub [10]), ikkita yetakchi ommaviy axborot vositasi materiali (WSJ [7], CNN [8]) va ikkita qonun [12, 13]. Manbalar to‘rt mezon bo‘yicha tanlandi: ilmiy yoki rasmiy xarakterda bo‘lishi, ma’lumotni tekshirib ko‘rish mumkinligi, asosan 2019–2025-yillarga tegishli bo‘lishi (asos solgan asarlar [9, 11] bundan mustasno) hamda hujum mexanizmini, real holatni yoki himoya chorasini yoritishi. Avval manbalar o‘qilib, hujum

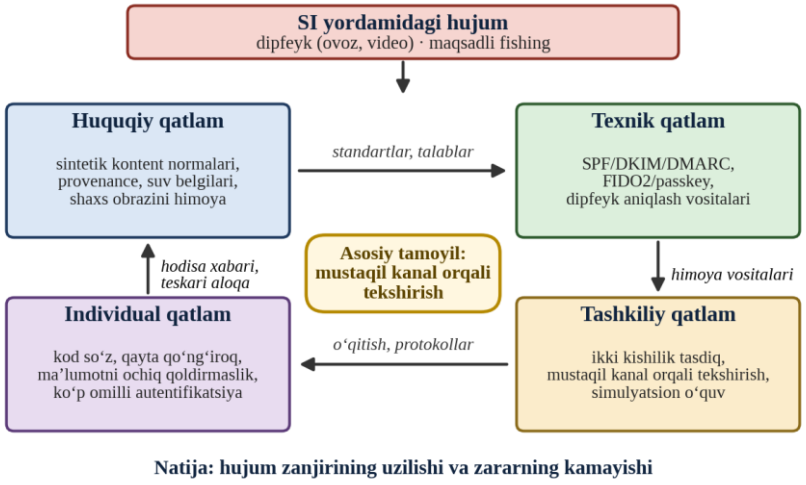
mexanizmlari va raqamli ko‘rsatkichlar ajratib olindi. Keyin ikki hodisa – 2019-yilda Buyuk Britaniyadagi energetika kompaniyasiga qilingan ovozli dipfeyk hujumi [7] va 2024-yilda Gonkongdagi Arup kompaniyasiga qilingan videokonferensiya hujumi [8] – holatlar tahlili (case study) usulida o‘rganildi. Oxirida hujum turlari va himoya choralari solishtirilib, qatlamlar bo‘yicha guruhlandi.

Natijalar

Heiding va hammualliflarning tajribasida SI to‘liq o‘zi yozgan fishing xabarlari ishtirokchilarning 54 foizini havolani bosishga undagan; bu mutaxassis odam yozgan xabarlar natijasiga teng, shaxsiylashtirilmagan nazorat xabarida esa ko‘rsatkich 12 foiz atrofida bo‘lgan [5]. Sumsub 2022-yildan 2023-yilgacha aniqlangan dipfeyk holatlari taxminan o‘n marta ko‘payganini xabar qilgan [10], bu raqam faqat tendensiyani ko‘rsatadi. Holatlar tahlilida 2019-yilgi hodisada energetika kompaniyasi rahbari nemis bosh kompaniya rahbarining klonlangan ovozini eshitib, taxminan 220 ming yevro o‘tkazgan [7]. 2024-yilda Arup moliya xodimi videokonferensiyada ko‘ringan hamkasblarining barchasi dipfeyk ekanini bilmay, bir necha tranzaksiya bilan taxminan 25 mln AQSh dollari yuborgan [8]. Ikkala holatda ham firibgar shoshilinchlik, yuqori mansabdor shaxs obro‘si va maxfiylik talabidan foydalangan; bular ijtimoiy muhandislikning eski usullaridir [11]. Bundan chiqadigan xulosa shuki, ko‘z va quloqqa ishonish endi tekshiruv bo‘la olmaydi, himoya esa soxta kontentni topishga emas, buyruqni mustaqil kanal orqali tasdiqlashga tayanishi kerak.

Himoya modeli va uning ilmiy yangiligi

Taklif qilinayotgan model to‘rt qatlamdan iborat (1-rasm). Texnik qatlamda SPF, DKIM va DMARC protokollari hamda FIDO2 kalitlari yoki passkey qo‘llanadi; ular faqat haqiqiy domen bilan ishlagani uchun fishing saytga kiritilgan ma’lumotdan foydalanib bo‘lmaydi. Dipfeykni aniqlash dasturlari foydali, lekin yaratish va aniqlash texnologiyalari doimiy poygada bo‘lgani uchun ular yagona himoya bo‘la olmaydi [4]. Tashkiliy qatlamda katta summali o‘tkazmani ikki xodim tasdiqlaydi, so‘rov oldindan ma’lum boshqa kanal orqali tekshiriladi, xodimlar dipfeyk namunalari bilan simulyatsiya mashg‘ulotlaridan o‘tadi. Individual qatlam oddiy foydalanuvchiga mo‘ljallangan: oilada kod so‘z kelishib olish, shubhali qo‘ng‘iroqni to‘xtatib o‘zi qayta qo‘ng‘iroq qilish, ovoz va videoni ijtimoiy tarmoqda ortiqcha qoldirmaslik, ko‘p omilli autentifikatsiyani yoqish. Huquqiy qatlamga sintetik kontentning kelib chiqishini belgilash (provenance) va suv belgilari kiradi [6]. O‘zbekistonda “Shaxsga doir ma’lumotlar to‘g‘risida”gi (2019) va “Kiberxavfsizlik to‘g‘risida”gi (2022) qonunlar [12, 13] mavjud, biroq sintetik kontent hamda shaxs ovozi va qiyofasidan ruxsatsiz foydalanishga oid aniq norma hozircha yo‘q.



1-rasm. Ko‘p qatlamli himoya modelining tuzilmasi va qatlamlararo bog‘lanishlar

Tahlil qilingan manbalarda himoya ko‘pincha alohida yo‘nalish sifatida ko‘riladi: dipfeykni aniqlash [4], kontent shaffofligi [6] yoki xodimlarni o‘qitish [11]. Taklif qilinayotgan modelning ilmiy yangiligi, ya’ni mavjud yondashuvlardan farqi uch narsada. Birinchidan, qatlamlar bir-biriga bog‘langan: huquqiy qatlam talab va standartni belgilaydi, texnik qatlam ularni vositaga, tashkiliy qatlam vositani qoidaga aylantiradi, individual qatlam esa amaldagi hodisalar haqidagi xabarni qaytarib uzatadi. Ikkinchidan, markaz soxtani aniqlashdan jarayonni mustaqil kanal orqali tekshirishga o‘tkazilgan, shuning uchun model hali ma’lum bo‘lmagan dipfeyk turlariga ham mos keladi. Uchinchidan, model oddiy foydalanuvchini va O‘zbekistonning huquqiy sharoitini ham hisobga oladi.

Xulosa

SI firibgarlikni arzonlashtirdi va ommalashtirdi: tanish ovoz, yuz va to‘g‘ri yozilgan matn endi ishonch belgisi emas, hujum quroliga aylanmoqda. Shu sababli taklif qilingan model “ko‘rganingga ishonma, jarayonni tekshir” tamoyiliga tayanadi. Model hozircha konseptual va amalda sinalmagan, statistika asosan AQSh va global hisobotlardan olingan; keyingi bosqichda uni mahalliy tashkilotlarda baholash rejalashtirilgan.

Foydalanilgan adabiyotlar

1. FBI Internet Crime Complaint Center (IC3). Internet Crime Report 2023. FBI, 2024.
2. Verizon. 2024 Data Breach Investigations Report. Verizon, 2024.
3. Chesney R., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review, 2019, Vol. 107, No. 6, pp. 1753–1819.
4. Mirsky Y., Lee W. The Creation and Detection of Deepfakes: A Survey // ACM Computing Surveys, 2021, Vol. 54, No. 1, Article 7.
5. Heiding F., Lermen S., Kao A., Schneier B., Vishwanath A. Evaluating Large Language Models’ Capability to Launch Fully Automated Spear Phishing Campaigns. – arXiv:2412.00586, 2024.
6. NIST AI 100-4. Reducing Risks Posed by Synthetic Content. NIST, 2024.
7. Stupp C. Fraudsters Used AI to Mimic CEO‘s Voice in Unusual Cybercrime Case // The Wall Street Journal, 30.08.2019.
8. Chen H., Magramo K. Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’ // CNN, 04.02.2024.
9. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative Adversarial Nets // Advances in Neural Information Processing Systems (NIPS), 2014, Vol. 27.
10. Sumsub. Identity Fraud Report 2023. – Sumsub, 2023.
11. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. – Wiley, 2018.
12. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, 2019-yil 2-iyul, O‘RQ-547.
13. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 2022-yil 15-aprel, O‘RQ-764.

GENERATIV SUN'IY INTELLEKT MUHITIDA MAXFIY AXBOROTNI SIZIB CHIQISHDAN HIMOYALASH

Bozorov O.N.
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti

Annotatsiya. Tezisda generativ sun'iy intellekt (SI) muhitida maxfiy axborot sizib chiqishining yangi kanallari tahlil qilinadi va matnli DLP klassifikatorlarini chetlab o‘tishga qaratilgan adversarial o‘zgartirishlar tizimlashtiriladi. Hujumlar to‘rt sinfga ajratiladi, har bir sinf uchun himoya usuli taklif etiladi va ular yagona ko‘p qatlamli aniqlash sxemasiga birlashtiriladi.

Kalit so‘zlar: maxfiy axborot sizib chiqishi, DLP, katta til modellari, adversarial barqarorlik, normallashtirish, sessiya tahlili, o‘zbek tili.

Аннотация. В диссертации анализируются новые каналы утечки конфиденциальной информации в среде генеративного искусственного интеллекта (ИИ) и систематизируются модификации, направленные на обход классификаторов текстовой утечки конфиденциальной информации (DLP). Атаки разделены на четыре класса, для каждого класса предложен метод защиты, и они объединены в единую многоуровневую схему обнаружения.

Ключевые слова: утечка конфиденциальной информации, DLP, большие языковые модели, устойчивость к атакам, нормализация, анализ сессий, узбекский язык.

Katta til modellari (KTM) asosidagi xizmatlar tashkilotlar faoliyatiga tez kirib kelmoqda. Xodim hujjatni tahrirlash, tarjima qilish yoki qisqacha mazmunini olish uchun uni tashqi SI xizmatiga yuklasa, ma'lumot tashkilot nazoratidan chiqib ketadi. OWASP KTM ilovalari xavflari ro‘yxatida maxfiy axborot oshkor bo‘lishini alohida ajratgan [1]. Modellar o‘qitish ma'lumotlarini eslab qolishi va ulardan ma'lumot qayta chiqarib olinishi [2], SI agentlari esa bilvosita prompt-in'ektsiya orqali ma'lumotlarni tashqariga uzatishga majburlanishi mumkinligi [3] ham ko‘rsatilgan.

Zamonaviy DLP tizimlarida matn ma'nosini tahlil qiluvchi neyron klassifikatorlar qo‘llaniladi, biroq ular sinonim bilan almashtirish [4], harf darajasidagi buzilishlar [5], ko‘rinmas Unicode belgilar va tashqi ko‘rinishi bir xil harflar [6] kabi kichik o‘zgartirishlarga zaif. Generativ SI bu muammoni keskinlashtiradi: endi matnni KTM yordamida bir necha soniyada qayta yozish mumkin. O‘zbek tilida ikki yozuv (lotin va kirill) hamda tutuq belgisining bir necha shakli (o‘, o', o‘, o`) mavjudligi zaiflikni yanada kuchaytiradi. Mavjud ishlarda barqarorlik asosan empirik baholanadi, DLP vazifasi uchun esa uning nazariy asoslari yetarlicha ishlab chiqilmagan.

Tadqiqot maqsadi – generativ SI muhitida maxfiy axborot sizib chiqishini adversarial o‘zgartirishlarga barqaror holda aniqlash usullarini ishlab chiqish.

Sizib chiqishning to‘rt asosiy kanali ajratiladi: tashqi KTMga yuboriladigan so‘rovlar; SI xizmatlariga yuklanadigan fayllar; SI agentlari va RAG tizimlarining tashqi manbalarga murojaatlari; korporativ ma'lumotlarda o‘qitilgan modellarning o‘zi. Sizdiruvchi ehtiyotsiz xodim yoki nazoratni chetlab o‘tishga urinuvchi shaxs bo‘lishi mumkin. Ikkinchi holatda u matnning ma'nosini saqlagan holda uni o‘zgartiradi va klassifikatorning maxfiylik bahosi $f(x)$ ni qaror chegarasi θ dan pastga tushirishga harakat qiladi ($f(x) \geq \theta$ bo‘lsa, matn maxfiy deb topiladi).

Hujumchi qo‘llaydigan obfuskatsiya, ya'ni nazoratni chetlab o‘tish uchun matnni niqoblash usullari to‘rt sinfga ajratiladi va har biriga alohida himoya usuli mos qo‘yiladi.

1. Grafik obfuskatsiya – lotin va kirill harflarini aralashtirish, tashqi koʻrinishi bir xil harflar (a/a, o/o, e/e, x/x, c/c), koʻrinmas Unicode belgilar, tutuq belgisining turli shakllari. Ularga qarshi klassifikatsiyadan oldin matnni yagona kanonik koʻrinishga keltiruvchi normallashtirish qoʻllaniladi: koʻrinmas belgilar oʻchiriladi, gomogliflar almashtiriladi, matn yagona yozuvga oʻtkaziladi. Belgilangan kanoniklashtirish qoidalari doirasida yozuv sathidagi ekvivalent oʻzgartirishlarning klassifikatsiya natijasiga ta'siri bartaraf etiladi. Oʻzbek tilida yozuvlar orasidagi moslik har doim bir qiymatli emas (masalan, «sh», «ch» birikmalari, «ц», «ъ» harflari), shuning uchun normallashtirish qoidalari maxsus ishlab chiqilishi lozim.

2. Semantik obfuskatsiya – parafraz, sinonim bilan almashtirish, KTM yordamida qayta yozish. Bunda matnning vektorli koʻrinishi biroz oʻzgaradi. Tasvir δ ga siljiganda baho koʻpi bilan $L \cdot \delta$ ga oʻzgaradi, shuning uchun har bir matn uchun barqarorlik zaxirasi

$$r(x) = \frac{|f(x) - \theta|}{L}$$

hisoblanadi: oʻzgartirish $r(x)$ dan kichik boʻlsa, qaror oʻzgarmaydi [8]. Bu baho f funksiyasi tanlangan vektorli tasvirlar metrikasida L-Lipshits shartini qanoatlantirganda oʻrinli. Zaxirasi kichik matnlar qoʻshimcha tekshiruvga yuboriladi. Zaxirani oshirish uchun oʻqitish toʻplami KTM yaratgan parafrazlar bilan boyitiladi (adversarial oʻqitish [9]).

3. Tillararo obfuskatsiya – boshqa tilga tarjima qilish, tillarni aralashtirish, base64 kabi kodlashlar, matnni rasm koʻrinishida yuborish. Koʻp tilli vektorli tasvirlarda [7] turli tillardagi bir xil ma'noli matnlar yaqin joylashgani sababli klassifikator tarjimaga nisbatan barqarorroq boʻladi. Kodlangan qismlar oldindan ochiladi, rasmdagi matn esa optik tanib olish orqali chiqarib olinadi.

4. Fragmentar obfuskatsiya – hujjatni kichik qismlarga boʻlib, bir necha soʻrov orqali yuborish. Alohida boʻlaklar xavfsiz koʻrinishi mumkinligi sababli xavf butun sessiya boʻyicha yigʻiladi:

$$R_t = \mathrm{e}^{-\Delta t/\tau} \cdot R_{t-1} + s_t,$$

bunda s_t – t-soʻrovning maxfiylik bahosi, Δt – soʻrovlar oraligʻi, τ – xavfning soʻnish vaqt masshtabi; R_t chegaradan oshsa, harakat bloklanadi. Unutish soʻrovlar soniga emas, vaqtga bogʻlangani sababli hujumchi boʻlaklar orasiga oddiy soʻrovlar qoʻshib xavfni «suyultira» olmaydi, boʻlaklar orasidagi vaqtni uzaytirish esa sizdirishni sekinlashtiradi. τ himoya kuchi va yolgʻon signallar soni oʻrtasidagi muvozanat asosida tanlanadi.

Usullar ketma-ket qatlamlarga birlashtiriladi: normallashtirish va dekodlash → koʻp tilli tasniflash va zaxirani hisoblash → sessiya xavfini yangilash → qaror qabul qilish. Qaror uch darajali: ruxsat berish, qoʻshimcha tekshiruv (zaxira kichik yoki sessiya xavfi chegaraga yaqin) va bloklash. Bu asossiz bloklashlarni kamaytiradi va shubhali holatlarni xavfsizlik xodimiga yoʻnaltiradi.

Maxfiy va ochiq oʻzbek tilidagi matnlarga toʻrt sinf hujumlarini avtomatik qoʻllash orqali adversarial test toʻplami yaratiladi. Asosiy koʻrsatkichlar: hujum muvaffaqiyati ulushi, hujumdan oldingi va keyingi toʻliqlik (recall), oddiy soʻrovlardagi yolgʻon signallar ulushi. Har bir himoya qatlamining hissasi ablatsiya orqali aniqlanadi.

Xulosa

Generativ SI muhitida DLP klassifikatorlarini chetlab oʻtishga qaratilgan hujumlar toʻrt sinfga ajratilib, har biri uchun himoya usuli taklif etildi: normallashtirish, barqarorlik zaxirasi va adversarial oʻqitish, koʻp tilli tasvirlar va dekodlash, sessiya boʻyicha xavfni yigʻish. Usullar uch darajali qarorga ega yagona sxemaga birlashtirildi. Natijalar oʻzbek tilidagi hujjatlar bilan ishlovchi tashkilotlarda DLP tizimlarini generativ SI muhitiga moslashtirishda qoʻllanilishi

mumkin. Kelgusi tadqiqotlar adversarial test to‘plamini yaratish, L konstantani amalda baholash usulini ishlab chiqish va taklif etilgan usullarni eksperimental tekshirishga qaratiladi.

Foydalanilgan adabiyotlar

1. OWASP Top 10 for Large Language Model Applications. OWASP Foundation, 2025.
2. Carlini N., Tramèr F., Wallace E. et al. Extracting Training Data from Large Language Models // Proc. 30th USENIX Security Symposium. 2021. P. 2633–2650.
3. Greshake K., Abdelnabi S., Mishra S. et al. Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // Proc. 16th ACM Workshop on Artificial Intelligence and Security (AISec). 2023. P. 79–90.
4. Jin D., Jin Z., Zhou J. T., Szolovits P. Is BERT Really Robust? A Strong Baseline for Natural Language Attack on Text Classification and Entailment // Proc. AAAI Conference on Artificial Intelligence. 2020. Vol. 34. P. 8018–8025.
5. Li J., Ji S., Du T., Li B., Wang T. TextBugger: Generating Adversarial Text Against Real-world Applications // Proc. NDSS Symposium. 2019.
6. Boucher N., Shumailov I., Anderson R., Papernot N. Bad Characters: Imperceptible NLP Attacks // Proc. 2022 IEEE Symposium on Security and Privacy (SP). 2022. P. 1987–2004.
7. Conneau A., Khandelwal K., Goyal N. et al. Unsupervised Cross-lingual Representation Learning at Scale // Proc. 58th Annual Meeting of the ACL. 2020. P. 8440–8451.
8. Cohen J., Rosenfeld E., Kolter Z. Certified Adversarial Robustness via Randomized Smoothing // Proc. 36th International Conference on Machine Learning (ICML). PMLR 97. 2019. P. 1310–1320.
9. Madry A., Makelov A., Schmidt L., Tsipras D., Vladu A. Towards Deep Learning Models Resistant to Adversarial Attacks // Proc. ICLR. 2018.

KORPORATIV TARMOQLARDA ANOMALIYALARGA ASOSLANGAN HUJUMLARNI ANIQLASH TIZIMLARIDA YOLG‘ON SIGNALLAR MUAMMOSI VA BAHOLASH METODIKASINING DOLZARB MASALALARI

Raxmonaliyev S.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu ishda korporativ tarmoqlarda mashinaviy o‘rganish asosida ishlovchi anomaliyalarni aniqlash tizimlarining amaliy samaradorligiga ta’sir qiluvchi yolg‘on signallar muammosi ko‘rib chiqiladi. FPR va hujumlar ulushi o‘rtasidagi bog‘liqlik analitik misol orqali baholanadi. Natijalar past FPR qiymatlarining o‘zi ham yuqori hajmdagi korporativ trafik sharoitida sezilarli miqdorda yolg‘on ogohlantirish hosil qilishi mumkinligini ko‘rsatadi. Shu asosda tizimlarni baholashda TPR@FPR, PR-AUC, kunlik ogohlantirishlar soni va LOAO kabi mezonlardan foydalanish maqsadga muvofiqligi asoslanadi.

Kalit so‘zlar: korporativ tarmoq, hujumlarni aniqlash tizimi, anomaliyalarni aniqlash, mashinaviy o‘rganish, yolg‘on signallar, bazaviy chastota, ogohlantirish byudjeti.

Аннотация. В статье анализируется уровень ложных срабатываний как основной фактор, ограничивающий практическое применение систем обнаружения аномалий на основе машинного обучения в корпоративных сетях. На аналитическом примере показано, что из-за проблемы базовой частоты даже малые значения FPR приводят к большому числу ложных оповещений. Рассмотрены недостатки методов оценки на открытых наборах данных и обоснована необходимость оценки по полноте при фиксированном FPR, бюджету оповещений и протоколу исключения неизвестных атак (LOAO).

Ключевые слова: корпоративная сеть, система обнаружения вторжений, обнаружение аномалий, машинное обучение, ложные срабатывания, базовая частота, бюджет оповещений.

Kirish

So‘nggi yillarda korporativ tarmoqlarga qarshi hujumlarning xarakteri sezilarli o‘zgardi. Buzg‘unchilar zararli fayl yuklash o‘rniga tobora ko‘proq haqiqiy hisob ma’lumotlari va operatsion tizimning qonuniy vositalaridan foydalanmoqda (living off the land, LOTL). Bunday faoliyat oldindan ma’lum namunalarga, ya’ni signaturalarga ega bo‘lmaydi. NIST SP 800-94 qo‘llanmasida ham signaturali aniqlash ma’lum tahdidlarga qarshi samarali bo‘lsa-da, ilgari uchramagan hujumlar va ma’lum hujumlarning yangi variantlari oldida ojiz qolishi qayd etilgan [2].

Mazkur cheklovni bartaraf etishga qaratilgan muhim yondashuvlardan biri D. Denning tomonidan 1987-yilda taklif qilingan: tizimning normal xulq-atvori profili quriladi va undan og‘ishlar hujum belgisi sifatida qaraladi [1]. Bugungi kunda bunday profillar asosan mashinaviy o‘rganish (machine learning, ML) yordamida quriladi. Shunga qaramay, anomaliyalarni aniqlash tizimlari korporativ amaliyotda kutilganchalik keng tarqalmadi. Buning asosiy sabablaridan biri – yolg‘on signallar (false positives) soni. Ushbu maqolada shu muammoning kelib chiqishi va uni to‘g‘ri baholash masalalari ko‘rib chiqiladi.

Asosiy qism

Korporativ tarmoqlarda barcha ehtimoliy hujumlarni to‘liq qamrab oluvchi va ishonchli yorliqlangan ma’lumotlar to‘plamini shakllantirish amaliy jihatdan murakkab: normal trafik hajmi

katta, hujumlar nisbatan kam va ayrim hujumlar oldindan noma’lum bo‘lishi mumkin. Shu sababli faqat normal trafikda o‘qitiladigan yarim nazoratli (semi-supervised) modellar – avtokodlovchi (autoencoder), bir sinfli tayanch vektorlar mashinasi (One-Class SVM, OC-SVM) va shu kabilar – bu sharoitga yaxshiroq mos keladi. Ular har bir tarmoq oqimiga anomaliya balini beradi, bal belgilangan τ chegaradan oshsa, oqim shubhali deb topiladi.

Muammo aynan shu chegarada. Amaliy tadqiqotlarda τ ayrim hollarda hujum yorliqlari mavjud bo‘lgan validatsiya ma’lumotlari asosida, jumladan F1 o‘lchovini optimallashtirish orqali tanlanadi. Real tarmoqda esa noma’lum hujumning yorlig‘i oldindan bo‘lmaydi, shuning uchun bunday sozlashni amalda takrorlab bo‘lmaydi. R. Sommer va V. Paxson ham tarmoq hujumlarini aniqlash ML qo‘llaniladigan boshqa sohalarga qaraganda ancha murakkab masala ekanini, xatolar narxi esa bu yerda ayniqsa yuqori ekanini ko‘rsatib bergan [4].

Yolg‘on signallar muammosining mohiyatini bazaviy chastota bilan izohlash mumkin [3]. Hujum oqimlari umumiy trafikning juda kichik qismini tashkil etadi, shuning uchun hatto past FPR ham kuniga ko‘p sonli yolg‘on ogohlantirish beradi:

$$FP \approx FPR \cdot N_{norm}, \quad (1)$$

bu yerda N_{norm} – kuniga kuzatiladigan normal oqimlar soni. Ogohlantirishlar ichidagi haqiqiy hujumlar ulushi, ya’ni aniqlik (precision) quyidagicha topiladi:

$$P = TPR \cdot N_{att} / (TPR \cdot N_{att} + FPR \cdot N_{norm}), \quad (2)$$

bu yerda N_{att} – hujum oqimlari soni, TPR – aniqlash darajasi.

Bog‘liqlikni ko‘rsatish uchun shartli misol olamiz: tarmoqda kuniga 10^6 normal va 100 ta hujum oqimi o‘tadi, detektor hujumlarning 90 foizini aniqlaydi. (1) va (2) formulalar bo‘yicha hisoblangan natijalar 1-jadvalda berilgan. Ta’kidlash kerakki, bu qiymatlar o‘lchov natijasi emas, tanlangan faraziy parametrlar uchun bajarilgan hisobdir.

1-jadval

FPR qiymatiga qarab kunlik yolg‘on ogohlantirishlar soni va aniqlik (shartli misol)

FPR	Kunlik yolg‘on ogohlantirishlar	Aniqlik (precision), %
10^{-2}	10 000	≈ 0,9
10^{-3}	1 000	≈ 8,3
10^{-4}	100	≈ 47,4

Jadvaldan ko‘rinib turibdiki, FPR = 1 % bo‘lganda detektor kuniga 10 mingta yolg‘on ogohlantirish beradi va ularning faqat bir foizga yaqini haqiqiy hujum bo‘ladi. Ushbu shartli misolda accuracy yuqori qiymatga ega bo‘lishi mumkin, biroq precisionning pastligi tizimning xavfsizlik operatsiyalari markazi (Security Operations Center, SOC) uchun amaliy qiymatini keskin kamaytiradi. Tahlilchilar ogohlantirishlar oqimidan charchaydi (alert fatigue), haqiqiy hodisalar esa e’tibordan chetda qoladi. Foydalanish mumkin bo‘lgan natijaga faqat FPR bir necha tartibga kamaytirilgandagina erishiladi. Demak, korporativ muhit uchun hal qiluvchi mezon – SOC qayta ishlay oladigan kunlik ogohlantirishlar soni, ya’ni ogohlantirish byudjeti (alert budget).

Shu nuqtai nazardan adabiyotdagi ko‘plab natijalarni ehtiyotkorlik bilan talqin qilish lozim. Birinchidan, accuracy va ROC egri chizig‘i ostidagi yuza (ROC-AUC) butun FPR oralig‘i bo‘yicha umumlashtiriladi va amalda muhim bo‘lgan kichik FPR sohasidagi farqlarni yashiradi. Bu sohani PR-AUC, belgilangan FPR darajasidagi to‘liqlik (masalan, TPR\@FPR = 10^{-3}) va kunlik ogohlantirishlar soni ancha to‘g‘ri aks ettiradi. Ikkinchidan, keng qo‘llaniladigan ochiq to‘plamlarda xatolar uchraydi: CIC-IDS2017 to‘plamida oqimlarni shakllantirish va yorliqlash bilan bog‘liq kamchiliklar aniqlangan [5]. Uchinchidan, yozuvlarni tasodifiy aralashtirib bo‘lishda

vaqt bo‘yicha o‘zaro bog‘liq oqimlar ham o‘qitish, ham test to‘plamiga tushadi va ko‘rsatkichlar sun’iy ravishda oshadi. D. Arp va hammualliflari bunday xatolarni xavfsizlik sohasidagi ML tadqiqotlarida keng tarqalgan muammolar qatorida tasniflagan [6]. To‘rtinchidan, noma’lum hujumlarni aniqlash qobiliyatini tekshirish uchun har bir hujum sinfi navbat bilan o‘qitish va sozlash bosqichlaridan butunlay chiqarib tashlanadigan LOAO (leave-one-attack-out) protokolini qo‘llash maqsadga muvofiq. Aks holda «noma’lum» deb hisoblangan hujum model uchun aslida tanish bo‘lib chiqadi.

Yolg‘on signallarni kamaytirish uchun ko‘p bosqichli aniqlash yondashuvi istiqbolli yo‘nalishlardan biri hisoblanadi. Xususan, M. Verkerken va hammualliflari anomaliya detektori va klassifikatorlarni birlashtirgan ierarxik sxemani taklif qilgan [7]. Biroq bunday yechimlarda chegaralar odatda yorliqlangan hujum ma’lumotlari asosida sozlanadi, ikkinchi bosqich esa ma’lum hujumlar haqidagi bilimga tayanadi. Bosqichlarning hissasi LOAO sharoitida alohida baholanmagan. Natijada noma’lum hujumlarga nisbatan amaliy ishchi nuqtadagi samaradorlik masalasi ochiq qolmoqda.

Xulosa

Tahlil natijalari korporativ tarmoqdagi anomaliyalarni aniqlash tizimini faqat umumiy accuracy yoki ROC-AUC orqali baholash yetarli emasligini ko‘rsatadi. Tizimning amaliy yaroqliligi, avvalo, belgilangan FPR sharoitidagi aniqlash darajasi va SOC tomonidan qayta ishlanishi mumkin bo‘lgan kunlik ogohlantirishlar soni bilan bog‘liq. Shu sababli bunday tizimlarni tuzatilgan ma’lumotlar to‘plamlarida, vaqt bo‘yicha bo‘linish va LOAO protokoli asosida baholash maqsadga muvofiq. Keyingi tadqiqot bosqichida thresholdni ogohlantirish byudjetiga mos ravishda kalibrlash hamda noma’lum hujumlarga nisbatan umumlashish qobiliyatini saqlagan holda yolg‘on signallarni kamaytiruvchi qo‘shimcha bosqichni ishlab chiqish ko‘zda tutiladi.

Foydalanilgan adabiyotlar:

1. Denning D.E. An Intrusion-Detection Model // IEEE Transactions on Software Engineering. – 1987. – Vol. SE-13, № 2. – P. 222–232.

2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS): NIST Special Publication 800-94. – Gaithersburg: NIST, 2007.

3. Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection // ACM Transactions on Information and System Security. – 2000. – Vol. 3, № 3. – P. 186–205.

4. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // Proc. IEEE Symposium on Security and Privacy. – 2010. – P. 305–316.

5. Engelen G., Rimmer V., Joosen W. Troubleshooting an Intrusion Detection Dataset: the CICIDS2017 Case Study // Proc. IEEE Security and Privacy Workshops (SPW). – 2021. – P. 7–12.

6. Arp D., Quiring E., Pendlebury F. et al. Dos and Don’ts of Machine Learning in Computer Security // Proc. 31st USENIX Security Symposium. – 2022. – P. 3971–3988.

7. Verkerken M., D’hooge L., Sudyana D., Lin Y.-D., Wauters T., Volckaert B., De Turck F. A Novel Multi-Stage Approach for Hierarchical Intrusion Detection // IEEE Transactions on Network and Service Management. – 2023. – Vol. 20, № 3. – P. 3915–3929. – DOI: 10.1109/TNSM.2023.3259474.

MASOFAVIY TA’LIM TIZIMLARIDA SUN’IY INTELLEKT ASOSIDA AUTENTIFIKATSIYA QILISH USULLARI

Fayziyeva D.S., Abdumuminova Sh.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda masofaviy o‘qitish tizimlarida talabaning shaxsini tasdiqlash muammosi ko‘rib chiqilgan. Login va parolga asoslangan autentifikatsiya talaba o‘z hisobini boshqa shaxsga berishi yoki onlayn imtihonni boshqa odam topshirishining oldini ololmaydi. Shu sababli yuz tasviri va klaviaturada yozish uslubini sun’iy intellekt yordamida tahlil qiladigan, tizimga kirishda ham, butun sessiya davomida ham ishlaydigan autentifikatsiya usuli taklif qilinadi.

Kalit so‘zlar: masofaviy o‘qitish, autentifikatsiya, sun’iy intellekt, biometriya, yuzni tanish, klaviatura dinamikasi, uzluksiz autentifikatsiya.

Аннотация. В тезисе рассмотрена проблема подтверждения личности студента в системах дистанционного обучения. Аутентификация по логину и паролю не позволяет предотвратить передачу учётной записи другому лицу или сдачу онлайн-экзамена другим человеком. Поэтому предлагается метод аутентификации, который с помощью искусственного интеллекта анализирует изображение лица и клавиатурный почерк и работает как при входе в систему, так и на протяжении всей сессии.

Ключевые слова: дистанционное обучение, аутентификация, искусственный интеллект, биометрия, распознавание лиц, клавиатурный почерк, непрерывная аутентификация.

Kirish

2020-yildagi pandemiya davrida ko‘plab oliy ta’lim muassasalari qisqa muddatda masofaviy o‘qitishga o‘tishga majbur bo‘ldi. O‘shandan beri Moodle kabi o‘quv boshqaruv tizimlari ta’lim jarayonining odatiy qismiga aylandi: talabalar ma’ruzalarni shu yerda tinglaydi, topshiriqlarni yuklaydi, oraliq va yakuniy nazoratlarni topshiradi. Masofaviy ta’limning qulayligi bilan birga bitta jiddiy muammo ham paydo bo‘ldi: o‘qituvchi ekranning narigi tomonida haqiqatan kim o‘tirganini bilmaydi.

Aksariyat tizimlarda autentifikatsiya hamon login va parol bilan cheklanadi. Parol faqat foydalanuvchi biladigan ma’lumotni tekshiradi, uni boshqa odamga aytish uchun esa bir daqiqa kifoya. NIST SP 800-63B hujjatida ham yuqori ishonch darajasi talab qilinadigan tizimlarda parolning o‘zi yetarli emasligi ko‘rsatilgan [1]. SMS orqali yuboriladigan bir martalik kod ham vaziyatni o‘zgartirmaydi, chunki talaba kodni ham boshqa shaxsga yuborishi mumkin. Bundan tashqari, ikkala usulda ham tekshiruv faqat tizimga kirish paytida bo‘ladi. Talaba tizimga o‘zi kirib, keyin imtihonni boshqa odamga topshirtirsa, buni aniqlashning iloji yo‘q.

Insonning yuzini yoki klaviaturada yozish uslubini esa boshqa odamga berib bo‘lmaydi. Chuqur neyron tarmoqlarining rivojlanishi bu belgilarni oddiy veb-kamera va klaviatura yordamida ancha aniq tahlil qilish imkonini berdi. Tadqiqotning maqsadi masofaviy o‘qitish tizimlari uchun shunday biometrik belgilarga asoslangan, sessiya davomida uzluksiz ishlaydigan autentifikatsiya usulini ishlab chiqishdir.

Biometrik tanib olishning asosiy tamoyillari A. Jain va hammualliflarining ishida batafsil yoritilgan [10]. Yuzni tanish sohasida so‘nggi o‘n yillikda katta o‘zgarishlar yuz berdi. FaceNet

[2] modeli yuz tasvirini qisqa sonli vektorga aylantirib, ikki tasvirning o‘xshashligini shu vektorlar orasidagi masofa orqali baholashni taklif qildi. ArcFace [3] esa bu yondashuvni takomillashtirib, turli shaxslarning vektorlari bir-biridan aniqroq ajralishiga erishdi. Klaviatura dinamikasi sohasida K. Killourhy va R. Maxion yaratgan ochiq to‘plam [4] ko‘plab tadqiqotlar uchun asos bo‘lib kelmoqda, bu sohadagi usullarning keng sharhi esa [5] ishda berilgan.

Biroq ushbu ishlarning aksariyatida bitta biometrik belgi alohida o‘rganiladi va sinovlar yaxshi sharoitda olingan ma’lumotlarda o‘tkaziladi. Masofaviy ta’limda vaziyat boshqacha: talabalarning ko‘pchiligi noutbukning past sifatli kamerasidan foydalanadi, xonalarning yoritilishi har xil, ayrimlar tizimga telefon orqali kiradi. Yuzni tanish tizimini oddiy fotosurat yoki boshqa ekrandagi video orqali aldashga urinishlar ham uchraydi.

Asosiy qism

Dastlab masofaviy o‘qitish tizimlarida autentifikatsiya bilan bog‘liq asosiy tahdidlar aniqlab olindi (1-jadval).

1-jadval

Masofaviy o‘qitish tizimlaridagi tahdidlar va ularga qarshi choralar

Tahdid	Qanday amalga oshiriladi	Qarshi chora
Hisobni boshqa shaxsga berish	Talaba login va parolini boshqa odamga aytadi	Kirishda yuzni tekshirish
Imtihonda shaxsni almashtirish	Talaba tizimga o‘zi kiradi, imtihonni boshqa odam ishlaydi	Sessiya davomida yuz va yozish uslubini tekshirish
Foto yoki video bilan aldash	Kamera oldiga rasm, telefon ekrani yoki soxta video qo‘yiladi	Jonlilik tekshiruvi
Parolni o‘g‘irlash	Fishing sahifa yoki boshqa saytdan sizib chiqqan parollar	Biometrik omil qo‘shish
Sessiyani egallab olish	Sessiya tokeni o‘g‘irlanib, boshqa qurilmada ishlatiladi	Qurilma va yozish profilini solishtirish

Taklif qilinayotgan usul uch bosqichda ishlaydi. Birinchi bosqich ro‘yxatdan o‘tish bo‘lib, u semestr boshida bir marta bajariladi. Talaba veb-kamera oldida bir necha soniya turadi va tayyor matnni klaviaturada teradi. Olingan tasvirlardan yuz vektori, terish jarayonidan esa talabaning yozish profili hosil qilinadi. Serverda faqat shu vektor va profil shifrlangan holda saqlanadi, asl tasvirlar o‘chirib yuboriladi.

Ikkinchi bosqich tizimga kirishda bajariladi. Login va parol to‘g‘ri kiritilgandan keyin kamera yoqiladi. Olingan kadr avval jonlilik tekshiruvidan o‘tadi, ya’ni kamera oldida tirik odam turganiga ishonch hosil qilinadi. Shundan keyingina ArcFace asosidagi model yuz vektorini hisoblaydi va u saqlangan vektor bilan kosinus o‘xshashligi orqali solishtiriladi.

Uchinchi bosqich sessiya davomida, ayniqsa test yoki imtihon paytida ishlaydi. Kamera tasodifiy vaqt oraliqlarida kadr oladi va yuz qayta tekshiriladi. Talaba javob yozayotganda esa uning terish uslubi fonda saqlangan profil bilan solishtirib boriladi. Talaba uchun bu tekshiruv deyarli sezilmaydi. Har bir bosqichda foydalaniladigan belgilar 2-jadvalda keltirilgan.

2-jadval

Autentifikatsiyada foydalaniladigan belgilar

Manba	Belgilar
Yuz tasviri	512 o‘lchamli yuz vektori; yuzning kadrdagi o‘rni; ko‘z qisish va bosh harakati; tasvir teksturasi va ekrandan qaytgan yorug‘lik izlari
Klaviatura	Tugmani bosib turish vaqti; bir tugmadan keyingisiga o‘tish vaqti; ikki va uch harfli birikmalarni terish vaqti; terish tezligi; xato va o‘chirish tugmasini bosish chastotasi
Kontekst	Qurilma va brauzer turi; IP manzil; kirish vaqti; sessiya davomiyligi

Jonlilikni tekshirish uchun ikki usul birga qo‘llaniladi. Passiv usulda konvolyutsion neyron tarmoq tasvir teksturasini tahlil qiladi: ekrandan yoki qog‘ozdan olingan tasvirda tirik yuzda bo‘lmaydigan o‘ziga xos izlar qoladi [8]. Faol usulda talabadan boshini o‘ngga burish yoki ko‘zini qisish kabi tasodifiy harakat so‘raladi. Faol tekshiruv faqat passiv usul ishonchsiz natija berganda ishga tushiriladi, aks holda talabani har safar bezovta qilish noqulay bo‘lardi. Modul ISO/IEC 30107-3 standartida belgilangan tartibda baholanadi [6].

Klaviatura dinamikasi uchun ikki yondashuv sinab ko‘riladi. Birinchisida har bir talaba uchun alohida bir sinfli model (One-Class SVM yoki Isolation Forest) uning o‘z yozish namunalarida o‘qitiladi. Ikkinchisida siam neyron tarmog‘i ishlatiladi. Bu tarmoq ikki terish namunasini taqqoslab, ular bir odamga tegishli yoki tegishli emasligini aniqlashni o‘rganadi. Uning afzalligi shundaki, yangi talaba qo‘shilganda modelni qayta o‘qitish shart emas.

Barcha tekshiruvlar natijasi bitta ishonch bahosiga birlashtiriladi, ammo har bir omilning vazni o‘zgarmas emas. Masalan, xona qorong‘i bo‘lsa yoki talaba kameradan uzoqlashsa, yuz tekshiruvi natijasiga kamroq ishoniladi va klaviatura dinamikasining ulushi oshiriladi. Ishonch bahosi belgilangan chegaradan pastga tushsa, tizim avval qayta tekshiruv so‘raydi. Shubha saqlanib qolsa, imtihon vaqtincha to‘xtatiladi va o‘qituvchiga xabar yuboriladi. Yakuniy qarorni har doim o‘qituvchi qabul qiladi, chunki tizim ham xato qilishi mumkin.

Modellarni sinash uchun yuzni tanish bo‘yicha LFW [7], jonlilik bo‘yicha Replay-Attack [8], klaviatura dinamikasi bo‘yicha CMU [4] to‘plamlaridan foydalaniladi. Ochiq to‘plamlar bilan bir qatorda talabalarning roziligi bilan real sharoitda ma’lumot yig‘ish ham rejalashtirilgan. Natijalar biometrik tizimlarda qabul qilingan FAR, FRR va EER ko‘rsatkichlari bo‘yicha, jonlilik moduli esa APCER va BPCER bo‘yicha baholanadi. Biz uchun FRR ko‘rsatkichi alohida muhim: tizim talabaning o‘zini tez-tez rad etsa, imtihon paytida ortiqcha asabiylashishga sabab bo‘ladi.

Biometrik ma’lumotlar bilan ishlashda huquqiy masalalarni ham chetlab o‘tib bo‘lmaydi. Yuz tasviri shaxsga doir ma’lumot hisoblanadi va unga ishlov berish «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun talablariga mos bo‘lishi kerak [9]. Shuning uchun taklif qilinayotgan usulda talabadan oldindan rozilik olinadi, asl tasvirlar saqlanmaydi, vektorlar shifrlanadi va ta’lim muassasasining o‘z serverida qoladi. Tekshiruv natijalarini faqat tegishli o‘qituvchi va tizim administratori ko‘ra oladi.

Tadqiqotning ilmiy yangiligi yuz tasviri, jonlilik belgilari va klaviatura dinamikasini sharoitga qarab o‘zgaradigan vaznlar orqali birlashtiruvchi, masofaviy ta’lim sharoitiga moslashtirilgan uzluksiz autentifikatsiya usulini taklif qilishdan iborat. Usul qo‘shimcha qurilma talab qilmaydi va oddiy veb-kamera hamda klaviatura bilan ishlaydi.

Xulosa

Masofaviy ta’limda baholash natijalariga ishonch ko‘p jihatdan talabaning shaxsi to‘g‘ri tasdiqlanganiga bog‘liq. Login va parol bu vazifani bajara olmaydi, chunki ularni osongina boshqa odamga berish mumkin. Taklif qilinayotgan usulda yuz tasviri va yozish uslubi tizimga kirishda ham, imtihon davomida ham tekshiriladi, jonlilik moduli esa soxta tasvir orqali aldashning oldini oladi. Keyingi bosqichda usulning prototipi Moodle uchun plagin ko‘rinishida ishlab chiqilib, talabalar ishtirokida sinovdan o‘tkaziladi.

Foydalanilgan adabiyotlar

1. Grassi P.A. et al. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B. – Gaithersburg: NIST, 2017.

2. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering // Proceedings of IEEE CVPR. – 2015. – P. 815–823.

3. Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition // Proceedings of IEEE/CVF CVPR. – 2019. – P. 4690–4699.

4. Killourhy K.S., Maxion R.A. Comparing Anomaly-Detection Algorithms for Keystroke Dynamics // Proceedings of IEEE/IFIP DSN. – 2009. – P. 125–134.

5. Banerjee S.P., Woodard D.L. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey // Journal of Pattern Recognition Research. – 2012. – Vol. 7, No. 1. – P. 116–139.

6. ISO/IEC 30107-3:2017. Information technology. Biometric presentation attack detection. Part 3: Testing and reporting.

7. Huang G.B., Ramesh M., Berg T., Learned-Miller E. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. – University of Massachusetts, Amherst, Technical Report 07-49, 2007.

8. Chingovska I., Anjos A., Marcel S. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing // Proceedings of BIOSIG. – 2012. – P. 1–7.

9. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni. 2019-yil 2-iyul, O‘RQ-547-son.

10. Jain A.K., Ross A., Prabhakar S. An Introduction to Biometric Recognition // IEEE Transactions on Circuits and Systems for Video Technology. – 2004. – Vol. 14, No. 1. – P. 4–20.

COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR DETECTING FRAUDULENT TRANSACTIONS

Yaqubova M.R.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotatsiya. Maqolada elektron to'lov tizimlaridagi kiberjinoyatlar, asosiy hujum turlari va ularni aniqlash usullari tahlil qilingan. Firibgarlik tranzaksiyalarini aniqlovchi mashinali o'qitish algoritmlarini sinflar nomutanosibligi, konsepsiya siljishi va real vaqt cheklovlarini hisobga olib taqqoslash metodikasi taklif etilgan. Gibrid arxitekturalar eng asosli tanlov ekani ko'rsatilgan.

Kalit so'zlar: elektron to'lov tizimlari, kiberjinoyat, firibgarlikni aniqlash, mashinali o'qitish.

Аннотация. В статье проанализированы киберпреступления в электронных платёжных системах, основные виды атак и методы их обнаружения. Предложена методика сравнения алгоритмов машинного обучения для выявления мошеннических транзакций с учётом дисбаланса классов, дрейфа концепции и ограничений реального времени. Показано, что гибридные архитектуры являются наиболее обоснованным выбором.

Ключевые слова: электронные платёжные системы, киберпреступность, обнаружение мошенничества, машинное обучение.

Introduction

Electronic payment systems (EPS) – card networks, online banking, mobile wallets and instant payments – are the backbone of modern commerce and an attractive target: global card fraud losses are estimated in the tens of billions of US dollars per year. Manually written rules can no longer keep up with attackers, and machine learning (ML) dominates the literature, yet studies use different datasets, metrics and preprocessing, so their results are hard to compare. The aim of this paper is to build a methodological basis for a fair comparison of ML algorithms for fraud detection.

Materials and methods

Cybercrime is divided into cyber-dependent crimes (malware, unauthorized access) and cyber-enabled crimes – traditional offences scaled up by technology; payment fraud usually combines both. By victim, fraud targets cardholders (account takeover), merchants (chargebacks, card testing) and issuers (synthetic identities). Fraud checks are made at authorization within tens to hundreds of milliseconds, so a model that cannot score in real time has little practical value.

The main attacks are phishing, malware (banking trojans, POS scrapers), card-not-present (CNP) fraud – the fastest-growing category in e-commerce – and identity theft. For ML they share three features: they are rare, they evolve in response to defenses, and their labels arrive with delay. Detection systems must also meet PCI DSS and ISO/IEC 27001 requirements, which favor explainable decisions.

The proposed comparison protocol: (1) a common dataset and preprocessing; (2) a time-based train/test split for concept drift; (3) imbalance handling (undersampling, SMOTE, class weights) inside training folds only; (4) cross-validated tuning; (5) evaluation on an untouched test set; (6) repeated runs with confidence intervals. Since in the ULB dataset only 492 of 284,807 transactions (0.17%) are fraudulent, accuracy is not used; the metrics are Precision, Recall, F1, AUPRC and ROC-AUC, plus cost-weighted error and latency.

Results

Rule-based systems are transparent but static and easily bypassed; signature-based methods are precise but blind to new schemes. Anomaly detection (Isolation Forest, autoencoders) finds unseen fraud without labels but gives many false alarms. Behavioral methods compare a transaction with the user's profile; aggregated features over the last hour, day and week improve detection. The comparison is given in Table 1.

Table 1

Comparison of fraud detection approaches

Approach	Detects new fraud	False positives	Interpret-ability	Maintenance	Typical role
Rule-based	Low	Medium–high	Very high	High (manual)	First-line filter
Signature-based	Very low	Very low	High	Medium	Known threats
Anomaly-based	High	High	Medium–low	Medium	Unlabeled detection
Behavioral	Medium–high	Medium	Medium	High (profiles)	Account takeover
Supervised ML	Medium	Low–medium	Varies	Medium (retraining)	Core risk score

The approaches complement each other, so platforms are hybrid, with supervised ML as the core score. ML algorithms are compared in Table 2.

Table 2

Characteristics of ML algorithms for fraud detection

Algorithm	Main strengths	Main limitations
Logistic Regression	Fast, interpretable, calibrated probabilities	Only linear relationships
Decision Tree	Interpretable rules, mixed features	High variance, overfitting
Random Forest	Robust, handles non-linearity	Larger memory, slower inference
Gradient boosting (XGBoost)	Often strongest on tabular data	Sensitive to hyperparameters
SVM	Effective in high dimensions	Poor scalability, hard to interpret
Neural networks	Learn complex and sequential patterns	Need more data, limited explainability

Discussion

No single method dominates on every criterion. Tree ensembles and boosting lead for tabular data, logistic regression is the interpretable baseline, and anomaly detectors help where labels are scarce; combining unsupervised and supervised learning improves detection. Published comparisons often use random splits, resample before splitting and report accuracy, which exceeds 99.8% even for a model that detects nothing; the proposed protocol removes these biases. The study is analytical, and the protocol still needs experimental validation.

Conclusion

Payment fraud combines phishing, malware, CNP fraud and identity theft into one attack chain, so detection must use transaction, device and behavioral data. PCI DSS and ISO/IEC 27001 do not prescribe algorithms but set requirements any ML system must meet. Rule-based and signature-based methods alone are insufficient against adaptive attackers. ML algorithms must be compared under a unified protocol using Precision, Recall, F1 and AUPRC instead of accuracy. The most promising architecture is hybrid: rules for known threats, a supervised model for scoring and an anomaly detector for new patterns.

References

1. Abdallah A., Maarof M. A., Zainal A. Fraud detection system: A survey // Journal of Network and Computer Applications. – 2016. – Vol. 68. – P. 90–113.

2. Carcillo F., Le Borgne Y.-A., Caelen O. et al. Combining unsupervised and supervised learning in credit card fraud detection // Information Sciences. – 2021. – Vol. 557. – P. 317–331.

3. Chen T., Guestrin C. XGBoost: A scalable tree boosting system // Proceedings of the 22nd ACM SIGKDD Conference. – 2016. – P. 785–794.

4. Dal Pozzolo A., Caelen O., Johnson R. A., Bontempi G. Calibrating probability with undersampling for unbalanced classification // IEEE Symposium Series on Computational Intelligence. – 2015. – P. 159–166.

5. Bahnsen A. C., Aouada D., Stojanovic A., Ottersten B. Feature engineering strategies for credit card fraud detection // Expert Systems with Applications. – 2016. – Vol. 51. – P. 134–142.

6. Cortes C., Vapnik V. Support-vector networks // Machine Learning. – 1995. – Vol. 20, No. 3. – P. 273–297.

7. Hilal W., Gadsden S. A., Yawney J. Financial fraud: A review of anomaly detection techniques and recent advances // Expert Systems with Applications. – 2022. – Vol. 193. – 116429.

8. Breiman L. Random forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32.

9. McGuire M., Dowling S. Cyber crime: A review of the evidence. Research Report 75. – London: Home Office, 2013.

10. PCI Security Standards Council. Payment Card Industry Data Security Standard, v4.0.1. – 2024.

11. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

12. The Nilson Report. Card fraud losses worldwide. – Carpinteria (CA): HSN Consultants. – URL: https://nilsonreport.com

MASHINALI O‘RGANISH ASOSIDA REST API LARGA QILINADIGAN HUJUMLARNI ANIQLASH TIZIMI

Bafoyeva Sh.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda REST API larga yo‘naltirilgan hujumlarni mashinali o‘rganish yordamida aniqlash masalasi ko‘rib chiqilgan. Imzolarga asoslangan WAF vositalari in’eksiya turidagi hujumlarni yaxshi ushlasa-da, avtorizatsiya va biznes-mantiq xatolaridan foydalanadigan hujumlarni ko‘pincha o‘tkazib yuboradi. Shu muammoni hal qilish uchun alohida so‘rov va foydalanuvchi sessiyasi xususiyatlarini birgalikda tahlil qiladigan gibrid aniqlash tizimi taklif qilinadi. Tizim tarkibida nazoratli klassifikator va anomaliyalarni aniqlash modeli birga ishlaydi.

Kalit so‘zlar: REST API, API xavfsizligi, mashinali o‘rganish, hujumlarni aniqlash, anomaliyalarni aniqlash, OWASP API Security Top 10.

Аннотация. В тезисе рассмотрена задача обнаружения атак на REST API методами машинного обучения. Сигнатурные WAF хорошо справляются с инъекциями, но часто пропускают атаки, использующие ошибки авторизации и бизнес-логики. Для решения этой проблемы предлагается гибридная система обнаружения, которая совместно анализирует признаки отдельных запросов и пользовательских сессий. В её составе работают классификатор, обученный с учителем, и модель обнаружения аномалий.

Ключевые слова: REST API, безопасность API, машинное обучение, обнаружение атак, обнаружение аномалий, OWASP API Security Top 10.

Kirish

Hozirgi kunda deyarli har qanday zamonaviy dasturiy mahsulot, xoh u mobil ilova, xoh internet-bank yoki elektron hukumat xizmati bo‘lsin, ma’lumotlarni REST API orqali uzatadi [2]. Veb-sayt ham, mobil ilova ham ko‘pincha bitta API dan foydalanadi, shuning uchun API dagi bitta xato butun tizim xavfsizligiga ta’sir qiladi. Hujumchilar ham buni yaxshi biladi: foydalanuvchi interfeysini chetlab o‘tib, to‘g‘ridan-to‘g‘ri API ga so‘rov yuborish ancha qulay.

OWASP tashkiloti 2023-yilda e’lon qilgan API Security Top 10 ro‘yxatining birinchi o‘rnida obyekt darajasidagi avtorizatsiyaning buzilishi (BOLA) turibdi [1]. Bu zaiflikdan foydalanish uchun maxsus vosita ham kerak emas. Masalan, talaba o‘z baholarini GET /api/v1/students/1452/grades so‘rovi orqali oladi. Agar server so‘rov yuborgan foydalanuvchi aynan 1452-raqamli talaba ekanini tekshirmasa, identifikatorni 1453 ga o‘zgartirib, boshqa talabaning baholarini ko‘rish mumkin bo‘ladi. Bunday so‘rovda hech qanday zararli belgi yo‘q, shuning uchun imzolar bazasiga tayanadigan WAF uni oddiy so‘rov deb hisoblaydi.

Bizning fikrimizcha, bu muammoni hal qilishda alohida so‘rovga emas, foydalanuvchining API dagi umumiy xatti-harakatiga qarash kerak. Bir daqiqa ichida yuzlab turli identifikatorlarga murojaat qilish oddiy foydalanuvchiga xos emas. Mashinali o‘rganish modellari normal trafik qanday ko‘rinishini o‘rganib, shunday og‘ishlarni avtomatik aniqlay oladi. Tadqiqotning maqsadi ham ana shunday tizimni ishlab chiqishdan iborat.

Veb-hujumlarni anomaliya sifatida aniqlash g‘oyasi yangi emas. C. Kruegel va G. Vigna 2003-yildayoq HTTP so‘rov parametrlarining uzunligi va belgilar taqsimotiga asoslangan statistik modellarni taklif qilgan [9]. Keyinchalik CSIC 2010 [6] va CIC-IDS2017 [7] to‘plamlari paydo

bo‘lgach, ularda qaror daraxtlari, tayanch vektorlar mashinasi va neyron tarmoqlari ko‘p marta sinovdan o‘tkazildi. Biroq bu ishlarning aksariyatida har bir so‘rov alohida baholanadi. CSIC 2010 to‘plamida esa BOLA yoki parol tanlash kabi hujumlar umuman yo‘q, chunki ularni bitta so‘rovga qarab aniqlab bo‘lmaydi. Tadqiqotimizda aynan shu jihatga e’tibor qaratilgan.

Asosiy qism

Tadqiqot davomida REST API ga qilinadigan hujumlarni aniqlash usuliga ko‘ra ikki guruhga ajratdik (1-jadval). Birinchi guruhdagi hujumlarda zararli ma’lumot so‘rovning o‘zida bo‘ladi. Ikkinchi guruhda esa har bir so‘rov alohida olinganda mutlaqo normal ko‘rinadi, hujum faqat so‘rovlar ketma-ketligida namoyon bo‘ladi.

1-jadval

REST API hujumlari va ularni aniqlash darajasi

Hujum turi	Misol	Aniqlash darajasi
SQL in’eksiya	/users?id=5' OR '1'='1	So‘rov tarkibi
XSS	name=<script>...</script>	So‘rov tarkibi
Path traversal	/files?path=../../etc/passwd	So‘rov tarkibi
BOLA	/students/1453, /1454, /1455 ... ga ketma-ket murojaat	Sessiya xatti-harakati
Parol tanlash	/auth/login ga qisqa vaqtda yuzlab urinish	Sessiya xatti-harakati
Scraping	Barcha /products/{id} sahifalarini ketma-ket yuklab olish	Sessiya xatti-harakati

Taklif qilinayotgan tizim to‘rt qismdan tashkil topgan. Birinchi qism ilovaga middleware sifatida ulanadi va har bir so‘rov hamda javob haqidagi ma’lumotlarni yozib boradi: vaqt, IP manzil, token, metod, yo‘l, parametrlar, javob kodi, javob hajmi va javob qaytarish vaqti. Ikkinchi qism bu yozuvlardan model uchun sonli xususiyatlar hisoblaydi. Uchinchi qism, ya’ni aniqlash moduli, xavf bahosini chiqaradi. To‘rtinchi qism shu baho asosida qaror qabul qiladi: so‘rovni o‘tkazib yuboradi, so‘rovlar tezligini cheklaydi, bloklaydi yoki administratorga xabar yuboradi.

Xususiyatlar ikki darajada hisoblanadi (2-jadval). So‘rov darajasidagi xususiyatlar har bir so‘rov uchun alohida olinadi. Sessiya darajasidagilari esa bitta token yoki IP manzildan kelgan so‘rovlar bo‘yicha sirpanuvchi vaqt oynasida hisoblanadi. Oyna uzunligini hozircha 1 va 5 daqiqa qilib tanladik, ammo bu qiymat tajriba natijalariga qarab o‘zgarishi mumkin.

2-jadval

Tizimda foydalaniladigan xususiyatlar

Daraja	Xususiyatlar
So‘rov darajasi	HTTP metodi; endpoint shabloni; parametrlar soni va uzunligi; maxsus belgilar ulushi; Shannon entropiyasi; SELECT, UNION, <script> kabi kalit so‘zlar bor-yo‘qligi; javob kodi va hajmi
Sessiya darajasi	Vaqt oynasidagi so‘rovlar soni; murojaat qilingan turli identifikatorlar soni; 401, 403 va 404 javoblar ulushi; turli endpointlar soni; so‘rovlar orasidagi vaqt; endpointlarga murojaat tartibi

Ma’lumotlarni tayyorlashda eng ko‘p vaqt URL manzillarni bir xil ko‘rinishga keltirishga ketadi. /students/1452/grades va /students/1453/grades aslida bitta endpoint, shuning uchun raqamli identifikatorlar va UUID lar {id} shabloniga almashtiriladi. Aks holda model har bir

manzilni yangi endpoint deb qabul qiladi. Yana bir muammo shundaki, real trafikda hujumli so‘rovlar ulushi juda kichik. Bu nomutanosiblikni kamaytirish uchun SMOTE usuli [10] va sinflarga vazn berishdan foydalaniladi. Ma’lumotlarni o‘qitish va test qismlariga ajratishda tasodifiy emas, vaqt bo‘yicha ajratish tanlandi: model o‘tgan haftadagi trafikda o‘qitilib, keyingi haftadagi trafikda tekshiriladi. Bu real sharoitga yaqinroq.

Aniqlash modulida ikki xil model parallel ishlaydi. Birinchisi Random Forest [3] yoki XGBoost [4] klassifikatori bo‘lib, u belgilangan ma’lumotlarda o‘qitiladi va ma’lum hujum turlarini aniqlaydi. Jadvalli ma’lumotlarda bu modellar odatda neyron tarmoqlardan qolishmaydi va ancha tez ishlaydi, bu esa har bir so‘rovni tekshirishda muhim. Ikkinchi model faqat normal trafikda o‘qitiladi, buning uchun Isolation Forest [5] va avtokodlovchi sinab ko‘riladi. Avtokodlovchi normal so‘rovni deyarli xatosiz qayta tiklaydi, notanish ko‘rinishdagi so‘rovda esa tiklash xatosi sezilarli oshadi. Shu orqali ilgari uchramagan hujumlarni ham ushlash mumkin. Ikki modelning natijasi vaznli yig‘indi orqali bitta xavf bahosiga birlashtiriladi.

Modellar parametrlari kross-validatsiya yordamida tanlanadi. Shuni ham hisobga olish kerakki, API trafigi vaqt o‘tishi bilan o‘zgaradi: yangi endpointlar qo‘shiladi, foydalanuvchilar soni ortadi. Shu sababli modelni bir marta o‘qitib qo‘yish yetarli emas, uni yangi loglar asosida davriy qayta o‘qitib borish rejalashtirilgan.

Qayd etish kerakki, taklif qilinayotgan tizim WAF o‘rnini bosmaydi. Imzolarga asoslangan qoidalar ma’lum in’eksiya hujumlarini tez va kam xato bilan to‘xtatadi. Mashinali o‘rganish modeli esa qoidalar qamrab olmagan holatlar uchun qo‘shimcha himoya qatlami vazifasini bajaradi. Gibrid yondashuvning kamchiligi ham bor: tizim murakkablashadi va ko‘proq hisoblash resursi talab qilinadi.

Tajribalar uchun uch manbadan foydalaniladi: CSIC 2010 [6] to‘plami, CIC-IDS2017 [7] to‘plamining veb-hujumlarga oid qismi va test muhitida ishga tushirilgan FastAPI ilovasining loglari. Uchinchi manba alohida ahamiyatga ega, chunki ochiq to‘plamlarda sessiya darajasidagi hujumlar deyarli yo‘q. Test ilovasiga normal foydalanuvchi trafigi skriptlar yordamida generatsiya qilinadi, BOLA va parol tanlash hujumlari esa nazorat ostida alohida bajariladi. Natijalar precision, recall, F1-ko‘rsatkich, ROC-AUC va yolg‘on signallar ulushi bo‘yicha baholanadi. API himoyasida oxirgi ko‘rsatkichga alohida e’tibor beriladi: tizim oddiy foydalanuvchilarni tez-tez bloklasa, undan amalda foydalanib bo‘lmaydi. Bundan tashqari, bitta so‘rovni tekshirishga ketadigan vaqt ham o‘lchanadi.

Xavfsizlik mutaxassisi uchun «so‘rov shubhali» degan signalning o‘zi yetarli emas, u nima uchun shunday qaror chiqarilganini bilishi kerak. Shu maqsadda SHAP usuli [8] qo‘llanilib, har bir signalga qisqa izoh qo‘shiladi, masalan: «oxirgi 2 daqiqada 40 ta turli talaba identifikatoriga murojaat qilingan». Tizimni FastAPI ilovasiga ulashda so‘rov darajasidagi tekshiruv real vaqtda bajariladi, sessiya tahlili esa fon rejimida ishlaydi. Shu tariqa API javob vaqtiga ta’sir imkon qadar kamaytiriladi.

Albatta, hujumchi tizimni aldashga harakat qilishi mumkin, masalan, so‘rovlarni sekinroq yuborish yoki zararli qismni URL yoki Base64 ko‘rinishida kodlash orqali. Buning oldini olish uchun so‘rovlar tahlildan oldin dekodlanadi, sessiya xususiyatlari esa bir nechta uzunlikdagi vaqt oynalarida hisoblanadi.

Tadqiqotning ilmiy yangiligi shundaki, REST API ga xos avtorizatsiya va biznes-mantiq hujumlarini aniqlash uchun so‘rov tarkibi va sessiya xatti-harakati xususiyatlari yagona modelda birlashtirildi, modelning qarorlari esa xavfsizlik mutaxassisi tushunadigan ko‘rinishda izohlab beriladi.

Xulosa

Faqat imzolarga tayanadigan himoya vositalari REST API ga qilinadigan hujumlarning muhim qismini, ayniqsa BOLA va parol tanlash kabi hujumlarni aniqlay olmaydi. Taklif qilinayotgan gibrid tizim bu bo‘shliqni qisman to‘ldiradi: klassifikator ma’lum hujumlarni, anomaliya detektori esa yangi turdagi hujumlarni aniqlaydi. Keyingi bosqichda tizim prototipi to‘liq ishlab chiqilib, modellar ochiq va real ma’lumotlarda bir-biri bilan solishtiriladi.

Foydalanilgan adabiyotlar:

1. OWASP. OWASP API Security Top 10 – 2023. URL: https://owasp.org/API-Security/
2. Fielding R.T. Architectural Styles and the Design of Network-based Software Architectures: PhD dissertation. – University of California, Irvine, 2000.
3. Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32.
4. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD Conference. – 2016. – P. 785–794.
5. Liu F.T., Ting K.M., Zhou Z.-H. Isolation Forest // Proceedings of the 8th IEEE International Conference on Data Mining. – 2008. – P. 413–422.
6. Giménez C.T., Villegas A.P., Marañón G.Á. HTTP Data Set CSIC 2010. – Spanish National Research Council (CSIC), 2010.
7. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proceedings of ICISSP. – 2018. – P. 108–116.
8. Lundberg S.M., Lee S.-I. A Unified Approach to Interpreting Model Predictions // Advances in Neural Information Processing Systems (NeurIPS). – 2017.
9. Kruegel C., Vigna G. Anomaly Detection of Web-based Attacks // Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS). – 2003. – P. 251–261.
10. Chawla N.V., Bowyer K.W., Hall L.O., Kegelmeyer W.P. SMOTE: Synthetic Minority Over-sampling Technique // Journal of Artificial Intelligence Research. – 2002. – Vol. 16. – P. 321–357.

KIBERSAVODXONLIKNI OSHIRISH MUAMMOLARINI HAL QILISH YO‘LLARI

Nabiyeva S.S.
UNICON.UZ - Fan-texnika va marketing tadqiqotlari markazi

Annotatsiya. Mazkur tezisda kiberxavfsizlikning zamonaviy muommolari hisoblanayotgan kibersavodxonlikni oshirish muommolari va ularni oldini olish yo‘llari keltirilgan.

Kalit so‘zlar: Kibersavodxonlik, kibergigiena, firibgarlik, shaxsiy ma’lumotlar, foydalanuvchi.

Аннотация. В данном тезисе представлены проблемы повышения киберграмотности, которые считаются современными проблемами кибербезопасности, и пути их предотвращения.

Ключевые слова: Киберграмотность, кибергигиена, мошенничество, личные данные, пользователь.

Kirish

Bugungi kunda raqamli texnologiyalar shunchaki qulaylik vositasi emas, balki davlatlar taraqqiyoti, iqtisodiy o‘sish va ijtimoiy farovonlikning asosiy omiliga aylandi. Internet, sun’iy intellekt, katta ma’lumotlar va bulutli xizmatlar insonning imkoniyatlarini keskin kengaytirdi. Bunday texnologiyalarning jadal rivojlanishi aholiga davlat xizmatlarini raqamli formatda taqdim etilishi, xizmatlarning tez, qulay va shaffof bo‘lishini ta’minlashi bilan birga onlayn xizmatlarning kopayishga hissa qo‘shmoqda. Bu esa o‘z navbatida ushbu xizmatlardan yanada kengroq foydalanishga qiziqish uyg‘otishi, shu bilan birga foydalanuvchidan o‘zining raqamli dunyosida ogohlikni talab qiladi.

Ma’lumotlarning maxfiyligi va xavfsizligi muammolari nafaqat foydalanuvchilar, balki davlat tashkilotlari uchun ham dolzarb hisoblanadi. Shu nuqtai nazardan, kibersavodxonlikka o‘qitish dasturlari doimiy ravishda yangilanib borilishi, bilim va ko‘nikmalarning dolzarbligi ta’minlanishi muhimdir. Foydalanuvchilarga raqamli xavfsizlikning barcha jihatlarini o‘rgatish zarur: ma’lumotlarni himoya qilishning asosiy tamoyillaridan tortib, hujumlardan himoya qilish, bulutli xavfsizlik kabi murakkabroq mavzulargacha.

Shu o‘rinda, O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi PF-38-son “O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida”gi Farmoni 2-bob 8-paragrfida “Kiberxavfsizlik sohasida kadrlar salohiyatini rivojlantirish hamda xodimlarning malakasini va aholining kiberxavfsizlik bo‘yicha huquqiy va raqamli madaniyati (kibersavodxonlik) darajasini oshirish” ga alohida e’tibor qaratilib, kibermakonda shaxs, jamiyat va davlat manfaatlarini samarali himoya qilish, axborot infratuzilmasining barqarorligini ta’minlash, raqamli iqtisodiyot tarmoqlarida kiberxavfsizlikni yanada kuchaytirishning ustuvor yo‘nalishlarini belgilash, kiberjinoyatchilikning oldini olish tizimini takomillashtirish, shuningdek, fuqarolarda kiberxavfsizlik madaniyatini shakllantirish va mustahkamlash to‘g‘risida ko‘rsatmalar keltirilgan.

Kibersavodxonlikni o‘rgatish raqamli xavfsizlikni ta’minlash strategiyasining ajralmas qismi hisoblanadi. Kibersavodxonlik foydalanuvchilarga nafaqat shaxsiy xavf-xatarlarning oldini olish, balki tashkilotlar va davlatlarning yanada xavfsiz faoliyat yuritishiga ko‘maklashadi

Asosiy qism

Global raqamli transformatsiya davrida kiberxavfsizlik sohasidagi malaka muvaffaqiyat kalitiga aylanmoqda. Raqamli texnologiyalar va kibersavodxonlik zamonaviy axborot jamiyatida har bir inson uchun shaxsiy ma’lumotlar xavfsizligini ta’minlash va texnologiyalardan samarali foydalanishning asosiy shartidir.

Kibersavodxonlik - bu raqamli muhitdan xavfsiz va samarali foydalanish imkonini beruvchi ko‘nikma va bilimlar, shuningdek, o‘zini ehtimoliy tahdid va xavflardan himoya qilish qobiliyatidir. Internet qanday ishlashi, turli onlayn xizmatlar va ilovalardan qanday xavfsiz foydalanish, shaxsiy ma’lumotlarni qanday himoya qilish va ehtimoliy tahdidlarni qanday aniqlash hamda ularni bartaraf qilish haqidagi bilimlarni o‘z ichiga oladi.

Kibersavodxonlikning yo‘qligi shaxsiy ma’lumotlarning sizib chiqishi, firibgarlik natijasida moliyaviy yo‘qotish, viruslar va boshqa zararli dasturlar bilan zararlanish kabi turli muammolarga olib kelishi mumkin.

Kibersavodxonlik foydalanuvchilarga Internetdan yanada mas’uliyatli foydalanishga yordam beradi. Masalan, u foydalanuvchilarga xavfsiz parollar yaratishni, shaxsiy ma’lumotlarni oshkor qilmaslikni, shubhali havolalarga kirmaslikni va firibgarlar bilan ishonchli muloqot qilishni o‘rgatadi.

Kibersavodxonlikni oshirish 4 darajada amalga oshirilishi shart.

1. Shaxs darajasida (kibergigiyena qoidalariga rioya qilish):

- *Murakkab parollar va ikki bosqichli autentifikatsiyadan foydalanish:* Har bir akkaunt uchun alohida, kamida 12 ta belgidan iborat (harf, raqam va belgilar aralashmasi) parollardan foydalanish kerak.

- *Fishingni tanib olish orqali tahdidlarni aniqlash:* Shubhali havolalarga kirmaslik. Ayniqsa “yutuq yutdingiz”, “bepul internet yoki pul tarqatilyapti”, “ovoz bering” mazmunidagi xabarlarga ishonmaslik lozim.

- *Dasturlarni muntazam yangilash:* Operatsion tizim va ilovalarni doimiy yangilab boorish kerak.

- *Noma’lum fayllarni yuklab olmaslik:* Telegram yoki brauzerlar orqali kelgan noma’lum .apk yoki .exe fayllarni yuklamaslik lozim.

2. Tashkilot va korxonalar darajasida (maxsus ta’lim va simulyatsiyalarni yo‘lga qo‘yish):

- *CyberTraining platformalaridan foydalanish:* Xodimlar yoki talabalar uchun maxsus platformalarda o‘quv kurslari va testlardan o‘tish.

- *Fishing simulyatsiyalari:* Tashkilot ichida xodimlarga soxta fishing xatlari yuborib, ularning hushyorligini amalda tekshirish va xatolarni tahlil qilish.

- *Doimiy brifinglar:* Texnologiyalar tez o‘zgargani sababli, kiberxavfsizlik qoidalari bo‘yicha doimiy qisqa seminar yoki brifinglar tashkil etish.

3. Ta’lim muassasalari darajasida:

- *Maktab va universitet dasturlari:* Informatika darslariga kiberxavfsizlik, axborotni himoyalash va raqamli madaniyat mavzularini chuqurlashtirilgan holda kiritish.

- *Interfaol va loyihaviy o‘qitish:* O‘quvchilarga shunchaki nazariya emas, balki real kiberhujumlar ssenariylarini o‘yin yoki loyiha shaklida tushuntirish (bu an’anaviy darslardan ko‘ra samaraliroq).

4. Davlat va jamiyat darajasida:

- *Ijtimoiy roliklar va ogohlantirishlar:* Banklar, Davlat xizmatlari va huquq-tartibot organlari tomonidan kiberfiribgarlikning yangi turlari (masalan, plastik kartadan pul o‘g‘irlash ssenariylari) haqida ijtimoiy tarmoqlar va ommaviy axborot vositalarida muntazam qisqa, tushunarli kontentlar chiqarish.

- *Maxsus ilovalar va botlar:* Aholi shubhali havolalarni yoki xabarlarni tekshirib olishi uchun maxsus kiber-yordamchi botlar va ilovalardan foydalanishni targ‘ib qilish.

Bugungi kunda kibersavodxonlikdan xabardor bo‘lish barchamiz uchun juda muhim, chunki raqamli tahdidlar manzarasi tubdan o‘zgargan: texnologiyalar murakkablashgani firibgarlarning usullari yanada murakkablashganligini ko‘rsatadi. Hozir foydalanuvchining o‘zi e’tiborsiz xatolarga yo‘l qo‘ysa, endi uni texnik himoya vositalari (antiviruslar, fayervollar) xavfsizlikni ta’minlay olmaydi. Kibersavodxonlik har bir foydalanuvchida o‘zining ishonchli chegaralarini yaratish orqali bu xavfni kamaytiradi. Chunki axborot xavfsizligi tadqiqotlari statistikasi shuni ko‘rsatadiki, dunyoda barcha muvaffaqiyatli kiberhujumlarning 60 foizdan 95 foizigacha bo‘lgan qismi insonning oddiy xatosi bilan boshlanadi. Jinoyatchilar uchun murakkab xavfsizlik tizimlarini buzishdan ko‘ra, e’tiborsiz xodim yoki oddiy foydalanuvchini aldash osonroq. Foydalanuvchining asosiy “kibergigiyenasi” bo‘lmasa, qimmatbaho himoya dasturlariga qilingan har qanday sarmoya befoyda bo‘lib qoladi. Bugungi kunda kibersavodxonlik shunchaki maxsus IT ko‘nikmasi emas, balki yo‘l harakati qoidalari yoki shaxsiy gigiyena kabi zamonaviy dunyoda xavfsiz qolishning asosiy qoidasidir. Bu jarayondagi eng muhim element kibersavodxonlik asosiy tahdidlar va himoya usullarini bilish bilan cheklanmasligini anglashdir. Bu bilimlarni doimiy ravishda yangilab borish, tanqidiy fikrlash va yangi chaqiriqlarga tezkor javob berishga tayyorlikni o‘z ichiga olgan “kibergigiyena”ni shakllantirishdir.

Shuningdek, kibersavodxonlikni rivojlantirish davlat organlari, ta’lim muassasalari va xususiy sektorning muvofiqlashtirilgan sa’y-harakatlarini talab qiladi. Faqat xavfsizlik ta’lim tizimining bir qismi bo‘lgan taqdirdagina barcha darajadagi dasturlar - maktabdan tortib korporativ va barqaror raqamli jamiyatni yaratish mumkin. Keng ommani kibersavodxonlikni o‘qitish va rivojlantirishga jalb etish axborot xavfsizlik madaniyatini shakllantirishga yordam beradi.

Xulosa

Raqamlashtirish hayotimizning barcha jabhalarini - xonadonimizdan tortib davlat boshqaruvigacha o‘zgartirmoqda. Axborot-kommunikatsiya texnologiyalarining rivojlanishi bilan ma’lumotlar xavfsizligi bilan bog‘liq xatarlar ham ortib boradi. Muhim tizimlar ishonchli himoyani talab qiladi, mutaxassislar esa o‘z bilim va ko‘nikmalarini doimiy ravishda yangilab borishlari lozim bo‘ladi. Hozirgi vaqtda biz guvohi bo‘layotgan tahdidlar, agar zarur choralar ko‘rilmasa, kelajakda ancha xavfli bo‘lishi mumkin. Buning uchun albatta yuqori texnologiyalardan samarali foydalangan holda foydalanuvchilar o‘rtasida kibersavodxonlikni targ‘ib qilish lozim.

Foydalanilgan adabiyotlar:

1. https://lex.uz/ru/docs/8079279

2.https://cyberleninka.ru/article/n/obuchenie-kibergramotnosti-pervyy-shag-k-tsifrovoy-bezopasnosti

3. https://gov.uz/oz/digital/news/news

RAQAMLI TRANSFORMATSIYA SHAROITIDA TIJORAT BANKLARINING MIJOZLAR BILAN ISHLASHIDA KIBERXAVFSIZLIKKA ASOSLANGAN YANGI YONDASHUVLAR

Istamova Sh.Sh.
Zarmed universiteti

Annotatsiya. Maqolada tijorat banklarining raqamli transformatsiyasi sharoitida mijozlarga xizmat ko‘rsatish modellari va ular bilan bog‘liq kiberxavfsizlik xatarlari tahlil qilinadi. Mobil banking, masofaviy identifikatsiya, sun’iy intellekt va ochiq bank xizmatlarining imkoniyatlari hamda firibgarlik, shaxsiy ma’lumotlar sizib chiqishi va ruxsatsiz tranzaksiyalar xavfi qiyosiy-tahliliy usulda ko‘rib chiqiladi. Banklarda mijoz tajribasi va axborot xavfsizligini uyg‘unlashtirish bo‘yicha amaliy takliflar ishlab chiqiladi.

Kalit so‘zlar: raqamli transformatsiya, tijorat banklari, mijoz tajribasi, kiberxavfsizlik, ko‘p omilli autentifikatsiya, raqamli firibgarlik, open banking.

Аннотация. В статье анализируются модели обслуживания клиентов коммерческих банков в условиях цифровой трансформации и связанные с ними риски кибербезопасности. На основе сравнительного анализа рассматриваются возможности мобильного банкинга, дистанционной идентификации, искусственного интеллекта и открытого банкинга, а также угрозы мошенничества, утечки персональных данных и несанкционированных операций. Предложены практические меры по согласованию качества клиентского обслуживания и информационной безопасности.

Ключевые слова: цифровая трансформация, коммерческие банки, клиентский опыт, кибербезопасность, многофакторная аутентификация, цифровое мошенничество, открытый банкинг.

Kirish

Raqamli transformatsiya tijorat banklari faoliyatida xizmat ko‘rsatish kanallari, ichki biznes jarayonlari va mijoz bilan munosabatlarni tubdan o‘zgartirmoqda. Mobil ilovalar orqali to‘lovlar, omonatlar, kredit arizalari va hisobvaraqlarni boshqarish imkoniyatining kengayishi bank xizmatlarini makon va vaqt jihatidan yanada qulaylashtiradi. Biroq masofaviy xizmat ko‘rsatish ko‘lamining ortishi kiberjinoyatchilar uchun yangi hujum yuzalarini ham shakllantiradi. Shu bois banklar uchun asosiy vazifa xizmatning tezkorligi bilan tranzaksiya ishonchliligini birgalikda ta’minlashdan iborat. O‘zbekistonda raqamlashtirish jarayonlarining strategik asoslari “Raqamli O‘zbekiston - 2030” strategiyasi hamda bank tizimini isloh qilishga oid hujjatlarda belgilangan [1;2].

Tadqiqot maqsadi va metodologiyasi

Tadqiqotning maqsadi tijorat banklarida mijozlar bilan ishlashning raqamli shakllarini kiberxavfsizlik nuqtayi nazaridan baholash va xizmat sifati hamda xavfsizlikni uyg‘unlashtiruvchi takliflarni shakllantirishdir. Ishda ilmiy adabiyotlar va normativ hujjatlarni tahlil qilish, qiyoslash, tizimlashtirish va sifat jihatidan xavf-xatarlarni baholash usullari qo‘llanildi. Tadqiqot birlamchi so‘rov yoki banklarning maxfiy operatsion ma’lumotlariga asoslanmagan; natijalar konseptual-tahliliy xarakterga ega. Shu sababli takliflarning miqdoriy samarasi alohida empirik tekshiruvni talab qiladi.

Asosiy natijalar va muhokama

Birinchidan, mobil va internet banking bank-mijoz munosabatlarini doimiy raqamli muloqotga aylantiradi. Mijoz bank filialiga bormasdan xizmat oladi, bank esa raqamli izlar asosida so‘rovlarni tezroq qayta ishlaydi. Shu bilan birga, fishing xabarlari, qalbaki ilovalar va ijtimoiy muhandislik usullari mijoz hisobvaraqlariga noqonuniy kirish ehtimolini kuchaytiradi. Shu sababli autentifikatsiyani faqat parol yoki SMS-kod bilan cheklamasdan, risk darajasiga mos qo‘shimcha tekshiruvlarni joriy etish maqsadga muvofiq [3].

Ikkinchidan, sun’iy intellekt va ma’lumotlar tahlili mijozlarga individual takliflar berish, shubhali tranzaksiyalarni aniqlash va xizmat ko‘rsatishdagi kechikishlarni kamaytirishga xizmat qilishi mumkin. Masalan, odatiy tranzaksiya xulq-atvoridan keskin farq qiluvchi operatsiya qo‘shimcha tekshiruvga yuboriladi. Biroq avtomatlashtirilgan baholashda noto‘g‘ri ijobiy signal, algoritmik tarafkashlik va shaxsiy ma’lumotlardan ortiqcha foydalanish xavfi ham mavjud. Demak, inson nazorati, qarorlarning izohlanishi va ma’lumotlarni minimallashtirish tamoyillari saqlanishi lozim [4].

Uchinchidan, open banking va API integratsiyalari banklar bilan moliyaviy texnologiya kompaniyalari o‘rtasida yangi xizmatlarni rivojlantiradi. Bunday modelda mijoz roziligi, uchinchi tomonning huquqlari, API kalitlari va sessiyalar xavfsizligi alohida ahamiyat kasb etadi. Ruxsatlar aniq chegaralanmagan bo‘lsa, ma’lumotlar nazoratsiz tarqalishi yoki begona tizimlar orqali noqonuniy so‘rovlar yuborilishi mumkin. Xalqaro amaliyotda API xavfsizligi uchun kuchli identifikatsiya, avtorizatsiya va doimiy monitoring muhim deb baholanadi [5].

To‘rtinchidan, bank xizmatlarining inklyuzivligi xavfsizlik siyosatining ajralmas qismi bo‘lishi kerak. Keksalar, raqamli savodxonligi cheklangan shaxslar va internet sifati past hududlar aholisi murakkab tekshiruv bosqichlarida qiyinchilikka duch kelishi mumkin. Shuning uchun xavfsizlikni kuchaytirish mijoz uchun tushunarli interfeys, oddiy ogohlantirishlar va muqobil yordam kanallari bilan birga amalga oshirilishi zarur.

1-jadval

Raqamli bank xizmatlarida imkoniyatlar va xavflar

Texnologiya	Mijoz uchun imkoniyat	Asosiy xavf va himoya
Mobil banking	24/7 operatsiyalar, tezkor to‘lov	Fishing; qurilma bog‘lash va ko‘p omilli autentifikatsiya
Sun’iy intellekt	Shaxsiylashtirish, firibgarlikni aniqlash	Noto‘g‘ri signal; inson nazorati va audit
Masofaviy identifikatsiya	Bankka bormasdan xizmat olish	Shaxsni soxtalashtirish; hujjat va tiriklik tekshiruvi
Open banking / API	Yagona raqamli ekotizim	Ruxsatsiz kirish; rozilik va API avtorizatsiyasi

Amaliy takliflar

Tahlil asosida tijorat banklari uchun quyidagi izchil yondashuv taklif etiladi: 1) yuqori riskli operatsiyalarda adaptiv ko‘p omilli autentifikatsiyani qo‘llash; 2) shubhali operatsiyalarni avtomatik aniqlashni inson tomonidan qayta ko‘rib chiqish mexanizmi bilan to‘ldirish; 3) mijozning shaxsiy ma’lumotlarini yig‘ish va saqlashda minimal zaruriyat tamoyiliga rioya qilish; 4) API hamkorlari uchun ruxsatlar va xavfsizlik auditini joriy etish; 5) mijozlarga firibgarlik sxemalari bo‘yicha qisqa, tushunarli ogohlantirishlar yuborish; 6) xizmat sifatini faqat tezlik bilan emas, balki muvaffaqiyatli tranzaksiyalar, shikoyatlar va xavfsizlik hodisalari bilan birgalikda baholash.

Takliflar natijasini o‘lchash uchun operatsiyani yakunlash vaqti, mijoz murojaatlarini hal qilish muddati, shubhali operatsiyalarning tekshiruv ulushi, noto‘g‘ri bloklangan operatsiyalar va tasdiqlangan firibgarlik holatlari kabi ko‘rsatkichlardan foydalanish mumkin. Ular bankning ichki ma’lumotlari asosida vaqt bo‘yicha solishtirilsa, raqamli innovatsiyalarning real samarasi aniqlanadi.

Xulosa

Raqamli transformatsiya tijorat banklarida mijoz bilan ishlashni tezkor, moslashuvchan va masofaviy shaklga olib chiqmoqda. Shu bilan birga, yangi texnologiyalar xavfsizlikka doir mas’uliyatni kamaytirmaydi, aksincha kuchaytiradi. Tahlil shuni ko‘rsatadiki, mijoz tajribasi, ma’lumotlar maxfiyligi, kuchli autentifikatsiya va firibgarlik monitoringini yagona boshqaruv tizimida uyg‘unlashtirish maqsadga muvofiq. O‘zbekiston banklari uchun texnologik yangilanishlarni raqamli savodxonlik va riskka asoslangan nazorat bilan birga olib borish barqaror raqamli xizmat ko‘rsatishning muhim shartidir.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni. “Raqamli O‘zbekiston - 2030” strategiyasi. https://lex.uz/docs/5030957

2. O‘zbekiston Respublikasi Prezidentining 2020-yil 12-maydagi PF-5992-son Farmoni. “2020–2025-yillarga mo‘ljallangan O‘zbekiston Respublikasining bank tizimini isloh qilish strategiyasi to‘g‘risida”. https://lex.uz/docs/4811025

3. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management. SP 800-63B. https://pages.nist.gov/800-63-3/sp800-63b.html

4. NIST. AI Risk Management Framework (AI RMF 1.0). 2023. https://doi.org/10.6028/NIST.AI.100-1

5. OWASP. API Security Top 10 - 2023. https://owasp.org/API-Security/editions/2023/en/0x11-t10/

SUN’IY INTELLEKT ASOSIDA MASOFAVIY TA’LIM TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA’MINLASH

Fayziyeva D.S., Ergasheva F.Y.
Muhammad al Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada sun’iy intellekt (SI) texnologiyalari joriy etilgan masofaviy ta’lim platformalarida axborot xavfsizligini ta’minlash masalalari kriptografik himoya va DevOps (DevSecOps) yondashuvi nuqtayi nazaridan tahlil qilinadi. Foydalanuvchi ma’lumotlarini shifrlash, kalitlarni boshqarish, SI modellarining zaif joylari hamda dasturiy ta’minotni yetkazib berish jarayonida xavfsizlikni avtomatlashtirish choralari ko‘rib chiqiladi.

Kalit so‘zlar: masofaviy ta’lim, sun’iy intellekt, axborot xavfsizligi, kriptografiya, DevOps, DevSecOps, autentifikatsiya, kiberhujum.

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности в системах дистанционного обучения на основе искусственного интеллекта (ИИ) с позиций криптографической защиты и подхода DevOps (DevSecOps). Анализируются шифрование данных обучающихся, управление ключами, уязвимости самих моделей ИИ, а также меры автоматизации безопасности в процессах разработки и доставки программного обеспечения. Обоснована необходимость комплексного сочетания криптографических средств, процессов DevSecOps, правовых норм и повышения культуры кибербезопасности пользователей.

Ключевые слова: дистанционное обучение, искусственный интеллект, информационная безопасность, криптография, DevOps, DevSecOps, аутентификация, кибератака.

Kirish

So‘nggi yillarda onlayn ta’lim ko‘pchilik uchun odatiy holga aylandi. Bugungi platformalar faqat dars materialini yetkazib bermaydi. Ular talabaning o‘zlashtirishini kuzatadi, individual topshiriqlar tavsiya qiladi, imtihonlarni masofadan nazorat qiladi. Bularning barchasi SI yordamida amalga oshiriladi. Biroq tizim qanchalik ko‘p ma’lumot yig‘sa, uni himoya qilish mas’uliyati ham shunchalik oshadi.

Zamonaviy ta’lim platformasi bitta dasturdan iborat emas. U ko‘plab mikroservislar, ma’lumotlar bazalari, bulutli infratuzilma va SI modellaridan tashkil topadi, ularning har biri muntazam yangilanib turadi. Yangilanishlar qancha tez chiqsa, xatoga yoki zaiflikka yo‘l qo‘yish ehtimoli ham shuncha yuqori bo‘ladi. Shu sababli ta’lim muhitida axborot xavfsizligini faqat tizim ishga tushirilgandan keyin emas, uni yaratish va yetkazib berish jarayonining har bir bosqichida ta’minlash kerak. Bu maqolada masala uch yo‘nalish, ya’ni sun’iy intellekt, kriptografiya va DevOps amaliyotlarining o‘zaro bog‘liqligi doirasida ko‘rib chiqiladi.

Asosiy qism

Birinchidan, SI asosidagi tizimlar katta hajmdagi shaxsiy ma’lumotlar bilan ishlaydi: ism-familiya, baholar, kirish vaqtlari, ba’zan esa yuz tasviri va ovoz yozuvlari. Bunday ma’lumotlar sizib chiqsa, inson obro‘siga ham, xavfsizligiga ham zarar yetishi mumkin. Shu sababli O‘zbekistonning “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonuni [1] talablariga rioya qilish platforma uchun majburiy shart hisoblanadi. Qonun talabini amalda bajarishning eng ishonchli yo‘li esa kriptografiyadir: ma’lumot tarmoq orqali uzatilganda TLS 1.3 protokoli [2] bilan, bazada

saqlanganda esa AES-256-GCM kabi autentifikatsiyalangan shifrlash algoritmi [3] bilan himoyalanishi lozim. Autentifikatsiyalangan rejimning afzalligi shundaki, u ma’lumotni yashirish bilan birga uning yo‘lda o‘zgartirilmaganini ham tekshirib beradi. Parollar esa ochiq holda emas, Argon2 [4] yoki bcrypt singari sekin ishlovchi xesh-funksiyalar yordamida, tasodifiy qo‘shimcha (tuz) bilan saqlanadi. Shunda baza o‘g‘irlangan taqdirda ham hujumchi parollarni tez tiklay olmaydi.

Ikkinchidan, kriptografik algoritmning bardoshliligi kalitlarning qanday boshqarilishiga bog‘liq. Amaliyotda eng ko‘p uchraydigan xato kuchsiz algoritm tanlash emas, balki kalitni dastur kodiga yoki konfiguratsiya fayliga ochiq yozib qo‘yishdir. Bunday fayl ko‘pincha umumiy omborga (repozitoriyga) tushib qoladi va u yerdan hujumchi qo‘liga o‘tadi. Shuning uchun kalitlar alohida maxfiylik saqlagichida (masalan, HashiCorp Vault yoki bulut provayderining KMS xizmatida) yuritilishi, ularning muddati cheklanishi va muntazam almashtirib turilishi kerak [5]. Mijoz va server o‘rtasidagi sessiya kalitlari har safar yangidan hosil qilinsa (Diffie-Hellman almashinuvi asosida), bitta kalit buzilganda ham avvalgi yozishmalar ochilib ketmaydi. Bu xususiyat oldinga maxfiylik (forward secrecy) deb ataladi. Raqamli imzo esa o‘quv materiallari, baholar va elektron sertifikatlarning haqiqiyligini tasdiqlashda qo‘llanadi.

Uchinchidan, SI modellarining o‘ziga xos zaifliklari bor. Masalan, o‘qitish jarayonida modelga zararli yoki buzilgan ma’lumot kiritilsa, tizim noto‘g‘ri baho berishi yoki noto‘g‘ri tavsiya chiqarishi mumkin. Bu hujum ma’lumotlarni zaharlash deb ataladi [6]. Shuningdek, modelning javoblari orqali uni o‘qitishda ishlatilgan maxfiy ma’lumotlarni tiklashga urinish holatlari ham ma’lum: a’zolikni aniqlash hujumlarida muayyan talaba ma’lumoti o‘qitish to‘plamida bo‘lgan-bo‘lmaganligi taxmin qilinadi [7]. Kirish ma’lumotiga qo‘shilgan sezilmas o‘zgarish ham modelni adashtirishi mumkin [8]. Bunday xavflarga qarshi o‘qitish ma’lumotlarining manbasini tekshirish, model fayllariga raqamli imzo qo‘yish, modelni faqat ishonchli omborlardan yuklash va kerak bo‘lganda differensial maxfiylik usullaridan [9] foydalanish tavsiya etiladi. Sezgir ma’lumotlar bilan ishlaganda gomomorf shifrlash va federativ o‘qitish [10] ham istiqbolli yo‘nalish hisoblanadi, ammo ular hisoblash resurslarini ko‘p talab qilishini unutmaslik kerak.

To‘rtinchidan, masofaviy imtihonlarda yuzni tanish va xatti-harakatni kuzatish tizimlari qo‘llanadi. Bu usullar akademik halollikni saqlashga yordam beradi, lekin o‘quvchining shaxsiy hayotiga aralashuv xavfini ham tug‘diradi. Bunda xavfsizlik bilan shaffoflik o‘rtasidagi muvozanatni topish muhim: foydalanuvchi qanday ma’lumot yig‘ilayotganini va qancha vaqt saqlanishini bilishi kerak. Biometrik ma’lumot parol kabi almashtirib bo‘lmaydi, shuning uchun yuz tasviri o‘rniga uning matematik shablonini shifrlangan holda saqlash, imtihondan keyin esa xom yozuvni belgilangan muddatda o‘chirish to‘g‘ri yondashuv hisoblanadi. Tizim xatosi talabaga nohaq ayb qo‘yilishiga olib kelmasligi uchun qaror doim inson tomonidan qayta ko‘rib chiqilishi lozim.

Beshinchidan, zamonaviy platformalar DevOps madaniyati asosida ishlaydi: dasturchilar o‘zgarishni kiritadi, CI/CD konveyeri uni avtomatik tekshiradi, yig‘adi va foydalanuvchilarga yetkazadi. Agar bu konveyer himoyalanmagan bo‘lsa, hujumchi uchun eng qulay kirish nuqtasiga aylanadi. DevSecOps yondashuvi [11] xavfsizlik tekshiruvlarini ishlab chiqish jarayonining oxiriga emas, uning boshiga olib keladi (“shift left” tamoyili). Amalda bu quyidagilarni anglatadi: kod omborga tushishidan oldin unda ochiq qolgan parol va kalitlarni qidiruvchi vositalar ishga tushiriladi; statik va dinamik tahlil (SAST, DAST) har bir o‘zgarishda avtomatik bajariladi; uchinchi tomon kutubxonalari zaifliklar bazasi bo‘yicha tekshiriladi, loyiha tarkibidagi

komponentlar ro‘yxati (SBOM) yuritiladi [12]. Konteyner tasvirlari (Docker image) raqamli imzolanadi va faqat imzosi tasdiqlangan tasvirgina ishga tushiriladi. Infratuzilma kod ko‘rinishida (Infrastructure as Code) yoziladi, shu sababli uning sozlamalaridagi xatolar ham joriy etishdan oldin tekshiriladi.

Oltinchidan, SI modellari uchun alohida MLOps jarayoni kerak bo‘ladi. Model ham oddiy dastur kabi versiyalanadi, sinovdan o‘tkaziladi va yangilanadi, ammo uning xatti-harakati ma’lumotga bog‘liq bo‘lgani uchun oddiy testlar yetarli emas. Har bir yangi versiyadan oldin modelning aniqligi va hujumlarga chidamliligi avtomatik sinovdan o‘tkazilishi, natijalar jurnalga yozilishi va ko‘rsatkich pasayganda yangilanish to‘xtatilishi kerak. Ish vaqtida esa model javoblari va so‘rovlar soni kuzatib boriladi: g‘ayritabiiy ko‘p so‘rov kelishi ko‘pincha model ma’lumotini chiqarib olishga urinish belgisidir. Jurnal yozuvlari (log) o‘zgartirib bo‘lmaydigan tarzda saqlanadi, bu hodisani keyinchalik tekshirishga imkon beradi.

Yettinchidan, ta’lim platformalari odatda boshqa tizimlar bilan, masalan, talabalar hisobi va elektron jurnal tizimlari bilan dasturiy interfeyslar (API) orqali bog‘lanadi. Har bir shunday ulanish alohida himoyani talab qiladi. Foydalanuvchi shaxsini tasdiqlash uchun OAuth 2.0 [13] va OpenID Connect standartlaridan, qisqa muddatli kirish tokenlaridan foydalanish, servislararo aloqani esa o‘zaro autentifikatsiya (mTLS) bilan himoyalash maqsadga muvofiq. Bundan tashqari, so‘rovlar sonini cheklash, kiruvchi ma’lumotlarni tekshirish va API orqali beriladigan ma’lumot hajmini minimal darajada tutish ommaviy ma’lumot sizib chiqishining oldini oladi. Bu choralar ham konveyerda avtomatik sinovdan o‘tkazilsa, yangi servis qo‘shilganda xavfsizlik talablari unutilib qolmaydi.

Sakkizinchidan, inson omilini ham unutmaslik lozim. Fishing xatlari, zaif parollar va o‘qituvchi hamda talabalarning kiberxavfsizlik bo‘yicha tayyorgarligi yetarli emasligi ko‘pincha eng katta zaiflik bo‘lib chiqadi. Dasturchilar jamoasi uchun ham xuddi shu gap o‘rinli: shifrlash kutubxonasini noto‘g‘ri sozlash yoki xavfsizlik ogohlantirishini e’tiborsiz qoldirish jiddiy oqibatga olib keladi. Shuning uchun xavfsizlik bo‘yicha o‘qitish faqat foydalanuvchilar uchun emas, platformani yaratuvchi va qo‘llab-quvvatlovchi mutaxassislar uchun ham muntazam o‘tkazilishi kerak.

Himoya choralari

Amaliyotda quyidagi yo‘nalishlar eng samarali hisoblanadi: ma’lumotlarni shifrlash (uzatishda ham, saqlashda ham); ko‘p bosqichli autentifikatsiya; foydalanuvchilarga faqat o‘ziga kerakli huquqlarni berish; tizim faoliyatini doimiy monitoring qilish va muntazam xavfsizlik auditi; shaxsiy ma’lumotlarni anonimlashtirish; hamda foydalanuvchilar uchun kiberxavfsizlik bo‘yicha qisqa o‘quv kurslari. Ularga qo‘shimcha ravishda kalitlarni maxsus saqlagichda yuritish va muddatli almashtirish; CI/CD konveyeriga avtomatik xavfsizlik tekshiruvlarini kiritish; kod, konteyner va model fayllarini raqamli imzolash; “Zero Trust” tamoyiliga [14] ko‘ra har bir so‘rovni, hatto ichki tarmoqdan kelgan bo‘lsa ham, qayta tekshirish zarur. SI modellari uchun esa kirish ma’lumotlarini tekshirish va model xatti-harakatini muntazam sinovdan o‘tkazish zarur [15].

Bu choralar bir martalik ish emas, balki doimiy takrorlanadigan sikl sifatida tashkil etilishi kerak: xavfni aniqlash, himoyani joriy etish, natijani o‘lchash va yaxshilash. Shunda platforma yangi tahdidlarga ham moslashib boradi. Ta’lim muassasasi uchun eng qulay yo‘l esa avval eng muhim ma’lumotlarni (baho, biometriya, hisob ma’lumotlari) himoyalab, so‘ng qolgan jarayonlarni bosqichma-bosqich xavfsiz qilishdir.

Xulosa. Sun’iy intellekt masofaviy ta’limning imkoniyatlarini kengaytirsa-da, yangi xavflarni ham keltirib chiqaradi. Xavfsizlikni faqat texnik vositalar bilan ta’minlab bo‘lmaydi. Buning uchun huquqiy me’yorlar, texnik himoya va foydalanuvchilarning xabardorligi birgalikda ishlashi kerak. Kriptografiya ma’lumotning maxfiyligi va yaxlitligini kafolatlaydi, biroq uning samarasi kalitlar to‘g‘ri boshqarilgandagina saqlanadi. DevSecOps esa bu himoyani har bir yangilanishda avtomatik ravishda qayta tekshirib turadi, MLOps amaliyotlari bilan birgalikda SI modellarining ishonchliligini ta’minlaydi. Kelgusida ta’lim muassasalari SI tizimlarini joriy etishdan oldin xavfsizlik talablarini loyihalash bosqichidayoq belgilashlari maqsadga muvofiq.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, 2019-yil 2-iyul, O‘RQ-547-son.
2. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018.
3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D, 2007.
4. Biryukov A., Dinu D., Khovratovich D., Josefsson S. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications. RFC 9106. IRTF, 2021.
5. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Part 1 Rev. 5, 2020.
6. Biggio B., Nelson B., Laskov P. Poisoning Attacks against Support Vector Machines. ICML, 2012.
7. Shokri R., Stronati M., Song C., Shmatikov V. Membership Inference Attacks Against Machine Learning Models. IEEE Symposium on Security and Privacy, 2017.
8. Goodfellow I., Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples. ICLR, 2015.
9. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science, 2014.
10. McMahan B., Moore E., Ramage D., Hampson S., Agüera y Arcas B. Communication-Efficient Learning of Deep Networks from Decentralized Data. AISTATS, 2017.
11. Kim G., Humble J., Debois P., Willis J. The DevOps Handbook. IT Revolution Press, 2016.
12. Souppaya M., Scarfone K., Dodson D. Secure Software Development Framework (SSDF) Version 1.1. NIST SP 800-218, 2022.
13. Hardt D. (ed.). The OAuth 2.0 Authorization Framework. RFC 6749. IETF, 2012.
14. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207, 2020.
15. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1, 2023.

ZAMONAVIY AXBOROT TIZIMLARIDA MA’LUMOTLAR BAZASI XAVFSIZLIGI VA ANOMAL SO‘ROVLARNI ANIQLASHNING DOLZARB MASALALARI

Chunayev N.E., Azimbekov S.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalarni universiteti

Annotatsiya: Maqolada ma’lumotlar bazasiga murojaatlarni monitoring qilish va anomal SQL so‘rovlarini aniqlash masalalari yoritiladi. Ma’lumotlar bazalarida saqlanadigan axborotlarning hajmi va ahamiyati ortib borishi natijasida ruxsatsiz murojaatlar, foydalanuvchi hisob qaydnomalaridan noodatiy foydalanish, katta hajmdagi ma’lumotlarni o‘qish va so‘rovlar sonining keskin ortishi kabi holatlarni o‘z vaqtida aniqlash zarurati kuchaymoqda. Ishda audit jurnallarini yig‘ish, normalizatsiya qilish, muhim xususiyatlarni ajratib olish, foydalanuvchi faoliyatining odatiy profilini shakllantirish hamda xavf ballini hisoblash bosqichlaridan iborat gibrid algoritm taklif etiladi. Qoidaviy tekshiruvlar statistik tahlil bilan birlashtirilib, shubhali faollikning sabablari tushuntiriladigan tarzda qayd etilishi ko‘zda tutiladi. Shuningdek, monitoring modulining arxitekturasi, funksional qismlari, ishlash ketma-ketligi va samaradorligini baholash mezonlari bayon qilinadi. Taklif etilayotgan yondashuv ma’lumotlar bazasi xavfsizligini kuchaytirish, audit jarayonini avtomatlashtirish va xavfli faoliyatni erta aniqlashga xizmat qilishi mumkin.

Kalit so‘zlar: ma’lumotlar bazasi, SQL, monitoring, anomal so‘rov, audit jurnali, anomaliyani aniqlash, foydalanuvchi profili, xavf balli, axborot xavfsizligi, dasturiy modul.

Аннотация: В статье рассматриваются вопросы мониторинга обращений к базам данных и выявления аномальных SQL-запросов. По мере увеличения объёма и значимости данных возрастает необходимость своевременно обнаруживать несанкционированные обращения, необычное использование учётных записей, чтение чрезмерно большого количества записей и резкое увеличение частоты запросов. Предлагается гибридный алгоритм, включающий сбор и нормализацию журналов аудита, извлечение значимых признаков, построение профиля обычной активности пользователя и вычисление оценки риска. Правила безопасности объединяются со статистическим анализом, а обнаруженные события фиксируются с указанием причин срабатывания. Также описываются архитектура программного модуля мониторинга, его функциональные компоненты, последовательность работы и критерии оценки эффективности. Предложенный подход может способствовать повышению безопасности баз данных, автоматизации аудита и раннему выявлению подозрительной активности.

Ключевые слова: база данных, SQL, мониторинг, аномальный запрос, журнал аудита, обнаружение аномалий, профиль пользователя, оценка риска, информационная безопасность, программный модуль.

Ma’lumotlar bazalari davlat tashkilotlari, ta’lim muassasalari, banklar, elektron savdo platformalari va boshqa axborot tizimlarining asosiy tarkibiy qismlaridan biri hisoblanadi. Ularda foydalanuvchilar haqidagi ma’lumotlar, moliyaviy yozuvlar, xizmatlar tarixi va tashkilot faoliyatiga oid boshqa muhim axborotlar saqlanadi. Ushbu ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash ma’lumotlar bazasi xavfsizligining ustuvor vazifasidir.

Kirish huquqlarini rollar asosida belgilash, autentifikatsiya mexanizmlaridan foydalanish va tarmoq darajasida himoya o‘rnatish muhim bo‘lsa-da, bu choralar barcha xavflarni to‘liq

bartaraf etmaydi. Qonuniy hisob qaydnomasi buzib kirilganida yoki ichki foydalanuvchi o‘z vakolatidan noo‘rin foydalanganida, so‘rovlar texnik jihatdan to‘g‘ri bajarilishi mumkin. Shuning uchun bajarilgan so‘rovlarning mazmuni va xulq-atvor xususiyatlarini kuzatish ham zarur.

An’anaviy audit jurnallari hodisalar tarixini saqlash imkonini beradi, biroq katta hajmdagi yozuvlarni qo‘lda tahlil qilish ko‘p vaqt talab etadi. Avtomatlashtirilgan monitoring moduli so‘rovlar chastotasi, bajarilish vaqti, xatolar, o‘qilgan ma’lumotlar hajmi va foydalanuvchi roliga moslikni birgalikda baholashi mumkin. Bunda har qanday noodatiy so‘rovni hujum deb qabul qilish to‘g‘ri emas; natija kontekst va qo‘shimcha tekshiruv bilan baholanishi kerak.

Tadqiqotning maqsadi ma’lumotlar bazasiga murojaatlarni monitoring qilish va anomal so‘rovlarni aniqlash uchun qoidaviy hamda statistik belgilarni birlashtiruvchi algoritmni ishlab chiqish konsepsiyasini bayon qilishdan iborat. Ushbu maqsadga erishish uchun audit jurnallarining asosiy maydonlari aniqlanadi, so‘rovlarni tavsiflovchi belgilar tanlanadi, xavf ballini hisoblash usuli taklif etiladi va monitoring modulining tarkibiy qismlari belgilanadi.

Tahlil uchun ma’lumotlar bazasi boshqaruv tizimining audit jurnallari, ilova jurnallari va autentifikatsiya hodisalaridan foydalanish mumkin. Jurnal yozuvida vaqt belgisi, foydalanuvchi yoki xizmat hisob qaydnomasi, mijoz manzili, so‘rov turi, murojaat qilingan obyekt, bajarilish holati, davomiylik va qaytarilgan qatorlar soni kabi maydonlar bo‘lishi maqsadga muvofiq. Maydonlar to‘plami ishlatilayotgan platforma va audit sozlamalariga bog‘liq.

1-jadval

Ma’lumotlar bazasi so‘rovlarini monitoring qilishda foydalaniladigan asosiy belgilar

Kuzatiladigan belgi	Tahlil usuli	Ehtimoliy xavf
So‘rovlar chastotasi	Belgilangan vaqt oralig‘ida so‘rovlar sonini hisoblash	Ommaviy yoki avtomatlashtirilgan foydalanish
Muvaffaqiyatsiz so‘rovlar	Xatolar soni va ulushini kuzatish	Ruxsatlarni sinash yoki noto‘g‘ri konfiguratsiya
Natija hajmi	Qaytarilgan qatorlar sonini odatiy ko‘rsatkich bilan solishtirish	Ma’lumotlarni ommaviy yig‘ish ehtimoli
Murojaat vaqti	Faollik vaqtini foydalanuvchi profiliga taqqoslash	Hisob qaydnomasidan noodatiy vaqtda foydalanish
Obyektga murojaat	Rol va ruxsat siyosati bilan tekshirish	Ruxsatsiz jadval yoki sxemaga kirish
So‘rov davomiyligi	Tarixiy qiymatlardan og‘ishni aniqlash	Resurs sarfi yoki og‘ir so‘rov

Dastlabki ishlov berishda yozuvlar yagona formatga keltiriladi, takroriy yoki noto‘g‘ri yozuvlar ajratiladi, vaqt formatlari standartlashtiriladi. Maxfiylikni ta’minlash maqsadida parollar, tokenlar va shaxsiy ma’lumotlarning ortiqcha yig‘ilishiga yo‘l qo‘ymaslik kerak. Zarur holatlarda SQL matnidagi parametr qiymatlari niqoblanadi yoki parametrsizlashtirilgan so‘rov shabloni saqlanadi.

Taklif etilayotgan algoritm qoidaviy va statistik tahlilni birlashtiradi. Qoidaviy tahlil aniq xavfsizlik shartlarini tekshiradi: masalan, foydalanuvchining roliga ruxsat etilmagan jadvalga murojaat qilishi yoki qisqa vaqt ichida ko‘p muvaffaqiyatsiz so‘rov yuborishi. Statistik tahlil esa muayyan foydalanuvchi yoki xizmatning odatiy faoliyatiga nisbatan chetga chiqishlarni aniqlaydi. Bunday yondashuv qat’iy qoidalar bilan bir qatorda foydalanuvchi xulq-atvoridagi o‘zgarishlarni ham hisobga olishga yordam beradi.

Xavf ballini hisoblash uchun har bir xususiyat 0 dan 1 gacha bo‘lgan oraliqda normallashtiriladi. S - so‘rovlar chastotasi bo‘yicha og‘ish, E - xatolar ulushi, V - ruxsat siyosatiga nomuvofiqlik, D - natija hajmi bo‘yicha og‘ish, T - noodatiy vaqt belgisi bo‘lsin. Umumiy xavf balli quyidagicha ifodalanadi:

$$R = wS \cdot S + wE \cdot E + wV \cdot V + wD \cdot D + wT \cdot T$$

Bu yerda wS, wE, wV, wD va wT - har bir belgining ahamiyatini belgilovchi vazn koeffitsiyentlari bo‘lib, ularning yig‘indisi 1 ga teng bo‘lishi mumkin. R qiymati belgilangan chegaradan oshganda tizim hodisani qayd etadi va mas’ul xodimga ogohlantirish yuboradi. Ruxsat siyosatining aniq buzilishi kabi kritik holatlar umumiy ball past bo‘lsa ham alohida ogohlantirishga sabab bo‘lishi lozim.

Chegaraviy qiymatlarni dastlabki kuzatish davrida to‘plangan ma’lumotlar asosida belgilash maqsadga muvofiq. Bunda modul avval faqat kuzatish rejimida ishlaydi, xavfsizlik mutaxassisi ogohlantirishlarni tekshiradi va qoidalarni moslashtiradi. Foydalanuvchi profilini yangilashda faqat tekshiruvdan o‘tgan yozuvlardan foydalanish zarur, aks holda zararli faoliyat odatiy xatti-harakat sifatida qabul qilinishi mumkin.

Dasturiy modulni oltita asosiy komponentga ajratish mumkin: jurnal yig‘uvchi, normalizator, xususiyatlar generatori, anomaliyani aniqlash mexanizmi, hodisalar ombori va monitoring interfeysi. Jurnal yig‘uvchi komponent audit yozuvlarini qabul qiladi. Normalizator maydonlarni yagona formatga keltiradi va maxfiy qiymatlarni niqoblaydi. Xususiyatlar generatori so‘rovlar chastotasi, xatolar ulushi, davomiylik va natija hajmi kabi ko‘rsatkichlarni hisoblaydi. Aniqlash mexanizmi qoidalar va statistik profil asosida xavf ballini chiqaradi.

Hodisalar omborida aniqlangan hodisaning vaqti, foydalanuvchi identifikatori, xavf darajasi, aniqlash sababi va ko‘rilgan choralar saqlanadi. Monitoring interfeysi esa hodisalarni vaqt, foydalanuvchi yoki xavf darajasi bo‘yicha filtrlash, tafsilotlarni ko‘rish va ogohlantirish holatini yangilash imkonini beradi. Har bir ogohlantirish sababini tushuntirish operatorga hodisani tezroq tekshirishga yordam beradi.

Prototipni ishlab chiqishda Python loglarni qayta ishlash va statistik hisob-kitoblar uchun, SQL esa hodisalar va konfiguratsiyalarni saqlash uchun ishlatilishi mumkin. Xizmatlararo interfeys uchun FastAPI, natijalarni ko‘rsatish uchun esa veb-panel kabi yechimlar tanlanishi mumkin. Bular tavsiya etiladigan texnologiyalar bo‘lib, yakuniy tanlov tashkilot infratuzilmasi, yuklama va xavfsizlik talablariga bog‘liq.

Shunday qilib ma’lumotlar bazasiga murojaatlarni monitoring qilish va anomal SQL so‘rovlarini aniqlash uchun qoidaviy hamda statistik tahlilni birlashtiruvchi algoritm taklif etildi. Yondashuv so‘rovlar chastotasi, xatolar ulushi, natija hajmi, murojaat vaqti, foydalanuvchi roli va so‘rov davomiyligi kabi belgilarni birgalikda baholaydi. Xavf balli orqali hodisalarni ustuvorlik bo‘yicha saralash, kritik qoidabuzarliklarni alohida qayd etish va tushuntiriladigan ogohlantirishlar yaratish mumkin.

Dasturiy modul jurnal yig‘uvchi, normalizator, xususiyatlar generatori, aniqlash mexanizmi, hodisalar ombori va monitoring interfeysidan tashkil topadi. Keyingi bosqichda prototipni amalda ishlab chiqish, belgilangan sinov to‘plamida precision, recall, F1 va kechikish mezonlari bo‘yicha baholash hamda turli ma’lumotlar bazasi boshqaruv tizimlari bilan integratsiya qilish rejalashtirilishi mumkin.

Foydalanilgan adabiyotlar

1. Scarfone K., Souppaya M. Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology, 2006.

2. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys, 2009, 41(3), Article 15.

3. Halfond W. G. J., Viegas J., Orso A. A Classification of SQL-Injection Attacks and Countermeasures. IEEE International Symposium on Secure Software Engineering, 2006.

4. OWASP Foundation. SQL Injection Prevention Cheat Sheet. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

5. NIST. Security and Privacy Controls for Information Systems and Organizations. Special Publication 800-53, Revision 5, 2020.

6. Microsoft Learn. SQL Server Audit (Database Engine). https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine

ОРГАНИЗАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК

Ганиев С.К., Абдуллаев Д.Г.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Аннотация: В статье рассматриваются проблемы, связанные с утечкой конфиденциальной информации, системы их решения и даются рекомендации по их защите. Рассматриваются их назначение, классификация и виды, а также области применения. Представлен анализ DLP-систем, простых в использовании и надежных в защите данных.

Ключевые слова: утечка информации, конфиденциальные данные, система, информационная безопасность, уязвимость, социальная инжинерия, мониторинг, атака, аудит, инцидент.

Annotatsiya: Ushbu maqolada maxfiy ma'lumotlarning sizib chiqishi bilan bog'liq muammolar, ularni hal qilishdagi foydalaniladigan tizimlari ko'rib chiqiladi va ularni himoya qilish bo'yicha tavsiyalar beriladi. Shuningdek, ularning maqsadi, tasnifi va turlari, shuningdek, qo'llanilishi sohalari muhokama qilinadi. Foydalanishi oson va ma'lumotlarni himoya qilishda ishonchli sanalgan DLP tizimlari tahlili keltirilgan.

Kalit so'zlar: axborotlarni sizib chiqishi, konfidensial ma'lumotlar, tizim, axborot xavfsizligi, zaiflik, ijtimoiy muhandislik, monitoring, hujum, audit, hodisa.

Защита конфиденциальных данных от утечек - сложная задача, которая требует комплексного подхода, включающего технические меры, обучение персонала и соблюдение законодательных норм. Утечки данных могут нанести серьёзный ущерб: финансовые потери, репутационные потери, повышенную угрозу кибератак.

Некоторые причины утечек конфиденциальных данных:

– человеческий фактор - ошибки сотрудников при обработке данных, например, отправка информации не тому человеку или неправильная настройка прав доступа;

– технические уязвимости - программные ошибки, неправильно настроенные серверы или устаревшее оборудование;

– социальная инженерия - злоумышленники используют психологические методы воздействия на сотрудников, чтобы выудить информацию (например, фальшивый запрос на доступ к данным);

– недостаточная защита каналов связи - если организации не принимают должных мер по защите каналов передачи данных, таких как электронная почта, облачные хранилища или мобильные устройства.

Система информационной безопасности защищает конфиденциальную информацию компании от несанкционированного копирования, передачи, вывода или загрузки вне организации. Такие системы ориентированы прежде всего на контроль и анализ действий легитимных пользователей, которые уже находятся внутри сети.

Одним из самых надежных средств защиты данных является установка DLP-системы. DLP-система - это комплексный подход к защите конфиденциальной информации организации от угроз утечек данных и корпоративного мошенничества.

Принцип работы DLP-систем в контексте защиты данных от утечки основывается на политиках безопасности. Они могут быть созданы заранее поставщиком системы. Тогда

они называются предустановленные. Либо созданными пользователем (пользовательские). Политики безопасности описывают потенциальные угрозы для предприятия, возникающие по вине сотрудников из-за нарушения трудового распорядка или попыток распространения информации. Система анализирует весь объем данных на предмет совпадения с условием инцидента безопасности, и, в случае соответствия, действие фиксируется как инцидент, в некоторых случаях блокируется, и установленный пользователь получает уведомление о случившемся [1].

Основные задачи DLP-систем

DLP-система - это широкоприменимый программный комплекс (ПК), который может решать различные задачи: начиная от полного мониторинга активности персонала за компьютерами в течение рабочего дня, заканчивая контролем наличия и конфигураций имеющегося оборудования на предприятии. Начинка зависит от разработчика и особенностей каждого ПК отдельно. Как правило к задачам, решаемым с помощью DLP-систем относятся:

– перехват и анализ веб-трафика с рабочих станций, на которых установлена система, в том числе активности в соцсетях, мессенджерах, интернет-серфинг и многое другое;

– автоматическое определение типов данных (персональные, финансовые, коммерческая тайна);

– защита конфиденциальных данных предприятия от разглашения, нецелевого использования, изменения и порчи;

– блокировка рисковых операций с данными и информирование установленного круга лиц об инциденте;

– предотвращение случайных утечек данных из-за неосторожности, халатности или ошибки;

– обеспечение соблюдения нормативных требований в области работы с персональными данными;

– мониторинг активности сотрудников и целевого использования рабочего времени и оборудования;

– отслеживание исполнения графика сотрудниками;

– автоматическое создание отчетов на основе полученной информации и пересылка указанным адресатам;

– учет и инвентаризация оборудования и другие задачи.

Информация, перехватываемая DLP-системами, может также использоваться для оптимизации бизнес-процессов и корректировки работы персонала. Фактически, работодатель может видеть слабые стороны в организации работы коллектива и, вследствие этого, выстраивать операционную деятельность с большей эффективностью. Также на основе полученных данных по инцидентам он может провести частичный или общий аудит систем безопасности, что приведет к снижению рисков повторения таких ситуаций.

Виды DLP-систем

Существует несколько видов DLP-систем, которые классифицируются по разным критериям. Один из наиболее распространенных критериев - это место развертывания системы в информационной инфраструктуре организации. По этому критерию можно выделить три основных вида DLP-систем:

1. Сетевая DLP-система (Network DLP) – система, которая устанавливается на сетевом оборудовании (маршрутизаторах, коммутаторах, шлюзах и т.д.) и анализирует весь сетевой трафик организации. Сетевая DLP-система позволяет контролировать все каналы передачи данных, такие как электронная почта, Интернет, FTP, VPN и т.д. Сетевая DLP-система может блокировать или предупреждать о попытках утечки данных в режиме реального времени.

2. Конечная DLP-система (Endpoint DLP) – система, которая устанавливается на конечных устройствах (компьютерах, ноутбуках, смартфонах и т.д.) и анализирует все действия пользователей с данными на этих устройствах. Конечная DLP-система позволяет контролировать все локальные операции с данными, такие как копирование, перемещение, удаление, печать, запись на внешние носители и т.д. Конечная DLPсистема может блокировать или предупреждать о попытках утечки данных в режиме реального времени или постфактум.

3. Централизованная DLP-система (Centralized DLP) – система, которая устанавливается на центральном сервере или облачном сервисе и анализирует все данные, которые хранятся или обрабатываются на этом сервере или сервисе. Централизованная DLP-система позволяет контролировать все данные, которые находятся в базах данных, файловых системах, облачных хранилищах, корпоративных приложениях и т.д. Централизованная DLP-система может блокировать или предупреждать о попытках утечки данных в режиме реального времени или постфактум [2].

Каждый из этих видов DLP-систем имеет свои преимущества и недостатки, а также свои сценарии применения. В зависимости от специфики организации и ее информационной безопасности можно выбрать один или несколько видов DLP-систем, а также использовать различные комбинации и интеграции между ними. Главное – определить, какие каналы утечки необходимо закрыть.

Применение DLP-систем в бизнесе. Применение DLP-систем не ограничено деятельностью предприятия или ее размером. Фактически, любая организация, будь то производство продукции, либо создание программных решений, нуждается в защите своих данных. А если учесть то, что система может одновременно с мониторингом конфиденциальности выполнять функции учета рабочего времени сотрудников и помогать в проведении аудита программ и оборудования - использование DLP становится еще более целесообразным.

Поэтому сегодня системы находят широкое применение в различных отраслях.

Банковский и финансовый сектор. Сюда относятся банки, страховые, кредитные и лизинговые компании, биржи и другие финансовые учреждения, которые оперируют огромными объемами персональных данных клиентов и специфика работы которых связана с постоянным обновлением и передачей информации разного рода.

DLP-системы помогают предотвращать возможные утечки информации по вине сотрудников, тем самым повышая общую информационную безопасность банковского и финансового сектора, что положительно влияет на доверие клиентов к этим организациям.

Учреждения здравоохранения. Медицинские учреждения несут ответственность перед пациентами. Они не только обеспечивают своевременную помощь болеющим, но и обязаны защищать от разглашения данные пациентов, включая историю болезни и результаты анализов. Использование DLP-системы позволяет предотвращать утечки этой информации, снижая риск раскрытия конфиденциальных данных.

Производство. Производство очень уязвимо перед атаками на информацию. Здесь одновременно сочетается сложность технических и технологических решений с использованием объектов интеллектуальной собственности, таких как чертежи, технические спецификации и ноу-хау. Эта особенность усложняет обеспечение ИБ производства и может привести к риску утечки информации. А потеря производственных секретов негативно отразится на работе производственного предприятия в целом, особенно в условиях жесткой конкуренции.

Государственные учреждения. Государственные учреждения обрабатывают большое количество данных, связанных с национальной безопасностью и персональной информацией граждан. DLP помогает предотвратить утечку этих данных.

Это только часть областей применения DLP-систем, но ими они не ограничиваются. Предприятия могут сами исследовать целесообразность применения программного комплекса защиты данных, например, используя бесплатные тестовые периоды, предлагаемые разработчиками. Также можно изучить практический опыт использования программных комплексов на примере отзывов предприятий в кейсах.

Минимизация рисков информационной и кадровой безопасности при применении DLP

В качестве основных рисков информационной и кадровой безопасности можно выделить следующие (см. табл. 1).

Таблица 1

Основные риски информационной и кадровой безопасности

Риск информационной безопасности	Риски кадровой безопасности
Утечка конфиденциальных данных	Ущерб репутации организации
Вред в результате нарушения функционирования информационного ресурса	Финансовый ущерб от действий сотрудника
Несанкционированное распространение (передача) информации	Несанкционированная передача информации
Умышленные действия сотрудников, направленные на причинение вреда компании	Хищение имущества, информации
Ошибки сотрудников (пользователей информационных ресурсов)	Раскрытие коммерческих секретов конкурентам
Доступ потенциально опасным обьектам во внешней сети	Уход к конкурентам ключевых сотрудников организации
Внешние атаки на информационные ресурсы организации	Высокая текучесть кадров
Вредоносное программное обеспечение (трояны, бэкдоры, шифровальщики и т.д.)	Отсутствие кадров нужной квалификации на рынке труда

На риски кадровой безопасности, не связанные с утечкой информации, – уход к конкурентам ключевых сотрудников организации, высокая текучесть кадров, отсутствие кадров нужной квалификации на рынке труда DLP-система влияния не оказывает. Некоторые смежные функции, связанные с мониторингом активности сотрудников, которые часто интегрируют в отечественные решения DLP, могут помочь в раннем выявлении желающих сменить место работы и "портящих" морально-психологический климат в коллективе, что позволит нейтрализовать такие риски, как текучесть кадров и уход работников к конкурентам. Очевидно, что риск отсутствия на рынке квалифицированных

кадров никакое решение по информационной безопасности минимизировать (а уж тем более нейтрализовать) не может.

Все остальные риски, перечисленные в табл. 1, могут быть минимизированы посредством применения DLP-систем. Давайте попробуем разобраться, каким образом.

1. Блокировка исходящих из информационной инфраструктуры потоков информации позволяет предотвратить утечку конфиденциальных данных, несанкционированное неумышленное распространение (передачу) информации, хищение информации и, как следствие, ущерб репутации организации в случае появления сведений об инциденте в средствах массовой информации. Включения функций блокировки в DLP-системе на практике стараются избегать, чтобы не произошла блокировка нужного информационного сообщения. Практика показывает, что указанный подход имеет право на существование. В ряде случаев блокировка может проявлять себя как эффективный элемент для помощи не только специалисту по информационной безопасности, но и самому работнику. Например, встречаются организации, которые настраивают DLP-систему таким образом, чтобы при блокировании информационного сообщения она отправляла уведомление не только специалисту по информационной безопасности, но и самому работнику для проверки правильности отправления информации нужному адресату. В этом случае DLP-система выступает как помощник, защищающий работника от ошибок (например, случайной отправки почты и т.п.). Кроме того, функциями DLP-системы, как правило, можно заблокировать доступ к потенциально опасным объектам во внешней сети.

2. Мониторинг информационных потоков внутри инфраструктуры позволяет минимизировать утечки информации, в том числе вызванные умышленными действиями сотрудников, и такие их последствия, как ущерб репутации организации и финансовый ущерб от действий работников. Кроме того, мониторинг информационных потоков помогает при выявлении внешних атак и активности вредоносного программного обеспечения. Конечно, это лишь некая вспомогательная функция DLP, которая не заменит системы класса SIEM, EDR и XDR. Мониторинг информационных потоков, в отличие от блокировки, сопряжен с рисками для самого специалиста по информационной безопасности, занимающегося таким мониторингом. Дело в том, что действия специалиста по информационной безопасности при использовании DLP-системы могут нарушать конституционные права и свободы человека, гражданина [3].

Таким образом, первое, на что рекомендуется обращать внимание специалисту по информационной безопасности при начале использования DLP (или при ее внедрении), – это наличие оформленного согласия пользователей информационной инфраструктуры на проведение подобного рода мониторинга их активности. Применение DLP-системы, особенно для "работы" с рисками кадровой безопасности, когда первичен мониторинг и контроль за сотрудниками, неизбежно приводит к необходимости обезопасить себя при помощи так называемой легализации этой системы.

Список литератур

1. Кучкаров Т.А. Методы и средства защиты информации от утечек. Учебное пособие. Самарканд-2025.издательство ООО “STAP-SEL”, 2025. 50-68 с.

2. Соколов, А. И. Технические средства защиты информации: технические каналы утечки информации : учеб. пособие / А. И. Соколов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2016. 34-62 с.

3. Бузов Г.А. Защита от утечки информации по техническим каналам. / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия - Телеком, 2002. 123-157 с.

ZERO-DAY KIBERHUJUMLARNI ANIQLASHDA FEDERATIV O‘QITISH VA ANOMALIYALARNI ANIQLASHGA ASOSLANGAN TAQSIMLANGAN IDS MODELI

Mamatqulova M.K., Alishev Sh.A.
Jizzax Sambhram universiteti

Annotatsiya. Maqolada ilgari ma’lum bo‘lmagan Zero-Day kiberhujumlarni aniqlash uchun federativ o‘qitish va anomaliyalarni aniqlashga asoslangan taqsimlangan IDS modeli taklif etiladi. Har bir tarmoq tuguni mahalliy trafikning faqat odatiy xatti-harakatini o‘rganuvchi autoencoder asosidagi detektorni o‘qitadi, dastlabki trafik tugunda qoladi markaziy server model parametrlarini birlashtirib (FedAvg/FedProx) umumiy model va aniqlash chegarasini shakllantiradi. Model arxitekturasi, o‘qitish algoritmi, xavfsizlik choralari, Non-IID ma’lumotlar bilan bog‘liq masalalar va zero-day holatini modellashtiruvchi tajriba rejasi bayon etiladi. Ish konseptual xarakterga ega tajriba natijalari keltirilmaydi.

Kalit so‘zlar: Zero-Day hujumlar, kiberxavfsizlik, IDS, federativ o‘qitish, anomaliyalarni aniqlash, autoencoder.

Аннотация. Предлагается модель распределённой системы обнаружения вторжений (IDS) на основе федеративного обучения и обнаружения аномалий для выявления ранее неизвестных атак нулевого дня. Каждый узел обучает локальный автоэнкодер на нормальном трафике, исходные данные остаются на узле, а центральный сервер агрегирует параметры моделей (FedAvg/FedProx) и формирует общую модель и порог обнаружения. Описаны архитектура, алгоритм обучения, меры безопасности, вопросы Non-IID данных и план экспериментов для сценария нулевого дня. Работа носит концептуальный характер, результаты экспериментов не приводятся.

Ключевые слова: атаки нулевого дня, кибербезопасность, IDS, федеративное обучение, обнаружение аномалий, автоэнкодер.

Kirish

Raqamli xizmatlar va internetga ulangan qurilmalar sonining ortishi axborot tizimlarini kiberhujumlardan himoya qilish masalasini dolzarb qilmoqda. Zero-Day hujumlari hali aniqlanmagan yoki himoya qoidalari bilan qamrab olinmagan zaifliklardan foydalanadi, shu sababli ularning imzosi himoya tizimida bo‘lmaydi va faqat ma’lum hujum belgilariga tayanuvchi usullar yetarli emas.

IDS tizimlari tarmoq trafigini kuzatib, shubhali faoliyat haqida ogohlantiradi. Mashinaviy o‘qitish tarmoqning odatiy holatini o‘rganib, undan farq qiluvchi holatlarni aniqlashga imkon beradi. Biroq bir nechta tashkilot ma’lumotlarini bitta joyga yig‘ish maxfiylik va ma’lumot uzatish bilan bog‘liq muammolarni keltirib chiqaradi. Federativ o‘qitishda ma’lumotlar emas, balki model yangilanishlari almashiladi, bu esa muammoni qisman hal etadi . Federativ IDS bo‘yicha so‘nggi sharhlar bu yo‘nalishning imkoniyat va cheklovlarini ko‘rsatadi.

Muammo va tadqiqot yondashuvi

Imzo asosidagi usul trafikni ma’lum hujum imzolari bilan taqqoslaydi va imzosi bazada bo‘lmagan yangi hujumni aniqlashda qiynaladi . Anomaliyalarni aniqlash esa tarmoqning odatiy xatti-harakatini o‘rganib, undan farq qiluvchi trafikni shubhali deb belgilaydi (masalan, ulanishlar sonining keskin ortishi). Biroq qonuniy yuklama ham o‘xshash holatni yuzaga keltirishi mumkin, shu sababli noto‘g‘ri ogohlantirishlar hisobga olinishi kerak. Federativ o‘qitishda har bir

ishtirokchi modelni mahalliy o‘qitib, yangilanishlarni serverga yuboradi va server ularni birlashtirib, umumiy modelni qaytaradi. Bu ma’lumotlarni markazlashtirish ehtiyojini kamaytiradi, ammo yangilanishlar o‘zi ham xavfsizlik xatarlariga ega . 1-jadvalda yondashuvlar sifat jihatidan (miqdoriy emas) taqqoslangan.

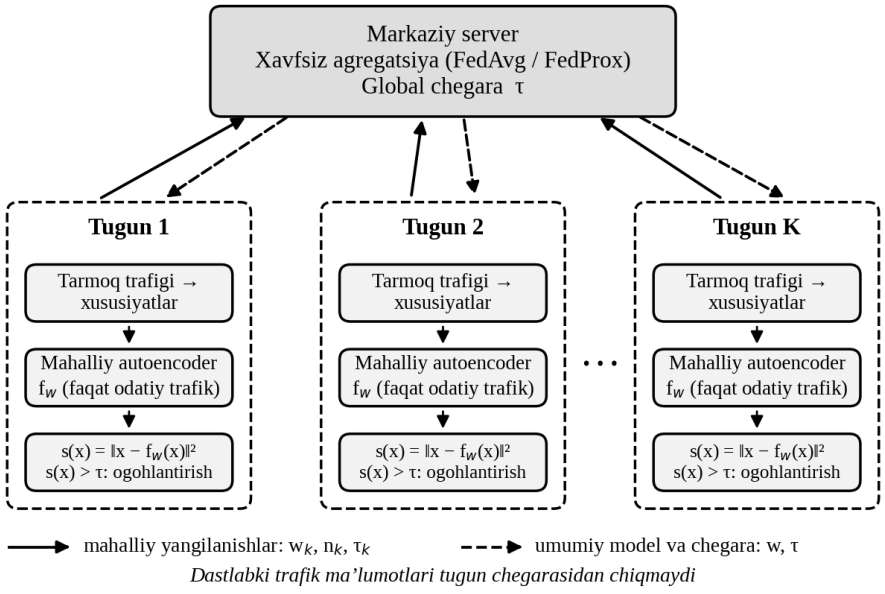
1-jadval

Yondashuvlarning sifat jihatidan qiyosiy tahlili

Yondashuv	Noma’lum hujumlarni aniqlash	Ma’lumotlar maxfiyligi	Asosiy cheklov
Imzo asosidagi IDS	Past: faqat ma’lum imzolar	Ma’lumotlar mahalliy qoladi	Yangi hujumlar o‘tkazib yuboriladi
Markazlashtirilgan anomaliya IDS	Imkoniyati bor	Trafik markazga uzatiladi	Maxfiylik xatarlari, ma’lumot hajmi
Faqat mahalliy anomaliya IDS	Imkoniyati bor, mahalliy ma’lumot bilan cheklangan	Ma’lumotlar mahalliy qoladi	Boshqa tugunlar tajribasidan foydalanmaydi
Taklif etilayotgan federativ IDS	Imkoniyati bor; tugunlar tajribasi birlashadi	Trafik mahalliy qoladi, parametrlar almashiladi	Non-IID, yangilanishlar xavfsizligi, aloqa xarajati

Taklif etilayotgan modelning arxitekturasi

Model (1-rasm) *K* ta tarmoq tuguni, har bir tugundagi mahalliy anomaliya aniqlash moduli va markaziy serverdan iborat. Har bir tugun faqat odatiy trafikni o‘rganadi keyin hujum turi haqida oldindan ma’lumot talab etilmaydi, odatiy taqsimotdan chetga chiqqan trafik esa yuqori anomaliya ballini oladi.



1-rasm. Taklif etilayotgan federativ IDS modelining arxitekturasi

1) Ma’lumotlarni tayyorlash va xususiyatlarni ajratish. Tarmoq oqimlari (flow) yozuvlari tozalanadi (bo‘sh, cheksiz, takroriy qiymatlar olib tashlanadi), normallashtiriladi (masalan, min–max), paketlar soni, oqim davomiyligi, trafik hajmi, paketlararo vaqt, TCP bayroqlari kabi belgilar tanlanadi so‘ngra doimiy va kuchli korrelyatsiyalangan belgilar chiqariladi.

2) Mahalliy o‘qitish. Har bir tugun autoencoder (f_w) ni faqat odatiy trafikda o‘qitadi, yo‘qotish funksiyasi (1) bilan beriladi, bunda n_k - *k*-tugundagi namunalar soni, x_i - oqimning

xususiyatlar vektori. Isolation Forest kabi daraxtli usullarda o‘rtalashtiriladigan vaznlar yo‘q, shu sababli ular faqat mahalliy taqqoslash (baseline) uchun ishlatiladi.

$$L_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} \|x_i - f_w(x_i)\|^2 \tag{1}$$

3) Yangilanishlarni yuborish va birlashtirish. Tugunlar dastlabki trafikni emas, faqat parametrlar w_k, soni n_k va mahalliy chegara τ_k ni himoyalangan (TLS/mTLS) kanal orqali yuboradi. Server parametrlarni FedAvg bo‘yicha (2) birlashtiradi. Non-IID holatda FedProx mahalliy maqsad funksiyasiga (3) regulyarizatsiya hadini qo‘shadi. Zararli ishtirokchilar ta’sirini kamaytirish uchun median yoki trimmed mean kabi robust hamda xavfsiz agregatsiya (secure aggregation) ko‘rib chiqiladi.

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1}, \quad n = \sum_{k=1}^{K} n_k \tag{2}$$

$$L_k^{\text{prox}}(w) = L_k(w) + \frac{\mu}{2} \|w - w^t\|^2 \tag{3}$$

4) Chegara va ogohlantirish. Yangilangan model tugunlarga qaytariladi. Yangi namuna x uchun anomaliya bali (4) bo‘yicha hisoblanadi. Chegara τ_k - tugunning odatiy validatsiya ballari p-kvantili (masalan, 95–99%), umumiy chegara esa (5) bo‘yicha topiladi; bu soddalashtirilgan yondashuv bo‘lib, tajribada tekshiriladi. Agar $s(x) > \tau$ bo‘lsa, hodisa jurnalga yoziladi va administratorga ogohlantirish yuboriladi (avtomatik bloklash uchun alohida IPS funksiyasi talab etiladi).

$$s(x) = \|x - f_w(x)\|^2 \tag{4}$$

$$\tau = \sum_{k=1}^{K} \frac{n_k}{n} \tau_k \tag{5}$$

bu yerda $\tau_k = Q_p(\{s(x) : x \in D_k^{\text{val}}\})$, Q_p - p-kvantil, D_k^{val} - odatiy validatsiya to‘plami. Umumiy tartib 1-algoritmda berilgan.

1-algoritm. Federativ o‘qitish va chegarani moslash

Kirish: K ta tugun; odatiy ma’lumotlar D_k; raundlar soni T; epoxalar soni E; kvantil p.

1. Server w^0 ni initsializatsiya qiladi. t = 0, 1, ..., T−1 uchun:

2. Server w^t ni tugunlarga yuboradi.

3. Har bir tugun E epoxa davomida $L_k(w)$ (yoki $L_k^{prox}(w)$) ni minimallashtirib, w_k^{t+1} ni serverga yuboradi.

4. Server w^{t+1} ni (2) bo‘yicha (yoki robust agregatsiya bilan) hisoblaydi.

5. Tugunlar τ_k ni topadi; server τ ni (5) bo‘yicha hisoblaydi. Chiqish: w^T, τ; qoida: $s(x) > \tau$ - ogohlantirish.

Afzalliklar, xatarlar va hal etilishi lozim masalalar

Afzalliklar. Dastlabki trafik markazga uzatilmasdan umumiy model o‘qitiladi. Model faqat odatiy trafikni o‘rganganligi sababli belgilangan hujum namunalari talab etilmaydi; federativ o‘z-o‘zini o‘qitadigan anomaliya aniqlash IoT tarmoqlarida ham ko‘rsatilgan . Biroq barcha Zero-Day hujumlarini topish kafolatlanmaydi va odatiy trafikka juda o‘xshash, sekin kechuvchi hujumlar aniqlanmay qolishi mumkin.

Xavfsizlik xatarlari. Federativ o‘qitish to‘liq maxfiylik kafolati emas balki yangilanishlar orqali bilvosita ma’lumot sizishi, zararli ishtirokchilar tomonidan modelni “zaharlash” yoki

chegarani sun’iy oshirish mumkin. Xavfsiz va robust agregatsiya, ishtirokchilarni tekshirish, kanal himoyasi va zarur holatda differensial maxfiylik (aniqlik pasayishi evaziga) qo‘llanadi.

Amaliy masalalar. (a) Tugunlar trafigi Non-IID bo‘ladi - FedProx va mahalliy chegara ko‘rib chiqiladi. (b) “Odatiy” ma’lumotda yashirin hujum izlari bo‘lishi mumkin - xatosi eng yuqori namunalarning kichik ulushini (1–5%) o‘qitishdan chiqarish yoki dastlabki filtrlash. (c) Noto‘g‘ri ogohlantirishlar darajasi chegaraga bog‘liq. (d) Trafik vaqt o‘tishi bilan o‘zgaradi (concept drift) - davriy qayta o‘qitish. (e) Aloqa xarajatini cheklash uchun yengil modellar tanlanadi.

Tajriba rejasi va baholash mezonlari

Samaradorlikni baholash uchun 2-jadvaldagi protokol taklif etiladi. Hozircha tajribalar bajarilmagan va natijalar keltirilmaydi.

2-jadval

Taklif etilgan protokol

Element	Reja
Ma’lumotlar	CIC-IDS2017 [17] va UNSW-NB15 [18] (ochiq); zarur bo‘lsa, Edge-IIoTset [19]
Tugunlar va o‘qitish	K = 5–10 virtual tugun, ma’lumotlar Non-IID bo‘linadi (kun, subtarmoq yoki Dirichlet); faqat odatiy trafik, aralashma ulushi 0%, 1%, 5%
Zero-day modellashtirish	Leave-one-attack-out: bitta hujum turi (masalan, DoS, Botnet, Web Attack) o‘qitish va validatsiyadan chiqarilib, faqat testda beriladi
Taqqoslash	(a) markazlashtirilgan autoencoder; (b) faqat mahalliy autoencoder; (c) mahalliy Isolation Forest; (d) taklif etilgan model (FedAvg, FedProx); (e) Snort/Suricata (ixtiyoriy)
Ko‘rsatkichlar	Precision, Recall (zero-day aniqlash darajasi), F1, FPR, ROC-AUC, yaqinlashish raundlari, bir raundda uzatiladigan hajm (MB)
Amalga oshirish	Python, PyTorch/TensorFlow, Flower [20]; kamida 5 ta tasodifiy urug‘ (seed), o‘rtacha ± standart og‘ish; K, E, μ, p ga sezgirlik tahlili

Tekshiriladigan farazlar: (H1) federativ model faqat mahalliy modelga nisbatan ilgari ko‘rilmagan hujumlar uchun yuqori Recall beradi. (H2) markazlashtirilgan modeldan sezilarli orqada qolmaydi, (H3) Non-IID sharoitida FedProx FedAvg‘dan barqarorroq. Bular natija emas, tekshirilishi lozim taxminlardir.

Xulosa

Maqolada Zero-Day kiberhujumlarni aniqlash uchun federativ o‘qitish va anomaliyalarni aniqlashga asoslangan taqsimlangan IDS modeli taklif qilindi: mahalliy autoencoder, parametrlarni markazda birlashtirish (FedAvg/FedProx), umumiy chegarani moslash va modelni tugunlarga qaytarish. Yondashuv ma’lumotlarni markazlashtirish ehtiyojini kamaytiradi, ammo noto‘g‘ri ogohlantirishlar, Non-IID ma’lumotlar, yangilanishlar xavfsizligi va noma’lum hujumlarni aniqlash darajasi alohida tekshirilishi kerak. Kelgusida 5-bo‘limdagi protokol bo‘yicha ochiq ma’lumotlar to‘plamlarida tajribalar o‘tkazilib, natijalar markazlashtirilgan va mahalliy modellar bilan solishtiriladi.

Foydalanilgan adabiyotlar

1. Chandola, V., Banerjee, A., & Kumar, V. Anomaly Detection: A Survey. ACM Computing Surveys, 41(3), Article 15, 2009. DOI: https://doi.org/10.1145/1541880.1541882.

2. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of AISTATS, PMLR 54, 1273–1282, 2017.

3. Kairouz, P., McMahan, H. B., et al. Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210, 2021. DOI: https://doi.org/10.1561/2200000083.

4. Khraisat, A., Alazab, A., Singh, S., Jan, T., & Gomez, A. Survey on Federated Learning for Intrusion Detection System: Concept, Architectures, Aggregation Strategies, Challenges, and Future Directions. ACM Computing Surveys, 57(1), Article 7, 2024. DOI: https://doi.org/10.1145/3687124.

5. Belenguer, A., Pascual, J. A., & Navaridas, J. A Review of Federated Learning Applications in Intrusion Detection Systems. Computer Networks, 258, 111023, 2025. DOI: https://doi.org/10.1016/j.comnet.2024.111023.

6. Sommer, R., & Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 305–316, 2010. DOI: https://doi.org/10.1109/SP.2010.25.

7. NIST. Privacy Attacks in Federated Learning. NIST Cybersecurity Insights, 24 January 2024. https://www.nist.gov/blogs/cybersecurity-insights/privacy-attacks-federated-learning.

8. Hinton, G. E., & Salakhutdinov, R. R. Reducing the Dimensionality of Data with Neural Networks. Science, 313(5786), 504–507, 2006. DOI: https://doi.org/10.1126/science.1127647.

9. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. Network and Distributed System Security Symposium (NDSS), 2018.

10. Liu, F. T., Ting, K. M., & Zhou, Z.-H. Isolation Forest. IEEE International Conference on Data Mining (ICDM), 413–422, 2008. DOI: https://doi.org/10.1109/ICDM.2008.17.

WEB ILOVALARNI HUJUMLARDAN HIMOYALASH DASTURIY VOSITASI XUSUSIYATLARI

Ibrohimov S.Sh.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda veb-ilovalarga qaratilgan zamonaviy kiberhujumlarning asosiy turlari, OWASP Top 10:2025 ro‘yxatidagi eng xavfli zaifliklar va ularga qarshi dasturiy himoya vositasini ishlab chiqish yondashuvlari tahlil qilinadi. Ko‘p qatlamli himoya arxitekturasi – WAF, RASP va xavfsiz kodlash amaliyotlarining o‘rni asoslanib, dasturiy vositaga qo‘yiladigan funksional talablar shakllantiriladi.

Kalit so‘zlar: veb-ilova xavfsizligi, OWASP Top 10, SQL injection, broken access control, WAF, RASP, hujum vektori, dasturiy himoya.

Аннотация. В тезисе анализируются основные виды современных кибератак на веб-приложения, наиболее опасные уязвимости из списка OWASP Top 10:2025 и подходы к разработке программного средства защиты. Обосновывается роль многоуровневой архитектуры защиты, включая WAF, RASP и практики безопасного кодирования, формулируются функциональные требования к программному средству.

Ключевые слова: безопасность веб-приложений, OWASP Top 10, SQL-инъекция, broken access control, WAF, RASP, вектор атаки, программная защита.

Kirish

Veb-ilovalar zamonaviy raqamli infratuzilmaning asosiy komponentiga aylangan. Bugungi kunda elektron tijorat, bank xizmatlari, davlat xizmatlari, ta’lim platformalari va korporativ boshqaruv tizimlari asosan brauzer orqali ishlaydigan dasturiy ta’minotga tayanadi. Foydalanuvchi tomonidan kundalik amalga oshiriladigan to‘lovlar, ma’lumot almashinuvi va xizmatlardan foydalanish jarayonining katta qismi aynan veb-ilovalar orqali kechadi. Shu bois veb-ilovalar nafaqat biznes va davlat xizmatlari uchun asosiy kanal, balki kiberjinoyatchilar uchun ham eng jozibador nishonlardan biri bo‘lib qolmoqda. 2025-yil davomida o‘tkazilgan xalqaro tadqiqotlarga ko‘ra, so‘ralgan tashkilotlarning 56 foizi so‘nggi 12 oy ichida veb-ilova orqali kompromatga uchrash holatini qayd etgan [1]. Bundan tashqari, tashqi muhitga ochiq ilovalarga qaratilgan hujumlar barcha boshlang‘ich kirish yo‘llarining 43,7 foizini tashkil etadi [2]. Bu ko‘rsatkichlar veb-ilovalar xavfsizligi masalasi shunchaki texnik ehtiyoj emas, balki tashkiliy va iqtisodiy zarurat ekanligini ko‘rsatadi. Birgina muvaffaqiyatli hujum natijasida tashkilot nafaqat moddiy zarar ko‘rishi, balki mijozlar ishonchini yo‘qotishi, shuningdek, shaxsiy ma’lumotlarni himoya qilish bo‘yicha qonuniy javobgarlikka tortilishi mumkin.
Veb-ilovalarga qaratilgan hujumlarning o‘ziga xos xususiyati shundaki, ular an’anaviy tarmoq himoyasi vositalari – firewall, antivirus va IDS/IPS tizimlari – tomonidan har doim ham aniqlanmaydi. Sababi, bunday hujumlar ko‘pincha qonuniy HTTP so‘rovlar ko‘rinishida amalga oshiriladi va ilova mantiqiy qatlamida amalga oshiriladi. Masalan, SQL injection hujumi oddiy foydalanuvchi kiritmasi orqali amalga oshirilishi mumkin, ammo u ma’lumotlar bazasiga bevosita ta’sir o‘tkazadi. Shu sababli veb-ilovalarni himoyalash uchun maxsus dasturiy vositalar – Web Application Firewall (WAF), Runtime Application Self-Protection (RASP) va boshqa yechimlar ishlab chiqish zarurati tug‘iladi. O‘zbekiston sharoitida ham bu masala dolzarb ahamiyat kasb etmoqda. Mamlakatda raqamlashtirish jarayonlarining jadal sur’atlarda rivojlanishi, davlat

xizmatlarining elektron shaklga o‘tkazilishi va xususiy sektorning raqamli transformatsiyasi veb-ilovalar sonining keskin oshishiga olib keldi. Bu esa o‘z navbatida ularni himoyalash uchun mahalliy sharoitga moslashtirilgan dasturiy yechimlarni ishlab chiqishni taqozo etadi. Ushbu ishning maqsadi – veb-ilovalarni hujumlardan himoyalash uchun dasturiy vosita ishlab chiqishda zamonaviy tahdid manzarasini, eng dolzarb zaifliklarni va samarali himoya arxitekturasini tahlil qilishdan iborat. Ishda quyidagi vazifalar belgilangan: veb-ilovalarga qaratilgan hujumlarning asosiy turlarini tasniflash; OWASP Top 10:2025 ro‘yxatidagi eng xavfli zaifliklarni tahlil qilish; ko‘p qatlamli himoya arxitekturasining tarkibiy qismlarini asoslash; dasturiy himoya vositasiga qo‘yiladigan funksional talablarni shakllantirish.

Asosiy qism

Veb-ilovalarga qaratilgan hujumlarning dinamikasi so‘nggi yillarda keskin o‘sish tendentsiyasini ko‘rsatmoqda. Radware kompaniyasining 2025-yil global tahdid tahliliga ko‘ra, tarmoq qatlamidagi DDoS hujumlari yillik hisobda 168,2 foizga, veb-DDoS hujumlari esa 101,4 foizga o‘sgan; zararli veb-ilova va API tranzaksiyalari 128 foizga ko‘paygan [2]. Zararli bot harakatlari ham 91,8 foizga oshgan. Bu raqamlar veb-ilovalar xavfsizligini ta’minlash shunchaki texnik ehtiyoj emas, balki iqtisodiy zarurat ekanligini ko‘rsatadi. Bunday o‘sish sur’atlari generativ sun’iy intellekt vositalarining keng tarqalishi, avtomatlashtirilgan hujum skriptlarining ommalashuvi va kiberjinoyatchilikning sanoat darajasiga ko‘tarilishi bilan bevosita bog‘liq. Hujumlarning eng keng tarqalgan turlari qatoriga SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE), Path Traversal, Security Misconfiguration va Broken Access Control kiradi. Har bir hujum turi o‘ziga xos zaiflikdan kelib chiqadi va tegishli himoya choralarini talab qiladi. Masalan, SQL Injection foydalanuvchi kiritmalarini tekshirmasdan to‘g‘ridan-to‘g‘ri SQL so‘rovlariga qo‘shish natijasida yuzaga keladi; XSS esa foydalanuvchi kiritmalarini HTML sahifasiga filtrsiz joylashtirish orqali amalga oshiriladi.

Veb-ilovalarga qaratilgan haqiqiy hujum hodisalarini tahlil qilish ham muhim ahamiyatga ega. 2025-yilda o‘tkazilgan tadqiqotda qayd etilgan 40 934 ta hujum hodisasi ichida SQL Injection 31,42 foiz bilan birinchi o‘rinni egallagan [1]. Bu shuni ko‘rsatadiki, ma’lumotlar bazasiga to‘g‘ridan-to‘g‘ri ta’sir o‘tkazishga qaratilgan hujumlar hanuz eng keng tarqalgan va xavfli tahdid bo‘lib qolmoqda. WebShell Upload (22,93%) va OS Command Injection (17,65%) keyingi o‘rinlarda turadi.

1-jadval

2025-yilda qayd etilgan hujum turlarining ulushi

Hujum turi	Ulushi, %
SQL Injection	31,42
WebShell Upload	22,93
OS Command Injection	17,65
Cross-Site Scripting(XSS)	12,40
Path Traversal	8,20
Boshqalar	7,40

1-jadvaldan ko‘rinib turibdiki, dastlabki uchta hujum turi barcha hodisalarning qariyb 72 foizini tashkil etadi. Bu esa himoya vositasini ishlab chiqishda aynan shu hujum turlariga qarshi samarali mexanizmlarni birinchi navbatda joriy etish zarurligini ko‘rsatadi.

Shu nuqtada veb-ilovalarni himoyalash uchun dasturiy vosita ishlab chiqishda qanday arxitektura tamoyillariga tayanish kerak degan savol tug‘iladi. Zamonaviy yondashuv ko‘p

qatlamli himoya (defense in depth) tamoyiliga asoslanadi. Bu tamoyilga ko‘ra, himoya bir necha mustaqil qatlamda tashkil etilishi kerak: tarmoq darajasidagi filtrlar, ilova darajasidagi himoya, ma’lumotlar darajasidagi shifrlash va monitoring tizimlari. Har bir qatlam o‘ziga xos tahdidlarni bartaraf etadi va bir qatlamning zaifligi boshqa qatlamlar tomonidan qoplanadi.

Dasturiy himoya vositasining birinchi qatlami - *Web Application Firewall (WAF)*. WAF kiruvchi HTTP/HTTPS so‘rovlarini oldindan belgilangan qoidalar to‘plami asosida tekshiradi va zararli trafikni filtrlaydi [4]. Zamonaviy WAF yechimlari nafaqat statik imzo asosidagi aniqlashdan, balki mashinaviy o‘qitish modellaridan ham foydalanadi. Cloudflare WAF misolida ko‘rish mumkinki, “WAF attack score” deb nomlangan mashinaviy o‘qitish qatlami SQL injection, cross-site scripting (XSS) va remote code execution (RCE) hujumlariga qarshi qo‘shimcha himoya ta’minlaydi [4]. WAF ning afzalligi shundaki, u ilova kodiga o‘zgartirish kiritmasdan ishlaydi va markazlashtirilgan tarzda boshqariladi.

Ikkinchi qatlam - *Runtime Application Self-Protection (RASP)*. RASP ilova ishlash vaqtida hujumlarni aniqlaydi va bloklaydi. Digital.ai kompaniyasining yondashuviga ko‘ra, RASP hooking, kod in’ektsiyasi va debugger kabi runtime hujumlarini real vaqtda aniqlab, ilovani o‘chirish yoki funksiyalarni cheklash kabi javob choralarini qo‘llay oladi [5]. An’anaviy WAF tashqi trafikni filtrlasa, RASP ilovaning ichidan kelayotgan tahdidlarni aniqlaydi - bu ikki yondashuv bir-birini to‘ldiradi. RASP ning afzalligi shundaki, u kontekstga asoslangan qaror qabul qiladi va noto‘g‘ri aniqlash (false positive) darajasini kamaytiradi.

Uchinchi qatlam - *xavfsiz kodlash amaliyotlari*. Dasturiy ta’minotni ishlab chiqish bosqichida xavfsizlikni ta’minlash eng samarali yondashuv hisoblanadi. Bu qatlam parametrlangan so‘rovlar (prepared statements) orqali SQL injection oldini olish, kirishni boshqarish siyosatlarini qat’iy belgilash, foydalanuvchi kiritmalarini har tomonlama validatsiya qilish va xato holatlarini xavfsiz boshqarishni o‘z ichiga oladi.

To‘rtinchi qatlam - *ma’lumotlar darajasidagi himoya*. Bu qatlam ma’lumotlar bazasida saqlanadigan sezgir ma’lumotlarni shifrlash, tranzaksiyalar yaxlitligini ta’minlash va barcha muhim operatsiyalarni audit jurnalida qayd etishni nazarda tutadi. Shifrlashda eskirgan va zaif algoritmlardan (masalan, MD5, SHA-1) foydalanishdan qochish, o‘rniga zamonaviy standartlarni (AES-256, SHA-256) qo‘llash zarur [6]. Ma’lumotlar darajasidagi himoya ayniqsa shaxsiy ma’lumotlarni qayta ishlashda muhim ahamiyatga ega, chunki bu qatlam ma’lumotlar bazasiga kirish huquqi qo‘lga kiritilgan taqdirda ham ma’lumotlarning maxfiy qolishini ta’minlaydi.

Xulosa qilib aytganda, mazkur tezisda veb-ilovalarni hujumlardan himoyalash dasturiy vositasini ishlab chiqish masalalari tahlil qilindi va quyidagi xulosalarga kelindi:

Birinchidan, veb-ilovalarga qaratilgan kiberhujumlar so'nggi yillarda keskin o'smoqda: tashkilotlarning yarmidan ko'pi veb-ilova orqali kompromatga uchrash holatini qayd etgan, tashqi muhitga ochiq ilovalarga qaratilgan hujumlar esa barcha boshlang'ich kirish yo'llarining qariyb yarmini tashkil etadi. Bu veb-ilovalar xavfsizligini texnik, tashkiliy va iqtisodiy zaruratga aylantiradi.

Ikkinchidan, hujum hodisalari tahlili SQL Injection, WebShell Upload va OS Command Injection yetakchi o'rin egallashini ko'rsatdi - dastlabki uchta hujum turi barcha hodisalarning qariyb 72 foizini tashkil etadi. Shu bois himoya vositasida birinchi navbatda aynan shu tahdidlarga qarshi mexanizmlarni joriy etish zarur.

Uchinchidan, samarali himoya ko'p qatlamli (defense in depth) arxitekturaga tayanishi asoslandi: WAF (tashqi trafikni filtrlash), RASP (runtime darajasidagi kontekstga asoslangan

himoya), xavfsiz kodlash amaliyotlari va ma'lumotlar darajasidagi himoya. WAF va RASP bir-birini to'ldiruvchi yondashuv bo'lib, ularni uyg'unlashtirish maqsadga muvofiqdir.

Foydalanilgan adabiyotlar:

1. Cybersecurity Insiders. Web Application Security Report 2025. – 2025.
2. Radware Global Threat Analysis Report 2025. Radware Ltd., 2026.
3. Cloudflare WAF Documentation. Cloudflare, Inc., 2026.
4. Digital.ai Runtime Application Self-Protection (RASP) Technical Overview. – 2025.
5. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – Boca
6. Raton: CRC Press, 1996.

TO‘LIQ BO‘LMAGAN TRAFIK BELGILARIDA SUN’IY IMMUN DETEKTORI QARORINING BARQARORLIGINI BAHOLASH

Boqiyev A.A., Haydarov E.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tarmoq telemetriyasidagi yetishmayotgan belgilar sun’iy immun detektorining moslik bahosini o‘zgartirishi mumkin. Ishda vaznlangan L_1 masofa va eksponensial moslik uchun quyi hamda yuqori chegaralar chiqarilib, qarorning barcha ruxsat etilgan to‘ldirishlarda saqlanishi tekshiriladi. Deterministik to‘rt belgili modelda bir xil 0,75 qamrovli ikki niqob turli barqarorlik holatlarini berdi. Moslik oralig‘i qaror chegarasini kesganda qo‘shimcha telemetriya so‘rash tavsiya etiladi. Natijalar analitik hisoblashga tegishli; real trafikda aniqlash sifati baholanmagan.

Kalit so‘zlar: sun’iy immun tizimi, tarmoq trafigi, antigen, detektor, yetishmayotgan belgi, moslik oralig‘i, qaror barqarorligi.

Аннотация. Отсутствующие признаки сетевой телеметрии могут изменять оценку сродства детектора искусственной иммунной системы. Для взвешенного расстояния L_1 и экспоненциального сродства выведены нижняя и верхняя границы, позволяющие проверять сохранение решения при всех допустимых заполнениях. В детерминированной модели с четырьмя признаками две маски с одинаковым покрытием 0,75 дали разные состояния устойчивости. Если интервал сродства пересекает порог, рекомендуется запросить дополнительную телеметрию. Результаты получены аналитическим расчётом; качество обнаружения на реальном трафике не оценивалось.

Ключевые слова: искусственная иммунная система, сетевой трафик, антиген, детектор, отсутствующий признак, интервал сродства, устойчивость решения.

Kirish

Sun’iy immun tizimida (AIS) trafik oqimi antigen vektori bilan ifodalanadi, detektor esa shu vektorga moslik asosida faollashadi. Normal va begona holatlarni ajratish tamoyili AISning klassik ishlarida shakllangan [1]. Amaliy kuzatuvda DNS jurnali uzilishi yoki oqimning bir yo‘nalishi ko‘rinmasligi ayrim belgilarni noma’lum qoldiradi. Bunday qiymatni nol bilan almashtirish kuzatilmagan hodisani o‘lchangan nolga tenglashtiradi.

Dissertatsiyaning antigen–detektor modeli bilan bog‘liq aniq masala - mavjud belgilar bo‘yicha qayta me’yorlangan moslikdan chiqarilgan qaror to‘liq ma’lumot kelganda o‘zgarishi mumkinligini aniqlashdir. Tadqiqot maqsadi yetishmayotgan koordinatalarni taxminiy qiymat bilan to‘ldirmasdan, moslikning mumkin bo‘lgan oralig‘i orqali qaror barqarorligini tekshirish qoidasini asoslashdan iborat.

Asosiy qism

Gower o‘xshashligida mavjud bo‘lmagan belgilarni hisobdan chiqarish qo‘llanadi [2]. Kryszkiewicz ushbu usulning cheklovlarini ko‘rsatib, o‘xshashlik uchun interval chegaralarini tadqiq qilgan [3]. Bu ishda interval tamoyili dissertatsiyaning II bobidagi vaznlangan L_1 masofa va eksponensial moslikka moslashtiriladi. Amaliy hissa - detektor koordinatalariga bog‘liq chegaralar, ularning qisqa asoslanishi va bir xil qamrovli niqoblar bo‘yicha qayta hisoblanadigan qiyosdir.

k ta belgi o‘quv ma’lumotlaridan olingan o‘zgarmas shkala bilan [0; 1] ga keltirilsin. x - antigen, d - to‘liq ma’lum detektor; $w_j \geq 0$ vaznlar yig‘indisi 1, σ > 0 esa moslik masshtabidir. To‘liq ma’lumot uchun bazaviy hisoblash quyidagicha:

$$\rho(x,d) = \sum_{j=1}^{k} w_j \left| x_j - d_j \right|, \quad A(x,d) = \exp\left(-\frac{\rho(x,d)}{\sigma}\right) \qquad (1)$$

(1) dagi ρ - vaznlangan masofa, A - moslik; ular va σ normallashtirilgan fazoda birliksiz. A xavf ehtimolligi emas. Har bir $m_j \in \{0; 1\}$ mavjudlik niqobi bo‘lib, 1 - belgi kuzatilganini bildiradi. Faqat kuzatilgan koordinatalar bo‘yicha bazaviy baho:

$$q = \sum_{j=1}^{k} w_j m_j, \quad b = \sum_{j=1}^{k} w_j m_j \left| x_j - d_j \right|$$

$$A_{\text{kuz}} = \exp\left(-\frac{b}{q\sigma}\right), \quad q > 0 \qquad (2)$$

Bu yerda q - kuzatilgan vaznlar yig‘indisi, b - ma’lum farqlarning to‘liq vaznlardagi hissasi. Noma’lum koordinatada $|x_j - d_j|$ ning eng kichik qiymati 0, eng kattasi $\max(d_j; 1 - d_j)$. Shu sababli yetishmayotgan hissani u bilan chegaralash mumkin:

$$u = \sum_{j=1}^{k} (1 - m_j) w_j \max\{d_j, 1 - d_j\}, \quad b \leq \rho(x,d) \leq b + u \qquad (3)$$

(3) ning chegaralari noma’lum koordinatalar [0; 1] da erkin tanlanganda erishiladi: minimum $x_j = d_j$ da, maksimum esa detektordan uzoqroq chetki nuqtada yuz beradi. Eksponensial funksiya masofa ortganda kamaygani uchun:

$$A_- = \exp\left(-\frac{b+u}{\sigma}\right), \quad A_+ = \exp\left(-\frac{b}{\sigma}\right), \quad A_- \leq A \leq A_+ \qquad (4)$$

A_- va A_+ - to‘liq moslikning quyi va yuqori chegaralari. θ ∈ (0; 1) oldindan belgilangan faollashish chegarasi bo‘lsin. $A_- \geq \theta$ bo‘lsa moslik borligi, $A_+ < \theta$ bo‘lsa moslik yo‘qligi barcha ruxsat etilgan to‘ldirishlarda saqlanadi. $A_- < \theta \leq A_+$ holatida qaror aniqlanmagan deb belgilanadi. Qarorni kechiktirish g‘oyasi tanib olishdagi rad etish varianti bilan bog‘liq [4]; bu yerda mezon statistik ishonch emas, (4) dagi deterministik oraliqdir.

Analitik hisoblash va natijalar

Hisoblashda x_1 - port xilma-xilligi, x_2 - muvaffaqiyatsiz ulanishlar ulushi, x_3 - normallashgan DNS intensivligi, x_4 - chiqish baytlari ulushi deb olinadi. Sun’iy parametrlar: x = (0,85; 0,75; 0,20; 0,80), d = (0,90; 0,80; 0,70; 0,90), w = (0,35; 0,25; 0,25; 0,15), σ = 0,20 va θ = 0,50. Ular optimal yoki real trafikdan baholangan qiymatlar emas. Niqoblangan koordinata algoritmdan yashiriladi; to‘liq x faqat nazorat hisobiga xizmat qiladi.

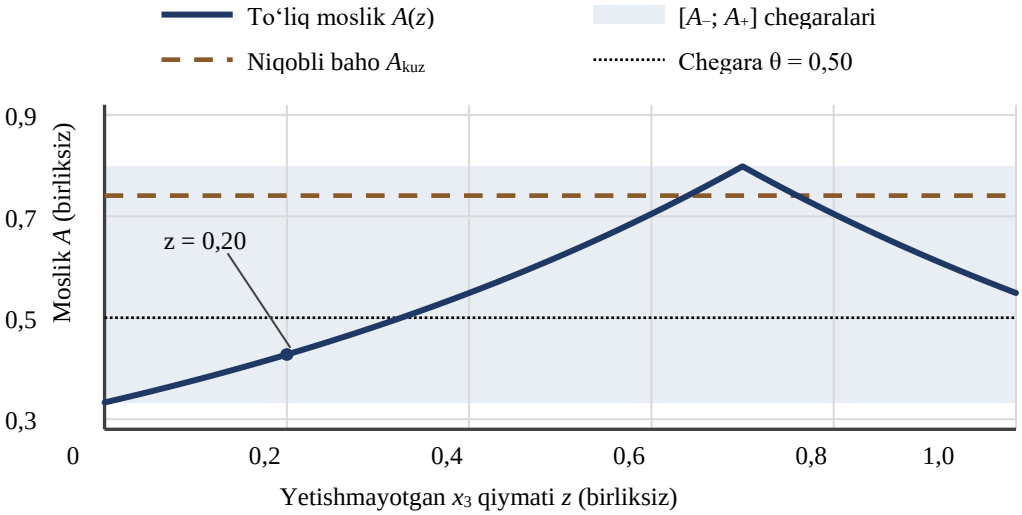
1-jadval

Bir xil vektorning turli mavjudlik niqoblaridagi hisoblangan mosligi

Kuzatuv holati	q	A_{kuz}	$[A_-; A_+]$	Interval qarori
Barcha belgilar	1,00	0,4274	[0,4274; 0,4274]	Moslik yo‘q
x_2 mavjud emas	0,75	0,3499	[0,1674; 0,4550]	Moslik yo‘q
x_3 mavjud emas	0,75	0,7408	[0,3329; 0,7985]	Aniqlanmagan
x_2 va x_3 mavjud emas	0,50	0,7225	[0,1304; 0,8500]	Aniqlanmagan

To‘liq vektorda ρ = 0,1700 va A = 0,4274. x_2 yo‘qligida q = 0,75 hamda $A_+ = 0,4550 < \theta$, demak moslik yo‘qligi barqaror. x_3 yo‘qligida aynan shu qamrovga qaramay b = 0,0450, u =

0,1750 va $[A_-; A_+]$ = [0,3329; 0,7985] olinadi. Nuqtaviy A_{kuz} = 0,7408 bahosi chegaradan yuqori, ammo nazoratdagi to‘liq baho undan past. Bu tasnif siljishi bo‘lib, zararli trafik bo‘yicha o‘lchangan yolg‘on signal emas.



1-rasm. $x_3 = z$ bo‘yicha to‘liq moslik, niqobli baho va hisoblangan chegaralar

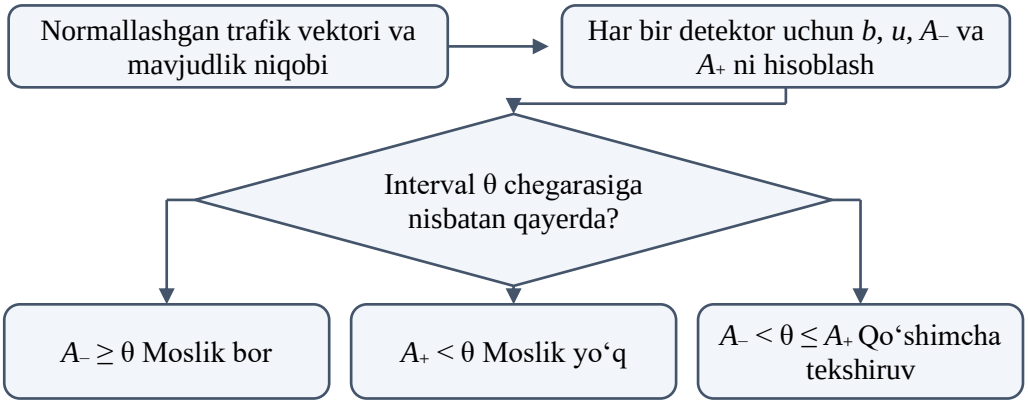
1-rasmda qolgan uch koordinata o‘zgarmas, noma’lum $x_3 = z$ esa [0; 1] da o‘zgaradi. (1) dan:

$$A(z) = \exp\left(-\frac{0{,}045 + 0{,}25|z - 0{,}70|}{0{,}20}\right) \qquad (5)$$

z = 0; 0,001; …; 1 to‘rida 1001 nuqta hisoblandi. (5) ning θ bilan kesishishi $z \approx 0{,}3255$ da yuz beradi, shuning uchun x_3 ni kuzatish qarorni aniqlashtiradi. Grafikdagi z = 0,20 nuqta jadvalning to‘liq vektor qatoriga mos.

Barcha 16 ta niqobda noma’lum har bir koordinata $\{0; d_j; x_j; 1\}$ to‘plamidan to‘ldirilib, jami 625 ta deterministik holat tekshirildi. Har birida to‘liq moslik (4) oralig‘ida qoldi va barqaror deb chiqarilgan qaror o‘zgarmadi. Bu tekshiruv sun’iy modelga tegishli.

Qaror qoidasining dasturiy qo‘llanishi



2-rasm. Moslik oralig‘i asosida qarorni tekshirishning taklif etilgan blok-sxemasi

2-rasmdagi qoida AIS Malware Shield tahlil yadrosida affinity bosqichiga qo‘shimcha tekshiruv sifatida qo‘llanishi mumkin. q = 0 bo‘lsa A_{kuz} hisoblanmaydi va telemetriya so‘raladi. Natijada niqob, q, interval, θ hamda model versiyasi birga qayd etiladi. N ta detektorli bankda har bir detektorning chegaralari hisoblanib, maksimal moslik uchun quyidagi konservativ oraliq ishlatiladi:

$$A_D = \max_{1\le \ell \le N} A_\ell, \quad \max_{1\le \ell \le N} A_{\ell,-} \le A_D \le \max_{1\le \ell \le N} A_{\ell,+} \qquad (6)$$

(6) da ℓ = 1, …, N - detektor indeksi, A_ℓ uning to‘liq mosligi; $A_{\ell,-}$ va $A_{\ell,+}$ (4) bilan olinadi. Bank uchun interval xavfsiz tashqi chegara bo‘lib, pastki chegara har doim erishiladigan minimum emas. Hisoblash O(Nk) tartibida qoladi; bu real kechikish o‘lchovi emas. “Moslik yo‘q” umumiy xavf yo‘qligini bildirmaydi. Detektor yoki immun xotirani yangilash uchun hodisaning mustaqil tasdig‘i zarur.

Xulosa

Niqobli bahoning o‘zi va qamrov q qaror barqarorligini kafolatlamasligi sonli qarshi misol bilan ko‘rsatildi. Vaznlangan masofaga bog‘liq interval esa qaysi qaror yetishmayotgan belgilar to‘ldirilganda ham saqlanishini tekshiradi. Amaliy foyda - noaniq hodisani qo‘shimcha telemetriya yoki ekspert ko‘rigiga yo‘naltirish. Hisoblar bir to‘liq ma’lum detektor va cheklangan sonli belgilar modeli uchun bajarildi. Belgilararo bog‘liqlik intervalni toraytirishi mumkin. Real trafikdagi recall, yolg‘on signal ulushi va ko‘rib chiqishga yuboriladigan hodisalar yukini o‘lchash keyingi empirik tekshiruvdir; bunday baholash IDPSni sozlash va kuzatish bilan birga olib boriladi

Foydalanilgan adabiyotlar

1. Forrest S., Perelson A. S., Allen L., Cherukuri R. Self-nonself discrimination in a computer. Proc. IEEE Symposium on Research in Security and Privacy. 1994. P. 202–212. DOI: 10.1109/RISP.1994.296580.

2. Gower J. C. A General Coefficient of Similarity and Some of Its Properties. Biometrics. 1971. Vol. 27, No. 4. P. 857–871. DOI: 10.2307/2528823.

3. Kryszkiewicz M. On Gower Similarity Coefficient and Missing Values. Proceedings of FedCSIS. ACSIS. 2023. Vol. 35. P. 1035–1040. DOI: 10.15439/2023F3575.

4. Chow C. K. On optimum recognition error and reject tradeoff. IEEE Transactions on Information Theory. 1970. Vol. 16, No. 1. P. 41–46. DOI: 10.1109/TIT.1970.1054406.

AXBOROT TIZIMLARIDA LOG-FAYLLARNI SAQLASHNING USULLARI VA ULARNING XAVFSIZLIK KAMCHILIKLARI

Xabibullayev J.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada axborot tizimlarida log-fayllarni saqlashning amalda qo‘llaniladigan beshta usuli – mahalliy saqlash, syslog orqali markazlashtirish, agentlar va log konveyerlari orqali SIEM tizimlariga yig‘ish, bulut provayderi log xizmatlari hamda arxiv va o‘zgarmas saqlash – tahlil qilingan. 2017–2026-yillarda qayd etilgan real hodisalar: hujumchilar tomonidan jurnallarni tozalash, Windows hodisalar jurnali xizmatini masofadan ishdan chiqarish, Fluent Bit log konveyeridagi zaifliklar, Microsoft bulut xizmatlarida xavfsizlik loglarining yo‘qolishi va litsenziya darajasiga bog‘liq log cheklovlari asosida har bir usulning xavfsizlik kamchiliklari ko‘rsatilgan. Hodisalar log hayotiy siklining manba, uzatish, saqlash va provayder bosqichlari bo‘yicha tasniflangan. Jurnal tozalash va to‘xtatishni aniqlash uchun amaliy nazorat ko‘rsatkichlari hamda log saqlashni mustahkamlash bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: log-fayl, hodisalar jurnali, syslog, SIEM, log konveyeri, jurnallarni tozalash, saqlash muddati, bulut loglari, yaxlitlik.

Аннотация. В статье проанализированы пять применяемых на практике способов хранения лог-файлов в информационных системах: локальное хранение, централизация через syslog, сбор в SIEM-системы с помощью агентов и конвейеров журналов, журнальные сервисы облачных провайдеров, а также архивное и неизменяемое хранение. Недостатки каждого способа показаны на основе реальных инцидентов 2017–2026 годов: очистки журналов злоумышленниками, удалённого вывода из строя службы журнала событий Windows, уязвимостей в конвейере журналов Fluent Bit, потери журналов безопасности в облачных сервисах Microsoft и ограничений журналирования, зависящих от уровня лицензии. Инциденты классифицированы по этапам жизненного цикла журнала: источник, передача, хранение и провайдер. Приведены практические индикаторы обнаружения очистки и остановки журналирования, а также рекомендации по укреплению хранения журналов.

Ключевые слова: лог-файл, журнал событий, syslog, SIEM, конвейер журналов, очистка журналов, срок хранения, облачные журналы, целостность.

Kirish

Log-fayllar, ya’ni hodisalar jurnallari, kiberinsidentni tekshirishda “nima, qachon va kim tomonidan sodir bo‘lgan” degan savollarga javob beruvchi asosiy manba hisoblanadi. Biroq so‘nggi yillardagi amaliyot loglarning mavjudligi hali ularning yaroqliligini anglatmasligini ko‘rsatmoqda.

Mandiant kompaniyasining M-Trends 2026 hisobotiga ko‘ra, 2025-yilda hujumchining tizimda aniqlanmasdan qolish vaqtining global medianasi 14 kunni tashkil etgan (2024-yilda – 11 kun). Ayrim kampaniyalarda bu ko‘rsatkich ancha yuqori: BRICKSTORM orqa eshigi bilan bog‘liq holatlarda o‘rtacha aniqlanmaslik muddati 393 kunga yetgan. Hisobotda ta’kidlanishicha, odatiy 90 kunlik log saqlash muddati bunday holatlarda dastlabki kirish vektorini aniqlashga imkon bermaydi, hujumchilar esa tizim loglarini tozalab, ma’lumotlarni o‘g‘irlash vaqt jadvalini

tiklashni deyarli imkonsiz qiladi. Natijada tashkilotlar eng yomon stsenariyni taxmin qilib, uni oshkor etishga majbur bo‘ladi.

Shu sababli loglarni boshqarish xalqaro tavsiyalar va me’yoriy hujjatlarda alohida o‘rin egallamoqda. 2024-yilda Avstraliya, AQSh va boshqa davlatlarning kiberxavfsizlik agentliklari birgalikda chiqargan qo‘llanmada samarali log boshqaruvining to‘rtta asosiy omilidan biri sifatida log yaxlitligini xavfsiz saqlash orqali ta’minlash belgilangan. AQSh Boshqaruv va byudjet idorasining 2026-yil 22-mayda imzolangan M-26-14 memorandumi federal idoralar uchun loglarni olti oy davomida faol qidiriladigan, o‘n ikki oy davomida esa tiklanadigan holatda saqlashni talab qiladi. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni muhim axborot infratuzilmasi obyektlarini himoya qilish talablarini belgilagan va bu talablarning bajarilishini ishonchli audit izisiz tekshirib bo‘lmaydi.

Ushbu maqolaning maqsadi – log-fayllarni saqlashning amalda qo‘llaniladigan usullarini tahlil qilish, ularning xavfsizlik kamchiliklarini real hodisalar asosida ko‘rsatish va kamchiliklarni aniqlash hamda kamaytirish bo‘yicha amaliy tavsiyalar ishlab chiqish.

Asosiy qism

Log-fayllarni saqlash usullari

Amaliyotda log-fayllar beshta asosiy usulda saqlanadi. Ko‘pchilik tashkilotlarda ular bir vaqtda, qatlamli tarzda qo‘llaniladi.

Mahalliy saqlash. Hodisa manbai yozuvni o‘zi joylashgan tizimga yozadi. Windows tizimlarida hodisalar jurnallari C:\Windows\System32\winevt\Logs katalogidagi .evtx fayllarida, Linux tizimlarida esa /var/log katalogida, systemd-journald xizmati jurnalida va auditd audit tizimi fayllarida saqlanadi. Jurnal hajmi cheklangan bo‘lib, to‘lganda eski yozuvlar ustidan yoziladi yoki rotatsiya qilinadi.

Syslog orqali markazlashtirish. Yozuvlar RFC 5424 standartidagi syslog formatida rsyslog yoki syslog-ng kabi dasturlar yordamida markaziy serverga uzatiladi. Uzatish UDP (514-port), TCP yoki TLS (6514-port, RFC 5425) orqali amalga oshiriladi. Amaliyotda soddaligi sababli hanuz UDP keng qo‘llaniladi.

Agentlar va log konveyerlari orqali SIEM tizimiga yig‘ish. Manbalardagi agentlar (Fluent Bit, Fluentd, Logstash, Windows Event Forwarding) loglarni yig‘adi, normallashtiradi va xavfsizlik hodisalarini boshqarish tizimiga (Splunk, Elastic, Wazuh, Microsoft Sentinel) uzatadi. Bu usul korrelyatsiya va real vaqtda aniqlash imkonini beradi, ammo yo‘lda qo‘shimcha dasturiy komponentlar paydo bo‘ladi.

Bulut provayderi log xizmatlari. Bulut xizmatlarida (Microsoft Purview Audit, Microsoft Entra, AWS CloudTrail, Azure Monitor) loglar provayder tomonidan yaratiladi va saqlanadi. Qaysi hodisalar qayd etilishi va ular qancha muddat saqlanishi ko‘pincha xizmat tarifiga bog‘liq bo‘ladi.

Arxiv va o‘zgarmas saqlash. Uzoq muddatli saqlash uchun loglar “sovuq” xotiraga, lentaga yoki qayta yozib bo‘lmaydigan (WORM – write once, read many) obyekt xotirasiga ko‘chiriladi. Bu usul o‘chirishdan himoya qiladi, biroq tezkor qidiruv va tahlilni qiyinlashtiradi.

1-jadval

Log-fayllarni saqlash usullari

Usul	Odatiy vositalar	Loglarni kim nazorat qiladi	Asosiy xavf
Mahalliy saqlash	Windows Event Log, journald, auditd, /var/log	Tizim ma’muri	Hujumchi tizim bilan birga loglarni ham egallaydi

Syslog markazlashtirish	rsyslog, syslog-ng	Log serveri ma’muri	UDP orqali himoyasiz uzatish
Agent va SIEM	Fluent Bit, Logstash, Splunk, Elastic, Wazuh	SIEM ma’muri	Konveyer zaifliklari, yagona ishonch nuqtasi
Bulut log xizmatlari	Purview Audit, Entra, CloudTrail	Bulut provayderi	Provayder nosozligi, tarifga bog‘liq cheklovlar
Arxiv va WORM	Obyekt xotirasi, lenta	Saqlash ma’muri	Sekin qidiruv, mustaqil tekshiruv yo‘qligi

Real hodisalar asosida kamchiliklar tahlili

Jurnallarni hujumchi tomonidan tozalash. Bu eng keng tarqalgan va eng ko‘p hujjatlashtirilgan kamchilik. 2026-yilda yangilangan MITRE ATT&CK bazasida “Defense Evasion” taktikasi ikkiga ajratilib, himoya vositalarini ishdan chiqarishga oid texnikalar yangi “Defense Impairment” (TA0112) taktikasiga o‘tkazildi; Windows hodisalar jurnallarini tozalash endi T1685.005 texnikasi sifatida qayd etiladi. Ushbu texnika bo‘yicha bazada APT28, APT38, APT41, Dragonfly, Volt Typhoon guruhlari, NotPetya, KillDisk, HermeticWiper zararli dasturlari hamda BlackCat, LockBit, Qilin, RansomHub to‘lov talab qiluvchi dasturlari qayd etilgan. Masalan, APT28 guruhi “wevtutil cl System” va “wevtutil cl Security” buyruqlari bilan jurnallarni tozalagan.

Eng xarakterli misollardan biri – Volt Typhoon guruhi. AQSh kiberxavfsizlik agentligi CISA va hamkorlarining 2024-yil fevraldagi AA24-038A ogohlantirishiga ko‘ra, guruh ayrim tashkilotlar tarmoqlarida kamida besh yil davomida yashirin kirish imkoniyatini saqlagan va Windows hodisalar jurnallarini tanlab tozalagan. Ogohlantirishda Event ID 1102 yozuvlarini – xavfsizlik jurnali tozalanganligi haqidagi hodisani – alohida tekshirish tavsiya etilgan. Bu misol mahalliy saqlashning asosiy kamchiligini ko‘rsatadi: tizimni egallagan hujumchi uning tarixini ham boshqaradi.

Jurnal yozish xizmatini ishdan chiqarish. Hujumchi jurnallarni o‘chirish o‘rniga ularni yozishni to‘xtatishi mumkin (T1685.001). 2024-yil yanvarida e’lon qilingan EventLogCrasher zaifligi bu xavfning amaliy darajasini ko‘rsatdi. Zaiflik Windows hodisalar jurnali xizmatini ishdan chiqarishga imkon beradi: mahalliy darajada oddiy foydalanuvchi huquqlari bilan, masofadan esa SMB orqali autentifikatsiyadan o‘tgan holda. Xizmat ikki marta qayta ishga tushadi, uchinchi nosozlikdan keyin esa to‘xtab qoladi. Bu vaqtda Windows loglarini qabul qiluvchi aniqlash tizimlari “ko‘r” bo‘lib qoladi, Application jurnali hodisalari esa umuman navbatga olinmaydi. Ma’lumot e’lon qilingan paytda Microsoft zaiflikni tuzatmagan, uchinchi tomon kompaniyasi esa vaqtinchalik mikropatch chiqargan.

Log infratuzilmasining o‘zidagi zaifliklar. Loglarni yig‘uvchi va uzatuvchi dasturiy ta’minot ham hujum obyekti bo‘lishi mumkin. 2021-yil dekabrida aniqlangan Log4Shell zaifligi (CVE-2021-44228) aynan loglash kutubxonasi orqali masofadan kod bajarishga imkon bergan edi. 2025-yil noyabrida Oligo Security kompaniyasi Fluent Bit log konveyerida beshta zaiflikni e’lon qildi. Ular orasida log teglarini soxtalashtirish (CVE-2025-12978), tekshirilmagan teglar orqali yozuvlarni soxtalashtirish (CVE-2025-12977), yo‘l bo‘ylab o‘tish orqali ixtiyoriy faylni qayta yozish (CVE-2025-12972) va autentifikatsiyani chetlab o‘tib soxta telemetriya yuborish (CVE-2025-12969) bor. Tadqiqotchilar ma’lumotiga ko‘ra, Fluent Bit 15 milliarddan ortiq marta o‘rnatilgan va yirik bulut provayderlari tomonidan ishlatiladi, zaifliklarning ayrimlari esa sakkiz yildan ortiq vaqt mavjud bo‘lgan. Bu holat SIEM tizimiga yetib kelgan yozuvlarning o‘zi ham soxtalashtirilgan bo‘lishi mumkinligini ko‘rsatadi.

Provayder tomonidagi loglarning yo‘qolishi. 2024-yil 2-sentabrda Microsoft kompaniyasining ichki monitoring agentidagi xato sababli bir qator bulut xizmatlarida xavfsizlik loglari to‘liq yig‘ilmay qoldi. Muammo 5-sentabrda aniqlangan va qariyb ikki hafta davomida to‘liq bartaraf etilmagan. Ta’sir doirasiga Microsoft Entra kirish va faoliyat loglari, Microsoft Sentinel xavfsizlik ogohlantirishlari, Azure Monitor va boshqa xizmatlar kirgan. Kompaniya hodisa xavfsizlik buzilishi bilan bog‘liq emasligini ma’lum qilgan, biroq yo‘qolgan ma’lumotlarning bir qismini tiklab bo‘lmasligini tan olgan. Ya’ni bulut log xizmatlarida mijoz o‘z loglarining to‘liqligini nazorat qila olmaydi.

Litsenziya darajasiga bog‘liq log cheklovlari. 2023-yilda Storm-0558 guruhi Microsoft Exchange Online orqali 22 ta tashkilot, jumladan AQSh davlat idoralarining elektron pochtasiga kirgan. AQSh Kiberxavfsizlik bo‘yicha tekshiruv kengashining (CSRB) 2024-yil martdagi hisobotida Microsoft hujumni o‘zi emas, mijozi – AQSh Davlat departamenti xabar bergandan keyin aniqlagani qayd etilgan. CISA ma’lumotiga ko‘ra, federal idora shubhali faollikni faqat eng yuqori tarifdagi kengaytirilgan audit loglari mavjud bo‘lgani uchun aniqlay olgan. Shundan so‘ng Microsoft Purview Audit (Standard) xizmatida loglarni saqlash muddatini 90 kundan 180 kungacha uzaytirdi va avval faqat Premium tarifda mavjud bo‘lgan elektron pochtaga kirish loglarini kengroq doiradagi mijozlarga ochdi. Bu holat xavfsizlik uchun muhim loglarning mavjudligi tijoriy tarifga bog‘liq bo‘lishi mumkinligini ko‘rsatadi.

Himoyasiz uzatish va mustaqil tekshiruvning yo‘qligi. RFC 5426 standarti UDP orqali syslog uzatish xabarlarning autentifikatsiyasi, butunligi va maxfiyligini ta’minlamasligini, yetkazib berish kafolatlanmasligini qayd etadi. Yuqoridagi barcha holatlarda yana bir umumiy kamchilik namoyon bo‘ladi: tashkilot auditor yoki sud ekspertizasiga loglarning yaratilgandan keyin o‘zgartirilmaganini mustaqil isbotlay olmaydi. B. Schneier va J. Kelsey ishonchsiz kompyuterda saqlanadigan jurnallar uchun kriptografik himoya zarurligini aynan shu sababli asoslagan.

Jurnal tozalash va to‘xtatishni aniqlashning amaliy ko‘rsatkichlari

Windows tizimlarida jurnal tozalash va to‘xtatish bo‘yicha aniq hodisa identifikatorlari mavjud (2-jadval). Ularni SIEM tizimida doimiy kuzatish eng arzon va samarali choralardan biri hisoblanadi.

2-jadval

Jurnal yaxlitligiga oid Windows hodisalari

Event ID	Jurnal	Hodisa mazmuni	Amaliy ahamiyati
1102	Security	Audit jurnali tozalandi	T1685.005 ning bevosita belgisi
104	System	Jurnal fayli tozalandi	System va boshqa jurnallar tozalanganini ko‘rsatadi
1100	Security	Hodisalarni qayd etish xizmati to‘xtatildi	T1685.001 yoki xizmat nosozligi belgisi
4719	Security	Tizim audit siyosati o‘zgartirildi	Qayd etiladigan hodisalar kamaytirilgan bo‘lishi mumkin
4616	Security	Tizim vaqti o‘zgartirildi	Vaqt tamg‘alari ishonchliligiga ta’sir qiladi

Bu ko‘rsatkichlarning muhim cheklovi bor: 1102 va 104 hodisalari aynan tozalangan jurnalning o‘ziga yoziladi. Agar loglar zudlik bilan tashqi tizimga uzatilmasa, hujumchi bu yozuvlarni ham yo‘q qilishi mumkin. Shuningdek, hodisa yozilmasligi – masalan, xizmat to‘xtatilganda yoki EventLogCrasher holatida – hech qanday yozuv qoldirmaydi. Shu sababli

manbadan kelayotgan log oqimining to‘satdan to‘xtashini kuzatish, M-Trends 2026 hisobotida ham tavsiya etilganidek, alohida ogohlantirish qoidasi sifatida sozlanishi kerak.

Tadqiqot natijalari

Ko‘rib chiqilgan hodisalar log hayotiy siklining qaysi bosqichida nosozlik yuz bergani bo‘yicha tasniflandi (3-jadval).

3-jadval

Real hodisalarning log hayotiy sikli bosqichlari bo‘yicha tasnifi

Hodisa	Yil	Bosqich	Kamchilik	Oqibat
NotPetya, APT28, ransomware	2017–	Saqlash	Mahalliy jurnalni tozalash	Hujum izlari yo‘qoladi
Log4Shell	2021	Manba	Loglash kutubxonasidagi zaiflik	Masofadan kod bajarish
Storm-0558	2023	Provayder	Tarifga bog‘liq log cheklovi	Hujumni aniqlash imkoniyati cheklanadi
EventLogCrasher	2024	Manba	Jurnal xizmatini ishdan chiqarish	Aniqlash tizimlari “ko‘r” bo‘ladi
Volt Typhoon	2024	Saqlash	Jurnallarni tanlab tozalash	Kamida 5 yil yashirin kirish
Microsoft loglari yo‘qolishi	2024	Provayder	Monitoring agentidagi xato	Loglarning bir qismi qaytarib bo‘lmas yo‘qolgan
Fluent Bit zaifliklari	2025	Uzatish	Teg va fayllarni soxtalashtirish	SIEM ga soxta yozuvlar yetib boradi
BRICKSTORM	2025	Saqlash	90 kunlik saqlash muddati	Dastlabki kirish vektorini aniqlab bo‘lmaydi

Tahlildan uchta amaliy xulosa kelib chiqadi.

Birinchidan, kamchiliklar log hayotiy siklining barcha bosqichida – manbada, uzatishda, saqlashda va provayder darajasida – namoyon bo‘lgan. Demak, loglarni markazlashtirish yoki bulutga ko‘chirish muammoni bartaraf etmaydi, faqat uning joyini o‘zgartiradi.

Ikkinchidan, hodisalarning ko‘pchiligida loglar ular qayd etayotgan tizim yoki o‘sha tizimni boshqaruvchi tomon nazoratida bo‘lgan. Mahalliy jurnalni hujumchi tozalaydi, SIEM ga kelayotgan oqimni konveyer zaifligi orqali soxtalashtiradi, bulut loglari esa provayder nosozligi yoki tarif cheklovi tufayli yo‘qoladi. Har bir holatda tashqi, mustaqil tekshiruv nuqtasi mavjud bo‘lmagan.

Uchinchidan, saqlash muddati amaliy jihatdan muhim parametr hisoblanadi. 90 kunlik muddat medianasi 14 kun bo‘lgan hujumlar uchun yetarli ko‘rinsa-da, aniqlanmaslik muddati 393 kunga yetgan kampaniyalarda dastlabki dalillar tekshiruv boshlanguncha yo‘qoladi.

Ushbu natijalar asosida log saqlashni mustahkamlash bo‘yicha quyidagi amaliy tavsiyalar ishlab chiqildi:

1. Loglarni manbadan zudlik bilan alohida ma’muriyatga ega markaziy tizimga uzatish va syslog uchun UDP o‘rniga TLS (6514-port) dan foydalanish.

2. Saqlash muddatini kamida 12 oy qilib belgilash: M-26-14 memorandumi 6 oy faol va 12 oy tiklanadigan saqlashni talab qiladi, M-Trends 2026 hisoboti esa tarmoq qurilmalarining ma’muriy loglarini kamida bir yil saqlashni tavsiya etadi.

3. 1102, 104, 1100, 4719 va 4616 hodisalari hamda manbadan log oqimining to‘xtashi uchun alohida ogohlantirish qoidalarini sozlash.

4. Log konveyeri komponentlarini muntazam yangilash, masalan, Fluent Bit ni zaifliklar tuzatilgan 4.1.1 yoki 4.0.12 versiyasigacha yangilash va in_forward kirishida umumiy kalit bilan autentifikatsiyani yoqish.

5. Bulut xizmatlarida qaysi xavfsizlik loglari joriy tarifga kirishini va ular qancha saqlanishini oldindan tekshirish, zarur bo‘lsa ularni o‘z saqlash tizimiga eksport qilish.

6. Loglarni qayta yozib bo‘lmaydigan xotirada saqlash va ularning yaxlitligini mustaqil tekshirish uchun kriptografik mexanizmlar – xesh zanjiri va tashqi guvohga qayd etiladigan nazorat qiymatlaridan foydalanish.

Xulosa

Log-fayllarni saqlashning amalda qo‘llaniladigan beshta usuli – mahalliy saqlash, syslog orqali markazlashtirish, agent va SIEM tizimlari, bulut log xizmatlari hamda arxiv va o‘zgarmas saqlash – tahlil qilinib, ularning har biri uchun asosiy xavf aniqlandi. 2017–2026-yillardagi real hodisalar kamchiliklarning log hayotiy siklining barcha bosqichlarida namoyon bo‘lishini ko‘rsatdi: jurnallarni tozalash va xizmatni ishdan chiqarish manba va saqlash bosqichida, konveyer zaifliklari uzatish bosqichida, loglar yo‘qolishi va tarif cheklovlari esa provayder bosqichida yuz bergan. Hodisalarning umumiy sababi – loglarning ular qayd etayotgan tizim yoki uni boshqaruvchi tomon nazoratida bo‘lishi va yaxlitlikni mustaqil tekshirish mexanizmining yo‘qligi. Jurnal tozalash va to‘xtatishni aniqlash uchun Windows hodisa identifikatorlariga asoslangan amaliy ko‘rsatkichlar va log saqlashni mustahkamlash bo‘yicha oltita tavsiya ishlab chiqildi. Keyingi tadqiqotlarda loglar yaxlitligini log egasi(owner)ga ishonmasdan tekshirish imkonini beruvchi kriptografik va taqsimlangan yondashuvlar, jumladan blokcheyn texnologiyasi asosidagi usullar tahlil qilinadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764-son, 15.04.2022.

2. Xabibullayev J.D., Ddos-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili, “Лучшие интеллектуальне исследования” международный научный электронный журнал, ЧАСТЬ-39 ТОМ-3, Февраль 2025, ISSN: 3030-3680.

3. Xabibullayev J.D., Chunayev N.E. Analysis of the capabilities of blockchain technology in data management, “Modern education and development” international interdisciplinary reasearch journal, Volume 2, Issue 27, June 2025. –P. 355-364

4. Mandiant, “M-Trends 2026”, Google Cloud, 2026.

5. Australian Signals Directorate’s Australian Cyber Security Centre et al., “Best practices for event logging and threat detection”.

6. Office of Management and Budget, Memorandum M-26-14, Executive Office of the President, Washington, DC, USA, May 2026.

7. MITRE Corporation, “Disable or Modify Tools: Clear Windows Event Logs (T1685.005)”, MITRE ATT&CK, v20, 2026.

8. CISA, NSA, FBI et al., “PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure”, Cybersecurity Advisory AA24-038A, Feb. 2024.

9. Help Net Security, “A zero-day vulnerability (and PoC) to blind defenses relying on Windows event logs”, Jan. 2024.

10. Oligo Security, “Critical vulnerabilities in Fluent Bit expose cloud environments to remote takeover”, Nov. 2025.

11. Help Net Security, “Microsoft lost some customers’ cloud security logs”, Oct. 2024.

ZARARLI APK FAYLLARNI ANIQLASH MUAMMOLARI VA MODELI

Nasrullayev N.B., Xamidov Sh.J.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Mirzayeva A.B.
EMU universiteti

Annotatsiya. Maqolada O‘zbekistonda bank-moliya xizmatlariga qaratilgan zararli APK fayllarni aniqlash muammolari tadqiq etilgan. IIV, Markaziy bank, CERT-CBU va Group-IB ma’lumotlari asosida tahdidning miqdoriy ko‘rsatkichlari hisoblangan, APK hujumining besh bosqichli zanjiri tuzilgan, statik, dinamik va mashinaviy o‘qitish usullari vaqt barqarorligi va soxta signal bo‘yicha qiyoslangan. Ko‘p bosqichli aniqlash konveyeri va uning samaradorlik ko‘rsatkichlari taklif etilgan.

Kalit so‘zlar: zararli APK, Android, SMS-stealer, dropper, statik va dinamik tahlil, mashinaviy o‘qitish, mobil banking.

Аннотация. В статье рассматриваются проблемы обнаружения вредоносных APK-файлов, направленных на банковские услуги Узбекистана. По данным МВД, Центрального банка, CERT-CBU и Group-IB рассчитаны количественные показатели угрозы, построена цепочка атаки, сопоставлены статические, динамические и ML-методы обнаружения, предложены многоэтапный конвейер и показатели его эффективности.

Ключевые слова: вредоносный APK, Android, SMS-стилер, дроппер, мобильный банкинг, машинное обучение.

Kirish

O‘zbekistonda kiberjinoyatlarning qariyb yarmi zararli APK fayllar orqali sodir etiladi: 2026-yil yanvar–sentabrda 69 962 ta jinoyat qayd etilgan, 1 trln so‘mdan ortiq zarar yetkazilgan, faqat 210 mlrd so‘m qaytarilgan. Bank kartalari soni 2023-2026-yillarda 34,2 mln dan 68,27 mln ga yetdi, to‘lov va o‘tkazmalarni amalga oshirishda SMS-kod ko‘p hollarda yagona tasdiqlash usuli bo‘lib qolmoqda. Group-IB ma’lumotlariga ko‘ra, Qwizzserial zararli dasturi taxminan 100 000 qurilmani zararlagan, 2025-yil oxirida esa shifrlovchi “dropper” ilovalar orqali Wonderland SMS-stealer keng tarqalgan. Ilmiy adabiyotda F-o‘lchov 0,99 ga yaqin uchraydi, biroq vaqt va sinf nisbati bo‘yicha xatolar bartaraf etilgach, natijalar sezilarli pasayadi.

Adabiyotlar tahlili va tadqiqot metodologiyasi

Drebin manifest va kod belgilari bilan zararli dasturlarning taxminan 94 foizini aniqlagan. MaMaDroid API ketma-ketligida F-o‘lchovni 0,99 gacha yetkazgan, ammo bir yildan keyin 0,86, ikki yildan keyin 0,75 ga tushgan. TESSERACT ishida xatolar bartaraf etilgach, samaradorlik 50 foizgacha pasaygan; vaqt barqarorligi AUT(F1, 24 oy) bo‘yicha Drebin uchun 0,58, MaMaDroid uchun 0,32, chuqur o‘qitish uchun 0,64 bo‘lgan. Guardsquare 15 ta bank ilovalarida Accessibility, overlay va SMS orqali kod o‘g‘irlash holatlarini, asosiy kanal sifatida Google Play dagi “dropper” ilovalarni qayd etgan. Moliya sohasida zararli dastur eng xavfli tahdid sifatida baholangan va ulardan himoyalanish uchun ikki darajali (avtomatik va tahlilchi) himoya tavsiya etilgan. Tabiiy tarqalish 1:44 bo‘lganda LLM larning aniqligi 2,3-3,8 foizdan oshmagan. O‘zbekiston bo‘yicha aniqlash sifatining miqdoriy baholari ochiq e’lon qilinmagan.

Tadqiqot statistik ma’lumotlarga (IIV, CERT-CBU, Markaziy bank, Group-IB, ilmiy ishlar) asoslangan. Qo‘llanilgan ko‘rsatkichlar:

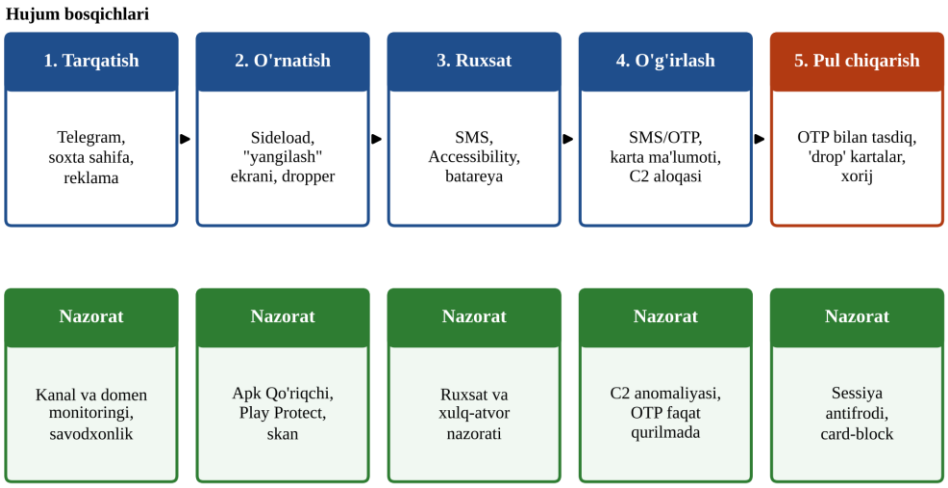
$$\bar{L} = L / N;\ \ R = Q / L;\ \ D = 1 - \prod(1 - d_i);\ \ \mathrm{PPV} = \mathrm{TPR}\cdot\pi / (\mathrm{TPR}\cdot\pi + \mathrm{FPR}\cdot(1 - \pi)) \qquad (1)$$

bu yerda L va N jami zarar va jinoyatlar soni, Q qaytarilgan summa, d_i i-bosqichning aniqlash ehtimoli (bosqichlar mustaqil deb faraz qilinadi), π zararli ilovalarning tabiiy ulushi.

Zararli APK tahdidining arxitekturasi

Hujum besh bosqichda amalga oshadi (1-rasm): tarqatish, o‘rnatish, ruxsat olish, ma’lumot o‘g‘irlash va pulni yechish. Jabrlanuvchi soxta sahifa, reklama yoki egallangan Telegram akkauntidan kelgan faylni “yangilanish” bahonasida o‘rnatadi. Ilova SMS, Accessibility va batareya optimizatsiyasi ruxsatlarini oladi, OTP va karta ma’lumotlarini C2 serveriga uzatadi; har bir nusxa o‘z C2 domeniga ega, dropper esa shifrlangan yuklamani o‘rnatilgandan keyin ishga tushiradi.

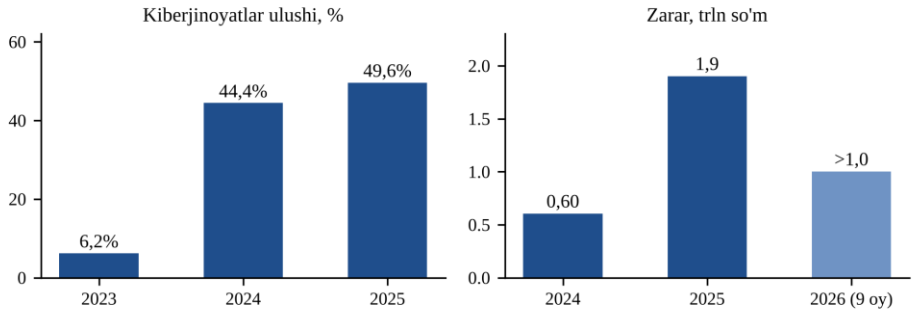
Texnik belgilar quyidagicha: SMS o‘qish va yuborish (READ/RECEIVE_SMS ruxsatli yangi o‘rnatilgan ilova) OTP ni o‘g‘irlash uchun; Accessibility xizmati ekranni kuzatish va ruxsatlarni o‘zi berish uchun (bank ilovasi ochilganda noma’lum xizmat faolligi); overlay va WebView soxta kirish oynasi uchun (bank ilovasi ustida chizilgan oyna); dropper shifrlangan yuklama uchun (ish vaqtida qo‘shimcha APK/DEX yuklanishi); C2 aloqasi (noma’lum domenga POST, har nusxada alohida domen). Ehtimollik va ta’sir bo‘yicha (1–3 shkala, muallif bahosi) eng yuqori xavf (3 × 3) SMS-stealer va dropperga tegishli. “Davlat yordami” niqobidagi soxta APK (3 × 2) va Accessibility/overlay trojanlari (2 × 3) keyingi o‘rinlarda. Dastlabki uch bosqichda to‘xtatilgan hujum zarar keltirmaydi; OTP hujumchiga o‘tgach, qaytarish ehtimoli keskin kamayadi.



1-rasm. APK orqali firibgarlik zanjiri va nazorat nuqtalari (muallif ishlanmasi; Group-IB, Guardsquare ma’lumotlari asosida)

Statistik tahlil

Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizga, 2025-yilda 49,6 foizga oshgan (2-rasm); zarar 2024-yildagi 603 mlrd so‘mdan 2025-yilda 1,9 trln so‘mga o‘sgan. CERT-CBU 2024-yilda 43 zararli ilovani aniqlagan: 11 tasi bank va to‘lov tashkilotlari, 2 tasi Markaziy bank, 8 tasi sud va ijro organlari nomida tarqatilgan.



2-rasm. Kiberjinoyatlar ulushi va zarar

1-jadval

Hisoblangan ko‘rsatkichlar

Ko‘rsatkich	Hisob	Qiymat
APK orqali jinoyatlar (taxminiy)	0,5 × 69 962	≈ 35 ming
Bitta jinoyatga o‘rtacha zarar	1 trln / 69 962	≥ 14,3 mln so‘m
Qaytarish darajasi	210 mlrd / 1 trln	≤ 21%
Qaytarilmagan zarar	1 trln − 210 mlrd	≥ 790 mlrd so‘m
Brend niqobidagi ilovalar ulushi	(11 + 2 + 8) / 43	48,8%
Zarar o‘sishi, 2025/2024	1,9 trln / 603 mlrd	3,15 baravar

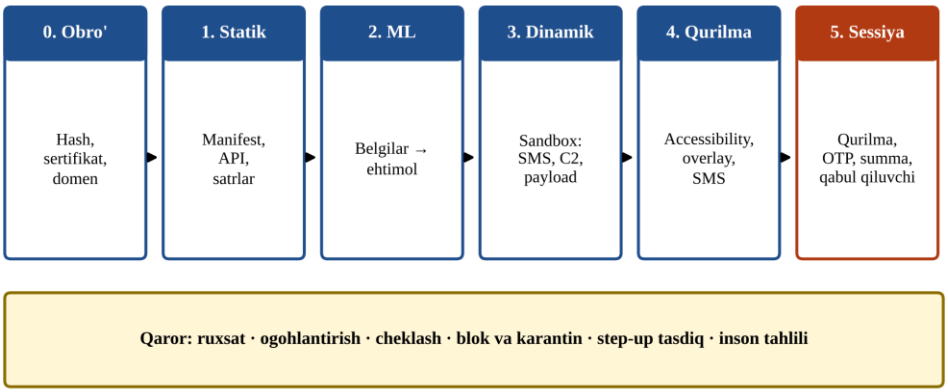
Natijalar talqini.

Zararning kamida to‘rtdan uch qismi qaytarilmaydi, shu sababli hujumni aniqlash va to‘xtatish keyingi bosqichlardagi tiklashdan samaraliroq. Soxta ilovalarning deyarli yarmi bank va davlat brendlari niqobida tarqaladi, demak, brend va domen monitoringi aniqlashning ajralmas qismi bo‘lishi kerak.

Mavjud yechimlar va aniqlash usullari

Usullarning kuchli va zaif tomonlari quyidagicha. Hash va obro‘ tekshiruvi tez va kam soxta signal beradi, ammo har bir nusxa uchun yangi C2 va hash paydo bo‘lgani sababli tez eskiradi. Statik belgilar bilan ML ilovani ishga tushirmasdan ishlaydi, biroq shifrlash va dropperga zaif (AUT 0,58). API ketma-ketligi obfuskatsiyaga chidamli, lekin ikki yilda F 0,99 dan 0,75 ga tushadi. Chuqur o‘qitish vaqt bo‘yicha barqarorroq (AUT 0,64), ammo ma’lumot va hisoblash talab qiladi. Dinamik tahlil yashirin yuklama va C2 ni ochadi, lekin sandbox dan qochish mumkin va sekin. Sessiya antifrodi APK turidan qat’i nazar ishlaydi, biroq hujum oxirida va soxta signal xarajati bilan.

Ikki holat muhim. Birinchidan, vaqt siljishi: modelni vaqt bo‘yicha (o‘tmishda o‘qitib, kelajakda sinash) baholash shart. Ikkinchidan, tabiiy tarqalish: TPR = 95%, FPR = 1% va $\pi = 0{,}1\%$ bo‘lganda PPV ≈ 8,7%, FPR = 0,1% bo‘lganda ≈ 48,7% (shartli hisob). Shu sabab bir necha bosqichli konveyer taklif etiladi (3-rasm): obro‘ va hash, statik tahlil + ML, dinamik tahlil, qurilmadagi xulq-atvor nazorati. Bosqichlar mustaqil bo‘lsa va shartli d = 0,40; 0,70; 0,50; 0,60 bo‘lsa, (1) bo‘yicha $D = 1 - 0{,}60 \cdot 0{,}30 \cdot 0{,}50 \cdot 0{,}40 = 96{,}4\%$; amalda bosqichlar bog‘liq (shifrlangan dropper obro‘ va statik tahlildan birga o‘tishi mumkin), shuning uchun real D past bo‘ladi.



3-rasm. Ko‘p bosqichli zararli APK aniqlash konveyeri

Mavjud choralar: bank ilovalaridagi antivirus 2026-yil birinchi yarmida qariyb 1,3 mln APK ni cheklagan, Apk Qo‘riqchi 3 mln foydalanuvchiga ulangan, 22-aprel talablari masofaviy boshqaruv aniqlanganda operatsiyani cheklashni nazarda tutadi. Platforma darajasida Android 16 noma’lum qo‘ng‘iroq paytida sideloading va Accessibility ruxsatini bloklaydi, dasturchi tekshiruvi 2026-yil 30-sentabrdan to‘rt mamlakatda boshlangan, 2027-yilda kengayishi rejalashtirilgan. Biroq mahalliy tizimlar faol foydalanuvchilar va bloklangan operatsiyalar bilan o‘lchanadi, TPR, FPR va vaqt barqarorligi e’lon qilinmaydi; antifrod natijalari ham notekis: oldi olingan 461,9 mlrd so‘mning 78 foizi ikki bank hissasiga to‘g‘ri keladi.

Takliflar va himoya modeli

NIST CSF 2.0 asosida to‘rt ustunli model taklif etiladi: oldini olish (kanal va domen monitoringi, savodxonlik), aniqlash (ko‘p bosqichli konveyer), himoya va javob (qurilmadagi xulq-atvor nazorati, OTP ni qurilmaga bog‘lash, kartani bloklash) hamda boshqaruv (vaqt bo‘yicha baholash). Asosi CERT-CBU, banklar, operatorlar va IIV o‘rtasida hash, sertifikat va C2-domen signallarini real vaqtda almashishdir.

2-jadval

Samaradorlik ko‘rsatkichlari (KPI), muallif taklifi

Yo‘nalish	KPI (mo‘ljal)	Muddat
Aniqlash konveyeri	Mustaqil o‘lchangan D ≥ 90%; FPR ≤ 0,1%	2027–2028
Vaqt bo‘yicha baholash	AUT(F1, 12 oy) ≥ 0,80; PPV hisoboti e’lon qilingan	har chorak
Qurilmadagi nazorat	Masofaviy boshqaruv aniqlangan seanslarda cheklash: 100%	2027
Signal almashinuvi	Karta/domen blok vaqti 24 soatdan 1 soatgacha	2027
Integral maqsad	APK orqali jinoyatlar ulushi 50% → 25%; qaytarish ≥ 50%	2030

KPI qiymatlari mo‘ljal sifatida taklif etilgan va har yili qayta ko‘rib chiqilishi lozim.

Amalga oshirish ketma-ketligi quyidagicha. Birinchi bosqichda (2027) banklar, mobil operatorlar va CERT-CBU o‘rtasida yagona signal almashinuvi tarmog‘i yaratiladi va tarqatish kanallari (soxta sahifalar, reklama, Telegram akkauntlari) monitoringi yo‘lga qo‘yiladi. Ikkinchi bosqichda aniqlash konveyeri milliy namunalar to‘plamida sinovdan o‘tkaziladi: har chorakda yangi nusxalar bilan vaqt bo‘yicha baholash (o‘tmishda o‘qitish, kelajakda sinash) o‘tkaziladi, PPV va soxta signal darajasi e’lon qilinadi. Uchinchi bosqichda qurilmadagi nazorat bank ilovalariga joriy etiladi: Accessibility xizmati yoki overlay aniqlanganda yuqori summali operatsiya cheklanadi, OTP faqat so‘rov yuborilgan qurilmada amal qiladi. Bu choralar foydalanuvchi qulayligini kamaytirmasligi uchun xavf darajasiga qarab tanlab qo‘llanishi kerak.

Xulosa

Zararli APK O‘zbekiston bank-moliya tizimidagi asosiy hujum vektoriga aylangan: 2026-yilning to‘qqiz oyida taxminan 35 ming holat, bitta jinoyatga kamida 14,3 mln so‘m zarar, qaytarish darajasi 21 foizdan oshmagan. Hujumni dastlabki uch bosqichda uzish eng samarali. Dropper va har bir nusxa uchun alohida C2 statik usullarni zaiflashtiradi, shu sabab aniqlash vaqt bo‘yicha va tabiiy tarqalishda baholanishi, himoya esa ko‘p bosqichli bo‘lishi kerak. Asosiy cheklov o‘z eksperimentining yo‘qligi: kelgusida mahalliy namunalar to‘plamida bosqichlarning hissasi, FPR va vaqt barqarorligini TESSERACT protokoli bo‘yicha o‘lchash lozim.

Foydalanilgan adabiyotlar

1. Infosecurity Magazine. Android SMS stealer infects 100,000 devices.
2. The Hacker News. Android malware operations merge, 22.12.2025. thehackernews.com
3. Pendlebury F. et al. TESSERACT. USENIX Security, 2019. arxiv.org/abs/1807.07838
4. Arp D. et al. Drebin: Effective and explainable detection of Android malware. NDSS, 2014. ndss-symposium.org
5. Mariconti E. et al. MaMaDroid.
6. Guardsquare. Financial Services Android Malware Landscape, 2024. guardsquare.com
7. Javaheri D. et al. Cybersecurity threats in FinTech. Expert Syst. Appl., 2024. doi.org/10.1016/j.eswa.2023.122697
8. Deininger P., Slany W. Open or Frontier? Computers, 2026, 15(9), 623. doi.org/10.
9. CyberInsider. Android 16 system-level advanced protection, 2025. cyberinsider.com
10. Android Authority. Android sideloading changes timeline, 2026. androidauthority.com
11. NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024. nist.gov

ZARARLI DASTURLARNI ANIQLASH VA AXBOROTNI HIMOYALASHDA ZAMONAVIY KIBERXAVFSIZLIK USULLARIDAN FOYDALANISH

Qaxramonov E.Q., Ismatov N.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada zararli dasturlarni aniqlash va axborotni himoyalashda qo‘llaniladigan zamonaviy kiberxavfsizlik usullari tahlil qilinadi. Signaturaviy, evristik, xulq-atvorga asoslangan, mashinaviy o‘qitish va sun’iy intellekt usullarining imkoniyatlari ko‘rib chiqiladi. Shuningdek, shifrlash, kirishni boshqarish, zaxira nusxalash, ko‘p faktorli autentifikatsiya va tarmoq monitoringining axborot xavfsizligidagi o‘rni yoritiladi. Ushbu vositalarni kompleks qo‘llash orqali axborot tizimlarining himoyalanganlik darajasini oshirish imkoniyatlari asoslanadi.

Kalit so‘zlar: zararli dastur, kiberxavfsizlik, axborotni himoyalash, zararli kod, signaturaviy tahlil, xulq-atvor tahlili, mashinaviy o‘qitish, sun’iy intellekt, shifrlash, autentifikatsiya.

Аннотация. В статье анализируются современные методы кибербезопасности, применяемые для обнаружения вредоносных программ и защиты информации. Рассматриваются возможности сигнатурного, эвристического и поведенческого анализа, машинного обучения и искусственного интеллекта. Также освещается роль шифрования, управления доступом, резервного копирования, многофакторной аутентификации и сетевого мониторинга в обеспечении информационной безопасности. Обосновывается возможность повышения защищённости информационных систем за счёт комплексного применения указанных средств.

Ключевые слова: вредоносное программное обеспечение, кибербезопасность, защита информации, вредоносный код, сигнатурный анализ, поведенческий анализ, машинное обучение, искусственный интеллект, шифрование, аутентификация.

Kirish

Raqamli texnologiyalarning keng joriy etilishi, axborot tizimlari va tarmoqlarining murakkablashuvi bilan bir qatorda, zararli dasturlar orqali amalga oshiriladigan kiberhujumlar soni va ularning texnik imkoniyatlari ham ortib bormoqda. Zararli dasturlar - viruslar, troyan dasturlar, ransomware, spyware, rootkit va boshqa zararli kodlar - axborot tizimlarining normal ishlashini buzish, ma’lumotlarni o‘g‘irlash, shifrlash, o‘zgartirish yoki ularga ruxsatsiz kirishni ta’minlash uchun qo‘llanilishi mumkin. Shu sababli zararli dasturlarni o‘z vaqtida aniqlash va axborotni himoyalash kiberxavfsizlikning asosiy vazifalaridan biri hisoblanadi.

An’anaviy antivirus vositalari asosan ma’lum zararli dasturlarning signaturalari asosida ishlaydi. Ushbu yondashuv ilgari aniqlangan tahdidlarni tezkor topishda samarali bo‘lsa-da, yangi, modifikatsiyalangan yoki signaturasi hali shakllantirilmagan zararli dasturlarni aniqlashda cheklovlarga ega. Ayniqsa, polimorfik va metamorfik zararli dasturlar, zero-day tahdidlar hamda yashirin faoliyat yurituvchi zararli kodlar an’anaviy aniqlash mexanizmlarining imkoniyatlarini sezilarli darajada cheklaydi.

Shu munosabat bilan zamonaviy kiberxavfsizlik tizimlarida xulq-atvor tahlili, evristik tahlil, sandbox texnologiyalari, mashinaviy o‘qitish va sun’iy intellektga asoslangan usullardan foydalanish tobora muhim ahamiyat kasb etmoqda. Mazkur usullar dasturiy obyektlarning faqat

tashqi belgilarini emas, balki ularning tizimdagi xatti-harakatini, resurslarga murojaatini, tarmoq faolligini va boshqa parametrlarini tahlil qilish orqali zararli faoliyatni aniqlash imkonini beradi.

Zararli dasturlarni aniqlash bilan bir qatorda, axborotni himoyalash jarayonida ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash ham muhim hisoblanadi. Bunda kriptografik himoya, autentifikatsiya va avtorizatsiya, kirishni boshqarish, zaxira nusxalash, segmentatsiya, tarmoq monitoringi va ko‘p qatlamli himoya mexanizmlaridan foydalanish samarali yondashuv sifatida qaraladi. Ayniqsa, yagona himoya vositasiga tayanish o‘rniga bir nechta himoya qatlamlarini o‘zaro integratsiya qilish axborot tizimlarining kiberbardoshliligini oshirishga xizmat qiladi.

Mazkur mavzuning dolzarbligi shundaki, zararli dasturlar doimiy ravishda takomillashib borayotgan sharoitda aniqlash va himoyalash mexanizmlarining ham moslashuvchan, avtomatlashtirilgan va kompleks bo‘lishi talab etiladi. Shu sababli zamonaviy kiberxavfsizlik usullarining imkoniyatlarini tizimli tahlil qilish, ularning afzallik va cheklovlarini aniqlash hamda ularni birgalikda qo‘llashning samarali yo‘nalishlarini asoslash muhim ilmiy-amaliy vazifa hisoblanadi.

Ushbu maqolaning maqsadi zararli dasturlarni aniqlash va axborotni himoyalashda qo‘llanilayotgan zamonaviy kiberxavfsizlik usullarini tahlil qilish, ularning funksional imkoniyatlari va cheklovlarini baholash hamda axborot tizimlarining himoyalanganlik darajasini oshirishga qaratilgan kompleks yondashuvlarni asoslab berishdan iborat.

Zararli dasturlarni aniqlash va axborotni himoyalash zamonaviy kiberxavfsizlik sohasining eng muhim ilmiy-amaliy yo‘nalishlaridan biri hisoblanadi. Zararli dasturlarning murakkablashuvi, ularning yashirin ishlash mexanizmlarining takomillashuvi hamda yangi hujum usullarining paydo bo‘lishi an’anaviy signaturaviy himoya vositalari bilan bir qatorda xulq-atvor tahlili, evristik usullar, mashinaviy o‘qitish va chuqur o‘qitish texnologiyalaridan foydalanishni talab etmoqda.

Asosiy qism

Mazkur tadqiqotda zararli dasturlarni aniqlash va axborotni himoyalashda qo‘llaniladigan zamonaviy kiberxavfsizlik usullarini baholash uchun tizimli, qiyosiy va funksional tahlil yondashuvlaridan foydalanildi. Tadqiqot jarayonida ilmiy adabiyotlarni o‘rganish, mavjud aniqlash usullarini taqqoslash, zararli dasturlarni aniqlash mexanizmlarini tasniflash va axborotni himoyalash vositalarining funksional imkoniyatlarini umumlashtirish usullari qo‘llanildi.

Dastlab zararli dasturlarni aniqlashning asosiy yondashuvlari - signaturaviy, evristik, xulq-atvorga asoslangan, statik va dinamik tahlil usullari o‘rganildi. Shuningdek, mashinaviy o‘qitish va chuqur o‘qitishga asoslangan intellektual aniqlash mexanizmlarining imkoniyatlari ko‘rib chiqildi. Har bir yondashuv aniqlash tezligi, yangi va modifikatsiyalangan zararli dasturlarni aniqlash qobiliyati, hisoblash resurslariga bo‘lgan talab hamda yolg‘on ijobiy va yolg‘on salbiy natijalar ehtimoli bo‘yicha qiyosiy baholandi.

Axborotni himoyalash vositalarini tahlil qilishda ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash mezonlari asos qilib olindi. Shu nuqtai nazardan shifrlash, ko‘p faktorli autentifikatsiya, kirishni boshqarish, zaxira nusxalash, tarmoq segmentatsiyasi, IDS/IPS, antivirus va EDR yechimlari hamda tarmoq monitoringi vositalarining o‘rni baholandi.

Tadqiqotda zararli dasturlarni aniqlash samaradorligini baholash uchun aniqlik darajasi, tahdidni aniqlash vaqti, yangi tahdidlarga moslashuvchanlik, real vaqt rejimida ishlash imkoniyati va tizimning umumiy barqarorligi kabi mezonlar belgilandi. Shu bilan birga, zamonaviy himoya vositalarining bir-biri bilan integratsiyalashuvi va ko‘p qatlamli himoya arxitekturasini shakllantirish imkoniyati ham alohida hisobga olindi.

Tadqiqotning metodologik asosini kompleks va ko‘p qatlamli himoya tamoyili tashkil etdi. Mazkur yondashuv zararli dasturlarni aniqlashni faqat antivirus yoki bitta aniqlash mexanizmi bilan cheklamasdan, signaturaviy, xulq-atvor, evristik va intellektual tahlil vositalarini axborotni himoyalashning boshqa choralariga uyg‘unlashtirilgan holda qo‘llash imkonini beradi.

Olingan tahliliy natijalar asosida zararli dasturlarni aniqlash va axborotni himoyalash samaradorligini oshirish uchun turli aniqlash usullari hamda himoya vositalarini yagona kompleks kiberxavfsizlik mexanizmi doirasida qo‘llash maqsadga muvofiq ekanligi asoslandi.

O‘tkazilgan tahlillar zararli dasturlarni aniqlashda an’anaviy va zamonaviy usullarning imkoniyatlari bir-biridan sezilarli darajada farq qilishini ko‘rsatdi. Signaturaviy aniqlash ma’lum zararli dasturlarni tez va aniq aniqlashda samarali bo‘lsa-da, yangi, o‘zgartirilgan yoki ilgari uchramagan zararli kodlarni aniqlashda cheklovlarga ega. Shu sababli zamonaviy kiberxavfsizlik tizimlarida signaturaviy usullarni evristik, xulq-atvorga asoslangan va intellektual tahlil vositalari bilan birgalikda qo‘llash zarur.

Xulq-atvor tahlili dasturiy obyektning tizimdagi harakatlarini kuzatish orqali zararli faoliyat belgilarini aniqlash imkonini beradi. Bunda fayllarga murojaat qilish, tizim sozlamalarini o‘zgartirish, shubhali tarmoq ulanishlarini yaratish yoki boshqa jarayonlarga aralashish kabi holatlar tahlil qilinadi. Ushbu yondashuv yangi zararli dasturlarni aniqlash imkoniyatini kengaytiradi, biroq noto‘g‘ri ijobiy natijalar paydo bo‘lish ehtimoli ham mavjud.

Evristik tahlil esa zararli dasturlarga xos bo‘lgan umumiy belgilar va xatti-harakatlar asosida tahdidlarni aniqlashga xizmat qiladi. Bu usul signaturasi mavjud bo‘lmagan zararli kodlarni aniqlashda foydali bo‘lsa-da, samaradorlik evristik qoidalar sifatiga va ularning muntazam yangilanib borishiga bog‘liq. Shuning uchun evristik mexanizmlar mustaqil himoya vositasi sifatida emas, balki boshqa aniqlash usullarini to‘ldiruvchi komponent sifatida samaraliroq hisoblanadi.

Tadqiqot natijalari mashinaviy o‘qitish va chuqur o‘qitish usullari zararli dasturlarni aniqlashning istiqbolli yo‘nalishlaridan biri ekanini ko‘rsatdi. Zararli dasturlarni aniqlashda qo‘llaniladigan asosiy zamonaviy usullarning ishlash prinsipi, afzalliklari va cheklovlari 1-jadvalda qiyosiy tarzda keltirilgan.

1-jadval.

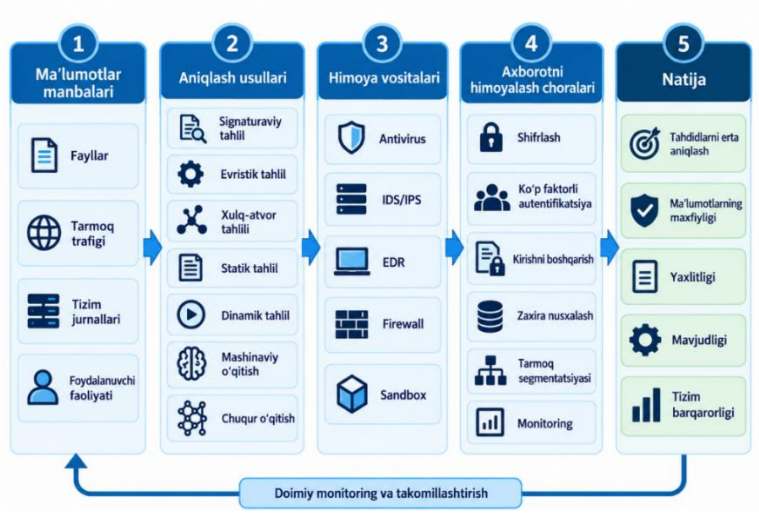
Zararli dasturlarni aniqlash usullarining qiyosiy tavsifi

Aniqlash usuli	Ishlash prinsipi	Afzalligi	Asosiy cheklovi	Qo‘llash sohasi
Signaturaviy tahlil	Fayl yoki kodni ma’lum zararli dastur signaturalari bilan taqqoslash	Ma’lum tahdidlarni tez va aniq aniqlaydi	Yangi va o‘zgartirilgan zararli dasturlarni aniqlash imkoniyati cheklangan	Antivirus tizimlari
Evristik tahlil	Shubhali kod tuzilmalari va zararli dasturlarga xos belgilarni tahlil qilish	Signaturasi mavjud bo‘lmagan tahdidlarni aniqlashi mumkin	Yolg‘on ijobiy natijalar yuzaga kelishi mumkin	Antivirus va antimalware vositalari
Xulq-atvor tahlili	Dastur ishlashi davomida uning tizimdagi harakatlarini kuzatish	Yangi va yashirin tahdidlarni aniqlash imkonini beradi	Monitoring va hisoblash resurslarini talab qiladi	EDR, endpoint monitoring

Statik tahlil	Dastur ishga tushirilmasdan uning kodi va fayl tuzilmasini tekshirish	Xavfsiz muhitda tezkor dastlabki tahlil qilish imkonini beradi	Obfuskatsiya va paklangan kod tahlilni murakkablashtiradi	Malware tahlili, antivirus
Dinamik tahlil	Dastur nazorat qilinadigan muhitda ishga tushirilib, xatti-harakati kuzatiladi	Real zararli faoliyat belgilarini aniqlash imkonini beradi	Vaqt va hisoblash resurslarini ko‘proq talab qiladi	Sandbox tizimlari
Mashinaviy o‘qitish	Belgilar asosida zararli va qonuniy dasturlarni tasniflash	Katta hajmdagi ma’lumotlarni avtomatik tahlil qiladi	Natija o‘quv ma’lumotlarining sifati va reprezentativligiga bog‘liq	Intellektual aniqlash tizimlari
Chuqur o‘qitish	Neyron tarmoqlar yordamida murakkab xususiyatlarni avtomatik o‘rganish	Murakkab belgilarni avtomatik ajratib olish imkoniyati	Katta ma’lumotlar va yuqori hisoblash quvvatini talab qilishi mumkin	Zamonaviy SI asosidagi himoya tizimlari

1-jadval tahlili shuni ko‘rsatadiki, zararli dasturlarni aniqlash usullarining har biri muayyan afzallik va cheklovlarga ega. Shu sababli amaliy kiberxavfsizlik tizimlarida signaturaviy, evristik, xulq-atvor, statik va dinamik tahlilni mashinaviy o‘qitish texnologiyalari bilan uyg‘unlashtirish aniqlash qamrovini kengaytirishga xizmat qiladi. Ushbu yondashuvlar katta hajmdagi ma’lumotlardan murakkab xususiyatlarni avtomatik ajratib olish, zararli va qonuniy faoliyat o‘rtasidagi farqlarni aniqlash hamda yangi tahdidlarga moslashish imkonini beradi. Biroq ularning samaradorligi o‘quv ma’lumotlarining sifati, modelning to‘g‘ri o‘qitilishi va real muhitdagi ma’lumotlarga moslashuvchanligiga bevosita bog‘liq.

Axborotni himoyalash jarayonida esa faqat zararli dasturlarni aniqlashning o‘zi yetarli emas. Ma’lumotlarning konfidensialligi, butunliligi va foydalanuvchanligini ta’minlash uchun ko‘p qatlamli himoya modeli talab etiladi. Zararli dasturlarni aniqlash va axborotni himoyalashda qo‘llaniladigan ko‘p qatlamli yondashuvning umumiy modeli 1-rasmda keltirilgan.



1-rasm. Zararli dasturlarni aniqlash va axborotni himoyalashning ko‘p qatlamli modeli

1-rasmda ko‘rsatilganidek, samarali kiberhimoya ma’lumotlar manbalarini kuzatish, zararli faoliyatni turli usullar yordamida aniqlash, himoya vositalarini qo‘llash hamda ma’lumotlarning konfidensialligi, butunliligi va foydalanuvchanligini ta’minlovchi choralarni

yagona tizimda birlashtirishni talab etadi. Ushbu jarayon doimiy monitoring va takomillashtirish bilan qo‘llab-quvvatlanganda zararli dasturlarning ta’sirini kamaytirish va axborot tizimining barqarorligini oshirish imkoniyati yuzaga keladi.

Bunda shifrlash, ko‘p faktorli autentifikatsiya, kirishni boshqarish, tarmoq segmentatsiyasi, zaxira nusxalash, IDS/IPS, EDR va uzluksiz monitoring vositalaridan birgalikda foydalanish muhim ahamiyatga ega.

Muhokama jarayonida aniqlangan yana bir muhim jihat shundaki, zararli dasturlarga qarshi samarali himoya profilaktik, aniqlovchi va javob beruvchi vositalarning uzviy integratsiyasiga bog‘liq. Masalan, autentifikatsiya va kirishni boshqarish ruxsatsiz kirish xavfini kamaytirsa, EDR va IDS/IPS vositalari zararli faoliyatni aniqlashga, zaxira nusxalash va tiklash mexanizmlari esa hujum oqibatlarini kamaytirishga xizmat qiladi.

Tahlil natijalariga ko‘ra, zamonaviy kiberxavfsizlik tizimining samaradorligi bir nechta asosiy omilga bog‘liq: tahdidlarni erta aniqlash, yangi va modifikatsiyalangan zararli dasturlarga moslashuvchanlik, yolg‘on ijobiy va yolg‘on salbiy natijalarni kamaytirish, real vaqt rejimida monitoring olib borish hamda himoya vositalarining o‘zaro integratsiyalashuvi.

Shu asosda zararli dasturlarni aniqlash va axborotni himoyalashda eng maqbul yondashuv sifatida signaturaviy, evristik, xulq-atvor va sun’iy intellektga asoslangan aniqlash usullarini ko‘p qatlamli himoya vositalari bilan birlashtirish taklif etiladi. Bunday yondashuv tahdidlarni aniqlash qamrovini kengaytiradi, axborot tizimining barqarorligini oshiradi va zararli dasturlar ta’siridan kelib chiqadigan xavflarni kamaytirishga xizmat qiladi.

Xulosa

Zararli dasturlarni aniqlash va axborotni himoyalashda zamonaviy kiberxavfsizlik usullaridan foydalanish muhim ahamiyatga ega. Signaturaviy usullar ma’lum tahdidlarni aniqlashda samarali bo‘lsa-da, yangi va modifikatsiyalangan zararli dasturlar uchun xulq-atvor, evristik va intellektual yondashuvlar talab etiladi. Tadqiqot natijalari samarali himoya bir nechta mexanizmlarning o‘zaro integratsiyasiga bog‘liqligini ko‘rsatdi. Antivirus, EDR, IDS/IPS, monitoring, autentifikatsiya, shifrlash va zaxira nusxalash vositalarini ko‘p qatlamli himoya tizimida qo‘llash maqsadga muvofiqdir. Sun’iy intellekt va mashinaviy o‘qitish tahdidlarni erta aniqlash va katta hajmdagi ma’lumotlarni tahlil qilish imkoniyatini kengaytiradi. Biroq ularning samaradorligi sifatli ma’lumotlar va to‘g‘ri sozlangan modellarga bog‘liq. Muntazam monitoring yolg‘on ijobiy va yolg‘on salbiy natijalarni kamaytirishga yordam beradi. Samarali kiberhimoya profilaktik, aniqlovchi va javob beruvchi choralarni birlashtirishi lozim. Bunday kompleks yondashuv tahdidlarni tez aniqlash va ularning zararini kamaytirishga xizmat qiladi.

Foydalanilgan adabiyotlar

13. Bensaoud A., Kalita J., Bensaoud M. A Survey of Malware Detection Using Deep Learning. // Machine Learning with Applications. – 2024. – Vol. 16. – Article 100546. DOI: 10.1016/j.mlwa.2024.100546.

14. Gorment N.Z., Selamat A., Lim K.C., Krejcar O. Machine Learning Algorithm for Malware Detection: Taxonomy, Current Challenges, and Future Directions. // IEEE Access. – 2023. DOI: 10.1109/ACCESS.2023.3256979.

15. Song J., Choi S., Kim J., Park K., Park C., Kim J., Kim I. A Study of the Relationship of Malware Detection Mechanisms Using Artificial Intelligence. // ICT Express. – 2024. – Vol. 10, No. 3. – P. 632–649. DOI: 10.1016/j.icte.2024.03.005.

16. Haydarov E., Abdullayev D. Korporativ tarmoqdagi zararkunanda dastur turlari va ularning qiyosiy tahlili. // Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-amaliy konferensiyasi materiallari. – Toshkent: TATU, 2025.

ZAIFLIKLARNI MAXSUS STANDARTLAR ORQALI ANIQLASH HAMDA NMAP VULSCAN MODULI NATIJALARI BILAN INTEGRATSIYALASH: RISKKA ASOSLANGAN MODEL

Tashev K.A., Yoqubjonov O.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada axborot tizimlaridagi zaifliklarni boshqarishning asosiy standartlari - CVE, NVD, CWE, CWSS va CVSS - hamda Nmap uchun Vulscan moduli imkoniyatlari penetratsion testlash nuqtayi nazaridan tahlil qilingan. Nazorat qilinadigan laboratoriya muhitida Apache HTTP Server 2.4.49 versiyasiga tegishli CVE-2021-41773 zaifligi misolida versiyaga asoslangan skanerlash natijalari standartlar ma'lumotlari bilan solishtirilib, faqat CVSS ballariga tayanishning cheklovlari ko‘rsatilgan. Natijalar asosida ekspluatatsiya ma'lumotlari (CISA KEV, EPSS), zaiflik og‘irligi va aktivning kritikligini birlashtiruvchi riskka asoslangan ustuvorlashtirish modeli taklif etilgan.

Kalit so‘zlar: zaifliklarni boshqarish, CVE, NVD, CWE, CVSS, EPSS, Vulscan, Nmap, penetratsion testlash.

Аннотация. В статье с позиции тестирования на проникновение проанализированы основные стандарты управления уязвимостями - CVE, NVD, CWE, CWSS и CVSS - и возможности модуля Vulscan для Nmap. В контролируемой лабораторной среде на примере уязвимости CVE-2021-41773 (Apache HTTP Server 2.4.49) результаты сканирования по версиям сопоставлены с данными стандартов и показаны ограничения опоры только на баллы CVSS. По результатам предложена модель приоритизации на основе риска, объединяющая данные об эксплуатации (CISA KEV, EPSS), степень серьёзности уязвимости и критичность актива.

Ключевые слова: управление уязвимостями, CVE, NVD, CWE, CVSS, EPSS, Vulscan, Nmap, тестирование на проникновение.

Kirish

Zaifliklarni boshqarishdagi asosiy qiyinchilik ularning sonidir. Jerry Gamblin tahliliga ko‘ra, 2025-yilda 48 185 ta CVE e'lon qilingan, bu 2024-yilga nisbatan 20,6 foizga ko‘p; 1999-yildan beri jami 308 920 ta yozuv to‘plangan [1]. Verizon DBIR 2025 hisobotiga ko‘ra, zaifliklarni ekspluatatsiya qilish buzilishlarning taxminan 20 foizida qayd etilgan va bir yilda 34 foizga oshgan [2]. Bunday sharoitda barcha zaifliklarni birdek tezlikda yopish imkonsiz, shuning uchun qaysi birini birinchi yopish kerakligini aniqlash asosiy vazifaga aylanadi.

Ma'lumotlar infratuzilmasining o‘zi ham o‘zgarmoqda. 2025-yil aprelida MITRE bilan tuzilgan CVE dasturi shartnomasi tugash arafasida CISA tomonidan 11 oyga uzaytirildi [3]. 2026-yil 15-aprelda esa NIST National Vulnerability Database (NVD) ni barcha CVE yozuvlarini boyitishdan xavfga asoslangan navbat tizimiga o‘tkazganini e'lon qildi: ustuvor boyitish CISA KEV katalogidagi, federal idoralar foydalanadigan va AQShning 14028-sonli farmoni bo‘yicha muhim dasturiy ta'minotga tegishli CVE'lar uchun saqlanib, qolganlari «boyitish rejalashtirilmagan» holatda qolishi mumkin; CVE'ni bergan tashkilot (CNA) bahoni allaqachon kiritgan bo‘lsa, NIST alohida baho bermaydi [4]. Demak, «har bir CVE uchun tayyor CVSS bali va mahsulotlar ro‘yxati mavjud» degan taxminga tayangan jarayonlar endi ishonchsiz.

Tadqiqotning maqsadi - zaiflik standartlarini tizimlashtirish, Nmap Vulscan moduli natijalarini laboratoriya sharoitida baholash va ularni ekspluatatsiya ma’lumotlari bilan birlashtiruvchi riskka asoslangan ustuvorlashtirish modelini taklif etishdir.

Tadqiqot metodologiyasi

Skanerlash faqat o‘zimizga tegishli, tashqi tarmoqdan ajratilgan laboratoriya muhitida o‘tkazildi. Penetratsion test va zaifliklarni skanerlash boshqa tashkilotlar tizimlarida faqat buyurtmachining yozma roziligi va aniq belgilangan qamrov mavjud bo‘lganda amalga oshiriladi. Tadqiqot to‘rt bosqichdan iborat bo‘ldi. Birinchidan, CVE, NVD, CWE, CWSS va CVSS standartlari vazifasi, tashkilotchisi va chiqish ma’lumotlari bo‘yicha solishtirildi [5–7]. Ikkinchidan, Nmap xizmat versiyalarini aniqlash rejimida Vulscan moduli bilan ishga tushirildi: `nmap -sV --script=vulscan/vulscan.nse <maqsad>` [8]. Uchinchidan, topilgan har bir CVE identifikatori bo‘yicha CWE turi, CVSS bali, CISA KEV katalogidagi holati [9] va EPSS ko‘rsatkichi [10] yig‘ildi. To‘rtinchidan, har bir topilma nazorat ostidagi tekshiruv orqali tasdiqlandi yoki rad etildi.

Namunaviy holat sifatida Apache HTTP Server 2.4.49 dagi CVE-2021-41773 tanlandi. U uchta jihati bilan qulay: yo‘l bo‘ylab o‘tish (path traversal) turidagi zaiflik; CISA KEV katalogiga kiritilgan; uni bartaraf etish uchun chiqarilgan 2.4.50 versiyasi tuzatishi to‘liq bo‘lmay chiqqan va alohida CVE-2021-42013 raqamini olgan [11, 12].

Standartlarning tasnifi va tajriba natijalari

Tahlil natijasida zaiflik ma’lumotlari ekotizimi yetti elementdan tashkil topgani aniqlandi (1-jadval). Ularning har biri turli savolga javob beradi: CVE «bu qaysi zaiflik?», CWE «qanday kamchilik sabab bo‘lgan?», CVSS «qanchalik og‘ir?», EPSS va KEV esa «uni haqiqatda ekspluatatsiya qilishyaptimi?» degan savolga.

1-jadval

Zaiflikni boshqarish standartlari va ularning vazifasi

№	Standart (tashkilot)	Vazifasi	Chiqish / shkala
1	CVE (MITRE)	Zaiflikka yagona identifikator berish	CVE-YYYY-NNNN, qisqa tavsif, havolalar
2	NVD (NIST)	CVE yozuvlarini boyitish: baho va ta’sir etuvchi mahsulotlar (CPE)	CVSS, CPE, CWE; 2026-yil aprelidan tanlab boyitish
3	CWE (MITRE)	Zaiflikni keltirib chiqargan kamchilik turlarini tasniflash	CWE-ID (masalan, CWE-22)
4	CWSS (MITRE)	Dasturdagi kamchiliklarni xavf, ta’sir va qiyinlik omillari bo‘yicha baholash	0–100 ball
5	CVSS (FIRST)	Zaiflik og‘irligini baholash	0–10: Past 0,1–3,9; O‘rta 4,0–6,9; Yuqori 7,0–8,9; Tanqidiy 9,0–10
6	EPSS (FIRST)	Keyingi 30 kunda ekspluatatsiya qilinish ehtimolini baholash	0–1 oralig‘ida ehtimollik
7	KEV (CISA)	Amalda ekspluatatsiya qilinishi tasdiqlangan zaifliklar katalogi	Katalogda bor / yo‘q

Vulscan natijalarini baholashda uchta xulosa olindi. Birinchi xulosa modulning tabiatiga bog‘liq: u aniqlangan xizmat versiyasini bir nechta zaiflik bazalari (CVE, Exploit-DB, OpenVAS va boshqalar) bilan solishtiradi, zaiflikni ekspluatatsiya qilib tekshirmaydi. Shu sababli natija «tasdiqlangan zaiflik» emas, «nomzod zaiflik» hisoblanadi. Banner yashirilgan yoki o‘zgartirilgan bo‘lsa, shuningdek tarqatuvchi tuzatishni versiya raqamini o‘zgartirmasdan kiritgan bo‘lsa, soxta ijobiy va soxta salbiy natijalar paydo bo‘ladi, bir xil zaiflik esa turli bazalarda takrorlanib chiqish hajmini oshiradi. Shuning uchun har bir topilma qo‘lda tekshirilishi va bazalar muntazam yangilanishi zarur.

Ikkinchi xulosa CVE-2021-41773 misolidan kelib chiqadi. Zaiflik Apache 2.4.49 versiyasida yo‘l normallashtirishga kiritilgan o‘zgarish tufayli paydo bo‘lgan va faqat shu versiyaga ta’sir qiladi: hujumchi URL yordamida Alias turidagi direktivalar bilan belgilangan kataloglardan tashqaridagi fayllarga murojaat qilishi mumkin, agar ular odatiy «require all denied» konfiguratsiyasi bilan himoyalanmagan bo‘lsa [11]. NVD ma’lumotlarida u CVSS v3.1 bo‘yicha 7,5 ball bilan, ya’ni «Tanqidiy» emas, «Yuqori» toifasida baholangan (hujum tarmoq orqali, murakkabligi past, imtiyoz va foydalanuvchi harakati talab qilinmaydi) [12], biroq u CISA KEV katalogida va EPSS bo‘yicha yuqori persentilda turadi [9, 10]. FIRST ta’kidlaganidek, CVSS xavfni emas, og‘irlikni o‘lchaydi, Threat va Environmental metrikalarni esa uni qo‘llovchi tashkilotning o‘zi to‘ldirishi lozim [7]. Bundan tashqari, 2.4.50 ga yangilash ham yetarli bo‘lmagan: tuzatishni to‘liq bartaraf etish uchun keyingi versiyaga o‘tish kerak bo‘ldi [11]. Demak, yangilash natijasini ham versiya darajasida qayta tekshirish lozim.

Uchinchi xulosa NVD’dagi o‘zgarishlar bilan bog‘liq. Vulscan natijalarini NVD’dan avtomatik boyitishga tayansak, yangi CVE’larning katta qismi uchun CVSS bali yoki CPE ro‘yxati bo‘lmasligi mumkin [4]. Shu sababli ustuvorlashtirish bitta manbaga emas, bir nechta signalga - CNA bahosi, KEV, EPSS va ishlab chiqaruvchi bildirishnomalariga - asoslanishi kerak.

Riskka asoslangan ustuvorlashtirish modeli

Natijalarga tayanib, topilmalarni to‘rt signal bo‘yicha saralaydigan model taklif etiladi: (1) zaiflik KEV katalogida yoki ommaviy ekspluatatsiya ma’lumoti mavjudmi; (2) EPSS ehtimoli qanday; (3) CVSS og‘irligi (iloji bo‘lsa Threat va Environmental metrikalar bilan to‘ldirilgan); (4) aktivning kritikligi va internetga ochiqligi. Daraja va muddatlar tashkilot ehtiyojiga moslashtiriladigan tavsiya sifatida berilgan (2-jadval).

2-jadval

Taklif etilgan ustuvorlik darajalari

№	Daraja	Shart	Tavsiya etilgan muddat
1	P1 - shoshilinch	KEV da bor yoki ommaviy ekspluatatsiya mavjud va xizmat internetga ochiq	24–72 soat; tuzatish imkoni bo‘lmasa vaqtinchalik himoya
2	P2 - yuqori	EPSS yuqori yoki CVSS ≥ 7,0 va aktiv muhim	14 kun
3	P3 - o‘rta	CVSS 4,0–6,9, ekspluatatsiya belgisi yo‘q	30 kun
4	P4 - past	Past og‘irlik, ichki va muhim bo‘lmagan aktiv	Odatiy yangilash davrida

Texnik qatlam. Aktivlar inventarizatsiyasi; Nmap va Vulscan bilan rejali skanerlash hamda har bir topilmani tasdiqlash; Vulscan bazalarini yangilab borish; KEV va EPSS ma’lumotlarini NVD’dan mustaqil ravishda avtomatik olish; yangilash imkoni bo‘lmaganda keraksiz xizmatlar

va modullarni o‘chirish, kataloglarga kirishni odatiy «require all denied» qoidasi bilan cheklash yoki veb-ilovalar uchun himoya devori orqali vaqtinchalik himoya.

Tashkiliy qatlam. Ustuvorlashtirish siyosati va muddatlarini rasmiylashtirish; KEV yangilanishlarini kuzatish; yangilashdan keyin versiyani qayta tekshirish; zaifliklar bo‘yicha hisobot berish tartibi; kritik axborot infratuzilmasi sub’ektlari uchun O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi ZRU-764-sonli Qonuni talablariga rioya qilish [13].

Inson qatlami. Administratorlar va xavfsizlik mutaxassislarini CVE, CWE va CVSS yozuvlarini o‘qishga hamda CVSS xavfni emas, og‘irlikni o‘lchashini tushunishga o‘rgatish. Samaradorlik uchta ko‘rsatkich bilan baholanadi: P1 zaifliklarni yopishning o‘rtacha vaqti, internetga ochiq aktivlarda yopilmagan P1 va P2 zaifliklar ulushi hamda skanerning soxta ijobiy natijalari ulushi.

Xulosa

Tadqiqot shuni ko‘rsatdiki, Vulscan kabi versiyaga asoslangan skanerlar zaifliklarni tezda aniqlashda foydali, ammo ularning natijasi nomzod ro‘yxati bo‘lib, tasdiqlash talab qiladi. CVE-2021-41773 misoli CVSS bahosi «Yuqori» bo‘lgan zaiflik amalda KEV katalogiga kirgan holatni va tuzatishning o‘zi ham to‘liq bo‘lmay chiqishi mumkinligini ko‘rsatdi. NVD tanlab boyitishga o‘tgani sababli ustuvorlashtirishda KEV, EPSS va tashkilot muhitiga xos ma’lumotlarning o‘rni oshadi. Keyingi tadqiqotlarda taklif etilgan modelni tashkilot ma’lumotlarida sinab, yopish vaqti va soxta ijobiy natijalar ko‘rsatkichlari bo‘yicha baholash hamda CVSS v4.0 ning Threat va Environmental metrikalarini avtomatik to‘ldirish usullarini o‘rganish rejalashtirilgan.

Adabiyotlar

1. Gamblin J. 2025 CVE Data Review. - 01.01.2026. - https://jerrygamblin.com/2026/01/01/2025-cve-data-review/

2. Verizon. 2025 Data Breach Investigations Report. - 2025.

3. The Record. CISA extends CVE program contract with MITRE for 11 months amid alarm over potential lapse. - 16.04.2025. - https://therecord.media/cisa-extends-cve-program-contract-with-mitre

4. NIST. NIST Updates NVD Operations to Address Record CVE Growth. - 15.04.2026. - https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth

5. MITRE. CVE Program (https://www.cve.org/); Common Weakness Enumeration (https://cwe.mitre.org/); Common Weakness Scoring System v1.0.1 (https://cwe.mitre.org/cwss/cwss_v1.0.1.html).

6. NIST. National Vulnerability Database. - https://nvd.nist.gov

7. FIRST. Common Vulnerability Scoring System v4.0: Specification Document. - https://www.first.org/cvss/

8. scipag. Vulscan - Nmap uchun zaifliklarni aniqlash moduli

9. CISA. Known Exploited Vulnerabilities Catalog.

10. FIRST. Exploit Prediction Scoring System (EPSS). - https://www.first.org/epss/

11. Apache Software Foundation. Apache HTTP Server 2.4 vulnerabilities (CVE-2021-41773, CVE-2021-42013). - https://httpd.apache.org/security/vulnerabilities_24.html

12. NVD. CVE-2021-41773 Detail. - https://nvd.nist.gov/vuln/detail/CVE-2021-41773

13. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi ZRU-764-sonli Qonuni. - 15.04.2022.

MATHEMATICAL MODEL OF STREAMING NETWORK TRAFFIC AND THE INFORMATION SECURITY MONITORING PROCESS

Rajabboyeva S.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Xaitbayev A.
Cyber University

Annotatsiya. Maqolada axborot xavfsizligi maqsadida oqimli tarmoq trafigini monitoring qilish jarayoni ketma-ket o‘zgarish nuqtasini aniqlash masalasi sifatida rasmiylashtirilgan. Trafik qat’iy uzunlikdagi vaqt oynalari bo‘yicha hisoblangan belgilar vektorlari ketma-ketligi, jumladan hajm ko‘rsatkichlari hamda manzil va port taqsimotlarining Shennon entropiyasi orqali ifodalanadi. Rekursiv yangilanuvchi bazaviy model, Mahalanobis turidagi anomaliya bahosi va bir tomonli CUSUM statistikasi doimiy xotira va har bir oynada doimiy hisoblash hajmiga ega detektorni hosil qiladi; uning qaror chegarasi soxta signalgacha o‘rtacha ish uzunligi (ARL) talabi bo‘yicha kalibrlanadi. Model NIST SP 800-137 uzluksiz monitoring tsikliga moslashtirilgan va CIC-IDS2017 to‘plamida baholash protokoli taklif etilgan.

Kalit so‘zlar: tarmoq trafigi; ma’lumotlar oqimi; anomaliyalarni aniqlash; entropiya; CUSUM; axborot xavfsizligi monitoringi.

Аннотация. В работе процесс мониторинга потокового сетевого трафика в целях информационной безопасности формализован как задача последовательного обнаружения разладки. Трафик представлен последовательностью векторов признаков, вычисляемых по окнам фиксированной длины, включая объёмные признаки и энтропию Шеннона распределений адресов и портов. Рекурсивно обновляемая базовая модель, оценка аномальности типа Махаланобиса и односторонняя статистика CUSUM образуют детектор с постоянным объёмом памяти и постоянной вычислительной сложностью на окно; порог принятия решения калибруется по требуемой средней длине серии до ложной тревоги (ARL). Модель согласована с циклом непрерывного мониторинга NIST SP 800-137, предложен протокол оценки на наборе данных CIC-IDS2017.

Ключевые слова: сетевой трафик; поток данных; обнаружение аномалий; энтропия; CUSUM; мониторинг информационной безопасности.

Introduction

Modern networks generate traffic faster than it can be stored and analysed offline, so security monitoring must work on streams: every observation is processed once, with bounded memory and bounded delay. A recent systematic survey of streaming anomaly detection in network security notes that conventional detectors perform well on static data but cannot learn online or update their models in real time, which is a serious obstacle when immediate feedback is required [1]. At the organizational level, NIST SP 800-137 describes information security continuous monitoring as an ongoing process that gives decision makers current awareness of threats, vulnerabilities and the effectiveness of deployed security controls [2]. What is often missing is a compact mathematical description that links the traffic stream, the detection algorithm and the monitoring cycle. The aim of this paper is to propose such a model.

Related work

Three lines of research underlie the proposed model. The first is statistical sequential analysis. Wang, Zhang and Shin applied the non-parametric CUSUM method to the behaviour of TCP SYN–FIN packet pairs at leaf routers, which made SYN-flood detection insensitive to site-specific traffic patterns and gave short detection latency in trace-driven simulations [4]. Tartakovsky, Polunchenko and Sokolov treated on-line detection as a quickest changepoint problem; on a real SYN-flood trace with 20 ms sampling, the Shiryaev–Roberts procedure detected the attack after about 0.14 s (7 samples) and CUSUM after about 0.21 s (10 samples), the former at the price of additional false alarms in the run shown, with thresholds set by Monte Carlo simulation to a chosen average run length [5].

The second line is information-theoretic. Lakhina, Crovella and Diot showed that the sample entropy of IP-address and port distributions reveals anomalies that are hard to isolate in traffic volume, and validated the approach on the Abilene and Géant backbone networks [6]. The third line is learning-based: Kitsune uses an ensemble of autoencoders trained online without labels and achieves performance comparable to offline detectors even on a Raspberry Pi [7]. For evaluation, CIC-IDS2017 provides labelled benign and attack traffic recorded over five days, with background traffic generated from the abstract behaviour of 25 users [3]; however, Rosay et al. reported problems in the flow features extracted from its packet captures, so features should be recomputed or corrected before use [8].

Mathematical model

Traffic stream and features

Let the packet stream be a sequence (τ_k, a_k), where τ_k is the arrival time and a_k is the vector of header attributes (source and destination address, destination port, protocol, length, TCP flags). Time is divided into windows of length Δ; window t covers $[(t-1)\Delta, t\Delta)$. For each window a feature vector in R^{d} is computed:

$$x_t = (n_t, b_t, s_t, H_{src,t}, H_{dst,t}, H_{port,t})^{\mathrm{T}}, \tag{1}$$

where n_t is the packet count, b_t the byte count, s_t the difference between the numbers of SYN and FIN packets, and H the Shannon entropy of the empirical distribution of source addresses, destination addresses and destination ports in the window:

$$H = -\sum_i p_i \log_2 p_i, \quad p_i = c_i / N_t, \tag{2}$$

with c_i the number of packets carrying the i-th distinct value and N_t the total packet count. Volume features capture floods, while entropies respond to dispersion or concentration of addresses and ports, as in scans and distributed attacks [6]. Here $d = 6$.

Adaptive baseline

Normal behaviour is described by an exponentially weighted mean and covariance, updated recursively with forgetting factor $\lambda \in (0,1)$:

$$\mu_t = (1-\lambda)\,\mu_{t-1} + \lambda\, x_t, \quad S_t = (1-\lambda)\,S_{t-1} + \lambda\,(x_t - \mu_t)(x_t - \mu_t)^{\mathrm{T}}. \tag{3}$$

The update is performed only for windows not flagged as anomalous, so that an ongoing attack does not contaminate the baseline. Both recursions need $O(d^2)$ memory and time regardless of stream length.

Anomaly score and detection statistic

The deviation of window t from the baseline is measured by a Mahalanobis-type distance, standardized so that its mean is close to zero under normal conditions:

$$D_t = (x_t - \mu_{t-1})^{\mathrm{T}}(S_{t-1} + \varepsilon I)^{-1}(x_t - \mu_{t-1}), \quad z_t = (D_t - d) / \sqrt{(2d)}, \tag{4}$$

where εI is a small regularizer; under a Gaussian approximation D_t follows a chi-square law with d degrees of freedom, whose mean is d and variance $2d$. Individual deviations are too noisy for reliable alarms, so the evidence is accumulated by a one-sided CUSUM statistic and the alarm time is its first threshold crossing:

$$y_t = \max\{0, y_{t-1} + z_t - \kappa\}, \quad y_0 = 0, \tag{5}$$

$$T = \min\{t \geq 1 : y_t \geq h\}, \tag{6}$$

where the reference value $\kappa \geq 0$ sets the smallest shift worth detecting and h is the decision threshold. The statistic has constant memory and one update per window, which suits on-line operation [4], [5].

Threshold calibration and quality criteria

The threshold is chosen to guarantee a required average run length to false alarm γ under normal traffic, and the price paid is the detection delay for a change at the unknown moment v:

$$E_\infty[T] \geq \gamma, \quad D_v = E_v[T - v \mid T \geq v]. \tag{7}$$

Raising h increases γ and the delay simultaneously, so h expresses the operator's tolerance for false alarms. In practice h is found by Monte Carlo simulation on attack-free traffic, as in [5]. Detection quality is also reported by true- and false-positive rates, precision and F1-score computed on labelled windows.

Monitoring process

Let $q_t \in \{0, 1\}$ be the state of the monitor. If $y_t < h$, then $q_t = 0$ and the baseline (3) is updated. If $y_t \geq h$, then $q_t = 1$: an alert is raised, the baseline is frozen and the statistic is restarted ($y_t := 0$), which corresponds to the multi-cyclic setting of quickest detection [5]. To support triage, the contribution of each feature to the alert is ranked by the standardized deviation

$$c_{j,t} = |x_{j,t} - \mu_{j,t-1}| / \sqrt{S_{jj,t-1}}, \tag{8}$$

so that, for example, a large contribution of n_t and s_t together with a drop of $H_{src,t}$ points to a flood from few sources, whereas a rise of $H_{port,t}$ points to port scanning. The cycle maps directly onto the ISCM process of NIST SP 800-137 [2]: strategy (choice of Δ, λ, κ, γ), implementation (stream processing of (1)–(6)), analysis (statistic y_t and contributions $c_{j,t}$), response (alert and mitigation) and review (periodic re-estimation of the baseline and re-calibration of h).

Evaluation protocol

The model is to be validated on CIC-IDS2017 [3]. Windows from the benign-only day are used to estimate the baseline and to calibrate h for several values of γ; windows from days containing denial-of-service, port-scan and botnet activity serve as test data. Because the flow features distributed with the dataset contain extraction errors [8], they will be recomputed from the raw packet captures. Three variants will be compared: the full model, a volume-only variant without entropies (to measure the gain from entropy [6]) and the learning-based detector Kitsune [7] as a baseline. For window lengths Δ of 1, 5 and 10 seconds the study will report true-positive rate, false-positive rate, F1-score and mean detection delay.

Conclusion

The proposed model describes the monitoring of a traffic stream as a chain of explicit mathematical objects: window features, an adaptive baseline, an anomaly score, a sequential detection statistic with a calibrated threshold, and a monitoring state that drives alerting and baseline updating. It uses constant memory and constant computation per window, and its parameters have a clear operational meaning through the average run length to false alarm and the detection delay. Further work will concern the experimental study described above, robust (heavy-

tailed) alternatives to the Gaussian approximation, and distributed monitoring at several network points.

References

1. Zhou P. et al. A survey of streaming data anomaly detection in network security // PeerJ Computer Science, 2025. DOI: 10.7717/peerj-cs.3066.

2. Dempsey K., Chawla N., Johnson L., Johnston R., Jones A., Orebaugh A., Scholl M., Stine K. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137, 2011. DOI: 10.6028/NIST.SP.800-137.

3. Sharafaldin I., Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization // Proc. 4th Int. Conf. on Information Systems Security and Privacy (ICISSP), 2018. arXiv:1804.03599.

4. Wang H., Zhang D., Shin K.G. Detecting SYN flooding attacks // Proc. IEEE INFOCOM, 2002.

5. Tartakovsky A.G., Polunchenko A.S., Sokolov G. Efficient computer network anomaly detection by changepoint detection methods // IEEE Journal of Selected Topics in Signal Processing, 2013, vol. 7, no. 1, pp. 7–11.

6. Lakhina A., Crovella M., Diot C. Mining anomalies using traffic feature distributions // Proc. ACM SIGCOMM, 2005, pp. 217–228.

7. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: an ensemble of autoencoders for online network intrusion detection // Proc. Network and Distributed System Security Symposium (NDSS), 2018. DOI: 10.14722/ndss.2018.23204.

8. Rosay A., Cheval E., Carlier F., Leroux P. Network intrusion detection: a comprehensive analysis of CIC-IDS2017 // Proc. ICISSP, 2022.

QUORUM-SIGNED PERMISSIONED BLOCKCHAIN WITNESS FOR SECURITY LOG INTEGRITY: PROTOTYPE AND FAULT-TOLERANCE EVALUATION

Xabibullayev J.D., Xamidov Sh.J.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotatsiya. Tezisda xavfsizlik jurnallari yaxlitligi isbotlarini qayd etish uchun kvorum imzoli ruxsat etilgan blokcheyn guvohi taklif etilgan. Har bir blok log davrining Merkle ildizi va xesh zanjiri qiymatini o‘z ichiga oladi hamda mustaqil tashkilotlarga tegishli n = 3f + 1 tugundan 2f + 1 tasining Ed25519 imzosi bilan haqiqiy hisoblanadi. Python prototipida hisoblash xarajati va yetti xil nosozlik hamda til biriktirish holati baholangan. Log egasi f ta tugun bilan til biriktirib tarixni qayta yozishga uringanda blok rad etilishi, chegaradan oshganda esa ikki blokni imzolagan tugunlar fosh etiladigan ayrilish (fork) aniqlanishi ko‘rsatilgan.

Kalit so‘zlar: xavfsizlik jurnallari, log yaxlitligi, ruxsat etilgan blokcheyn, tashqi guvoh, kvorum sertifikati, Ed25519, Vizantiya xatolariga chidamlilik.

Аннотация. В тезисе предложен свидетель на основе разрешённого блокчейна с кворумными подписями для фиксации доказательств целостности журналов безопасности. Каждый блок содержит корень дерева Меркла и значение хеш-цепочки периода журнала и действителен только при наличии подписей Ed25519 от 2f + 1 из n = 3f + 1 узлов независимых организаций. На прототипе на Python оценены вычислительные затраты и семь сценариев отказов и сговора. Показано, что попытка владельца журнала переписать историю в сговоре с f узлами отклоняется, а при превышении порога возникает обнаруживаемое ветвление с доказательством против узлов, подписавших оба блока.

Ключевые слова: журналы безопасности, целостность журналов, разрешённый блокчейн, внешний свидетель, кворумный сертификат, Ed25519, византийская отказоустойчивость.

Introduction

Hash chains and Merkle trees detect modification, deletion and insertion of log records, but they cannot detect truncation of the log tail or a full recomputation of the chain by the log owner unless the period roots are anchored in an external witness that the owner does not control [3, 4]. Both attacks pass the internal check, because a recomputed chain is consistent with itself, and they are revealed only by comparison with the values held by the witness.

The witness therefore becomes the new root of trust. A single witness server only moves the trust from the log owner to the witness operator. A public blockchain removes the operator, but brings transaction fees, confirmation delays and publication of metadata outside the organization. The capabilities of blockchain technology for data management and attack prevention have been analysed in [1, 2]. A permissioned blockchain run by several independent organizations, for example the log owner, a sector CERT, an external auditor and the regulator, is a practical middle ground [8, 9], provided that it tolerates both crashed and malicious nodes. Byzantine fault-tolerant protocols guarantee safety while the number of faulty nodes f satisfies $n \geq 3f + 1$ [5].

The aim of this work is to design a quorum-signed witness for log anchoring, to implement it as a working prototype and to measure its cost and its behaviour under crash faults, collusion with the log owner and attempts to rewrite the anchored history.

Threat model and anchor block

The log owner controls the log gateway and may collude with up to f witness nodes; the other nodes follow the protocol, and the auditor knows the public keys of all nodes. For each period h the gateway computes the Merkle root R_h of the period records and the head c_h of the hash chain and forms the anchor block

$$B_h = (h, prev, R_h, c_h), \quad prev = H(B_{h-1}),$$

where H is SHA-256. Only these 32-byte values leave the organization; the log records themselves stay with the owner.

Quorum signing protocol

Each of the n = 3f + 1 witness nodes belongs to a different organization and holds its own Ed25519 key pair [6, 7]. A node signs a block only if the block extends its own ledger and if it has not signed another block at the same height (Listing 1). The block is committed when the gateway collects a quorum certificate QC_h of q = 2f + 1 signatures from distinct nodes; otherwise anchoring halts and an alert is raised. Any two quorums of size 2f + 1 share at least f + 1 nodes, so at least one honest node lies in the intersection, and two conflicting blocks cannot both be certified while no more than f nodes are malicious. The auditor accepts a block only with a valid certificate (Listing 2) and compares R_h and c_h with values recomputed from the logs (Fig. 1).

Unlike full PBFT [5] or HotStuff [10], the protocol has a single signing round and no leader election: the gateway is untrusted and can only propose blocks. If the gateway stops proposing, the missing heights are themselves an alarm signal for the auditor.

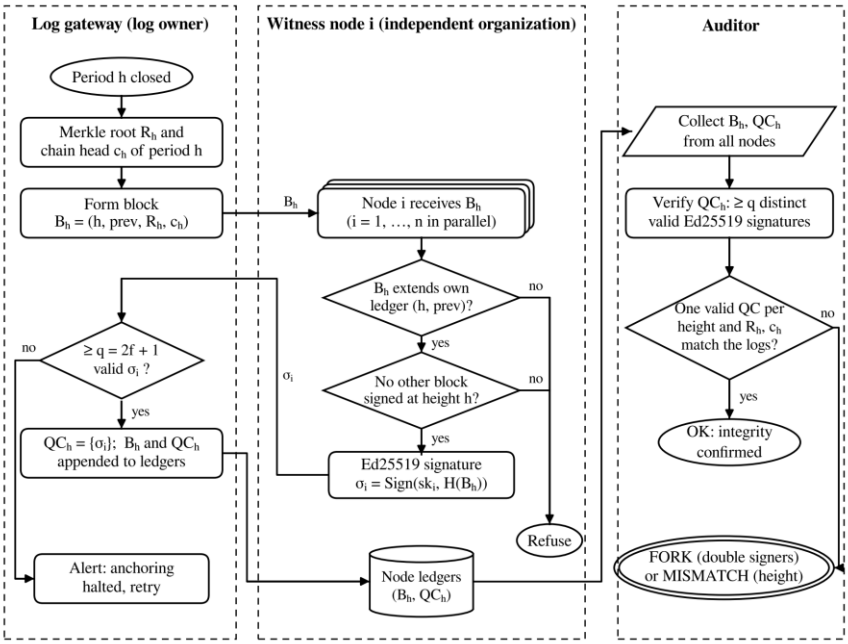


Fig. 1. Block diagram of quorum-signed anchoring and audit

Listing 1. Safety rule of a witness node (Python)

```
def vote(self, block):
    if not self.online:
        return None
    h = block_hash(block)                # SHA-256 of the block
    if not self.byzantine:
        prev = self.ledger[-1]["hash"] if self.ledger else GENESIS.hex()
        if block["height"] != len(self.ledger) or block["prev"] != prev:
            return None                  # does not extend own ledger
```

```
        if self.voted.get(block["height"], h) != h:
            return None                 # another block signed at h
    self.voted[block["height"]] = h
                                return self.sk.sign(h)          # Ed25519 signature
```

Listing 2. Quorum certificate verification by the auditor (Python)

```
def verify_qc(block, qc, registry, q):
    h, signers = block_hash(block), set()
    for name, sig in qc:
        try:
            registry[name].verify(bytes.fromhex(sig), h)
            signers.add(name)           # count each node once
        except (KeyError, InvalidSignature):
            pass                        # unknown node or bad signature
    return len(signers) >= q
```

Research results

The protocol was implemented as the quorum_witness.py program in Python 3.13 with the cryptography library (Ed25519) and hashlib (SHA-256). Nodes were run in one process, so network latency is excluded, on a Linux virtual server with two vCPUs. Two experiments were carried out.

In the first experiment, an Ed25519 signature took 39.8 μs to create and 147.5 μs to verify. One day of anchoring with a one-minute period (1440 blocks) was then committed and audited for n = 4, 7 and 10 nodes (Table 1).

Table 1

Cost of quorum signing and auditing

n	f	q	Commit time per block, ms	QC size, bytes	Audit of 1440 blocks, s
4	1	3	2.63	195	1.01
7	2	5	7.63	325	1.48
10	3	7	14.63	455	1.93

Even with ten organizations, committing a block costs less than 15 ms of computation, and the certificate (q signatures of 64 bytes plus a one-byte node identifier) stays below 0.5 KB. With a one-minute period this is less than 0.03 % of one CPU core, and a full day of anchors is audited in about 1–2 s. In a real deployment the commit latency will be dominated by one network round trip between the gateway and the nodes.

In the second experiment, a log of 6000 records was split into ten periods of 600 records, and seven scenarios were simulated (Table 2). In the rewrite scenarios, right after height 3 was committed, the log owner proposed a forged block for the same height.

Table 2

Behaviour under crash faults, collusion and tampering

Scenario	Faulty nodes	Blocks committed	Forged block	Audit result
S1. All nodes honest (n = 4)	–	10/10	–	OK
S2. Node D crashed	1 crash	10/10	–	OK
S3. Nodes C and D crashed	2 crash	0/10	–	Anchoring halted, alert
S4. Owner and node D rewrite h = 3	1 Byzantine	10/10	1 of 3 signatures, rejected	OK

S5. Owner and nodes C, D rewrite h = 3; node B was offline at h = 3	2 Byzantine	10/10	3 of 3 signatures, accepted	Fork at h = 3; C and D double-signed
S6. Same as S5 with n = 7	2 Byzantine	10/10	3 of 5 signatures, rejected	OK
S7. Owner edits record 3457 after anchoring	–	10/10	–	Mismatch at h = 5

With up to f faulty nodes the witness remained both live and safe (S2, S4). Two crashed nodes out of four stopped anchoring but never produced a wrong block (S3): the protocol prefers safety to liveness, and the halt is itself an alarm. In S5 the bound $n \geq 3f + 1$ is exceeded, and the forged block was certified. The fork, however, is not silent: the auditor found two valid certificates at height 3, and the signatures of nodes C and D in both certificates are cryptographic evidence of their misbehaviour. With seven nodes the same coalition failed (S6). Scenario S7 confirms that any later edit of an anchored record is localized to its period.

Conclusion

1. A quorum-signed permissioned witness for anchoring log integrity proofs has been designed: a node signs at most one block per height, and a block is valid with 2f + 1 Ed25519 signatures of different organizations.

2. Experiments with a working prototype showed a low cost: less than 15 ms of computation and less than 0.5 KB of certificate per block for up to ten nodes, and 1–2 s to audit one day of anchors.

3. While $n \geq 3f + 1$, neither crash faults nor collusion of the log owner with f nodes can rewrite the anchored history; beyond this bound a rewrite produces a detectable fork with proof against the double-signing nodes. At least four independent organizations are therefore recommended, and seven where collusion of two of them is plausible.

Future work will cover a networked deployment on Hyperledger Fabric with a BFT ordering service and an adaptive choice of the anchoring period.

References

12. Xabibullayev J.D., Ddos-hujumlarning oldini olishda blockchain texnologiyasining imkoniyatlarini tahlili, “Лучшие интеллектуальные исследования” международный научный электронный журнал, ЧАСТЬ-39 ТОМ-3, Февраль 2025, ISSN: 3030-3680.

13. Xabibullayev J.D., Chunayev N.E. Analysis of the capabilities of blockchain technology in data management, “Modern education and development” international interdisciplinary research journal, Volume 2, Issue 27, June 2025. – P. 355-364.

14. B. Schneier and J. Kelsey, “Secure audit logs to support computer forensics”, ACM Transactions on Information and System Security, vol. 2, no. 2, pp. 159–176, 1999.

15. S. A. Crosby and D. S. Wallach, “Efficient data structures for tamper-evident logging”, in Proc. 18th USENIX Security Symposium, 2009, pp. 317–334.

16. M. Castro and B. Liskov, “Practical Byzantine fault tolerance”, in Proc. 3rd Symposium on Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.

17. D. J. Bernstein, N. Duif, T. Lange, P. Schwabe and B.-Y. Yang, “High-speed high-security signatures”, Journal of Cryptographic Engineering, vol. 2, no. 2, pp. 77–89, 2012.

18. S. Josefsson and I. Liusvaara, “Edwards-Curve Digital Signature Algorithm (EdDSA)”, RFC 8032, IETF, Jan. 2017.

19. E. Androulaki et al., “Hyperledger Fabric: a distributed operating system for permissioned blockchains”, in Proc. 13th EuroSys Conference, 2018, Art. no. 30.

20. B. Putz, F. Menges and G. Pernul, “A secure and auditable logging infrastructure based on a permissioned blockchain”, Computers & Security, vol. 87, 101602, 2019.

21. M. Yin, D. Malkhi, M. K. Reiter, G. Golan-Gueta and I. Abraham, “HotStuff: BFT consensus with linearity and responsiveness”, in Proc. ACM PODC, 2019, pp. 347–356.

BIOMETRIK AUTENTIFIKATSIYANI JORIY ETISH ASOSIDA AXBOROT TIZIMLARIDA XAVFSIZLIK DARAJASINI OSHIRISH MODELI VA ALGORITMI

Xudoykulov Z.T., Xayrullayeva E.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada axborot tizimlarida foydalanuvchini sessiya davomida uzluksiz biometrik autentifikatsiya qilish asosida xavfsizlik darajasini oshirish modeli va algoritmi taklif etilgan. Model multimodal biometrik baholarni sifat va aniqlikka qarab birlashtiradi, ishonch darajasini vaqt bo‘yicha dinamik yangilaydi va kirish huquqlarini resurs sezgirligiga qarab adaptiv boshqaradi.

Kalit so‘zlar: uzluksiz autentifikatsiya, biometriya, ishonch darajasi, multimodal birlashtirish, xatar asosidagi kirish nazorati, FAR, FRR, EER.

Аннотация. В работе предложены модель и алгоритм повышения уровня безопасности информационных систем на основе непрерывной биометрической аутентификации пользователей в течение сессии. Модель объединяет мультимодальные биометрические оценки с учётом их качества и точности, динамически обновляет уровень доверия во времени и адаптивно управляет правами доступа в зависимости от чувствительности ресурса.

Ключевые слова: непрерывная аутентификация, биометрия, уровень доверия, мультимодальное объединение, контроль доступа на основе риска, FAR, FRR, EER.

Kirish

Axborot tizimlarida foydalanuvchini aniqlash odatda sessiya boshida bir marta (parol, token yoki biometrik namuna orqali) amalga oshiriladi. Bunday yondashuvning asosiy kamchiligi shundaki, autentifikatsiyadan keyin tizim foydalanuvchi almashganini yoki sessiya o‘g‘irlanganini sezmaydi. Sessiyani o‘g‘irlash, qurilma qarovsiz qolganda unga begona shaxsning kirishi, masofaviy ishlashdagi hisob ma’lumotlarini uzatish kabi hujumlar shu bo‘shliqdan foydalanadi.

Biometrik autentifikatsiyani joriy etish (davriy yoki uzluksiz) shu muammoni hal qiladi. Tizim sessiya davomida foydalanuvchi shaxsini passiv tarzda qayta-qayta tasdiqlab turadi. Tadqiqotning maqsadi uzluksiz biometrik autentifikatsiya asosida xavfsizlik darajasini adaptiv boshqaruvchi model va algoritm ishlab chiqishdir.

Muammoning qo‘yilishi

Foydalanuvchi sessiyasi vaqt bo‘yicha diskret lahzalar t_1, t_2, …, t_n da kuzatiladi. Har bir lahzada n ta biometrik manba (yuz, klaviatura dinamikasi, sichqoncha harakati, ovoz, mobil qurilma sensorlari) dan signal olinadi. Vazifa: har bir t lahzada foydalanuvchi qonuniy ekanligi ehtimolini baholash va shu bahoga qarab kirish huquqlarini dinamik boshqarish orqali quyidagi ikki ko‘rsatkichni birgalikda yaxshilash:

– xavfsizlik: begona shaxsning qabul qilinish ehtimoli (FAR) pasayadi;
– qulaylik: qonuniy foydalanuvchining keraksiz bloklanishi (FRR) minimal bo‘ladi.

Taklif etilayotgan model

Model to‘rt modul va ishonch darajasi (trust score) tushunchasiga tayanadi.

Biometrik ma’lumot yig‘ish va sifatni baholash. Har bir i-modallik uchun moslik bahosi $s_i(t) \in [0, 1]$ va namuna sifati $q_i(t) \in [0, 1]$ aniqlanadi. Sifati past namunalar (yomon yoritilish, shovqin, kam bosilgan tugmalar) natijaga kam ta’sir qiladi.

Multimodal birlashtirish (score-level fusion). Birlashgan baho vaznli yig‘indi sifatida hisoblanadi:

$$S(t) = \Sigma w_i \cdot q_i(t) \cdot s_i(t) / \Sigma w_i \cdot q_i(t),$$

bu yerda $w_i = (1/EER_i) / \Sigma_j(1/EER_j)$, ya’ni xatosi kam modallikka katta vazn beriladi.

Ishonch darajasining dinamik yangilanishi. Yangi namuna bo‘lmagan vaqt oralig‘ida ishonch eksponensial so‘nadi, yangi namuna kelganda esa tekislanib yangilanadi:

$$T(t_k) = \lambda \cdot T(t_{k-1}) \cdot e^{(-\gamma \cdot \Delta t)} + (1 - \lambda) \cdot S(t_k),$$

bu yerda $\lambda \in (0, 1)$ tarixning ta’sir darajasi, γ ishonchning vaqt bo‘yicha so‘nish tezligi, $\Delta t = t_k - t_{k-1}$. Bu formula bitta noto‘g‘ri bahodan kelib chiqadigan yolg‘on blokirovkalarni yumshatadi, biroq uzoq muddat biometrik kuzatuv bo‘lmasa, ishonchni baribir pasaytiradi.

Xatarga asosli kirish siyosati. Har bir resursga sezgirlik darajasi $R \in [0, 1]$ beriladi (masalan, ochiq ma’lumot 0.1, moliyaviy operatsiya 0.9). Dinamik chegaralar:

$$\theta_yuqori(R) = \theta_0 + \alpha \cdot R, \quad \theta_quyi = \beta \cdot \theta_yuqori(R).$$

Qaror qoidasi:

– $T \geq \theta$_yuqori: to‘liq kirish;

– θ_quyi $\leq T < \theta$_yuqori: cheklangan kirish va qo‘shimcha tekshiruv (step-up autentifikatsiya: parol, OTP);

– $T < \theta$_quyi: sessiyani bloklash va xavfsizlik hodisasini qayd etish.

Algoritm

1. Sessiya boshlanganda boshlang‘ich autentifikatsiya o‘tkaziladi va $T(t_0) = T_0$ o‘rnatiladi.
2. Har $\Delta\tau$ oraliqda (yoki voqealar bo‘yicha) mavjud modalliklardan s_i va q_i olinadi.
3. Sifati $q_i < q_min$ bo‘lgan namunalar chiqarib tashlanadi.
4. S(t) vaznli birlashtirish orqali hisoblanadi.
5. T(t) so‘nish va tekislash formulasi bilan yangilanadi.
6. So‘ralayotgan resursning R qiymatiga qarab θ_yuqori va θ_quyi aniqlanadi.
7. Qaror qabul qilinadi: ruxsat berish, step-up yoki bloklash.
8. Barcha qarorlar audit jurnaliga yoziladi; foydalanuvchi qayta tasdiqlansa T yangilanadi.
9. Sessiya tugamaguncha 2-bosqichdan takrorlanadi.

Algoritmning hisoblash murakkabligi bir iteratsiyada O(n) (n modallik soni), shuning uchun u real vaqt rejimida ishlay oladi.

Kutilayotgan natijalar va baholash

Modelni baholash uchun ISO/IEC 19795 bo‘yicha FAR, FRR, EER, shuningdek hujumni aniqlash vaqti (time-to-detect) va sessiyadagi o‘rtacha uzilishlar soni ishlatiladi. Ochiq to‘plamlarda (masalan, klaviatura dinamikasi va sichqoncha harakati ma’lumotlari) simulyatsiya qilinganda quyidagi natijalar kutiladi:

– bitta modallikka nisbatan EER ning sezilarli kamayishi (multimodal birlashtirish hisobiga);

– bir martalik autentifikatsiyaga nisbatan hujumni aniqlash vaqtining keskin qisqarishi;

– xatarga asoslangan chegaralar tufayli qonuniy foydalanuvchi uchun noqulayliklarning kamayishi.

Xulosa

Taklif etilgan model biometrik autentifikatsiyani sessiya boshidagi bir martalik tekshiruvdan uzluksiz jarayonga aylantiradi. Ishonch darajasining dinamik yangilanishi, sifat va aniqlikka asoslangan multimodal birlashtirish hamda resurs sezgirligiga bog‘liq adaptiv chegaralar xavfsizlik darajasini oshiradi va foydalanuvchi qulayligini saqlaydi. Keyingi tadqiqotlar yo‘nalishi: biometrik shablonlarni himoyalash (template protection), yashirin hujumlarga (spoofing, deepfake) qarshi liveness-tekshiruv va maxfiylikni saqlovchi federativ o‘qitish.

Foydalanilgan adabiyotlar

1. Jain A.K., Ross A., Prabhakar S. An Introduction to Biometric Recognition // IEEE Transactions on Circuits and Systems for Video Technology, 2004.

2. Sim T., Zhang S., Janakiraman R., Kumar S. Continuous Verification Using Multimodal Biometrics // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007.

3. Niinuma K., Park U., Jain A.K. Soft Biometric Traits for Continuous User Authentication // IEEE Transactions on Information Forensics and Security, 2010.

4. ISO/IEC 19795-1: Biometric performance testing and reporting.

5. NIST SP 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management.

SUN’IY INTELLEKT YORDAMIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH

Norboboyeva G.Z.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda kompyuter tarmoqlarida uchraydigan zamonaviy kiberhujumlarni aniqlashda sun’iy intellekt texnologiyalaridan foydalanish imkoniyatlari tahlil qilinadi. An’anaviy axborot xavfsizligi vositalarining imkoniyatlari va cheklovlari ko‘rib chiqilib, mashinali o‘rganish hamda chuqur o‘rganish algoritmlarining tarmoq trafigidagi shubhali faoliyatni aniqlashdagi ahamiyati yoritiladi. Shuningdek, sun’iy intellekt asosidagi hujumlarni aniqlash tizimlarining samaradorligi, mavjud muammolari va ularni takomillashtirish yo‘llari bayon etiladi.

Kalit so‘zlar: Axborot xavfsizligi, sun’iy intellekt, kiberxavfsizlik, kiberhujum, kompyuter tarmoqlari, mashinali o‘rganish, tarmoq trafigi, anomaliyalarni aniqlash.

Аннотация. В данной работе анализируются возможности использования технологий искусственного интеллекта для обнаружения современных кибератак на компьютерные сети. Рассматриваются возможности и ограничения традиционных средств информационной безопасности, а также подчеркивается важность алгоритмов машинного обучения и глубокого обучения в обнаружении подозрительной активности в сетевом трафике. Описывается также эффективность систем обнаружения атак на основе искусственного интеллекта, существующие проблемы и пути их улучшения.

Ключевые слова: Информационная безопасность, искусственный интеллект, кибербезопасность, кибератака, компьютерные сети, машинное обучение, сетевой трафик, обнаружение аномалий.

Kirish

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida davlat tashkilotlari, bank-moliya muassasalari, ta’lim tizimi va xususiy korxonalar faoliyatida kompyuter tarmoqlaridan foydalanish ko‘lami ortib bormoqda. Axborot almashinuvi va ma’lumotlarni masofadan qayta ishlash imkoniyatlarining kengayishi bilan bir qatorda, axborot tizimlariga nisbatan kiberhujumlar xavfi ham kuchaymoqda.Kiberhujumlar axborotning maxfiyligi, yaxlitligi va mavjudligiga tahdid soladi. Jumladan, zararli dasturlar, xizmat ko‘rsatishni rad etish hujumlari (DoS/DDoS), fishing, parollarni taxmin qilish va tarmoqdagi zaifliklardan foydalanish tashkilotlarning axborot resurslariga jiddiy zarar yetkazishi mumkin.

An’anaviy himoya vositalari, xususan, imzoga asoslangan hujumlarni aniqlash tizimlari avvaldan ma’lum bo‘lgan tahdidlarni aniqlashda samarali hisoblanadi. Biroq yangi yoki o‘zgartirilgan hujumlar mavjud qoidalar va imzolar orqali aniqlanmasligi mumkin. Shu sababli tarmoq faoliyatini tahlil qilish, odatiy xatti-harakatlardan chetlanishlarni aniqlash va yangi tahdidlarni baholash imkoniyatiga ega bo‘lgan intellektual usullarga ehtiyoj ortmoqda.Mazkur tadqiqotning maqsadi sun’iy intellekt, xususan, mashinali o‘rganish algoritmlaridan foydalanib, kompyuter tarmoqlaridagi kiberhujumlarni aniqlash usullarini o‘rganish va ularning afzalliklari hamda cheklovlarini tahlil qilishdan iborat.

Asosiy qism

Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash uchun xavfsizlik devorlari (firewall), hujumlarni aniqlash tizimlari (IDS) va hujumlarning oldini olish tizimlari (IPS) kabi vositalardan foydalaniladi. Ushbu vositalar tarmoq trafigini belgilangan qoidalar, xavfsizlik siyosatlari va ma’lum hujumlarning belgilariga muvofiq tekshiradi.Imzoga asoslangan aniqlash usulida tarmoq paketlari yoki hodisalar ma’lum hujum namunalari bilan solishtiriladi. Ushbu yondashuv ilgari aniqlangan tahdidlarni tezkor aniqlash imkonini beradi. Uning asosiy cheklovi yangi, noma’lum yoki sezilarli darajada o‘zgartirilgan hujumlarni aniqlash qobiliyatining cheklanganligidir.

Anomaliyaga asoslangan aniqlash usulida esa tarmoqning odatiy faoliyati o‘rganilib, undan sezilarli farq qiluvchi holatlar shubhali deb baholanadi. Bunday usul yangi tahdidlarni aniqlashda foydali bo‘lishi mumkin, ammo qonuniy faoliyatdagi noodatiy o‘zgarishlar ham noto‘g‘ri ogohlantirishlarni keltirib chiqarishi ehtimoli mavjud.Shu nuqtayi nazardan, an’anaviy xavfsizlik vositalarini sun’iy intellektga asoslangan tahlil usullari bilan birlashtirish tarmoq himoyasining samaradorligini oshirishga xizmat qilishi mumkin.

Sun’iy intellekt kompyuter tizimlariga ma’lumotlarni tahlil qilish, qonuniyatlarni aniqlash va muayyan vazifalar bo‘yicha qarorlarni qo‘llab-quvvatlash imkonini beruvchi texnologiyalar majmuasidir. Kiberxavfsizlik sohasida uning muhim yo‘nalishlaridan biri mashinali o‘rganish hisoblanadi.Mashinali o‘rganish algoritmlari tarmoq trafigi, ulanishlar soni, paketlar hajmi, ulanish davomiyligi, protokollar va boshqa xususiyatlar asosida normal hamda shubhali faoliyatni farqlash uchun o‘qitilishi mumkin.Kiberhujumlarni aniqlashda quyidagi algoritmlardan foydalanish mumkin:Ushbu yondashuvda algoritm oldindan belgilangan sinflarga ajratilgan ma’lumotlar asosida o‘qitiladi. Masalan, tarmoq ulanishlari “normal” va “hujum” sinflariga ajratilishi mumkin. Qaror daraxtlari (Decision Tree), Random Forest va Support Vector Machine (SVM) kabi algoritmlar ushbu vazifada qo‘llanilishi mumkin.

Ushbu usulda ma’lumotlarning oldindan belgilangan sinflari talab qilinmaydi. Klasterlash va boshqa anomaliyalarni aniqlash algoritmlari tarmoqdagi noodatiy xatti-harakatlarni topishda yordam beradi. Masalan, K-means klasterlash algoritmi o‘xshash tarmoq ulanishlarini guruhlash uchun ishlatilishi mumkin. Biroq klasterlashning o‘zi har doim ham hujum mavjudligini tasdiqlamaydi.Neyron tarmoqlar katta hajmdagi va murakkab tuzilishga ega ma’lumotlarni tahlil qilishda qo‘llaniladi. Ular vaqt bo‘yicha ketma-ketliklarni yoki murakkab bog‘liqliklarni o‘rganishi mumkin. Shu bilan birga, bunday modellarni o‘qitish uchun ko‘proq hisoblash resurslari, sifatli ma’lumotlar va ehtiyotkor sozlash talab etiladi.Sun’iy intellektga asoslangan hujumlarni aniqlash tizimini yaratish bir necha bosqichdan iborat.Birinchi bosqichda tarmoq trafigi yoki xavfsizlik jurnallari (loglar) yig‘iladi. Ma’lumotlar qonuniy va ruxsat etilgan manbalardan olinishi, shaxsiy ma’lumotlarni himoya qilish talablariga rioya etilishi lozim.Ikkinchi bosqichda ma’lumotlar dastlabki qayta ishlashdan o‘tkaziladi. Takroriy yozuvlar, yetishmayotgan qiymatlar va texnik xatolar tekshiriladi. Shundan so‘ng model uchun muhim xususiyatlar tanlanadi.Uchinchi bosqichda tegishli algoritm tanlanib, mavjud ma’lumotlar asosida o‘qitiladi. Model samaradorligini xolis baholash uchun ma’lumotlar o‘qitish, validatsiya va test to‘plamlariga ajratilishi kerak. Ma’lumotlar to‘plamida o‘qitish va test davrlariga tegishli yozuvlarning o‘zaro aralashib ketishi natijalarni sun’iy ravishda yaxshilab ko‘rsatishi mumkin. Shu sababli ma’lumotlarni ajratish usuli tadqiqot maqsadiga mos tanlanishi zarur. To‘rtinchi bosqichda model yangi tarmoq ma’lumotlarini tahlil qilib, shubhali hodisalarni belgilaydi. Zarurat tug‘ilganda, aniqlangan hodisalar xavfsizlik mutaxassisi tomonidan tekshiriladi. Muhim tizimlarda avtomatik bloklash kabi choralarni qo‘llashdan oldin noto‘g‘ri qarorlarning ehtimoliy oqibatlari ham baholanishi kerak.Beshinchi bosqichda modelning natijalari muntazam kuzatilib, yangi ma’lumotlar asosida uning ishlashi qayta baholanadi. Chunki tarmoqdan foydalanish xususiyatlari va hujum usullari vaqt o‘tishi bilan o‘zgarishi mumkin.

Sun’iy intellekt modelining samaradorligini faqat umumiy aniqlik ko‘rsatkichi bilan baholash yetarli emas. Ayniqsa, hujumlar soni normal tarmoq ulanishlariga nisbatan kam bo‘lgan holatlarda yuqori aniqlik ko‘rsatkichi modelning barcha hujumlarni yaxshi aniqlashini anglatmaydi.

Shu sababli quyidagi mezonlardan foydalanish maqsadga muvofiq:Accuracy (umumiy aniqlik) - to‘g‘ri tasniflangan barcha holatlarning umumiy namunalar soniga nisbati.Precision (aniq ijobiy natija ulushi) - hujum deb belgilangan holatlarning qanchasi haqiqatan hujum ekanini ko‘rsatadi.

Recall (sezgirlik) - mavjud hujumlarning qanchasi to‘g‘ri aniqlanganini ifodalaydi.F1-score - precision va recall ko‘rsatkichlari o‘rtasidagi muvozanatni ifodalaydi.False Positive Rate - normal faoliyatning noto‘g‘ri ravishda hujum sifatida belgilanish darajasi.Ushbu ko‘rsatkichlar birgalikda tahlil qilinsa, modelning turli sharoitlardagi imkoniyatlarini aniqroq baholash mumkin. Shuningdek, real vaqt rejimida aniqlash kechikishi va hisoblash xarajatlarini ham hisobga olish zarur.

Sun’iy intellekt asosidagi hujumlarni aniqlash tizimlarida bir qator muammolar mavjud. Birinchidan, o‘qitish ma’lumotlari yetarli bo‘lmasligi yoki real tarmoq sharoitlarini to‘liq aks ettirmasligi mumkin. Ikkinchidan, normal va zararli faoliyat o‘rtasidagi farqlarni aniqlash murakkab bo‘lishi mumkin. Uchinchidan, noto‘g‘ri ogohlantirishlarning ko‘pligi xavfsizlik mutaxassislarining ish yukini oshiradi.Bundan tashqari, tajovuzkorlar mashinali o‘rganish modellarini chalg‘itishga qaratilgan usullardan foydalanishi mumkin. Shu sababli modelning ishonchliligini tekshirish, ma’lumotlarni himoyalash va tizimni muntazam yangilab borish muhimdir.Mazkur muammolarni kamaytirish uchun sifatli va xilma-xil ma’lumotlar to‘plamlaridan foydalanish, turli algoritmlarni taqqoslash, modelni mustaqil test ma’lumotlarida sinash hamda natijalarni xavfsizlik mutaxassislari bilan birgalikda tekshirish tavsiya etiladi. Sun’iy intellektni an’anaviy xavfsizlik vositalari bilan birgalikda qo‘llash ham himoya tizimining ishonchliligini oshirishga yordam berishi mumkin.

Xulosa

O‘tkazilgan tahlil shuni ko‘rsatadiki, sun’iy intellekt va mashinali o‘rganish texnologiyalari kompyuter tarmoqlaridagi kiberhujumlarni aniqlash imkoniyatlarini kengaytiradi. Ushbu texnologiyalar tarmoq trafigidagi murakkab qonuniyatlarni o‘rganish, shubhali faoliyatni aniqlash va xavfsizlik hodisalarini saralashda foydali vosita bo‘lib xizmat qilishi mumkin.Biroq sun’iy intellektga asoslangan tizimlar barcha kiberhujumlarni mutlaq aniqlik bilan aniqlay olmaydi. Ularning samaradorligi ma’lumotlar sifati, algoritm tanlovi, modelni baholash usuli va real tarmoq sharoitlariga bog‘liq. Shuning uchun bunday tizimlarni joriy etishda aniqlik, sezgirlik, noto‘g‘ri ogohlantirishlar soni va ishlash tezligini birgalikda baholash zarur.

Xulosa qilib aytganda, sun’iy intellektni an’anaviy himoya vositalari, muntazam monitoring va mutaxassis nazorati bilan birlashtirish zamonaviy kompyuter tarmoqlarida axborot xavfsizligini mustahkamlashning istiqbolli yo‘nalishlaridan biridir.

Foydalanilgan adabiyotlar:

1. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016.
2. Sommer, R., Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. 2010 IEEE Symposium on Security and Privacy, 2010, pp. 305–316.
3. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, 2007.
4. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1, 2023.
5. Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116.

KORPORATIV TARMOQLARDA KOMPYUTER XAVFSIZLIGI MUAMMOSI VA ZAMONAVIY HIMOYA YONDASHUVLARI

Sayfullayev Sh.B.
Muhammad al-Xorazmiy nomidagi nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu tezisda korporativ tarmoqlarda kompyuter xavfsizligining dolzarb muammolari va ularga qarshi zamonaviy himoya yondashuvlari tahlil qilingan. Raqamli texnologiyalarning jadal rivojlanishi fonida global va O‘zbekiston miqyosida kiberhujumlarning keskin ortishi statistik ma’lumotlar (2021-2024-yillar) asosida ko‘rsatib o‘tilgan. An’anaviy perimetr himoyasi modelining samarasizligi sababli, muallif tomonidan Zero Trust Architecture (ZTA) - “hech kimga, hech narsaga ishonma, hamma narsani tekshir” tamoyili hamda mikrosegmentatsiya usullarini joriy etish taklif qilingan. Shuningdek, zamonaviy himoya vositalarining qiyosiy tahlili keltirilgan bo‘lib, “Raqamli O‘zbekiston - 2030” strategiyasi doirasida korporativ xavfsizlikni ta'minlashning muhimligi ta’kidlangan.

Kalit so‘zlar: kiberxavfsizlik, korporativ tarmoqlar, kiberhujumlar, Zero Trust Architecture (ZTA), mikrosegmentatsiya, zamonaviy tahdidlar, perimetr himoyasi, APT hujumlari.

Аннотация: В данных тезисах анализируются актуальные проблемы компьютерной безопасности в корпоративных сетях и современные подходы к защите. На фоне стремительного развития цифровых технологий на основе статистических данных (2021-2024 гг.) показан резкий рост кибератак в глобальном масштабе и в Узбекистане. В связи с неэффективностью традиционной модели защиты периметра автор предлагает внедрение архитектуры нулевого доверия (Zero Trust Architecture - ZTA) - принципа «никому и ничему не доверяй, всё проверяй», а также методов микросегментации. Также представлен сравнительный анализ современных средств защиты и подчеркнута важность обеспечения корпоративной безопасности в рамках стратегии «Цифровой Узбекистан – 2030».

Ключевые слова: кибербезопасность, корпоративные сети, кибератаки, архитектура нулевого доверия (ZTA), микросегментация, современные угрозы, защита периметра, APT-атаки

Kirish

Raqamli texnologiyalarning jadal rivojlanishi korporativ infratuzilmalarni tobora murakkab va zaifroq qilmoqda. 2024-yilda global miqyosda kiberxavfsizlik sohasida qayd etilgan yo‘qotishlar 9.5 trln AQSh dollarini tashkil etdi va bu ko‘rsatkich 2025-yilda 10.5 trln dollarga yetishi kutilmoqda. O‘zbekiston ham ushbu global muammodan chetda qolmayapti; statistik ma'lumotlarga ko‘ra, mamlakatimizda kiberhujumlar soni so‘nggi ikki yil ichida 5 barobardan ortiq oshgan bo‘lib, 2024-yilda taxminan 16 800 000 ta hujum qayd etilgan.

1-jadval.

O‘zbekistonda qayd etilgan kiberhujumlar soni (2021–2024)

Yil	Hujumlar soni	O‘tgan yilga nisbatan o‘sish
2021	2 100 000	-
2022	4 500 000	+114%
2023	11 200 000	+149%
2024	16 800 000 (taxminiy)	+50%

Muammoning qo‘yilishi va zamonaviy tahdidlar xususiyati

Zamonaviy kibertahdidlar asosan murakkablashgan, avtomatlashtirilgan va ko‘p vektorli xususiyatga ega. Hozirgi hujumlar ko‘p bosqichli bo‘lib, Advanced Persistent Threat (APT) guruhlari maqsadli tashkilotning tizimida o‘rtacha 207 kun davomida aniqlanmay faoliyat yuritadi.

2-jadval.

Korporativ tarmoqlarga xos tahdidlar tasnifi

1. Tashqi tahdidlar	2. Ichki tahdidlar	3. Tarmoq infratuzilmasi	4. Ta’minot zanjiri
- Ransomware - DDoS - Phishing / Social Eng. - Zero-day zaifliklar	- Xodimlar xatolari - Zararli xodimlar - Hisob ma'lumotlari o‘g‘irlanishi	- MitM hujumlari - ARP / DNS spoofing - Lateral movement - Privilege escalation	- Dasturiy ta'minot zaifliklari - Uchinchi tomon xizmatlari - Shadow IT qurilmalari

Yechim va zamonaviy himoya arxitekturasi. Bugungi kunda bulutli xizmatlar, masofaviy ish va mobil qurilmalarning keng tarqalishi an'anaviy perimetr himoyasi (“qal’a va xandaq”) modelini samarasiz qilib qo‘ydi. Buning o‘rniga zamonaviy Zero Trust Architecture (ZTA) - “hech kimga, hech narsaga ishonma, hamma narsani tekshir” tamoyiliga o‘tish talab etiladi.



1-rasm. Zero Trust Arxitekturasining soddalashtirilgan ishlash sxemasi

ZTA doirasida eng samarali yechimlardan biri bu mikrosegmentatsiya hisoblanadi. Tarmoqni graflar nazariyasi asosida mayda, izolyatsiyalangan xavfsizlik domenlariga bo‘lish orqali lateral movement hujumlarini samarali cheklash va inson omilidan kelib chiqadigan zarar ko‘lamini minimallashtirish mumkin.



2-rasm. Mikrosegmentatsiya orqali tarmoqning mantiqiy bo‘linishi

3-jadval.

Zamonaviy himoya vositalarining qiyosiy tahlili

Himoya vositasi	Asosiy funksiyasi	Zaif tomonlari	Tavsiya etiladigan qo‘shimcha yechim
Firewall	Perimetr himoyasi	Ichki tahdidlarga qarshi samarasiz	Domenlar chegarasida qo‘llash
IDS/IPS	Hujumlarni aniqlash	Noma'lum hujumlarni aniqlay olmaydi	Intellektual monitoring tizimi
ACL	Kirishni nazorat qilish	Statik, moslashuvchanligi past	Dinamik domenlar bilan almashtirish
SIEM	Hodisalarni boshqarish	Katta hajmdagi ma’lumotlar tahlili qiyin	Grafga asoslangan tahlil

VPN	Shifrlangan ulanish	Lateral movement'dan himoyalamaydi	Domenlar segmentatsiyasi
Antivirus	Zararli dasturlarni aniqlash	Zero-day hujumlarga qarshi zaif	Tizimli yondashuv komponenti

Xulosa qilib aytganda, korporativ tarmoqlar xavfsizligini ta’minlash faqat texnologik vositalarni joriy etish bilan cheklanib qolmasdan, balki arxitekturaviy va protsedural yondashuvlarni ham talab qiladi. O‘zbekiston Respublikasining “Raqamli O‘zbekiston - 2030” strategiyasi va kiberxavfsizlik sohasidagi qonunchilik talablari doirasida, korporativ tarmoqlarda Zero Trust arxitekturasini hamda domenli mikrosegmentatsiyani joriy etish orqali zamonaviy murakkab kiberhujumlarga qarshi mustahkam proaktiv himoyani shakllantirish zarur.

Foydalanilgan adabiyotlar ro‘yhati

1. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston - 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni.

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni hamda kiberxavfsizlikni kuchaytirish bo'yicha tegishli PQ-153-son qarori.

3. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. National Institute of Standards and Technology.

4. MITRE Corporation. (2024). *MITRE ATT&CK® Framework*. (Elektron resurs: attack.mitre.org).

YURAK-QON TOMIR KASALLIKLARINI TASHXISLASHDA FEDERATIV O‘QITISH VA KRIPTOGRAFIK HIMOYA ASOSIDA BEMOR MA’LUMOTLARI XAVFSIZLIGINI TA’MINLASH

Seidullayev M.K.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Jumatashov A.B.
M. Auezov nomidagi Janubiy Qozog‘iston universitetining Chirchiq shahridagi filiali

Annotatsiya. Mazkur ishda yurak-qon tomir kasalliklarini sun’iy intellekt asosida tashxislash jarayonida bemorlarning tibbiy ma’lumotlari maxfiyligini ta’minlash masalasi o‘rganiladi. Federativ o‘qitish texnologiyasi asosida turli tibbiyot muassasalarida saqlanayotgan ma’lumotlarni markazlashtirmasdan yagona diagnostika modelini shakllantirish imkoniyati tahlil qilinadi. Elektrokardiogramma (EKG), fotopletizmografiya (PPG), fonokardiogramma (PCG) va elektron tibbiy yozuvlarga asoslangan yondashuvlarning xususiyatlari qiyoslanadi. Tibbiy ma’lumotlarni uzatishda shifrlash, foydalanuvchilarni autentifikatsiya qilish, xavfsiz agregatsiya va differensial maxfiylik mexanizmlarini birlashtiruvchi himoyalangan interaktiv diagnostika tizimining konseptual arxitekturasi taklif etiladi. Tizimning samaradorligini baholash uchun diagnostik sifat, aloqa xarajatlari va axborot xavfsizligi ko‘rsatkichlari belgilab beriladi.

Kalit so‘zlar: sun’iy intellekt, yurak-qon tomir kasalliklari, federativ o‘qitish, kiberxavfsizlik, kriptografik himoya, EKG, tibbiy ma’lumotlar, differensial maxfiylik, xavfsiz agregatsiya.

Аннотация. В данной работе рассматривается проблема обеспечения конфиденциальности медицинских данных пациентов при диагностике сердечно-сосудистых заболеваний на основе искусственного интеллекта. Анализируется возможность формирования единой диагностической модели с использованием технологии федеративного обучения без централизованного сбора данных, хранящихся в различных медицинских учреждениях. Проводится сравнительный анализ подходов, основанных на электрокардиограмме (ЭКГ), фотоплетизмографии (ФПГ), фонокардиограмме (ФКГ) и электронных медицинских записях. Предлагается концептуальная архитектура защищённой интерактивной диагностической системы, объединяющая механизмы шифрования данных при передаче, аутентификации пользователей, безопасной агрегации и дифференциальной приватности. Для оценки эффективности системы определяются показатели качества диагностики, коммуникационных затрат и информационной безопасности.

Ключевые слова: искусственный интеллект, сердечно-сосудистые заболевания, федеративное обучение, кибербезопасность, криптографическая защита, ЭКГ, медицинские данные, дифференциальная приватность, безопасная агрегация.

Kirish

Yurak-qon tomir kasalliklarini erta aniqlash va ularning rivojlanish xavfini baholash zamonaviy tibbiyotning muhim ilmiy-amaliy vazifalaridan biridir. Sun’iy intellekt algoritmlari elektrokardiogramma signallari, fiziologik ko‘rsatkichlar va elektron tibbiy yozuvlarni tahlil qilish orqali diagnostik qarorlarni qo‘llab-quvvatlash imkonini beradi. Biroq bunday tizimlarni amaliyotga joriy etish nafaqat diagnostik aniqlik, balki bemorlarning shaxsiy ma’lumotlarini

himoyalash, ma’lumotlar yaxlitligini ta’minlash va ruxsatsiz foydalanishning oldini olishni ham talab qiladi.

Markazlashtirilgan mashinali o‘qitish yondashuvida turli tibbiyot muassasalariga tegishli ma’lumotlar yagona serverga uzatilishi mumkin. Bunday arxitektura ma’lumotlar sizib chiqishi va markaziy serverga qaratilgan kiberhujumlar xavfini oshiradi. Ushbu muammoning istiqbolli yechimlaridan biri federativ o‘qitish (Federated Learning, FL) hisoblanadi. Unda model har bir muassasada mahalliy ma’lumotlar asosida o‘qitiladi va umumiy modelni yangilash uchun parametrlar yoki gradientlar uzatiladi.

Ryu va hammualliflarning 2025-yilda *Healthcare* jurnalida chop etilgan tadqiqotida yurak-qon tomir kasalliklarini bashorat qilish bo‘yicha 28 ta ilmiy ish, jumladan, 17 ta biosignalga va 11 ta elektron tibbiy yozuvlarga asoslangan tadqiqot tahlil qilingan [1]. Ushbu natijalar federativ o‘qitishning tibbiy diagnostikada qo‘llanilishini ma’lumotlar turiga mos ravishda loyihalash zarurligini ko‘rsatadi.

Tadqiqotning maqsadi yurak-qon tomir kasalliklarini tashxislashda bemor ma’lumotlarining maxfiyligini saqlashga yo‘naltirilgan federativ o‘qitish va kriptografik himoya mexanizmlariga asoslangan interaktiv diagnostika tizimining konseptual modelini ishlab chiqish.

Tadqiqot metodologiyasi va qiyosiy tahlil

Tadqiqotning nazariy asosini federativ o‘qitish, tibbiy ma’lumotlarni himoyalash va sun’iy intellekt yordamida klinik qarorlarni qo‘llab-quvvatlashga oid ilmiy ishlar tashkil etadi. Asosiy manba sifatida Ryu va hammualliflarning [1] sharh maqolasi tanlandi.

1-jadval.

Yurak-qon tomir kasalliklarini tashxislashda federativ o‘qitish yondashuvlarining qiyosiy tahlili

Tahlil mezoni	Biosignallarga asoslangan yondashuv	Elektron tibbiy yozuvlarga asoslangan yondashuv
Asosiy ma’lumotlar	EKG, PPG, PCG	Tashxislar, laboratoriya natijalari, klinik yozuvlar
Asosiy vazifa	Yurak ritmi va fiziologik signallarni tahlil qilish	Kasallik xavfini baholash va klinik qarorni qo‘llab-quvvatlash
Manbadagi tadqiqotlar soni	17 ta	11 ta
Asosiy texnik muammolar	Signallar farqi, vaqtga sezgirlik, qurilmalararo tafovut	Ma’lumotlar formati va klinik taqsimotning farqlanishi
Federativ yondashuvdagi imkoniyat	Shaxsiylashtirilgan monitoring va tezkor tahlil	Ko‘p markazli ma’lumotlardan birgalikda foydalanish
Muhim xavfsizlik talabi	Qurilmalar va uzatiladigan model yangilanishlarini himoyalash	Kirishni boshqarish va xavfsiz agregatsiya
Taklif etiladigan himoya	Shifrlangan aloqa, autentifikatsiya, zaruratda differensial maxfiylik	Shifrlash, xavfsiz agregatsiya, audit va rollarga asoslangan kirish

Jadvaldan ko‘rinadiki, biosignallarga asoslangan tizimlar uzluksiz monitoring va tezkor tahlil uchun, elektron tibbiy yozuvlarga asoslangan tizimlar esa ko‘p markazli klinik ma’lumotlarni umumlashtirish uchun qulay. Biroq har ikkala yondashuvda ham mahalliy ma’lumotlar taqsimotining farqlanishi modelning umumlashtirish qobiliyatiga ta’sir qilishi

mumkin. Shu sababli tizimni ishlab chiqishda ma’lumotlar turiga mos o‘qitish algoritmlari va himoya mexanizmlarini tanlash zarur.

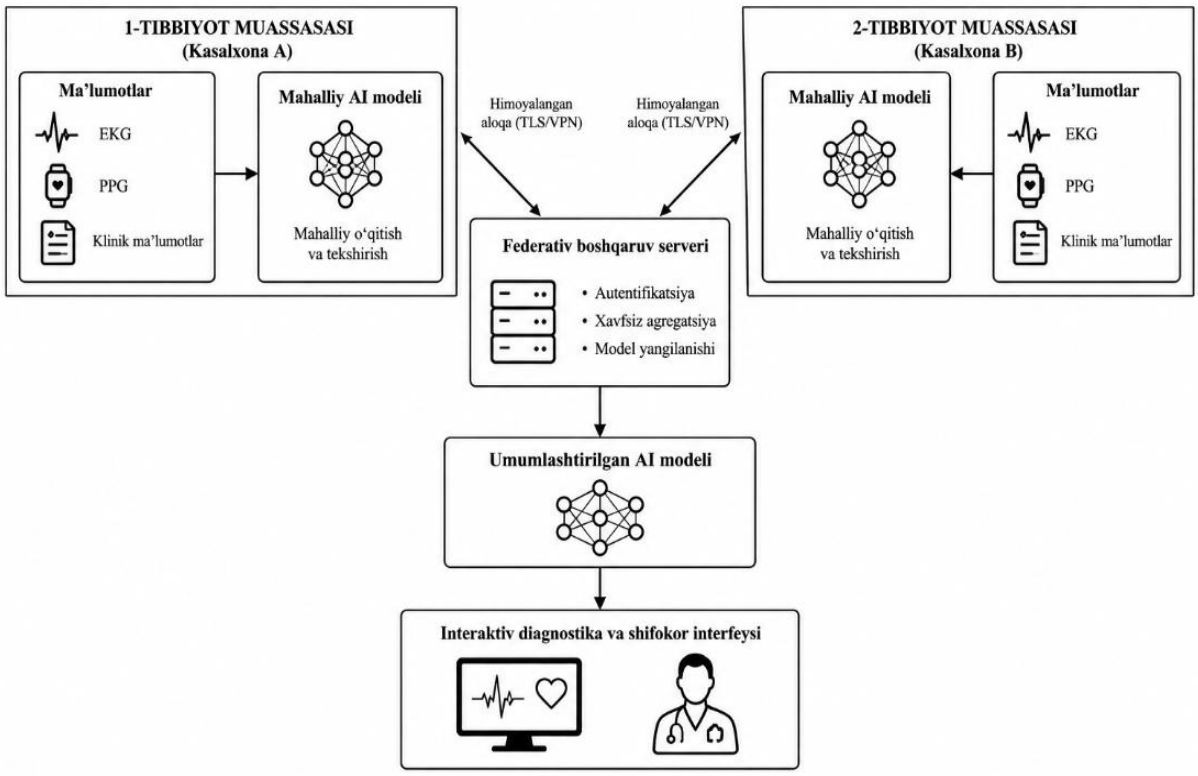
Taklif etilayotgan tizim arxitekturasi

Tadqiqot doirasida federativ o‘qitish, kriptografik himoya va interaktiv diagnostika modullarini birlashtiruvchi konseptual arxitektura taklif etiladi.

Tizim quyidagi asosiy modullardan tashkil topadi:

1. Ma’lumotlarni yig‘ish moduli. EKG, PPG va boshqa fiziologik signallar, shuningdek, tegishli klinik ko‘rsatkichlar yig‘iladi va dastlabki qayta ishlashdan o‘tkaziladi.

2. Mahalliy o‘qitish moduli. Har bir tibbiyot muassasasi o‘z ma’lumotlari asosida sun’iy intellekt modelini o‘qitadi. Bemorlarning dastlabki yozuvlari boshqa muassasalarga yuborilmaydi.



1-rasm. Yurak-qon tomir kasalliklarini xavfsiz tashxislashning taklif etilayotgan arxitekturasi

3. Xavfsizlik moduli. Muassasalar va server o‘rtasidagi aloqa shifrlanadi, foydalanuvchilar autentifikatsiya qilinadi, kirish huquqlari tekshiriladi. Model yangilanishlari uchun ham yaxlitlikni tekshirish va ruxsatsiz o‘zgartirishlardan himoyalash mexanizmlari qo‘llanadi.

4. Federativ agregatsiya moduli. Mahalliy model yangilanishlari birlashtirilib, umumiy model hosil qilinadi. Masalan, FedAvg algoritmi ishtirokchilar modellari parametrlarini mahalliy ma’lumotlar hajmiga mos vaznlarda birlashtirish uchun ishlatilishi mumkin.

5. Interaktiv diagnostika moduli. Umumiy model klinik signallarni tahlil qiladi va shifokorga xavf ko‘rsatkichlari, ehtimoliy anomaliyalar hamda qarorni izohlashga yordam beruvchi ma’lumotlarni taqdim etadi.

Ushbu arxitekturaning asosiy xususiyati shundaki, dastlabki tibbiy ma’lumotlar mahalliy muassasada saqlanadi, o‘qitish jarayoni esa muassasalararo hamkorlik asosida tashkil etiladi.

Kiberxavfsizlik tahdidlari va himoya mexanizmlari

Federativ o‘qitish tibbiy ma’lumotlarni markazlashtirish zaruratini kamaytiradi, biroq model yangilanishlarini uzatish va birlashtirish jarayonida yangi xavfsizlik muammolari yuzaga kelishi mumkin.

2-jadval.

Taklif etilayotgan tizim uchun tahdidlar va himoya choralari

Tahdid	Ehtimoliy oqibat	Taklif etiladigan himoya mexanizmi
Tibbiy ma’lumotlarni uzatish vaqtida ushlab qolish	Bemor ma’lumotlarining oshkor bo‘lishi	TLS kabi himoyalangan aloqa protokollari
Ruxsatsiz foydalanuvchi kirishi	Ma’lumotlarni ko‘rish yoki o‘zgartirish	Kuchli autentifikatsiya va rollarga asoslangan kirish
Model yangilanishidan ma’lumotni tiklashga urinish	Maxfiy ma’lumotlarning bilvosita oshkor bo‘lishi	Xavfsiz agregatsiya va zaruratga qarab differensial maxfiylik
Zararli model yangilanishi	Diagnostik natijalarning buzilishi	Yangilanishlarni tekshirish, anomaliyalarni aniqlash va ishtirokchilarni nazorat qilish
Server yoki xizmatga DoS-hujum	Diagnostika xizmatining uzilishi	Tarmoq monitoringi, tezlikni cheklash va zaxira infratuzilmasi
Modelning turli muassasalarda turlicha ishlashi	Ayrim guruhlarda diagnostik sifatning pasayishi	Tashqi validatsiya va guruhlar kesimida sifatni baholash

Jadvaldagi himoya choralari bir-birini to‘ldiradi. Masalan, TLS aloqa kanalidagi ma’lumotlarni himoyalashga yordam beradi, lekin model yangilanishlaridan ma’lumot tiklash xavfini o‘z-o‘zidan bartaraf etmaydi. Shu sababli xavfsiz agregatsiya va zaruratga qarab differensial maxfiylik qo‘llanishi mumkin.

Xavfsiz agregatsiya serverga alohida ishtirokchining model yangilanishini bevosita ko‘rmasdan umumiy natijani hisoblash imkonini berishi mumkin. Differensial maxfiylik esa model yangilanishlariga nazorat qilinadigan shovqin qo‘shish orqali ayrim shaxsiy yozuvlarning ta’sirini kamaytiradi. Biroq bu usullarni qo‘llashda hisoblash xarajatlari, model sifati va maxfiylik darajasi o‘rtasidagi muvozanat alohida baholanishi lozim.

Taklif etilayotgan algoritm va baholash mezonlari

Taklif etilayotgan tizimning ishlash jarayoni quyidagi bosqichlardan iborat:

1. Tibbiyot muassasasi tizimga autentifikatsiyadan o‘tgan holda ulanadi.
2. Mahalliy tibbiy ma’lumotlar tekshiriladi va tayyorlanadi.
3. Sun’iy intellekt modeli mahalliy ma’lumotlar asosida o‘qitiladi.
4. Model yangilanishlari himoyalangan kanal orqali federativ serverga yuboriladi.
5. Server ishtirokchilarning yangilanishlarini tekshiradi va xavfsiz agregatsiyani amalga oshiradi.
6. Umumiy model parametrlari muassasalarga qaytariladi.
7. Yangilangan model mustaqil ma’lumotlar to‘plamida baholanadi va interaktiv diagnostika moduliga joriy etiladi.

Diagnostik samaradorlikni baholashda aniqlik, sezgirlik, spetsifiklik va F1-ko‘rsatkichidan foydalanish mumkin. Masalan, sezgirlik kasallikka ega bo‘lgan holatlarning qanchasi to‘g‘ri

aniqlanganini, spetsifiklik esa kasallik mavjud bo‘lmagan holatlarning qanchasi to‘g‘ri tasniflanganini ifodalaydi.

3-jadval

Tizim samaradorligini baholash uchun taklif etiladigan ko‘rsatkichlar

Ko‘rsatkich	Baholash maqsadi
Accuracy	Umumiy tasniflash aniqligini aniqlash
Sensitivity (Recall)	Kasallik mavjud holatlarni aniqlash qobiliyatini baholash
Specificity	Kasallik mavjud bo‘lmagan holatlarni to‘g‘ri aniqlashni baholash
F1-score	Precision va recall o‘rtasidagi muvozanatni baholash
Aloqa hajmi (MB)	Federativ o‘qitishdagi tarmoq xarajatlarini aniqlash
O‘qitish vaqti (s)	Modelni yangilash uchun sarflanadigan vaqtni o‘lchash
Maxfiylik parametri (ε)	Differensial maxfiylik qo‘llanganda himoya darajasini tavsiflash
Ruxsatsiz kirish holatlari	Autentifikatsiya va kirishni boshqarish samaradorligini baholash

Tajriba bosqichida federativ modelni mahalliy o‘qitish va markazlashtirilgan o‘qitish bilan taqqoslash, turli muassasalardagi ma’lumotlar taqsimoti farqining ta’sirini aniqlash va himoya mexanizmlarining hisoblash xarajatlarini o‘lchash maqsadga muvofiq. Diagnostik natijalar mustaqil sinov ma’lumotlarida baholanishi, model turli bemor guruhlarida bir xil darajada ishonchli ishlashi ham tekshirilishi kerak.

Xulosa

O‘tkazilgan adabiyotlar tahlili yurak-qon tomir kasalliklarini tashxislashda federativ o‘qitishning istiqbolli yo‘nalish ekanini ko‘rsatadi. Biosignallarga asoslangan yondashuvlar tezkor monitoring va individual tahlil uchun, elektron tibbiy yozuvlarga asoslangan yondashuvlar esa ko‘p markazli klinik qarorlarni qo‘llab-quvvatlash uchun muhim imkoniyatlarga ega [1].

Tadqiqot doirasida bemorlarning dastlabki ma’lumotlarini mahalliy muassasalarda saqlash, model yangilanishlarini himoyalangan kanallar orqali uzatish, xavfsiz agregatsiya va autentifikatsiyani qo‘llashga asoslangan konseptual arxitektura taklif etildi. Shuningdek, tizimning samaradorligini baholash uchun diagnostik sifat, aloqa xarajatlari va axborot xavfsizligi ko‘rsatkichlari belgilandi.

Taklif etilgan arxitektura kelgusida dasturiy prototip yaratish va tajribalar o‘tkazish uchun asos bo‘lib xizmat qilishi mumkin. Uning ilmiy-amaliy qiymatini aniqlash uchun diagnostik aniqlik, maxfiylik darajasi, hujumlarga chidamlilik va hisoblash xarajatlarini real yoki ochiq tibbiy ma’lumotlar to‘plamida tajribaviy tekshirish zarur.

Foydalanilgan adabiyotlar

1. Ryu H., Lee M., Kim S.-H., Kim J. H., Yang H.-J. Federated Learning for Cardiovascular Disease Prediction: A Comparative Review of Biosignal- and EHR-Based Approaches. *Healthcare*. 2025; 13(21): 2811. DOI: https://doi.org/10.3390/healthcare13212811.

2. McMahan B., Moore E., Ramage D., Hampson S., y Arcas B. A. Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*. 2017; 54: 1273–1282.

3. Dwork C. Differential Privacy. *Automata, Languages and Programming: 33rd International Colloquium (ICALP)*. 2006; 4052: 1–12.

RAQAMLI INFRATUZILMALARGA QARATILGAN TARMOQ HUJUMLARINI MASHINALI O‘QITISH USULLARI YORDAMIDA TASNIFLASH

Kadirov M.M., Karimova N.O., Zokirova F.R.
Islom Karimov nomidagi Toshkent davlat texnika universiteti

Annotatsiya. Ushbu maqolada raqamli infratuzilmalarda axborot xavfsizligini ta’minlash va kiberhujumlarni aniqlashda mashinaviy o‘qitish algoritmlarining samaradorligi tadqiq etilgan. Tadqiqot doirasida NSL-KDD ma’lumotlar to‘plamidan foydalanilib, kiberhujumlar to‘rtta asosiy toifaga (DoS, Probe, R2L, U2R) ajratilgan. Kiberxavfsizlik tahdidlarini tasniflash uchun qarorlar daraxti (Decision Tree), tasodifiy o‘rmon (Random Forest), k ta eng yaqin qo‘shni (k-NN) hamda tyanch vektorlar usuli (SVM) modellarining imkoniyatlari Precision, Recall va F-score metrikalari orqali qiyosiy baholangan.

Kalit so‘zlar: raqamli infratuzilma, axborot xavfsizligi, NSL-KDD, mashinali o‘qitish, kiberhujumlar, DoS, U2R, R2L, sinflar nomutanosibligi.

Аннотация. В данной статье исследуется эффективность алгоритмов машинного обучения в обеспечении информационной безопасности цифровых инфраструктур и обнаружении кибератак. В рамках исследования использован набор данных NSL-KDD, в котором кибератаки разделены на четыре основные категории (DoS, Probe, R2L, U2R). Для классификации угроз кибербезопасности была проведена сравнительная оценка возможностей таких моделей, как дерево решений (Decision Tree), случайный лес (Random Forest), метод k-ближайших соседей (k-NN) и метод опорных векторов (SVM), с использованием метрик Precision, Recall и F-score.

Ключевые слова: цифровая инфраструктура, информационная безопасность, NSL-KDD, машинное обучение, кибератаки, DoS, U2R, R2L, дисбаланс классов.

Kirish

Raqamli infratuzilmalarda axborotni muhofaza qilishdan maqsad axborotning sirqib chiqib ketishi, ma’lumotlarga ruxsatsiz va qasddan ta’sir etishi natijasida axborot egasiga, foydalanuvchiga zarar yetkazilishining oldini olish. Hozirgi vaqtda raqamli infratuzilmalarda axborot tizimlarining keng rivojlanishi va joriy etilishi natijasida ularda yuzaga kelishi mumkin bo‘lgan zaifliklar soni ham ortib bormoqda. Turli sohalarda raqamli xizmatlarni optimallashtirishga bo‘lgan doimiy ehtiyoj axborot xavfsizligi tizimlarini muntazam takomillashtirish hamda kiberxavfsiz hisoblash usullarini yaratishni taqozo etmoqda. Bugungi kunda zamonaviy kiber-tendensiyalar va istiqbolli texnologiyalar ko‘plab tashkilotlar tomonidan amaliyotga joriy etilmoqda yoki ularning yaqin kelajakka mo‘ljallangan strategik kiber-himoya rejalaridan mustahkam o‘rin olmoqda. Axborot tizimlaridagi anomal xatti-harakatlarni aniqlash va tasniflashda mashinali o‘qitish algoritmlari keng qo‘llanilmoqda.

Asosiy qism

Mashinali o‘qitish algoritmlari ma’lumotlardan o‘rganish va yangi turdagi tahdidlarga qarshi turish imkoniyatiga ega. Ko‘plab mashinali o‘qitish algoritmlari nisbatan kam hisoblash resurslari bilan ham yetarlicha tez ishlashi mumkin.

Raqamli infratuzilmalarga bo‘ladigan tahdidlarni quyidagi ko‘rinishda tafsiflash mumkin. 1-jadvalda raqamli infratuzilmalarga bo‘ladigan tahdidlarning tavsifi keltirilgan.

1-jadval

Raqamli infratuzilmalarga bo‘ladigan tahdidlarning tavsifi

№	Tasniflash mezoni	Tahdid turlari
1	Tarmoq qatlamiga ko‘ra	Jismoniy qatlam (Physical), ma’lumotlarni bog‘lash qatlami (Data Link), tarmoq qatlami (Network), transport qatlami (Transport), ilovalar qatlami (Application)
2	Tahdid manbaiga ko‘ra	Inson omili, texnik tahdidlar, atrof-muhit tahdidlari, tashkiliy tahdidlar
3	Faoliyatiga ko‘ra	Passiv hujumlar, aktiv hujumlar
4	Manbasiga ko‘ra	Ichki tahdidlar, tashqi tahdidlar
5	Maqsadiga ko‘ra	Maxfiylik, yaxlitlik, foydalanishlilik
6	Avtomatlashtirish darajasiga ko‘ra	Qo‘lda bajariladigan hujumlar, avtomatlashtirilgan hujumlar, sun’iy intellect yordamidagi hujumlar.
7	Hujum usuliga ko‘ra	Malware, DoS/DDoS, phishing, spoofing, man-in-the-middle, password attacks, injection attacks, botnet, ransomware, zero-day

Tadqiqot NSL-KDD ma’lumotlar to‘plamida olib boriladi. Ushbu to‘plam KDD’99 ma’lumotlar bazasining takomillashtirilgan variant hisoblanadi [1]. Tadqiqotda hujumlar to‘rtta asosiy toifaga bo‘lingan:

– DoS (Denial of Service) - xizmat ko‘rsatishni rad etish. Ko‘p miqdordagi trafik hosil qilinib, server ortiqcha yuklanadi yoki uning faoliyati bloklanadi.

– U2R (User to Root) - ro‘yxatdan o‘tgan foydalanuvchining mahalliy superfoydalanuvchi, ya’ni administrator imtiyozlarini qo‘lga kiritishi.

– R2L (Remote to Local) - masofadagi kompyuterdan mahalliy kompyuterga ruxsatsiz kirish huquqini qo‘lga kiritish.

– Probe - tizimdagi zaifliklarni aniqlash va keyinchalik ulardan foydalanish maqsadida tizimni skanerlash.

Ma’lumotlarni normallashtirish

Ayrim mashinali o‘qitish algoritmlari barcha belgilarni yagona vektor sifatida qayta ishlaydi. Belgilarning qiymatlari turli diapazonlarda bo‘lsa, hisoblash natijalari noto‘g‘ri yoki samarasiz bo‘lishi mumkin [2].

Ushbu muammoni bartaraf etish uchun ma’lumotlar 0 dan 1 gacha bo‘lgan oraliqqa Min-Max usuli bilan normallashtirilgan.

$$x' = \frac{x - \min(X)}{\max(X) - \min(X)} \quad (1)$$

Bu yerda:

– x – belgining dastlabki qiymati;

– x' normallashtirilgan qiymat;

– $\min(X)$ – tegishli belgi uchun eng kichik qiymat;

– $\max(X)$ – tegishli belgi uchun eng katta qiymat.

Mazkur o‘zgartirish belgilarni bir xil diapazonga keltirishga xizmat qiladi.

NSL-KDD ma’lumotlar to‘plamini tasniflash uchun mashinali o‘qitishning quyidagi algoritlari qo‘llanilgan:

Qarorlar daraxti (Decision Tree Classifier). Shoxlarni qisqartirish tashlash ishonchlilik ko‘rsatkichi asosida amalga oshiriladi [3]. Ushbu ko‘rsatkich noto‘g‘ri tanilgan misollar sonining jami misollar soniga nisbatini ifodalaydi:

$$C_k = \frac{N_{nk}}{N_k} \quad (2)$$

Bu yerda:

- $N_{nk} - k$-sinfga tegishli noto‘g‘ri tanilgan misollar soni;
- $N_k - k$-sinfga tegishli jami misollar soni.

Tarmoqlanish eng kichik axborot entropiyasi qiymati asosida amalga oshiriladi:

$$H(x) = -\sum_{i=1}^{N} p(i) log_2 p(i) \quad (3)$$

Bu yerda:

– x - N ta mumkin bo‘lgan holatga ega tasodifiy hodisa;
– $p(i)$ - i-belgining qarorlar daraxtidagi navbatdagi tugun sifatida tanlanish ehtimoli.

Qarorlar daraxtining chuqurligi 21 ga teng.

Tasodifiy o‘rmon (Random Forest). Ansambl 10 ta qaror daraxtidan iborat. Yakuniy klassifikatorning chuqurligi 15 ga teng.

Tasodifiy o‘rmonni qurishda quyidagi usullardan foydalanilgan:

Bagging (bootstrap aggregating) - o‘qitish misollarini bir tekis taqsimot qonuni asosida tasodifiy tanlash va tanlangan misollarni dastlabki o‘qitish to‘plamiga qaytarish usuli. Bu ortiqcha o‘rganish (overfitting), ya’ni o‘qitish to‘plamidagi barcha misollarni shunchaki yodlab olish holatining oldini olish imkonini beradi.

Boosting - kuchsiz qaror daraxtlarini o‘qitish va ularni birlashtirish orqali kuchli klassifikator hosil qilish usuli. Bunda noto‘g‘ri tasniflangan o‘qitish misollarining vazni oshiriladi, to‘g‘ri tasniflangan misollarning vazni esa kamaytiriladi. Bu keyingi o‘qitish bosqichlarida noto‘g‘ri tasniflangan misollarga ko‘proq e’tibor qaratish imkonini beradi.

k ta eng yaqin qo‘shni (k-Nearest Neighbors, k-NN). Algoritmning asosiy parametri - qo‘shnilar soni. Tadqiqotda $k = 3$ qiymati tanlangan.

Parametrlarni min–max usuli yordamida normallashtirish:

$$x_i = \frac{x_i - x_{min}}{x_{min} - x_{max}}$$

Tayanch vektorlar usuli (Support Vector Machine, SVM). Tadqiqotda radial bazis funksiyasi yadrosi qo‘llanilgan:

$$k(x, x') = e^{-\gamma \|x - x'\|^2}$$

Bu yerda $\gamma = 2$.

SVM algoritmi sinflarni ajratish uchun qaror chegaralarini shakllantiradi.

Tasniflash algoritmlarini baholash metrikalari

Mashinaviy o‘qitishda tuzilgan modellar samaradorligini baholash uchun quyidagi metrikalardan foydalaniladi [4, 5]: Precision - aniqlik; Recall - to‘liqlik yoki sezgirlik; F-score – F-mezon; OC egri chizig‘i; AUC-ROC – ROC egri chizig‘i ostidagi maydon; AUC-PR – Precision-Recall egri chizig‘i ostidagi maydon.

Tasniflash jarayonida to‘rtta natija turi mavjud:

– TP (True Positive) – to‘g‘ri aniqlangan ijobiy holat.
– TN (True Negative) – to‘g‘ri aniqlangan salbiy holat.
– FP (False Positive) – noto‘g‘ri ijobiy natija.
– FN (False Negative) – noto‘g‘ri salbiy natija.

Ushbu natijalarni 2 jadvalda tasvirlash mumkin.

2 jadval

Xatolar matritsasi

Algoritm bashorati	Haqiqiy sinf $y = 1$	Haqiqiy sinf $y = 0$
$y' = 1$	TP – to‘g‘ri ijobiy	FP – noto‘g‘ri ijobiy
$y' = 0$	FN – noto‘g‘ri salbiy	TN – to‘g‘ri salbiy

Precision (Aniqlik) klassifikator ijobiy deb belgilagan obyektlarning qanchasi haqiqatan ham ijobiy ekanini ko‘rsatadi [6].

$$Precision = \frac{TP}{TP + FP}$$

Recall (To‘liqlik) haqiqiy ijobiy obyektlarning qanchasi algoritm tomonidan to‘g‘ri aniqlanganini ko‘rsatadi.

$$Recall = \frac{TP}{TP + FN}$$

Recall noto‘g‘ri salbiy natijalar bilan bog‘liq muammolarni baholashga yordam beradi. U algoritm ijobiy deb noto‘g‘ri belgilagan obyektlar sonini bevosita ko‘rsatmaydi.

F-mezon Precision va Recall ko‘rsatkichlarini birlashtiruvchi garmonik o‘rtacha qiymatdir.

F-score (me’yor) precision (aniqlik) va recall (to‘liqlik) ko‘rsatkichlarini o‘zida birlashtiradi, shu bilan birga ma’lumotlarning taqsimlanishiga e’toborli bo‘lib qoladi.

$$F - score = \frac{2 \cdot recall \cdot precision}{recall + precision}$$

Tasniflash algoritmlarini baholash natijalari

Matritsadagi qiymatlar har bir sinfdagi yozuvlar soniga nisbatan normallashtirilgan. Tahlil natijalariga ko‘ra:

– DoS, normal va Probe sinflari ko‘pchilik algoritmlar tomonidan nisbatan yaxshi tasniflangan.

– R2L va U2R sinflari ko‘pincha normal sinf sifatida noto‘g‘ri tasniflangan.

– Bu holat o‘qitish ma’lumotlaridagi sinflar nomutanosibligi, ya’ni kam uchraydigan sinflar uchun ma’lumotlarning yetarli emasligi bilan izohlanadi.

Ma’lumotlar to‘plamida har bir yozuv tegishli yorliq bilan belgilangan. Zararli trafik aniqlansa, unga muayyan hujum turi biriktiriladi. Har bir yozuv 41 ta belgi bilan tavsiflanadi. Agar yozuv yorlig‘i sinf deb qaralsa, uning belgilari shu sinfni ifodalovchi atributlar sifatida ishlatiladi. Ma’lumotlar to’plamda duration, protocol_type, service, flag, land, wrong_fragment, urgent, num_failed_logins, logged_in, root_shell, num_root, num_access_files, is_host_login, count, srv_count kabi har bir yozuv 41 ta belgi bilan tavsiflanadi.

3-jadval

Algoritmlar bo‘yicha Precision qiymatlari

Algoritm	DoS	Normal	Probe	R2L	U2R
Qarorlar daraxti	0,96	0,70	0,56	0,97	0,58
Random Forest	0,96	0,67	0,86	0,96	0,75
k-NN	0,96	0,66	0,81	0,93	0,79
SVM	0,97	0,62	0,80	0,95	0,80

4-jadval

Algoritmlar bo‘yicha Recall qiymatlari

Algoritm	**DoS**	**Normal**	**Probe**	**R2L**	**U2R**
Qarorlar daraxti	0,80	0,95	0,63	0,11	0,22
Random Forest	0,82	0,97	0,72	0,03	0,09
k-NN	0,79	0,98	0,66	0,03	0,16
SVM	0,72	0,98	0,5	0,02	0,06

5-jadval

Algoritmlar bo‘yicha F-score qiymatlari.

Algoritm	DoS	Normal	Probe	R2L	U2R
Qarorlar daraxti	0,87	0,81	0,59	0,2	0,32
Random Forest	0,88	0,79	0,78	0,08	0,16
k-NN	0,87	0,79	0,73	0,07	0,27
SVM	0,83	0,76	0,61	0,04	0,11

Xulosa

Taqdim etilgan natijalar tahlili shuni ko‘rsatadiki, o‘qitish ma’lumotlaridagi sinflar nomutanosibligi sababli mashinaviy o‘qitish algoritmlari NSL-KDD to‘plamida barcha hujum toifalarini bir xil darajada samarali tasniflay olmaydi.

Ushbu muammoni hal qilish uchun sinflar muvozanatini yaxshilash talab etiladi. Maqolada quyidagi yondashuvlar taklif qilingan:

1. Kam uchraydigan sinflardagi yozuvlarni takrorlash orqali sinflar muvozanatini yaxshilash.

2. Ko‘p sinfli tasniflash o‘rniga ikkilik tasniflashdan foydalanish: «normal» va «normal bo‘lmagan» trafik.

Foydalanilgan adabiyotlar

1. Thomas R., Pavithran D. A Survey of Intrusion Detection Models based on NSL-KDD Data Set. NSL-KDD ma’lumotlar to‘plamiga asoslangan ruxsatsiz kirishlarni aniqlash modellari sharhi. 5-xalqaro HCT Information Technology Trends konferensiyasi materiallari, Dubay, BAA, 2018-yil 28–29-noyabr. IEEE, 2018, 286–291-bet.

2. Mitchell T. Machine Learning. Mashinaviy o‘qitish. Nyu-York: McGraw-Hill, 1997. 414 bet.

3. Safavian, S. R., & Landgrebe, D. (1991). A survey of decision tree classifier methodology. IEEE transactions on systems, man, and cybernetics, 21(3), 660-674.

4. Sheluxin O.I., Eroxin S.D., Vanyushina A.V. Mashinaviy o‘qitish usullari yordamida IP-trafikni tasniflash. Moskva: Goryachaya liniya–Telekom, 2018. 284 bet.

5. Dhanabal L., Shantharajah S.P. A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms. Tasniflash algoritmlariga asoslangan ruxsatsiz kirishlarni aniqlash tizimlari uchun NSL-KDD ma’lumotlar to‘plamini o‘rganish. International Journal of Advanced Research in Computer and Communication Engineering, 2015, 4-jild, 6-son, 446–452-bet.

6. Goutte, C., & Gaussier, E. (2005, March). A probabilistic interpretation of precision, recall and F-score, with implication for evaluation. In European conference on information retrieval (pp. 345-359). Berlin, Heidelberg: Springer Berlin Heidelberg.

SUN’IY INTELLEKT ASOSIDA TARMOQ HUJUMLARINI ERTA ANIQLASHNING DOLZARB MUAMMOLARI VA RIVOJLANISH ISTIQBOLLARI

G‘ulomov Sh.R., Nasriddinova P.F.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada sun’iy intellekt asosida tarmoq hujumlarini erta aniqlashga oid ilmiy tadqiqotlar va zamonaviy yondashuvlar tahlil qilinadi. Mashinaviy va chuqur o‘rganish usullarining kiberxavfsizlikdagi imkoniyatlari, shuningdek, ularni real tarmoq infratuzilmalariga joriy etish bilan bog‘liq cheklovlar ko‘rib chiqiladi. Tarmoq hujumlarini aniqlash tizimlarini baholashda aniqlik ko‘rsatkichlari bilan bir qatorda, aniqlash kechikishi, yolg‘on ogohlantirishlar va turli tarmoq sharoitlarida barqaror ishlashning ahamiyati asoslanadi. Shuningdek, sun’iy intellekt modellarini tarmoqdagi o‘zgarishlarga moslashtirish va ularning amaliy samaradorligini oshirish istiqbollari yoritiladi.

Kalit so‘zlar: sun’iy intellekt, tarmoq hujumlari, erta aniqlash, mashinaviy o‘rganish, chuqur o‘rganish, anomaliyalarni aniqlash, moslashuvchan sun’iy intellekt.

Аннотация. В статье анализируются научные исследования и современные подходы к раннему обнаружению сетевых атак на основе искусственного интеллекта. Рассматриваются возможности методов машинного и глубокого обучения в обеспечении кибербезопасности, а также ограничения, связанные с их внедрением в реальные сетевые инфраструктуры. Обосновывается важность учета не только показателей точности обнаружения сетевых атак, но и времени обнаружения, количества ложных срабатываний и устойчивости функционирования в различных сетевых условиях. Кроме того, освещаются перспективы адаптации моделей искусственного интеллекта к изменениям сетевого трафика и повышения эффективности их практического применения.

Ключевые слова: искусственный интеллект, сетевые атаки, раннее обнаружение, машинное обучение, глубокое обучение, обнаружение аномалий, адаптивный искусственный интеллект.

Kirish

Raqamli texnologiyalar, bulutli hisoblash xizmatlari va o‘zaro bog‘langan qurilmalar sonining ortishi tarmoq infratuzilmalarining murakkablashishiga olib kelmoqda. Shu bilan birga, taqsimlangan xizmat ko‘rsatishni rad etish (DDoS), zararli dasturlar, hisob ma’lumotlarini qo‘lga kiritish va ko‘p bosqichli hujumlar kabi kiberxavflar axborot tizimlari xavfsizligiga jiddiy tahdid tug‘dirmoqda. Bunday sharoitda hujum sodir bo‘lganidan keyin unga javob berish bilan cheklanmasdan, zararli faoliyatning dastlabki belgilarini imkon qadar erta aniqlash muhim ahamiyat kasb etadi.

An’anaviy imzo va qoidalarga asoslangan tizimlar ma’lum hujum namunalarini aniqlashda samarali bo‘lishi mumkin. Biroq yangi yoki o‘zgartirilgan hujumlar mavjud qoidalarga mos kelmaganda, ularni aniqlash imkoniyati cheklanadi. Sun’iy intellekt texnologiyalari tarmoq trafigi, tizim jurnallari va boshqa xavfsizlik ma’lumotlaridagi yashirin qonuniyatlarni aniqlash orqali ushbu cheklovlarni kamaytirish imkonini beradi [1].

Shu sababli sun’iy intellekt asosida tarmoq hujumlarini erta aniqlashning mavjud yondashuvlarini tahlil qilish, ularning kamchiliklarini aniqlash va kelgusidagi ilmiy tadqiqotlar uchun ustuvor yo‘nalishlarni belgilash dolzarb vazifalardan biri hisoblanadi.

Asosiy qism

So‘nggi yillarda kiberxavfsizlik sohasida va tarmoq hujumlarini aniqlashda ko‘plab ilmiy tadqiqotlar olib borilmoqda. Olib borilgan tadqiqotlarning to‘g‘rilik darajasi (Accuracy), musbat bashoratlarning aniqligi (Precision), musbat sinfni aniqlash qamrovi (Recall) hamda F1-mezon (F1-score) baholash ko‘rsatkichlari yuqori darajali bo‘lsada ilmiy izlanishlarni real tarmoq infratuzilmalariga joriy qilish muhim muammolardan biri sifatida qolmoqda. Bunga misol sifatida

bir qancha ilmiy izlanishlar tahlil qilinib, baholash ko‘rsatkichlari yuqori darajaligi bo‘yicha saralab olindi va maqolada mualliflar ushbu tadqiqotlarni laboratoriya sharoitida bajarganini va real infratuzilmalarda joriy etishda cheklovlar mavjudligini tan olishgan. [2] [3] [4] [5]

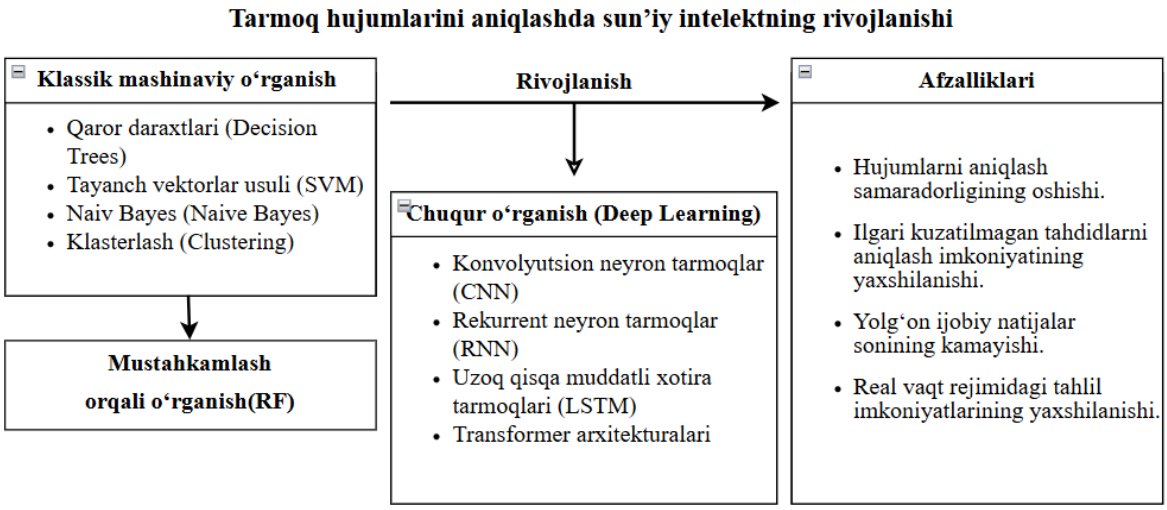
1-jadval

Tarmoq hujumlarini aniqlash bo’yicha ilmiy tadqiqotlarning qiyosiy sharhi

№	Muallif, yil	Usullar	Baholash ko‘rsatkichlari	Asosiy natija	Real infratuzilmaga joriy etishdagi cheklov
1	Sharafaldin va boshq., 2018 (CICIDS 2017)	Real trafikka yaqin yangi ma’lumotlar to’plami va trafik xususiyatlarini tavsiflash	Precision, Recall, F1, Accuracy	Zamonaviy hujumlar (DDoS, brute force, botnet va b.) bilan ishonchliroq benchmark berdi	Sinov faqat laboratoriya to‘plamida, kechikish va real trafikdagi barqarorlik tekshirilmagan
2	Vaswani va boshq., 2017	Transformer	-	Uzoq masofali bog’liqliklarni modellashtirishva keyinchalik IDS uchun moslashtirilmoqda	Kiberxavfsizlik uchun bevosita emas, hisoblash jihatidan qimmat
3	Kipf va Welling, 2017	Graf konvolyutsion tarmoqlari (GCN)	Accuracy (graf tugunlarini tasniflash)	IDS da lateral harakatni aniqlashda qo’llaniladi	IDS uchun maxsus emas, katta dinamik graflarda masshtablash qiyin
4	Nawale va Shingate, 2026	Nazorat ostidagi, nazoratsiz, chuqur o’rganish va graf modellari	Accuracy, Precision, Recall, F1, ROC-AUC, FPR	Sun’iy intelekt usullari an’anaviy tizimlardan ustun, biroq muammolar saqlanadi	Eksperiment o’tkazilmagan, adversarial hujumlar, tushuntirib berish, real vaqt va ma’lumotlar nomutanosibligi hal etilmagan

Yuqoridagilardan kelib chiqib real tarmoq infratuzilmalarida samarali joriy qilish bo‘yicha klassik sun’iy intelekt texnologiyalari bilan birga vaqt omilini hisobga olgan holda baholash usulini ishlab chiqishga e’tibor qaratish, moslashuvchan sun’iy intelekt texnologiyasini joriy qilish, adversial texnologiyasini va izohlanuvchi sun’iy intelekt texnologiyalari arxitekturalarini amalga oshirish kiberxavfsizlikning sun’iy intelekt yordamida tarmoq hujumlarini aniqlash bo‘yicha rivojlanish bosqichi hisoblanadi [6].

Sun’iy intellekt asosida tarmoq hujumlarini erta aniqlash samaradorligini oshirishda modellarning aniqlik ko‘rsatkichlari bilan bir qatorda, hujumni aniqlash uchun sarflanadigan vaqtni ham hisobga olish muhimdir. Chunki hujumni yuqori aniqlik bilan tasniflaydigan model ham zararli faoliyatni kech aniqlasa, uning amaliy samaradorligi pasayishi mumkin. Shu sababli mashinaviy va chuqur o‘rganish modellarini baholashda aniqlash kechikishi, yolg‘on ogohlantirishlar soni hamda turli hujum turlarini aniqlash qobiliyatini birgalikda tahlil qilish maqsadga muvofiq.



1-rasm. Sun’iy intelekt yordamida tarmoq hujumlarini aniqlash bo‘yicha rivojlanish bosqichi

Bundan tashqari, tarmoq infratuzilmalaridagi trafik xususiyatlari vaqt o‘tishi bilan o‘zgarishi mumkin. Shu bois sun’iy intellekt modellarini yangi ma’lumotlar asosida moslashtirish va ularning samaradorligini muntazam baholab borish istiqbolli yo‘nalishlardan biri hisoblanadi. Kelgusidagi tadqiqotlarda aniqlashning tezkorligi va ishonchliligini birgalikda ta’minlaydigan, turli tarmoq sharoitlarida barqaror ishlaydigan yondashuvlarni ishlab chiqishga e’tibor qaratish zarur. Bu esa sun’iy intellekt texnologiyalarini real tarmoq infratuzilmalarida samarali qo‘llash imkoniyatlarini kengaytiradi.

Xulosa

Xulosa qilib aytganda, sun’iy intellekt texnologiyalari tarmoq hujumlarini aniqlash, tasniflash va ularning dastlabki belgilarini aniqlash imkoniyatlarini kengaytiradi. O‘tkazilgan tahlil shuni ko‘rsatadiki, mashinaviy va chuqur o‘rganish usullari yuqori natijalarga erishish imkonini bersa-da, ularni real tarmoq infratuzilmalarida samarali qo‘llash uchun aniqlash tezkorligi, yolg‘on ogohlantirishlar va turli tarmoq sharoitlarida barqaror ishlash kabi omillarni ham hisobga olish zarur.

Kelgusidagi tadqiqotlarda tarmoq trafikidagi o‘zgarishlarga moslasha oladigan, hujumlarni qisqa vaqt ichida aniqlaydigan va qabul qilingan qarorlarni izohlash imkonini beradigan sun’iy intellekt yondashuvlarini takomillashtirish muhim ahamiyatga ega. Bunda modellarni nafaqat an’anaviy aniqlik ko‘rsatkichlari, balki aniqlash kechikishi va yolg‘on ogohlantirishlar darajasi bo‘yicha ham kompleks baholash lozim. Mazkur yo‘nalishlarning rivojlantirilishi sun’iy intellekt asosidagi tarmoq hujumlarini aniqlash tizimlarining ishonchliligini oshirish hamda ularni real sharoitlarda samarali qo‘llashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Andrew Ross and Finale Doshi-Velez. 2018. Improving the adversarial robustness and interpretability of deep neuralnetworks by regularizing their input gradients.

2. Sharafaldin I., Habibi Lashkari A., Ghorbani A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP, 2018, pp. 108–116

3. Vaswani A. va boshq. Attention Is All You Need. NeurIPS, 2017

4. Kipf T., Welling M. Semi-Supervised Classification with Graph Convolutional Networks. ICLR, 2017

5. Nawale S., Shingate S. A Review of AI Techniques for Cybersecurity Threat Detection. IJSRP, 2026, vol. 16, issue 2, pp. 250–256

6. Dusmurod Kilichev, Wooseong Kim. 2026. Real-time intrusion detection in IoT networks: A hybrid framework of offline ML and online DL. Internet of Things 102039.

THE IMPORTANCE OF EARLY ATTACK DETECTION IN ENSURING NETWORK SECURITY

Barotova Z.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Abduvoxidov D.
Prosecutor General's Office of the Republic of Uzbekistan

Annotatsiya. Ushbu tadqiqotda xavfsizlikni ta'minlashda hujumlarni erta aniqlashning ahamiyati tahlil qilingan bo'lib, hujumlarni erta aniqlash xavfsizlik samaradorligiga qay darajada ta'sir ko'rsatishi masalalari ko'rib chiqiladi. Tadqiqot davomida hujumlarning amalga oshirilish bosqichlari va erta aniqlashning qay bosqichda qanday darajada ta'sir o'tkazishi hamda real vaqt metrikalarining erta aniqlash bilan bog'liqligi tahlil qilingan bo'lib, aniqlash kechikishi, aniqlash vaqti, yolg'on ko'rsatkich darajasi kabi metrikalarning IDS samaradorligiga ta'siri ham yoritiladi. Zamonaviy texnologiyalarnin tarmoq trafigidagi aniqlash imkoniyatlari va cheklovlari hamda kelajak istiqbolli yo'nalishlari keltiriladi.

Kalit so'zlar: tarmoq xavfsizligi, hujumlarni aniqlash tizimi, hujumlarni erta aniqlash, aniqlash kechikishi, aniqlash vaqti, real vaqt rejimi.

Аннотация. В данном исследовании анализируется важность раннего обнаружения атак для обеспечения безопасности и рассматривается степень влияния раннего обнаружения атак на эффективность безопасности. В ходе исследования анализируются этапы реализации атак и степень их влияния на раннее обнаружение, а также взаимосвязь между метриками реального времени и ранним обнаружением, и освещается влияние таких метрик, как задержка обнаружения, время обнаружения и частота ложных срабатываний, на эффективность систем обнаружения вторжений (IDS). Представлены возможности и ограничения современных технологий обнаружения сетевого трафика, а также перспективные направления развития.

Ключевые слова: сетевая безопасность, система обнаружения атак, раннее обнаружение атак, задержка обнаружения, время обнаружения, режим реального времени.

Introduction

Today, digital technology is permeating virtually every sphere of human activity. While the reliance of processes – ranging from public administration, education, healthcare, and e-commerce to service delivery in numerous state enterprises and data transmission on network infrastructure is a key driver of progress, the expansion of digital services also increases the scope of security threats.

Attacks on network systems can vary in nature; given the potential severity of the damage and consequences they entail, the critical factor in ensuring security is not merely the detection process itself, but the speed at which detection occurs.

Although security tools such as firewalls, antivirus software, access control systems, and the like are essential components of security, the increasing sophistication of modern attacks can limit the operational effectiveness and capabilities of these mechanisms. In this context, Intrusion Detection Systems (IDS) have emerged as vital tools for monitoring suspicious activity. When developing modern Intrusion Detection Systems (IDS), addressing the challenge of early attack detection requires balancing accuracy with metrics such as detection time, latency, and real-time

operational capability. Employing machine learning and deep learning techniques offers a viable solution, though the effectiveness of these methods depends on several criteria. In modern network security, the priority lies not merely in identifying suspicious activity, but in detecting threats and taking action as quickly as possible. This study examines the importance of early attack detection and the challenges associated with real-time detection, while also analyzing approaches to improving early attack detection capabilities.

Main part

In modern network infrastructures, detecting cyberattacks solely through the resulting damage or system failure is insufficient for ensuring security. Most attacks unfold not as isolated incidents, but as a series of interconnected actions. An attacker initially gathers information about the network environment, active devices, open ports, services, and potential vulnerabilities; subsequently, they exploit identified opportunities to gain system access, escalate privileges, or compromise a target resource [1]. Therefore, the final stage of a network attack is not its starting point, but rather the culmination of various indicators that emerged during earlier phases.

This situation imposes a crucial requirement on the issue of attack detection: it is necessary to detect an attack not merely after it has occurred, but based on the initial observable signs of the attack process. In the study by Ahmad et al. [2], an early intrusion detection approach was proposed; the authors defined the detection of an attack as early as possible as the research objective and utilized an "earliness" metric.

In terms of network traffic, the initial stages of an attack often manifest not through massive volumes of malicious traffic, but rather through relatively subtle indicators, such as changes in request frequency, unusual communication between source and destination nodes, sequential port scanning, repetitive connection attempts, alterations in packet flow, or a surge in authentication attempts. Consequently, an early detection system must be capable of identifying these preliminary changes without waiting for the onset of large-scale malicious traffic.

At this juncture, it is important to distinguish between the concepts of "detection" and "early detection". While the primary question in the first instance is "Is the traffic an attack or normal traffic?", the second instance adds a further question: "At what stage of the attack can this determination be made?" It is precisely this second question that is crucial for ensuring network security in real time.

To detect an attack early, it is crucial to first understand the stages of its execution. The attack is carried out in the following sequence (Figure 1).

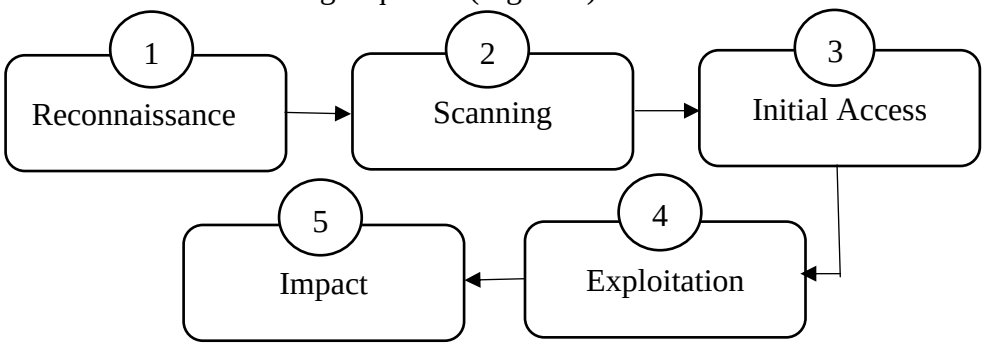


Figure 1. Stages of carrying out the attack

The scientific and practical significance of early detection

The primary advantage of early attack detection lies not merely in the act of detection itself, but in providing the security system with additional time to respond. If an initial sign of an attack is detected, a security administrator or an automated defense mechanism can implement measures

such as blocking the suspicious source, restricting connections, rerouting traffic, initiating further inspection, or temporarily limiting access to the protected resource. Figure 2 illustrates the cause-and-effect chain of early versus late attack detection, highlighting the distinction between the concepts of detection and timely detection, as well as the impact of these metrics on effectiveness.

Table 1.

Stages of attack progression and observable signs for early detection

Step	Potential Network Indicators	Potential Network Indicators
Reconnaissance	Sequential requests to ports and services, scanning of multiple nodes	Allows for warning before the attacker's subsequent actions
Scanning	Requests to numerous IPs/ports within a short timeframe	Helps identify the attack infrastructure
Initial Access	Unusual connections, repeated authentication attempts	Increases the chance of stopping unauthorized access early
Exploitation	Changes in traffic characteristics and protocol behavior	Enables detection of the vulnerability exploitation phase
Impact	Sudden traffic spikes, service disruption	Often indicates a late stage of the attack

In their research, Puccetti et al. [3] argue that detection timeliness is often undervalued and propose incorporating the detection latency metric when evaluating IDS performance. According to this proposal, the following two requirements for real-time IDS must be considered in conjunction:

$$Effective\ detection = Accuray + Timely\ detection \quad \textbf{(1)}$$

Analyzing modern IDS approaches from the perspective of early detection

Signature-based, anomaly-based, and ML/DL-based IDS types are employed to detect network attacks. Their capabilities for early attack detection vary, and simply enhancing an algorithm's classification ability is insufficient for achieving early detection. For instance, a 2023 study addressed the challenge of detecting attacks using fewer packets, and experimental results showed that the classical Random Forest (RF) algorithm outperformed DL algorithms [4]. This implies that, regarding early detection, model complexity does not necessarily equate to effectiveness. When selecting a model, it is essential to consider decision-making time alongside accuracy.

Table 2.

Comparison of IDS approaches from the perspective of early detection

Approach	Main principle	Early detection capability	Limitation
Signature-based	Searching for known attack patterns	Fast for known attacks	Limited ability to detect new or modified attacks
Anomaly-based	Detecting deviations from normal traffic	High potential for unknown attacks	Risk of false positives
ML-based	Decision-making based on learned traffic characteristics	Capable of identifying initial statistical patterns	Dependence on data quality and the model
DL-based	Automatic learning of complex features	Promising for raw or complex traffic patterns	Computational cost and inference time

Key factors influencing real-time early detection

The practical effectiveness of an early detection system depends on several interconnected factors. These can be broadly categorized into data, models, and time. From this perspective, detection time and detection latency should not be viewed merely as technical metrics, but rather as indicators that determine the speed at which security measures are activated.

Table 3.

Key requirements for a real-time early detection system

Group	Factor	Impact on the system
Data	Traffic quality	Incorrect or missing features reduce detection quality
Data	Number of features	Excessive features can increase computational load
Model	Classification accuracy	Determines the ability to correctly identify an attack
Model	False positive/FAR	Leads to normal traffic being incorrectly flagged as malicious
Model	Adaptability	Determines the ability to adapt to new traffic and evolving attacks
Time	Detection time	Represents the time elapsed until an attack is detected
Time	Detection latency	Represents the delay between the occurrence of an attack and the alert
System	Computational cost	Affects real-time processing capability
System	Throughput	Determines system performance under high traffic volumes

This is a key aspect of the 2026 study by Puccetti and Ceccarelli [5]: the authors argue that evaluating an IDS solely based on whether or not it detects an attack is insufficient, and that the timeliness of detection requires separate assessment.

Prospects for improving early detection systems

The analysis above indicates that the future improvement of IDS should not be limited solely to developing more complex classification algorithms. As a promising solution, IDS must encompass the following capabilities in the future:

- *determining the minimum amount of traffic required to make a decision*. The system should be capable of making a determination as soon as sufficient attack-characterizing features have emerged, rather than waiting for the entire session to conclude.
- *feature optimization.* The presence of redundant or low-informativeness features can complicate the model and increase computational load in real-time operations. Therefore, an early detection system must consider not only the discriminative power of features but also the speed at which they can be computed.
- *hybrid and adaptive detection.* This involves employing a fast, lightweight classification mechanism at an early stage, while refining the final decision through additional traffic analysis in cases where the initial determination is ambiguous. Kim and Park's "deferred-decision" approach exemplifies this principle: the system reduces the risk of misclassification by gathering additional data in certain instances rather than making an immediate decision.
- *establishing early detection as a distinct evaluation criterion.* In addition to traditional metrics such as accuracy, precision, recall, and F1-score, the use of indicators like detection time, detection latency, and earliness helps to better characterize the model's capabilities under real-world network conditions.

Conclusion

Analysis reveals that the early detection of network attacks determines a security system's capability for rapid response, not merely its ability to detect threats. Detecting an attack based on initial traffic indicators makes it possible to limit the extent of damage and activate protective measures in a timely manner.

When evaluating the effectiveness of real-time Intrusion Detection Systems (IDS), it is essential to consider metrics such as detection time, detection latency, and false positive rate, alongside accuracy, precision, and recall. While machine learning and deep learning methods enhance early detection capabilities, their practical effectiveness depends on balancing accuracy, speed, and computational cost.

Therefore, improving modern early attack detection systems requires simultaneously ensuring timeliness, reliability, and compliance with real-time requirements.

References:

1. T. Kim and W. Pak, "Real-time network intrusion detection using deferred decision and hybrid classifier," *Future Generation Computer Systems*, vol. 132, pp. 51–66, 2022, doi: 10.1016/j.future.2022.02.011.

2. T. Ahmad, D. Truscan, J. Vain, and I. Porres, "Early Detection of Network Attacks Using Deep Learning," in *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2022, pp. 30–39, doi: 10.1109/ICSTW55395.2022.00020.

3. "Early Detection of Intrusion in SDN," in *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, Miami, FL, USA, 2023, doi: 10.1109/NOMS56928.2023.10154272.

4. C. Callegari, S. Giordano, and M. Pagano, "A Real Time Deep Learning Based Approach for Detecting Network Attacks," *Big Data Research*, vol. 36, Art. no. 100446, 2024, doi: 10.1016/j.bdr.2024.100446.

5. T. Puccetti and A. Ceccarelli, "On detection latencies of network intrusion detectors – discussion and application," *Empirical Software Engineering*, vol. 31, Art. no. 23, 2026, doi: 10.1007/s10664-025-10766-3.

6. P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Computer Communications*, vol. 34, no. 18, pp. 2227–2235, 2011, doi: 10.1016/j.comcom.2011.07.001.

UCH POG‘ONALI RAQAMLI OGOHLANTIRUVCHI SIGNAL MODELINING QAROR QOIDALARI VA XAVFSIZLIK TAMOYILLARI

Polvanov R.B., Muxamedaliyeva N.M.
O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti, Harbiy tibbiyot instituti

Annotatsiya. Maqolada ichki ishlar organlari (IIO) xodimlarida psixologik yordamga muhtojlikni erta aniqlash uchun mo‘ljallangan uch pog‘onali raqamli ogohlantiruvchi signal modelining konseptual qaror tamoyillari, klinik xavfsizlik qoidalari va axborot xavfsizligi talablari bayon etilgan. Model klinik suhbat, standartlashtirilgan psixometrik metodikalar, Physiognomics.uz raqamli psixologik portreti va elektron tibbiy kontekstni yagona integral xulosaga birlashtiradi. Asosiy tamoyil - algoritm signali tashxis yoki kadrlar qarori emas, balki mutaxassis tasdig‘idan keyin yo‘naltirishga aylanadigan marshrutlash vositasidir.

Kalit so‘zlar: erta ogohlantirish, signal modeli, ruhiy salomatlik, suitsid profilaktikasi, raqamli psixodiagnostika, shaxsga doir ma’lumotlar, kiberxavfsizlik, maxfiylik.

Аннотация. В статье описываются концептуальные принципы принятия решений, правила клинической безопасности и требования к информационной безопасности трехэтапной цифровой модели предупреждающих сигналов, предназначенной для выявления необходимости психологической помощи у сотрудников органов внутренних дел (ОВД). Модель объединяет клиническое интервью, стандартизированные психометрические методы, цифровой психологический портрет Physiognomics.uz и электронный медицинский контекст в единый интегрированный вывод. Главный принцип заключается в том, что сигнал алгоритма - это не диагноз или кадровое решение, а инструмент маршрутизации, который после подтверждения специалистом становится направлением к другому специалисту.

Ключевые слова: раннее предупреждение, модель сигнала, психическое здоровье, профилактика самоубийств, цифровая психодиагностика, персональные данные, кибербезопасность, конфиденциальность.

Kirish

Klinik tibbiyotda erta ogohlantirish tizimlari bir nechta fiziologik ko‘rsatkichni yagona signalga aylantirib, yomonlashuv xavfi bo‘lgan bemorlarni o‘z vaqtida aniqlash imkonini beradi; NEWS shkalasi bunga klassik misoldir [1]. Ruhiy salomatlik monitoringida bunday yondashuvni to‘g‘ridan-to‘g‘ri ko‘chirish murakkab. 365 ta tadqiqotni qamragan metatahlil an’anaviy xavf omillarining suitsidal xulq-atvorni bashorat qilish qobiliyati zaif ekanini ko‘rsatgan [2], 64 ta prognostik model tahlilida esa suitsiddan o‘lim uchun ijobiy prognostik qiymat aksariyat modellarda 1% dan oshmagan [3]. Yuz harakatlarining emotsional ma’nosi kontekst, madaniyat va individual farqlarga bog‘liq bo‘lgani sababli raqamli vizual belgilar mustaqil diagnostik asos bo‘la olmaydi [4]. Algoritmlar maqsadli yorliq noto‘g‘ri tanlanganda tizimli tarafkashlikni takrorlashi ham isbotlangan [5].

Xalqaro klinik qo‘llanmalar «past/o‘rta/yuqori xavf» toifalarini davolanishga kirishni belgilash uchun qo‘llamaslikni, ularning o‘rniga ehtiyojlar va xavfsizlikni baholashni tavsiya etadi [6]; zamonaviy yondashuv xavfni bashorat qilishdan klinik formulirovka va profilaktikaga o‘tishni taklif qiladi [7]. Shu bilan birga, huquqni muhofaza qilish organlari xodimlarida stigma va maxfiylik buzilishidan qo‘rqish yordam so‘rashning asosiy to‘siqlaridan biri bo‘lib qolmoqda. Demak, xodimlar uchun signal tizimi ikki shartni bir vaqtda bajarishi kerak: klinik jihatdan xavfsiz bo‘lishi (algoritm xatosi xodimga zarar yetkazmasligi) va axborot jihatidan himoyalangan bo‘lishi (ruhiy salomatlik ma’lumotlari xizmat qarorlariga «sizib» chiqmasligi). Ushbu ikkinchi jihat tibbiy raqamli tizimlarni kiberxavfsizlik nuqtai nazaridan loyihalash vazifasi bilan bevosita bog‘liq.

Material va metodlar

Tadqiqot konseptual-metodologik xususiyatga ega. Qaror tamoyillari klinik va texnik mutaxassislardan iborat multidisiplinar ekspert guruhi tomonidan ekspert muhokamasi orqali ishlab chiqildi. Muhokama uchun asos sifatida erta ogohlantirish tizimlari [1], suitsidal xavfni prognozlash cheklovlari [2; 3], yuz ifodalarini talqin qilish chegaralari [4], algoritmik tarafkashlik [5] va klinik formulirovka [7] bo‘yicha dalillar tanqidiy tahlil qilindi. Har bir qoida uch savolga javob berishi talab qilindi: qaysi turdagi ma’lumot signalni ishga tushiradi, signal qanday klinik harakatga olib keladi va algoritm xato qilganda xodim qanday himoyalanadi.

Modelni validatsiya qilish rejasi prognostik va diagnostik modellarga qo‘yiladigan xalqaro talablarga muvofiq tuzildi: natijalarni taqdim etishda TRIPOD+AI [8], siljish xavfi va qo‘llanuvchanlikni baholashda PROBAST+AI [9] mezonlariga amal qilinadi, etalon sifatida raqamli natijalardan bexabar mutaxassislarning klinik xulosasi qabul qilinadi, ehtimoliy chiqishlar uchun kalibrovka alohida tekshiriladi [10]. Ma’lumotlarni himoya qilish talablari «Shaxsga doir ma’lumotlar to‘g‘risida»gi [11] va «Kiberxavfsizlik to‘g‘risida»gi [12] qonunlar hamda ISO/IEC 27001 axborot xavfsizligini boshqarish tizimi tamoyillari [13] asosida shakllantirildi. Tahdidlar modeli tuzishda tashqi hujumlar bilan bir qatorda ichki noto‘g‘ri foydalanish ssenariylari ham ko‘rib chiqildi.

Natijalar

Ekspert muhokamasi natijasida modelning to‘rt komponenti - signal pog‘onalari mantig‘i, klinik xavfsizlik qoidalari, ma’lumotlar xavfsizligi arxitekturasi va sifat ko‘rsatkichlari guruhlari ishlab chiqildi.

Signal pog‘onalari mantig‘i. Signal pog‘onalari xavf darajasini emas, balki zarur klinik harakat turini bildiradi. Birinchi pog‘ona - rejali kuzatuvni davom ettirish; ikkinchi pog‘ona - mutaxassis bilan qo‘shimcha suhbat va psixoprofilaktik ish; uchinchi pog‘ona - shoshilinch klinik baholash. Pog‘onalarni belgilovchi mezonlar va chegara qiymatlari klinik protokolda qayd etiladi va mahalliy validatsiya natijalari bo‘yicha qayta ko‘rib chiqiladi. Integral xulosa bir yo‘nalishda shakllanadi: yuqori pog‘onaga mos keladigan har qanday klinik mezon past pog‘onadagi boshqa natijalardan ustun turadi, ya’ni yaxshi ko‘rsatkichlar xavotirli belgini «neytrallashtira» olmaydi.

Klinik xavfsizlik qoidalari. Birinchidan, eng yuqori pog‘ona faqat klinik mezonlar bilan ishga tushadi va hech qachon faqat raqamli portret asosida berilmaydi. Ikkinchidan, portret faqat pog‘onani oshirish, ya’ni qo‘shimcha klinik suhbatga yo‘naltirish huquqiga ega va xavf baholashini hech qachon pasaytirmaydi. Uchinchidan, signal ekspert qarori emas: u mutaxassisning klinik tasdig‘idan keyingina yo‘naltirishga aylanadi, mutaxassis algoritm tavsiyasini rad etganda sababi qayd etiladi. To‘rtinchidan, raqamli komponent uchun oldindan qabul mezonlari belgilanadi; ular mahalliy ma’lumotlarda bajarilmasa, komponentning roli xodimning o‘z bazaviy darajasiga nisbatan dinamik kuzatuv bilan avtomatik cheklanadi. Beshinchidan, soxta signallar va ortiqcha yo‘llanmalar ulushi xavfsizlik ko‘rsatkichi sifatida alohida hisobga olinadi.

Ma’lumotlar xavfsizligi arxitekturasi. Model uchun quyidagi texnik-tashkiliy talablar taklif etildi. (1) Konturlarni ajratish: tibbiy mazmun (javoblar, ballar, portret ko‘rsatkichlari, klinik xulosa) va ma’muriy qism (tekshiruvdan o‘tganlik va yo‘naltirish bajarilganligi maqomi) alohida saqlanadi; ma’muriy foydalanuvchi signal pog‘onasini ham, javoblarni ham ko‘rmaydi. (2) Psevdonimlashtirish: tahlil shaxssizlashtirilgan kod bo‘yicha olib boriladi, identifikatsiya kaliti alohida, kirish huquqi cheklangan muhitda saqlanadi va faqat klinik zarurat bo‘lganda mas’ul shifokor tomonidan ochiladi. (3) Kriptografik himoya: uzatishda zamonaviy TLS protokoli, saqlashda simmetrik shifrlash qo‘llanadi; aloqa uzilganda ma’lumotlar shifrlangan oflayn navbatda turadi. (4) Rolga asoslangan kirish va har bir ko‘rish, o‘zgartirish va eksport amalini qayd etuvchi o‘zgartirib bo‘lmaydigan audit jurnali. (5) Minimallashtirish: yuz tasviri biometrik ma’lumot sifatida alohida rozilik asosida qayta ishlanadi, uni saqlash muddati protokolda cheklanadi. (6) Versiyalash: har bir signal algoritm

versiyasi va kiruvchi ma’lumotlar manbasi bilan birga qayd etiladi, bu natijani keyinchalik mustaqil tekshirish imkonini beradi.

Sifat ko‘rsatkichlari. Model uch guruh ko‘rsatkich bilan baholanadi: klinik (sezgirlik, spetsifiklik, mutaxassislar bilan muvofiqlik, kalibrovka), jarayon (tekshiruvni yakunlaganlar ulushi, signaldan konsultatsiyagacha bo‘lgan vaqt, keyingi kontakt bajarilishi) va xavfsizlik (soxta signallar ulushi, ortiqcha yo‘llanmalar, ruxsatsiz kirishga urinishlar va audit jurnalidagi og‘ishlar).

Muhokama. Taklif etilgan model NEWS kabi klinik erta ogohlantirish tizimlarining mantiqini [1] ruhiy salomatlik sohasiga moslashtiradi, biroq bir muhim farq bilan: u individual hodisani bashorat qilishga da’vo qilmaydi. Prognostik modellarning past ijobiy prognostik qiymati [3] va xavf omillarining zaif bashorat qobiliyati [2] sharoitida signalni «xavf darajasi» sifatida emas, balki aniq klinik harakatga bog‘langan marshrut sifatida talqin qilish NICE NG225 tavsiyalariga [6] va klinik formulirovka konsepsiyasiga [7] mos keladi. Eng yuqori pog‘onani faqat klinik mezonlarga bog‘lash qoidasi algoritmik xatoning eng og‘ir oqibatlari - asossiz cheklov yoki, aksincha, xavotirli holatni o‘tkazib yuborish ehtimolini kamaytiradi.

Raqamli portretga ruxsat etilgan rolning torligi ham dalillarga asoslangan: yuz ifodalari va ichki holat o‘rtasidagi bog‘liqlik universal emas [4], shuning uchun portret faqat qo‘shimcha suhbatga yo‘naltirishni kuchaytiruvchi, lekin xavfni hech qachon pasaytirmaydigan komponent sifatida qoldirildi. Oldindan belgilangan qabul mezonlari va kalibrovka tekshiruvi [10] komponent haqiqiy klinik ma’lumotlarda o‘zini oqlamagan taqdirda uning rolini avtomatik cheklaydi. Bu yondashuv DECIDE-AI tavsiyalarida [14] ta’kidlangan inson va algoritmning o‘zaro ta’siri, mutaxassis tavsiyani rad etgan holatlar va xatolarni hujjatlashtirish talablariga javob beradi. Maqsadli yorliqni tanlashda murojaatlar soni kabi bilvosita ko‘rsatkichlardan qochish tizimli tarafkashlik xavfini kamaytiradi [5].

Axborot xavfsizligi nuqtai nazaridan modelning asosiy xavfi tashqi hujumdan ko‘ra ichki noto‘g‘ri foydalanish - ruhiy salomatlik ma’lumotlarining kadrlar qarorlariga ta’sir qilishidir. Shu sababli konturlarni ajratish, psevdonimlashtirish va audit jurnali texnik chora bo‘lishi bilan birga xodimlar ishonchini ta’minlovchi klinik choradir: maxfiylikka ishonch bo‘lmasa, xodimlar javoblarini «yumshatadi» va skrining sezgirligi pasayadi. Boshqacha aytganda, kiberxavfsizlik bu tizimda diagnostik aniqlikning shartlaridan biriga aylanadi. «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun huquqiy oqibatlarga olib keladigan faqat avtomatlashtirilgan qarorlarni cheklaydi [11]; modelda mutaxassis tasdig‘ining majburiyligi ushbu talabni bevosita amalga oshiradi. Yevropa Ittifoqining sun’iy intellekt to‘g‘risidagi reglamenti ish joyida emotsiyalarni aniqlash tizimlarini tibbiy va xavfsizlik maqsadlaridan tashqari taqiqlaydi [15]; bu norma O‘zbekistonda bevosita amal qilmasa-da, raqamli vizual tahlilni faqat tibbiy maqsadda va qat’iy kafolatlar bilan qo‘llash zarurligini tasdiqlaydi.

Tadqiqot cheklovlari: model konseptual darajada asoslangan va hali prospektiv validatsiyadan o‘tmagan; pog‘onalar mezonlari mahalliy ma’lumotlarda qayta ko‘rib chiqilishi mumkin; modelning suitsidal hodisalarni kamaytirishga ta’siri uzoq muddatli kuzatuv va yetarli statistik quvvatni talab qiladi.

Xulosa

Klinik mezonlarga tayangan, raqamli portretni yordamchi komponent sifatida qo‘llaydigan uch pog‘onali integral xulosa modeli IIO xodimlarida psixologik yordamga muhtojlikni xavfsiz va qayta takrorlanadigan tarzda marshrutlash uchun konseptual jihatdan asoslandi. Eng yuqori pog‘onani faqat klinik mezonlar bilan bog‘lash va portretga xavfni pasaytirish huquqini bermaslik qoidalari algoritmik xatolarning klinik oqibatlarini minimallashtiradi. Tibbiy va ma’muriy konturlarni ajratish, psevdonimlashtirish, kriptografik himoya va audit jurnali ruhiy salomatlik ma’lumotlarining xizmat qarorlariga ta’sir qilishining oldini oladi hamda amaldagi qonunchilik talablariga javob beradi. Modelning profilaktik samaradorligi davriy monitoringda klinik, jarayon va xavfsizlik ko‘rsatkichlari bo‘yicha alohida baholanadi.

Foydalanilgan adabiyotlar

1. Smith G. B., Prytherch D. R., Meredith P. [et al.] The ability of the National Early Warning Score (NEWS) to discriminate patients at risk of early cardiac arrest, unanticipated intensive care unit admission, and death // Resuscitation. – 2013. – Vol. 84, № 4. – P. 465–470. DOI: 10.1016/j.resuscitation.2012.12.016

2. Franklin J. C., Ribeiro J. D., Fox K. R. [et al.] Risk factors for suicidal thoughts and behaviors: a meta-analysis of 50 years of research // Psychological Bulletin. – 2017. – Vol. 143, № 2. – P. 187–232. DOI: 10.1037/bul0000084

3. Belsher B. E., Smolenski D. J., Pruitt L. D. [et al.] Prediction models for suicide attempts and deaths: a systematic review and simulation // JAMA Psychiatry. – 2019. – Vol. 76, № 6. – P. 642–651. DOI: 10.1001/jamapsychiatry.2019.0174

4. Barrett L. F., Adolphs R., Marsella S. [et al.] Emotional expressions reconsidered: challenges to inferring emotion from human facial movements // Psychological Science in the Public Interest. – 2019. – Vol. 20, № 1. – P. 1–68. DOI: 10.1177/1529100619832930

5. Obermeyer Z., Powers B., Vogeli C. [et al.] Dissecting racial bias in an algorithm used to manage the health of populations // Science. – 2019. – Vol. 366, № 6464. – P. 447–453. DOI: 10.1126/science.aax2342

6. National Institute for Health and Care Excellence. Self-harm: assessment, management and preventing recurrence. NICE guideline NG225. – London : NICE, 2022. – URL: https://www.nice.org.uk/guidance/ng225

7. Pisani A. R., Murrie D. C., Silverman M. M. Reformulating suicide risk formulation: from prediction to prevention // Academic Psychiatry. – 2016. – Vol. 40, № 4. – P. 623–629. DOI: 10.1007/s40596-015-0434-6

8. Collins G. S., Moons K. G. M., Dhiman P. [et al.] TRIPOD+AI statement: updated guidance for reporting clinical prediction models that use regression or machine learning methods // BMJ. – 2024. – Vol. 385. – Art. e078378. DOI: 10.1136/bmj-2023-078378

9. Moons K. G. M., Damen J. A. A., Kaul T. [et al.] PROBAST+AI: an updated quality, risk of bias, and applicability assessment tool for prediction models using regression or artificial intelligence methods // BMJ. – 2025. – Vol. 388. – Art. e082505. DOI: 10.1136/bmj-2024-082505

10. Van Calster B., McLernon D. J., van Smeden M. [et al.] Calibration: the Achilles heel of predictive analytics // BMC Medicine. – 2019. – Vol. 17. – Art. 230. DOI: 10.1186/s12916-019-1466-7

11. Shaxsga doir ma’lumotlar to‘g‘risida : O‘zbekiston Respublikasining 02.07.2019 yildagi O‘RQ-547-son Qonuni. – URL: https://lex.uz/docs/4396428

12. Kiberxavfsizlik to‘g‘risida : O‘zbekiston Respublikasining 15.04.2022 yildagi O‘RQ-764-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi (LexUZ).

13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. – Geneva : ISO, 2022. – 19 p.

14. Vasey B., Nagendran M., Campbell B. [et al.] Reporting guideline for the early-stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI // BMJ. – 2022. – Vol. 377. – Art. e070904. DOI: 10.1136/bmj-2022-070904

15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. – 2024. – L series. – URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

LOG-FAYLLARNI SAQLASH KAMCHILIKLARINI BARTARAF ETISH USULLARI VA ULAR ORASIDA BLOKCHEYN TEXNOLOGIYASINING O‘RNI

Xabibullayev J.D., Xamidov Sh.J.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada an’anaviy log saqlash modelining avvalgi tadqiqotda aniqlangan sakkizta kamchiligini bartaraf etish usullari tahlil qilingan. Usullar to‘rt guruhga ajratilgan: uzatish kanalini himoyalash, ishonchli saqlash va vaqt, kriptografik va Merkle daraxtiga asoslangan shaffof jurnallar, blokcheyn asosidagi taqsimlangan guvoh. Har bir usulning qaysi kamchilikni bartaraf etishi qiyosiy jadvalda ko‘rsatilgan. Hech bir usul barcha kamchiliklarni yakka o‘zi qamrab olmasligi, blokcheyn esa administratorga ishonch bilan bog‘liq kamchiliklar – tarixni qayta yozish, yagona ishonch nuqtasi va uchinchi tomon tekshiruvi masalalarini hal qilishda alohida o‘rin tutishi asoslangan. Blokcheyn hal qilmaydigan masalalar ham aniqlangan.

Kalit so‘zlar: log-fayl, yaxlitlik, syslog, TLS, vaqt tamg‘asi, kriptografik jurnal, Merkle daraxti, blokcheyn, ruxsatli blokcheyn.

Аннотация. В статье проанализированы методы устранения восьми недостатков традиционной модели хранения журналов, выявленных в предыдущем исследовании. Методы разделены на четыре группы: защита канала передачи, надёжное хранение и время, криптографические и прозрачные журналы на основе дерева Меркла, распределённый свидетель на основе блокчейна. В сравнительной таблице показано, какие недостатки устраняет каждый метод. Обосновано, что ни один метод в отдельности не охватывает все недостатки, а блокчейн занимает особое место в решении проблем, связанных с доверием к администратору: перезаписи истории, единой точки доверия и проверки третьей стороной. Определены также задачи, которые блокчейн не решает.

Ключевые слова: лог-файл, целостность, syslog, TLS, временная метка, криптографический журнал, дерево Меркла, блокчейн, разрешённый блокчейн.

Kirish

Avvalgi tadqiqotimizda log-fayllarni saqlashning an’anaviy modeli tahlil qilinib, uning sakkizta xavfsizlik kamchiligi aniqlangan edi: loglarning qayd etilayotgan tizim ichida saqlanishi (K1), kriptografik himoyaning yo‘qligi (K2), uzatish kanalining himoyasizligi (K3), jurnal yozishni to‘xtatish imkoniyati (K4), vaqt tamg‘alarining ishonchsizligi (K5), rotatsiya cheklovlari (K6), markazlashgan tizimning yagona ishonch nuqtasiga aylanishi (K7) va uchinchi tomon tekshiruvining imkonsizligi (K8). Ulardan to‘rttasi – K1, K2, K7 va K8 – log tizimi administratoriga shartsiz ishonchdan kelib chiqadi.

Ushbu maqolaning maqsadi – har bir kamchilikni bartaraf etishning mavjud usullarini tahlil qilish, ularning cheklovlarini aniqlash va bu usullar orasida blokcheyn texnologiyasining o‘rnini belgilash.

Uzatish kanalini himoyalash

Syslog xabarlarini TLS protokoli orqali uzatishni belgilovchi RFC 5425 standarti uzatish paytida xabarlarning maxfiyligi va butunligini hamda serverning autentifikatsiyasini ta’minlaydi va K3 kamchiligini bartaraf etadi. Imzolangan syslog xabarlari standarti (RFC 5848) esa xabar manbaini autentifikatsiya qiladi va tartib raqamlari orqali yo‘qolgan xabarlarni aniqlash imkonini beradi; bu K4 kamchiligini qisman yumshatadi. Ushbu usullarning cheklovi shundaki, ular xabarni

faqat yo‘lda himoyalaydi: xabar qabul qiluvchi serverda saqlangandan keyin uning administratori uni o‘zgartira oladi.

Ishonchli saqlash va vaqt

Qayta yozib bo‘lmaydigan (WORM – write once, read many) saqlash yozuvlarni belgilangan muddat davomida o‘zgartirish va o‘chirishdan himoyalaydi. Loglarni zudlik bilan alohida serverga uzatish va saqlash ma’murini tizim ma’muridan ajratish K1 va K6 kamchiliklarini sezilarli kamaytiradi. Biroq bu usullar saqlash tizimi yoki uning ma’muriga ishonchni saqlab qoladi va uchinchi tomonga yaxlitlikni isbotlay olmaydi.

Vaqt tamg‘alarining ishonchliligi (K5) ikki darajada ta’minlanadi. Tarmoq vaqtini autentifikatsiyalash standarti (NTS, RFC 8915) vaqt manbaini soxtalashtirishdan himoyalaydi. Ishonchli vaqt tamg‘asi xizmati (RFC 3161) esa ma’lumot xeshiga imzolangan vaqt belgisini berib, yozuv ma’lum paytda mavjud bo‘lganini isbotlaydi. Cheklov – vaqt tamg‘asi xizmatiga ishonch va har bir so‘rov uchun tarmoq murojaati zarurati.

Kriptografik va shaffof jurnallar

B. Schneier va J. Kelsey har bir yozuvni xabar autentifikatsiya kodi bilan himoyalash va kalitni har qadamda bir tomonlama funksiya bilan yangilash g‘oyasini taklif etgan: hujumchi joriy kalitni qo‘lga kiritsa ham, oldingi yozuvlarni sezdirmasdan o‘zgartira olmaydi. D. Ma va G. Tsudik bu sxemaning jurnal oxirini kesish hujumiga zaifligini ko‘rsatib, ochiq tekshiriladigan oldinga xavfsiz agregat imzolarni taklif etgan. Bu usullar K2 kamchiligini bartaraf etadi.

Merkle daraxti asosidagi shaffof jurnallar yanada kuchli kafolat beradi. S. Crosby va D. Wallach tomonidan taklif etilgan “tarix daraxti” yozuvning jurnalga kiritilganligini va jurnalning ikki versiyasi o‘zaro mosligini logarifmik hajmdagi isbot bilan tekshirish imkonini beradi. Shu tamoyil Certificate Transparency standartida (RFC 9162) qo‘llanilib, internetdagi TLS sertifikatlari ommaviy jurnallarda qayd etiladi. Bu usullarning umumiy cheklovi – mustaqil guvohning yo‘qligi: kriptografik jurnal tekshiruv kalitini saqlovchi tomonga, shaffof jurnal esa jurnal versiyalarini o‘zaro solishtiruvchi auditorlarga tayanadi.

Blokcheyn asosidagi taqsimlangan guvoh

Blokcheyn texnologiyasi aynan mustaqil guvoh muammosini hal qiladi: log yozuvlarining yoki ularning Merkle ildizlarining xeshi bir-biridan mustaqil tugunlar tomonidan yuritiladigan reyestrga yoziladi va keyinchalik uni bitta tomon o‘zgartira olmaydi. Tadqiqotlarda ikki yondashuv ajralib turadi.

Birinchisi – log ildizlarini ochiq blokcheynga qayd etish. J. Cucurull va J. Puiggalí xavfsiz log ildizlarini ochiq blokcheynga yozish orqali ularni o‘zgartirib bo‘lmaydigan qilishni taklif etgan. Bu usul qo‘shimcha infratuzilma talab qilmaydi, biroq tashqi tarmoqqa bog‘liq va tranzaksiyalarning tasdiqlanishi kechikadi.

Ikkinchisi – ruxsatli blokcheyn. A. Ahmad va hammualliflari audit yozuvlarini PBFT konsensusli ruxsatli blokcheynda replikatsiya qilgan. B. Putz, F. Menges va G. Pernul har bir log yozuvining mavjudlik isbotini Exonum platformasidagi ruxsatli blokcheynda saqlovchi infratuzilmani yaratgan; uning prototipida o‘rtacha 3 000–3 500 tranzaksiya/s o‘tkazuvchanlik qayd etilgan, 4, 7 va 10 tugunli konfiguratsiyalar esa mos ravishda 1, 2 va 3 ta Vizantiya tuguniga chidagan. Bu Vizantiya xatolariga chidamli konsensusning $n \geq 3f + 1$ shartiga mos keladi.

Blokcheynning cheklovlarini ham aniq belgilash zarur. Birinchidan, u jurnal yozish xizmati to‘xtatilgan holatni (K4) va kiritish paytida noto‘g‘ri ma’lumot yozilishini aniqlay olmaydi: blokcheyn faqat unga yetkazilgan narsani himoya qiladi. Ikkinchidan, yozuv yaratilgan paytdan blokcheynga qayd etilgunga qadar himoyasiz oyna mavjud. Uchinchidan, ruxsatli

blokcheyn tugunlari turli tashkilotlar yoki bo‘linmalar nazoratida bo‘lmasa, konsensus kafolati o‘z mazmunini yo‘qotadi.

Tadqiqot natijalari

Tahlil natijalari 1-jadvalda umumlashtirilgan. Baholash ko‘rib chiqilgan manbalar asosida sifat jihatdan amalga oshirilgan: “+” – usul kamchilikni bartaraf etadi, “±” – qisman bartaraf etadi, “–” – bartaraf etmaydi.

1-jadval

Log saqlash kamchiliklari va ularni bartaraf etish usullari

Kamchilik	TLS / imzolangan syslog	WORM saqlash	NTS / vaqt tamg‘asi	Kriptografik jurnal	Merkle jurnal	Blokcheyn
K1. Tizim ichida saqlash	±	+	–	±	±	+
K2. Kriptografik himoya yo‘q	±	±	±	+	+	+
K3. Himoyasiz uzatish	+	–	–	–	–	–
K4. Jurnal yozishni to‘xtatish	±	–	–	–	–	–
K5. Ishonchsiz vaqt tamg‘asi	–	–	+	–	–	±
K6. Rotatsiya cheklovlari	–	+	–	–	–	±
K7. Yagona ishonch nuqtasi	–	±	–	–	±	+
K8. Mustaqil tekshiruv yo‘q	–	–	±	±	+	+

Jadvaldan uchta xulosa kelib chiqadi. Birinchidan, hech bir usul barcha kamchiliklarni yakka o‘zi qamrab olmaydi; samarali himoya bir nechta usulning qatlamli birikmasini talab qiladi. Ikkinchidan, blokcheyn administratorga ishonch bilan bog‘liq kamchiliklarni – K1, K7 va K8 ni – to‘liq bartaraf etuvchi yagona usul hisoblanadi. Uchinchidan, K3 va K4 kamchiliklari blokcheyn tomonidan hal etilmaydi va uzatish darajasidagi himoya hamda jurnal yozilishini monitoring qilishni talab qiladi.

Ushbu xulosa amaliy tajriba bilan ham tasdiqlandi. Xesh zanjiri asosidagi jurnal prototipida modellashtirilgan beshta hujumdan ikkitasi – butun zanjirni qayta hisoblash va jurnal oxirini kesish – ichki kriptografik tekshiruvdan o‘tib ketdi va faqat tashqi guvohga qayd etilgan qiymat yordamida aniqlandi. Bu natija kriptografik jurnal tashqi guvohsiz K1 va K7 kamchiliklarini bartaraf eta olmasligini va blokcheyn qatlamining zarurligini ko‘rsatadi.

Xulosa

An’anaviy log saqlash modelining sakkizta kamchiligini bartaraf etish usullari to‘rt guruhga ajratilib, o‘zaro solishtirildi. Uzatish kanalini himoyalash, ishonchli saqlash va vaqt, kriptografik va shaffof jurnallar alohida kamchiliklarni bartaraf etadi, biroq ularning barchasi qandaydir tomonga ishonchni saqlab qoladi.

Blokcheyn texnologiyasi bu ishonchni bir-biridan mustaqil tugunlar o‘rtasida taqsimlab, tarixni qayta yozish, yagona ishonch nuqtasi va uchinchi tomon tekshiruvi masalalarini hal qiladi.

Blokcheyn mustaqil yechim emas: jurnal yozishning to‘xtatilishi, uzatish xavfsizligi va kiritish paytidagi to‘g‘rilik boshqa usullar bilan ta’minlanishi kerak.

Shu sababli log-fayllar yaxlitligini ta’minlashning istiqbolli yo‘nalishi – uzatish himoyasi, kriptografik zanjir, Merkle agregatsiyasi va ruxsatli blokcheyn qatlamini birlashtiruvchi qatlamli model. Bunday modelda yozuv yaratilishidan blokcheynga qayd etilgunga qadar bo‘lgan himoyasiz oyna va blokcheyn yuklamasi o‘rtasidagi muvozanatni asoslab tanlash keyingi tadqiqotlarning asosiy vazifasi hisoblanadi.

Foydalanilgan adabiyotlar

1. B. Schneier and J. Kelsey, “Secure audit logs to support computer forensics”, ACM Trans. Inf. Syst. Secur., vol. 2, no. 2, pp. 159–176, May 1999, doi: 10.1145/317087.317089.

2. D. Ma and G. Tsudik, “A new approach to secure logging”, ACM Trans. Storage, vol. 5, no. 1, pp. 1–21, Mar. 2009, doi: 10.1145/1502777.1502779.

3. S. A. Crosby and D. S. Wallach, “Efficient data structures for tamper-evident logging”, in Proc. 18th USENIX Security Symp., Montreal, Canada, 2009, pp. 317–334.

4. J. Cucurull and J. Puiggalí, “Distributed immutabilization of secure logs”, in Security and Trust Management (STM 2016), LNCS, vol. 9871. Cham, Switzerland: Springer, 2016, pp. 122–137.

5. B. Putz, F. Menges and G. Pernul, “A secure and auditable logging infrastructure based on a permissioned blockchain”, Comput. Secur., vol. 87, Art. no. 101602, 2019, doi: 10.1016/j.cose.2019.101602.

TARMOQ OQIMINI TAHLIL QILISH ASOSIDA HUJUMLARNI ANIQLASHNING MA’LUMOT SIZISHIGA CHIDAMLI USUL VA ALGORITMLARI

Maxkamova D.B.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada tarmoq oqimlari asosida hujumlarni aniqlash tizimlarini (NIDS) baholashdagi ma’lumot sizishi va domenlararo beqarorlik muammolari tahlil qilinadi. Sizish kanalini miqdoriy o‘lchovchi nazoratli sinov usuli, IP-manzillarga tayanmaydigan surrogat servis-graf qurish usuli hamda faqat normal trafikda o‘qitiladigan FlowGuard o‘z-o‘zini nazorat qiluvchi modeli taklif etiladi. CORAL asosidagi belgisiz domenga moslashtirish algoritmi va uning qo‘llanilish shartini belgisiz tekshiruvchi indikator keltiriladi. Natijalar NetFlow v2 formatidagi uchta ochiq etalon to‘plamda yagona sizish nazorat protokoli doirasida tasdiqlangan.

Kalit so‘zlar: hujumlarni aniqlash tizimi, tarmoq oqimi, NetFlow, ma’lumot sizishi, graf neyron tarmog‘i, o‘z-o‘zini nazorat qiluvchi o‘qitish, domenga moslashtirish, CORAL.

Аннотация. В статье анализируются две системные проблемы оценки систем обнаружения атак (NIDS) на основе сетевых потоков - утечка данных и междоменная нестабильность. Предлагаются метод контролируемого зонда для количественного измерения канала утечки, метод построения суррогатного сервис-графа без опоры на IP-адреса, а также самоконтролируемая модель FlowGuard, обучаемая только на нормальном трафике. Приводятся алгоритм доменной адаптации без меток на основе CORAL и индикатор проверки условия его применимости. Результаты подтверждены на трёх открытых эталонных наборах формата NetFlow v2 в рамках единого протокола оценки.

Ключевые слова: система обнаружения атак, сетевой поток, NetFlow, утечка данных, графовая нейронная сеть, самоконтролируемое обучение, доменная адаптация, CORAL.

Kirish

Shifrlangan trafik ulushining keskin o‘sishi paket mazmunini bevosita tahlil qilishga asoslangan an’anaviy himoya vositalarining imkoniyatlarini cheklab qo‘ydi. Natijada tarmoq monitoringining og‘irlik markazi oqim darajasidagi statistik telemetriyaga, ya’ni NetFlow va IPFIX yozuvlariga ko‘chdi, hujumlarni aniqlash tizimlarida (NIDS) esa mashinali va chuqur o‘qitish usullari yetakchi yondashuvga aylandi [3]. Ayniqsa tarmoq oqimlarini graf ko‘rinishida tasvirlab, ularni qimmat qo‘lda belgilanadigan sinf belgilarisiz, o‘z-o‘zini nazorat qiluvchi rejimda o‘qitadigan graf neyron tarmoqlari istiqbolli yo‘nalish sifatida rivojlanmoqda [2], [5].

Biroq ushbu yo‘nalishda e’lon qilinayotgan yuqori natijalarning ishonchliligi jiddiy savol ostida qolmoqda. Baholash bosqichida yuzaga keladigan ma’lumot sizishi, xususan, hujum sinfi belgilaridan foydalanadigan maqsadli kodlash, trening va test bo‘linishlarida takrorlanadigan identifikatorlar (portlar, IP-manzillar) hamda vaqt tartibini buzuvchi tasodifiy bo‘linishlar natijalarni sun’iy oshirib yuboradi. Bundan tashqari, bitta to‘plamda yuqori ko‘rsatkich bergan modellarning boshqa tarmoq muhitiga ko‘chuvchanligi tizimli baholanmagan, mavjud tadqiqotlar esa bu rejimda samaradorlikning keskin pasayishini qayd etadi [1]. Shu ikki muammo o‘z-o‘zini nazorat qiluvchi graf NIDS modellarini real tarmoq infratuzilmasiga joriy etish yo‘lidagi asosiy ilmiy to‘siq hisoblanadi.

O‘zbekiston Respublikasida axborot xavfsizligini ta’minlash davlat siyosatining ustuvor yo‘nalishlaridan biri sifatida belgilangan: «Kiberxavfsizlik to‘g‘risida»gi Qonun (2022-yil 15-aprel, O‘RQ-764) hamda «Raqamli O‘zbekiston - 2030» strategiyasi bilan milliy axborot-kommunikatsiya infratuzilmasini kiberhujumlardan himoya qilish va zamonaviy intellektual himoya vositalarini joriy etish vazifalari qo‘yilgan. Milliy tarmoqlarning o‘ziga xos trafik tarkibi sharoitida xorijiy to‘plamlarda o‘qitilgan modellarning to‘g‘ridan-to‘g‘ri ko‘chirilishi aynan domenlararo beqarorlik tufayli samarasiz bo‘lishi mumkin. Tadqiqotning maqsadi - tarmoq oqimini tahlil qilish asosida hujumlarni aniqlashning ma’lumot sizishiga chidamli, yangi tarmoqqa qo‘shimcha o‘qitishsiz ko‘chuvchan va hisoblash jihatidan yengil usul va algoritmlarini ishlab chiqishdir.

Asosiy qism. Ma’lumot sizishini miqdoriy o‘lchash uchun nazoratli sinov usuli taklif etildi. Tekshirilayotgan xususiyat kanali bo‘yicha alohida nazoratli klassifikator o‘qitilib, uning to‘plam ichidagi va to‘plamlararo ko‘rsatkichlari orasidagi tafovut Δ sinf belgisi sizishining o‘lchovi sifatida qabul qilinadi. Hujumning haqiqiy xulq-atvor alomati ikki rejimda ham ishlashi kerak; kanal faqat bitta to‘plamda ishlasa, u sinf belgisining o‘rnini bosuvchi xususiyat hisoblanadi. Nazorat guruhi sifatida statistik xususiyatlar olinadi: ularning Δ i sizishni emas, tarmoq muhitlari orasidagi taqsimot siljishini ko‘rsatadi. Sinovlar bitta urug‘da o‘tkazildi (1-jadvalda tarqoqlik ko‘rsatkichi yo‘q); kuzatilgan farqlar urug‘ tarqoqligidan ancha katta. Natijalar 1-jadvalda keltirilgan.

1-jadval

Nazoratli zond natijalari: port kanali orqali yorliq sizishi

Trening to‘plami	Kanal	To‘plam ichida ROC-AUC	To‘plamlararo ROC-AUC
NF-UNSW-NB15-v2	port	0,8581	0,9564
NF-UNSW-NB15-v2	statistik	0,9864	0,1041
NF-BoT-IoT-v2	port	0,9980	0,6146
NF-BoT-IoT-v2	statistik	0,9700	0,3545

NF-BoT-IoT-v2 to‘plamida yolg‘iz port kanali to‘plam ichida ROC-AUC = 0,998 va PR-AUC = 1,000 ko‘rsatkichini beradi, to‘plamlararo rejimda esa bu qiymatlar 0,615 va 0,0613 gacha tushadi (Δ = 0,383): port identifikatorlari sun’iy generatsiyalangan to‘plamda sinf belgisining o‘rnini bosuvchi xususiyat sifatida ishlaydi. NF-UNSW-NB15-v2 da port kanali to‘plamlararo rejimda pasaymaydi (Δ = −0,098), ya’ni bu to‘plamda sizish kanali sifatida namoyon bo‘lmadi. Statistik kanalda ikkala to‘plamda ham katta Δ kuzatiladi (0,882 va 0,616), bu sizishni emas, domen siljishini ifodalaydi. IP sinovi tasodifiy va manba IP bo‘yicha guruhlangan bo‘linishda deyarli o‘zgarmadi (PR-AUC 0,901 va 0,899), demak manba IP kodlash bu to‘plamda hal qiluvchi sizish kanali emas; guruhlash faqat manba manzil bo‘yicha bajarilgani uchun manzil kanali to‘liq yopilgan deb bo‘lmaydi. Bu salbiy natija ochiq qayd etildi.

Sinov natijalari asosida sizish-nazorat siyosati ishlab chiqildi. IP-manzillar to‘liq chiqariladi, portlar uchta toifaga (tizimli, ro‘yxatga olingan, dinamik) o‘tkaziladi, sinf belgisiga bog‘liq kodlashlar taqiqlanadi, hajmiy va vaqt xususiyatlariga ln(1 + x) qo‘llanadi, standartlashtirish parametrlari esa faqat trening to‘plamining normal oqimlarida hisoblanadi. Siyosatning chiqishi - har bir oqim uchun 41 o‘lchamli xususiyat vektori.

IP-manzillarsiz graf kontekstini saqlab qolish uchun surrogat servis-graf qurish usuli taklif etildi. Grafning tugunlari xizmat turlariga, qirralari esa oqimlarga mos keladi. Tugun kaliti

PROTOCOL, L7_PROTO, yo‘nalish, port toifasi to‘rtligi bilan aniqlanadi va to‘plamga xos hech qanday identifikatorni o‘z ichiga olmaydi. Kalit fazosining to‘plamdan mustaqil chegara bilan chegaralanganligi rasmiy tasdiqlangan va empirik jihatdan ham kuzatildi: NF-UNSW-NB15-v2 va NF-BoT-IoT-v2 ning trening-normal va test bo‘limlarida tugunlar soni 99–432 oralig‘ida bo‘ldi. Usul yangi xizmatlarga o‘z-o‘zidan moslashadi: ilgari uchramagan ilova-qatlam protokoli paydo bo‘lsa, graf unga yangi tugun qo‘shadi, tugunning konteksti faqat shu protokolning birinchi oqimlaridan hisoblanadi va modelni qayta o‘qitish talab etilmaydi.

FlowGuard usuli faqat normal trafikda o‘qitiladi va rekonstruksiya xatosiga tayanadi. Model oqim xususiyatlarini servis-graf bo‘ylab tarqatuvchi enkoderdan, ularni qayta tiklovchi MLP dekoderdan va faqat normal oqimlarda o‘qitiladigan MSE yo‘qotish funksiyasidan iborat bo‘lib, qaror chegarasi trening normallarining tiklash xatolari bo‘yicha belgilanadi. Oqim semantikasini saqlovchi augmentatsiya algoritmi taklif etilib, ablatsion tahlil o‘tkazildi: none, mask, drop va mask+drop konfiguratsiyalarida ROC-AUC 0,9623–0,9683 oralig‘ida qoldi, ya’ni modelning asosiy samarasi augmentatsiyalarga emas, graf strukturasi va rekonstruksiya maqsadiga tayanadi.

Eksperimentlar NetFlow v2 standart formatidagi uchta ochiq to‘plamda - NF-UNSW-NB15-v2 (hujum ulushi ≈3,8 %), NF-BoT-IoT-v2 (≈99,6 %) va NF-CSE-CIC-IDS2018-v2 (≈11,8 %) - beshta mustaqil urug‘da o‘tkazildi; har to‘plamdan trening uchun 100 000 normal oqim, test uchun 200 000 oqim ajratildi [4], [6], [7], [8]. To‘plam ichidagi rejimda FlowGuard ishonchli natija berdi (NF-UNSW-NB15-v2 uchun ROC-AUC = 0,9682 ± 0,0007; NF-CSE-CIC-IDS2018-v2 uchun 0,9148 ± 0,0031). Xolis taqqoslashda to‘plam ichidagi rejimda FlowGuard bazaviy usullardan ustun emas (NF-UNSW-NB15-v2 da PR-AUC: FlowGuard 0,564, Isolation Forest 0,314, PCA-rekonstruksiya 0,578, MLP-avtoenkoder 0,639). Usulning afzalligi aniqlikda emas, sizishga chidamlilikda, to‘plamlararo ko‘chirish barqarorligida va minimal resurs talabida. To‘plamlararo rejimda graf komponenti ikki korporativ tarmoq orasida modelni o‘zgartirmasdan ko‘chirganda ROC-AUC ni 0,10–0,12 ga oshiradi va natijalarni 20–25 baravar barqarorlashtiradi.

To‘plamlararo ko‘chuvchanlikni ta’minlash uchun CORAL [9] usuliga asoslangan, sinf belgilarisiz (belgisiz) tarmoq muhitiga moslashtirish algoritmi ishlab chiqildi. Klassik CORAL to‘rt jihatdan takomillashtirildi: (1) kovariatsiya matritsalari regulyarizatsiya bilan barqarorlashtirildi; (2) moslashtirish IP-manzillarsiz, sizish-nazorat siyosatidan o‘tgan xususiyatlar fazosida bajariladi; (3) maqsad oqimlari manba fazosiga o‘tkaziladi, shu sababli o‘qitilgan model va uning chegarasi o‘zgarishsiz qoladi; (4) moslashtirish qo‘llanishdan oldin belgisiz himoya sharti ($\varphi > 0,9$ bo‘lsa to‘xtatish) bilan tekshiriladi. Algoritm yangi tarmoqda na sinf belgilarini, na qo‘shimcha o‘qitishni talab qiladi. Uchta to‘plamning 3×3 matritsasi bo‘yicha natijalar 2-jadvalda keltirilgan. Moslashtirish uch yo‘nalishda aniqlikni sezilarli oshirdi (masalan, 0,331 dan 0,926 gacha), bir yo‘nalishda neytral bo‘ldi, hujum ustun bo‘lgan ikki yo‘nalishda esa himoya sharti uni to‘xtatadi, chunki aks holda natija teskarilanadi.

2-jadval

CORAL asosidagi belgisiz domenga moslashtirish natijalari

Yo‘nalish	Hujum ulushi	ROC-AUC	ROC-AUC	φ sharti
BoT-IoT → UNSW	0,038	0,3312	0,9261	bajarilgan
IDS2018 → UNSW	0,038	0,4417	0,8969	bajarilgan
UNSW → IDS2018	0,118	0,5118	0,6601	bajarilgan
BoT-IoT → IDS2018	0,118	0,5765	0,5887	bajarilgan

Yo‘nalish	Hujum ulushi	ROC-AUC	ROC-AUC	φ sharti
UNSW → BoT-IoT	0,996	0,1655	0,0108	buzilgan
IDS2018 → BoT-IoT	0,996	0,5765	0,0131	buzilgan

2-jadvaldan ko‘rinadiki, xom to‘plamlararo ko‘chirish oltita yo‘nalishning barchasida ishlamaydi. CORAL BoT-IoT → UNSW yo‘nalishida ROC-AUC ni 0,3312 dan 0,9261 gacha (bazaviy ulushga nisbatan PR-lift 0,9 dan 9,2 gacha), IDS2018 → UNSW yo‘nalishida esa 0,4417 dan 0,8969 gacha oshirdi. Usulning chegaraviy sharti - maqsad oqimida normal trafik ustunligi - ikki tomonlama tasdiqlandi: shart buzilgan ikki yo‘nalishda (himoya o‘chirilgan holda) ROC-AUC 0,01 darajasiga quladi, shart bajarilgan to‘rt yo‘nalishda esa zarar kuzatilmadi. Shu sababli shartni maqsad tarmoqda belgisiz tekshiruvchi φ(xom) indikatori va $\varphi > 0,9$ to‘xtatish qoidasi taklif etildi. Qoida olti yo‘nalishning barchasida to‘g‘ri qaror qabul qildi: buzilgan yo‘nalishlarda φ(xom) = 0,988 va 0,907, qolgan to‘rttasida 0,797 dan oshmadi.

Taklif etilgan usul va algoritmlar o‘n modulli yagona dasturiy ishlov berish zanjiri - FlowGuard dasturiy majmuasi va tahlilchi uchun FlowGuard Inspector ilovasi ko‘rinishida amalga oshirildi. Modelning hisoblash samaradorligi - 32 617 parametr, 0,13 MB hajm, bitta oqimni baholash vaqti to‘rtta protsessor ipida 1,43–1,88 μs, grafik protsessorda 0,08–0,09 μs. Bu sekundiga yuz minglab oqimni real vaqt rejimida qayta ishlash va maxsus tezlatgichsiz, resursi cheklangan monitoring tugunlariga joylashtirish imkonini beradi. Chegara sezgirligi tahlili qoidaning to‘g‘ri ishlashini tasdiqladi: maqsadli $\alpha = 0,01$ da haqiqiy FPR 0,0098, to‘liqlik 0,692, aniqlik 0,735 va F1 0,713 bo‘lib, konservativ rejim F1 bo‘yicha optimal chiqdi.

Xulosa

Tadqiqotda tarmoq oqimlari asosida hujumlarni aniqlashning ma’lumot sizishiga chidamli usul va algoritmlari majmuasi ishlab chiqildi. Nazoratli sinov usuli etalon to‘plamlarda sizish kanallarini miqdoriy o‘lchash imkonini berdi va port identifikatorlarining sinf belgisi o‘rnini bosuvchi xususiyat sifatida ishlashini NF-BoT-IoT-v2 to‘plamida ko‘rsatdi. IP-manzillarga tayanmaydigan surrogat servis-graf identifikatorlarni kodlash kanalini qurilish bo‘yicha yopadi va induktivlikni ta’minlaydi. CORAL asosidagi moslashtirish algoritmi qo‘shimcha o‘qitishsiz to‘plamlararo ko‘chirishni amalga oshiradi, uning qo‘llanilish sharti esa maqsad tarmoqda belgisiz tekshiriladi. Model 0,13 MB hajmda va mikrosekund darajasidagi tezlikda ishlaydi.

Olingan natijalar asosida amaliy tavsiyalar belgilandi: NIDS modelini baholashda bitta to‘plamdagi ko‘rsatkichni yakuniy sifat o‘lchovi deb olmasdan, uni kamida ikkita to‘plamda, shu jumladan boshqa to‘plamga ko‘chirilgan holda sinash; port va IP xususiyatlarini modelga kiritishdan oldin ularni nazoratli sinov bilan tekshirish, chunki to‘plam ichida yuqori, to‘plamlararo past natija bergan xususiyat sizish kanalidir; modelni yangi tarmoqqa joriy etishda moslashtirishni faqat yangi tarmoq namunasida normal trafik ustunligi belgisiz tekshiruv ($\varphi \le 0,9$) bilan tasdiqlangandan keyin qo‘llash, bu esa zararli holatni oldindan aniqlash imkonini beradi; qaror chegarasini konservativ ($\alpha \approx 0,01$) belgilab, ogohlantirishlarni servis-tugun hamda vaqt oynasi kesimida yagona hodisaga birlashtirish. Kelgusi tadqiqotlar graf signalini vaqt bo‘yicha kontekst bilan kuchaytirish va milliy tarmoq ma’lumotlarida himoyalangan holda dastlabki sinov o‘tkazish yo‘nalishlarida davom ettiriladi.

Foydalanilgan adabiyotlar

1. *Cantone M.*, Marrocco C., Bria A. On the cross-dataset generalization of machine learning for network intrusion detection. arXiv:2402.10974, 2024.

2. *Caville E.*, Lo W.W., Layeghy S., Portmann M. Anomal-E: A self-supervised network intrusion detection system based on graph neural networks. Knowledge-Based Systems, Elsevier, 2022, vol. 258, art. 110030.

3. *Khraisat A.*, Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, Springer, 2019, vol. 2, no. 1, art. 20.

4. *Koroniotis N.*, Moustafa N., Sitnikova E., Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, Elsevier, 2019, vol. 100, pp. 779–796.

5. *Lo W.W.*, Layeghy S., Sarhan M., Gallagher M., Portmann M. E-GraphSAGE: A graph neural network based intrusion detection system for IoT. NOMS 2022 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2022, pp. 1–9.

6. *Moustafa N.*, Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference (MilCIS), IEEE, 2015, pp. 1–6.

7. *Sarhan M.*, Layeghy S., Portmann M. Towards a standard feature set for network intrusion detection system datasets. Mobile Networks and Applications, Springer, 2022, vol. 27, pp. 357–370.

8. *Sharafaldin I.*, Lashkari A.H., Ghorbani A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSP 2018, SciTePress, 2018, pp. 108–116.

9. *Sun B.*, Feng J., Saenko K. Return of frustratingly easy domain adaptation. Proceedings of the AAAI Conference on Artificial Intelligence, AAAI Press, 2016, vol. 30, no. 1, pp. 2058–2065.

ELEKTRON POCHTA TIZIMLARIDA XABARLARINI VEKTORLASH USULLARI

Nasrullayev N.B., Xamidov Sh.J.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Mirzayeva A.B.
EMU universiteti

Annotatsiya. Tezisda elektron pochta xabarlarini sonli belgilarga aylantirishning statistik, taqsimlangan va kontekstual usullari qiyosiy tahlil qilinadi. BoW, TF–IDF, LSA, Word2Vec, GloVe, fastText, Doc2Vec, BERT va Sentence-BERT imkoniyatlari yoritilib, leksik, semantik va tuzilmaviy belgilarni birlashtiruvchi model taklif etiladi. Ish tanlangan ilmiy manbalar sharhiga asoslangan; yangi tajriba natijalari da'vo qilinmaydi.

Kalit so'zlar: elektron pochta, vektorlash, TF–IDF, embedding, BERT, spam, fishing, gibrid model.

Аннотация. В диссертации представлен сравнительный анализ статистических, распределенных и контекстуальных методов преобразования электронных писем в числовые символы. Рассматриваются возможности BoW, TF–IDF, LSA, Word2Vec, GloVe, fastText, Doc2Vec, BERT и Sentence-BERT, а также предлагается модель, объединяющая лексические, семантические и структурные символы. Работа основана на обзоре избранных научных источников; новые экспериментальные результаты не приписываются.

Ключевые слова: электронная почта, векторизация, TF–IDF, встраивание, BERT, спам, фишинг, гибридная модель.

Kirish

Elektron pochta xabarlarini avtomatik saralash, mavzu bo'yicha guruhlash, semantik qidirish hamda spam va fishingni aniqlashda matnni kompyuter qayta ishlay oladigan sonli ko'rinishga o'tkazish zarur. Vektorlash xabarning tanlangan xususiyatlarini belgilangan o'lchamli fazoda ifodalaydi. Bunda vektorlashtiruvchi model va yakuniy tasniflagich alohida komponentlardir: masalan, TF–IDF belgilar hosil qiladi, logistik regressiya esa ushbu belgilar asosida sinfni bashorat qiladi.

Tadqiqotning maqsadi - asosiy vektorlash usullarining elektron pochta uchun afzallik va cheklovlarini aniqlash hamda ularni birlashtirish algoritmini shakllantirish. Tahlil manbalarga tayangan maqsadli adabiyotlar sharhidir; u barcha nashrlarni qamrab oluvchi sistematik sharh emas. Asosiy mezonlar semantik axborotni saqlash, hisoblash sarfi, izohlanuvchanlik va xabarning tuzilishidan foydalanishdir.

Xabarni ifodalash va dastlabki ishlov

Xabar sarlavha, asosiy matn, xizmat maydonlari, havolalar va ilova metama'lumotlaridan tarkib topadi. MIME qismlarini ajratish, kodlashni tiklash va HTMLdan matn olishdan keyin ushbu qismlar alohida saqlanadi. Fishing tahlilida URL va domenlarni butunlay o'chirish foydali belgilarni yo'qotishi mumkin. Matnni tozalash bilan birga havolalar soni, jo'natuvchi va javob manzili domenlarining mosligi kabi belgilar alohida olinishi taklif etiladi.

Statistik vektorlash

BoW usulida lug'atdagi har bir birlik uchun xabarda uchrash soni hisoblanadi. TF–IDF esa ko'p xabarda takrorlanadigan birliklarning vaznini kamaytiradi. Quyida TF sifatida oddiy chastota qo'llangan silliqlangan variant keltiriladi:

$$x_j = \text{count}(t_j, d); \quad w_j = x_j \left[\ln\left(\frac{N+1}{df_j+1}\right) + 1\right] \qquad (1)$$

Bu yerda d - xabar, t_j - lug'at birligi, N - o'qitish xabarlari soni, df_j - t_j qatnashgan o'qitish xabarlari soni. Masalan, «hisobni tasdiqlang» iborasi bigramma sifatida olinishi mumkin. So'z va

belgi n-grammalari lokal ketma-ketlikni saqlaydi, ammo to‘liq gap ma’nosini ifodalamaydi. Lug‘at va IDF faqat o‘qitish qismida aniqlanishi kerak.

O‘lchamni kamaytirish va taqsimlangan vektorlar

LSA hujjat–termin matritsasini kichik rangli yaqinlashuv orqali zich fazoga proyeksiyalaydi. Agar A matritsaning satrlari xabarlar, ustunlari terminlar bo‘lsa, qisqartirilgan singulyar qiymatlar ajratish quyidagicha yoziladi:

$$A \approx U_k \Sigma_k V_k^T; \quad z_d = x_d V_k \tag{2}$$

Bu yerda k - saqlanadigan komponentlar soni; x_d - yangi xabarning o‘sha lug‘atdagi satr vektori. LSA siyrak belgilarni ixchamlashtiradi, biroq komponentlar bevosita tushunarli so‘zlarga teng emas va kontekstga bog‘liq ma’nolarni to‘liq ajratmaydi.

Word2Vecning CBOW va Skip-gram modellari so‘z–kontekst munosabatlaridan zich vektorlarni o‘rganadi. GloVe esa korpusdagi so‘zlarning birga uchrash statistikasi asosida vektorlar hosil qiladi. Ushbu statik modellarda bir so‘zning turli kontekstlardagi ko‘rinishlari odatda bir xil vektorga ega. Butun xabarni ifodalash uchun so‘z vektorlarini birlashtirish talab etiladi; oddiy variant - vaznli o‘rtacha:

$$z_d = \frac{\sum_{i=1}^{n} a_i e_i}{\sum_{i=1}^{n} a_i} \tag{3}$$

Bu yerda e_i - i-token vektori, a_i - uning musbat vazni, masalan, IDF; n - tokenlar soni. Bunday birlashtirish hisoblash jihatidan sodda, lekin so‘z tartibi va inkor kabi munosabatlarni yetarlicha saqlamaydi. Vektori mavjud bo‘lmagan yoki bo‘sh xabarlar uchun alohida ishlov belgilanadi.

fastText so‘zni belgilar n-grammalari orqali ifodalab, o‘qitishda uchramagan so‘zlarga ham vektor hosil qilish imkonini beradi. Bu xususiyat morfologik shakllar va ayrim yozuv variantlari uchun foydali bo‘lishi mumkin; biroq o‘zbekcha xabarlar yoki ataylab buzilgan yozuvlarda ustunlikni alohida tekshirish lozim. Doc2Vec esa hujjat vektorini o‘qitish maqsadiga kiritadi; yangi xabar uchun inferensiya bosqichi talab etiladi.

Kontekstual vektorlash

BERT tokenni chap va o‘ng kontekstini hisobga olgan holda ifodalaydi. Xabar tasnifida maxsus CLS tokeni yoki tokenlarni birlashtirish orqali olingan tasvir ishlatilishi mumkin. Oddiy BERT vektorining kosinus masofasi avtomatik ravishda sifatli semantik o‘xshashlikni kafolatlamaydi. Sentence-BERT aynan o‘xshashlikka mos gap vektorlarini o‘rganish uchun ishlab chiqilgan:

$$\mathrm{sim}(z_a, z_b) = \frac{z_a^T z_b}{\|z_a\|_2 \, \|z_b\|_2} \tag{5}$$

Uzun xabar tanlangan modelning token chegarasidan oshsa, uni bo‘laklab kodlash va bo‘lak vektorlarini birlashtirish kerak. Model tili, tokenizatori va pooling usuli natijaga ta’sir qiladi. O‘zbekcha, ruscha va inglizcha aralash pochta uchun ko‘p tilli modelni mahalliy korpusda baholash taklif etiladi.

1-jadval

Vektorlash usullarining sifat jihatidan taqqoslanishi

Usul	Tasvir	Afzallik	Asosiy cheklov
BoW va TF–IDF	Siyrak, lug‘at o‘lchamida	Tezkor bazaviy yechim; termin vaznlari ko‘rinadi	Parafraz va chuqur kontekstni sust aks ettiradi
LSA	Zich, k o‘lchamli	O‘lchamni kamaytiradi; yashirin bog‘lanishlar	Chiziqli yaqinlashuv; talqin murakkab
Word2Vec va GloVe	Zich, statik so‘z vektorlari	So‘zlar o‘rtasidagi semantik yaqinlik	Xabar uchun agregatsiya kerak; ma’no kontekstga moslashmaydi
fastText	Zich, subso‘zli	Yangi so‘z shakllariga vektor hisoblaydi	Statik ma’no; murakkab kontekst cheklangan
Doc2Vec	Zich hujjat vektori	Hujjat tasvirini bevosita o‘rganadi	Korpus va inferensiya sozlamalariga bog‘liq

BERT oilasi	Kontekstual token vektorlari	Kontekst va vazifaga moslashtirish	Ko‘proq resurs; uzunlik chegarasi
Sentence-BERT	Zich gap yoki matn vektori	Semantik qidiruv va klasterlash	Til va sohaga moslikni tekshirish zarur

Gutiérrez va hammualliflar o‘xshash ko‘rsatkichlarga ega qonuniy va fishing xabarlarini tuzib, vektorlash qaysi farqlarni saqlashini tekshirgan. Bu yondashuv umumiy aniqlikdan tashqari belgilarning mazmunini tekshirish zarurligini ko‘rsatadi. Jáñez-Martino va hammualliflar inglizcha va ispancha spamni 11 mavzuga ajratishda 16 kombinatsiyani baholagan; inglizcha korpusda TF–IDF va logistik regressiya uchun F1 = 0,953 qayd etilgan. Bu natija spamni qonuniy xabardan ajratish vazifasiga teng emas.

2-jadval

SEMD-600 korpusida zararli dastur bilan bog‘liq spamni aniqlash natijalari

Model	Precision	Recall	F1	Accuracy, %
TF–IDF + LR	0,768	0,763	0,763	76,4
fastText	0,730	0,643	0,681	68,7
BERT	0,733	0,734	0,730	71,9
DistilBERT	0,774	0,792	0,781	77,0

Mazkur kichik korpusda DistilBERT yaxshi muvozanat bergan, ammo TF–IDF + LR BERTdan yuqori F1 ko‘rsatgan. TF–IDF bazaviy natijasi maqolada avvalgi ishga tayangan; tajribalar butun model tizimlarini solishtiradi. Shu sababli farqlarni faqat vektorlash usuliga bog‘lash va boshqa korpusga umumlashtirish mumkin emas.

Taklif etilayotgan gibrid model va algoritm

Zhang va hammualliflar xabar sarlavhasi va tanasidan 79 ta statik belgi olib, ularni matn belgilari bilan birlashtirgan. Ushbu dalilga tayangan holda leksik, semantik va tuzilmaviy axborotni qo‘shuvchi quyidagi model tavsiya etiladi. Bu yangi isbotlangan algoritm emas, balki amaliy tekshiruv uchun metodik taklifdir:

$$z_d = [\alpha\, \hat{t}_d \parallel \beta\, \hat{s}_d \parallel \gamma\, \tilde{m}_d] \quad (6)$$

Bu yerda $\hat{t}_d$ - L2-normalangan TF–IDF vektori; $\hat{s}_d$ - L2-normalangan Sentence-BERT vektori; $\tilde{m}_d$ - o‘qitish qismida hisoblangan parametrlar bilan standartlashtirilgan metama’lumot vektori. $\parallel$ - ketma-ket birlashtirish; α, β, γ - validatsiyada tanlanadigan nomanfiy vaznlar. Yakuniy o‘lcham lug‘at hajmi, semantik vektor o‘lchami va metabelgilar sonining yig‘indisidir. TF–IDF blokining siyrak ko‘rinishini saqlash xotira sarfini kamaytiradi.

Algoritmning kirishi - belgilangan elektron xabarlar korpusi; chiqishi - o‘rgatilgan vektorlash tizimi va tasnif modeli. Xabarlar quyidagi ketma-ketlikda qayta ishlanadi:

1. MIME qismlari ajratiladi; mavzu, matn, URL va xizmat maydonlari olinadi. Takroriy va juda o‘xshash xabarlar aniqlanadi.

2. Korpus o‘qitish, validatsiya va testga bo‘linadi. Bir yozishma yoki bir kampaniyaning o‘xshash xabarlari turli qismlarga tarqalmasligi ta’minlanadi; imkon bo‘lsa vaqt bo‘yicha ajratish qo‘llanadi.

3. Faqat o‘qitish qismidan TF–IDF lug‘ati va IDF, shuningdek metabelgilarni masshtablash parametrlari aniqlanadi.

4. Sarlavha va matn uchun semantik vektor hisoblanadi. Uzun xabarlar bo‘laklanadi; havolalar soni, domenlar mosligi, HTML ulushi va ilovalar haqidagi belgilar olinadi.

5. Belgilar (5) bo‘yicha birlashtiriladi. Logistik regressiya o‘qitiladi; vaznlar, regulyarizatsiya va qaror chegarasi validatsiyada tanlanadi.

6. Sozlamalar muzlatilgach, test qismida yakuniy baho olinadi. Faqat TF–IDF, faqat semantik vektor va to‘liq model bir xil bo‘linishda solishtiriladi.

$$P(y = 1 \mid d) = \frac{1}{1 + \exp(-(w^T z_d + b))} \quad (7)$$

Bu yerda $y = 1$ - tanlangan zararli xabar sinfi, w va b - o‘rganiladigan parametrlar. Baholashda precision, recall, F1, PR–AUC, qonuniy xabarlarning xato bloklanish ulushi va ishlash

vaqti birga ko‘rsatiladi. Ko‘p sinfli vazifada macro-F1, klasterlash yoki qidiruvda esa vazifaga mos alohida mezon ishlatiladi. Gibrid modelning foydasi uning bloklarini navbat bilan chiqarib tashlash tajribasi orqali aniqlanadi.

Xulosa

Elektron pochta xabarlarini vektorlash uchun yagona universal usul mavjud emas. TF–IDF izohlanadigan bazaviy model sifatida, fastText subso‘zli tasvir uchun, BERT tasnifga mos kontekstual belgilar, Sentence-BERT esa semantik qidiruv uchun ko‘rib chiqilishi mumkin. Tanlangan tadqiqotlar murakkab model har bir vazifada ustun kelmasligini ko‘rsatadi. Leksik, semantik va tuzilmaviy belgilarni birlashtirish istiqbolli yo‘nalish bo‘lib, uning samarasi takrorlanishlardan tozalangan va vaqt bo‘yicha ajratilgan mahalliy korpusda tekshirilishi kerak.

Foydalanilgan adabiyotlar

1. Salton G., Buckley C. Term-weighting approaches in automatic text retrieval. Information Processing & Management. 1988. Vol. 24, No. 5. P. 513–523.

1. Deerwester S., Dumais S. T., Furnas G. W., Landauer T. K., Harshman R. Indexing by Latent Semantic Analysis. Journal of the American Society for Information Science. 1990. Vol. 41, No. 6. P. 391–407.

2. Mikolov T., Chen K., Corrado G., Dean J. Efficient Estimation of Word Representations in Vector Space. 2013. arXiv:1301.3781.

3. Pennington J., Socher R., Manning C. D. GloVe: Global Vectors for Word Representation. EMNLP. 2014. P. 1532–1543.

4. Bojanowski P., Grave E., Joulin A., Mikolov T. Enriching Word Vectors with Subword Information. TACL. 2017. Vol. 5. P. 135–146.

5. Le Q., Mikolov T. Distributed Representations of Sentences and Documents. ICML. PMLR 32(2). 2014. P. 1188–1196.

6. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL-HLT. 2019. P. 4171–4186.

7. Reimers N., Gurevych I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. EMNLP-IJCNLP. 2019. P. 3982–3992.

8. Gutiérrez L. F., Abri F., Armstrong M., Siami Namin A., Jones K. S. Phishing Detection through Email Embeddings. 2020. Preprint, arXiv:2012.14488.

9. Jáñez-Martino F., Alaiz-Rodríguez R., González-Castro V., Fidalgo E., Alegre E. Classifying spam emails using agglomerative hierarchical clustering and a topic-based approach. 2024.

10. Jáñez-Martino F., Fidalgo E., Alaiz-Rodríguez R., Carofilis A., Martínez-Mendoza A. Comparative Analysis of Natural Language Processing Models for Malware Spam Email Identification. NLPAICS. 2024. P. 59–63.

11. Zhang H., Shi Y., Liu M., Chen L., Wu S., Xue Z. A combined feature selection approach for malicious email detection based on a comprehensive email dataset. Cybersecurity. 2025. Vol. 8. Article 14.

BANK-MOLIYA TIZIMIDA XAVFSIZLIKNI TA’MINLASH MUAMMOLARI VA MODELI

Nasrullayev N.B., Xamidov Sh.J.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Mirzayeva A.B.
EMU universiteti

Annotatsiya. Maqolada raqamli to‘lovlarning jadal o‘sishi sharoitida O‘zbekiston bank-moliya tizimida axborot va kiberxavfsizlikni ta’minlash muammolari tadqiq etiladi. Markaziy bank va IIVning 2019–2026-yillardagi rasmiy ma’lumotlari asosida kiberjinoyatlarning o‘sish sur’atlari, zichligi, bitta jinoyatga to‘g‘ri keladigan zarar, zarar koeffitsienti va qaytarish darajasi hisoblangan, xavflar matritsasi va firibgarlik hujumi zanjiri modeli tuzilgan. O‘zbekiston, Rossiya, Qozog‘iston, Yevropa Ittifoqi va Buyuk Britaniyaning regulyativ yondashuvlari qiyoslanib, samaradorlik ko‘rsatkichlariga ega ko‘p qatlamli kiberbarqarorlik modeli taklif etilgan.

Kalit so‘zlar: bank-moliya tizimi, kiberxavfsizlik, axborot xavfsizligi, to‘lov tizimlari, firibgarlik, Markaziy bank, antifrod tizimlari, raqamli banking.

Аннотация. В статье анализируются проблемы обеспечения информационной и кибербезопасности банковско-финансовой системы Узбекистана в условиях быстрой цифровизации платежей. На основе официальных данных Центрального банка и МВД за 2019–2026 гг. рассчитаны темпы роста киберпреступности, удельный ущерб и коэффициент возврата средств, построена матрица рисков и модель цепочки мошеннической атаки. Сопоставлены регуляторные подходы Узбекистана, России, Казахстана, ЕС и Великобритании, предложена многоуровневая модель киберустойчивости с ключевыми показателями эффективности.

Ключевые слова: банковская система, кибербезопасность, мошенничество, антифрод, платёжные системы, киберустойчивость.

Kirish

Statistik ma’lumotlarga ko‘ra respublikada muomalada 70,9 milliondan ortiq bank kartasi, 439 462 ta to‘lov terminali hamda 45 311 ta bankomat va infokiosklar mavjud. Bu aholi uchun qulay, lekin jinoyatchilarga ham keng imkoniyat ochib beradi. Onlayn xizmatlarning ortib borgani sari hujum yuzasi ham kengaymoqda, jumladan firibgarlar zararli APK ilovalar, fishing havolalar, ijtimoiy muhandislik va deepfake texnologiyalaridan foydalanmoqdalar. Barcha jinoyatlarning 49,6 foizi axborot texnologiyalari yordamida sodir etilgan, ularning 96 foizida mablag‘lar elektron to‘lov tizimlari orqali o‘g‘irlangan. Aksariyat holatlarda bankning axborot tizimiga buzib kirilmaydi. Kodni aytib yuboradigan yoki pulni o‘z qo‘li bilan o‘tkazib beradigan mijozning o‘zi bo‘lib qolmoqda.

Bank-moliya tizimi arxitekturasi va kiberxavflar

O‘zbekiston bank tizimi ikki pog‘onali: yuqorida tartibga soluvchi va to‘lov infratuzilmasi operatori sifatida Markaziy bank, tijorat banki, to‘lov tashkilotlari va boshqa kredit tashkilotlari faoliyat yuritadi.

Tartibga solish va nazorat qatlami. Markaziy bank bank-moliya tashkilotlari faoliyatini litsenziyalaydi va nazorat qiladi. Markaziy bank to‘lov tizimi operatorlari, kredit va to‘lov tashkilotlarida kiberxavfsizlik bo‘yicha muvofiqlashtiruvchi organ hisoblanadi, uning tarkibida

“CERT-CBU” kiberxavfsizlik markazi tuzilgan. Kiberxavfsizlik sohasidagi vakolatli davlat organi - Davlat xavfsizlik xizmati, kiberjinoyatlarga qarshi kurash bo‘yicha vakolatli organ Ichki ishlar vazirligi.

To‘lov infratuzilmasi qatlami. Markaziy bank banklararo to‘lov tizimi, tezkor to‘lovlar tizimi, hisob-kitoblar kliring tizimi va yagona QR-online tizimini yuritadi. Chakana karta to‘lovlari Uzcard (Yagona umumrespublika protsessing markazi) va Humo (Milliy banklararo protsessing markazi) milliy tizimlari orqali o‘tadi; ular Visa, Mastercard, UnionPay bilan integratsiyalashgan

Ishtirokchilar qatlami. Bu qatlamga tijorat banklari, to‘lov tashkilotlari, mikromoliya tashkilotlari va kredit byurolari kiradi. Ularning har biri o‘z avtomatlashtirilgan bank tizimi, protsessingi va mobil ilovasiga ega, shu sababli himoya darajasi bir xil emas.

Hujumlarni kimga qaratilganiga qarab uch guruhga ajratish qulay: mijozga, to‘lov infratuzilmasiga va bankning ichki tizimlariga qaratilganlar. Amaliyotda ko‘p uchraydigan usullar 1-jadvalda jamlangan.

1-jadval

Plastik kartalarga qaratilgan asosiy hujum usullari

№	Usul	Qanday amalga oshiriladi	Nimadan foydalaniladi
1	Vishing - telefon orqali aldash	Bank yoki to‘lov tizimi xodimi niqobida qo‘ng‘iroq qilinadi, hisobni «himoyalash» bahonasida karta raqami va SMS-kod so‘raladi	Shoshilinch qaror, bankka bo‘lgan ishonch
2	Fishing sayt va soxta ilova	Asl saytga o‘xshatilgan domen yoki rasmiy do‘kondan tashqari o‘rnatiladigan ilova kirish ma’lumotlarini yig‘adi	Domen nomiga e’tibor bermaslik
3	Bank troyani	Qurilmaga o‘rnatilgach, SMS va push-xabarlarni ushlab qoladi, ekranni masofadan boshqaradi	Ilovaga berilgan ortiqcha ruxsatlar
4	SIM-kartani qayta rasmiylashtirish	Abonent raqami boshqa shaxs nomiga o‘tkaziladi va tasdiqlash kodlari o‘sha raqamga keladi	Aloqa operatorining identifikatsiya tartibi
5	Skimming va shimming	Bankomat yoki terminalga qo‘shimcha qurilma o‘rnatilib, karta ma’lumotlari bilan PIN nusxalanadi	Magnit yo‘lak, qurilmalar ustidan nazorat
6	Kartasiz (CNP) operatsiyalar	O‘g‘irlangan rekvizitlar 3-D Secure yoqilmagan onlayn savdo nuqtalarida ishlatiladi	Savdo nuqtasining sozlamalari
7	Drop-kartalar	Uchinchi shaxs kartasi haq evaziga olinadi, o‘g‘irlangan pul shu karta orqali tarqatiladi va naqdlashtiriladi	Hisoblar monitoringidagi bo‘shliqlar

Jadvalning birinchi yarmidagi usullar insonga, ikkinchi yarmidagilari texnik zaifliklarga tayanadi. Milliy statistika birinchi guruh ustunligini tasdiqlaydi: 2024-yilda mijoz nomiga firibgarlik yo‘li bilan onlayn kredit rasmiylashtirish bo‘yicha murojaatlar 42 foizga ko‘paygan, Markaziy bank joriy etgan cheklov esa 285 mlrd so‘mlik kreditning firibgarga o‘tishiga yo‘l

qo‘ymagan. Bunga insayderlar orqali ma’lumot sizishi ham qo‘shiladi. Bu xalqaro adabiyotdagi xulosaga mos: sxemalar tez o‘zgaradi, aniqlash usullari esa ularning ortidan yetib boradi.

Bu sxemalarning ish berishiga to‘rt sabab bor. SMS orqali keladigan bir martalik kod ikkinchi omil sifatida ishonchsiz, chunki uni SIM-kartani qayta rasmiylashtirish yoki troyan orqali qo‘lga kiritish mumkin. Fishing sahifasini asl saytdan ajratish ko‘pchilikka qiyin. Banklarning antifrod tizimlari alohida-alohida ishlaydi. Nihoyat, o‘g‘irlangan pul bir necha daqiqada bir nechta begona karta orqali tarqatiladi. Adabiyotda bunday hisoblar «money mule» deb ataladi va pul yuvish zanjirining asosiy bo‘g‘ini hisoblanadi.

Banklardagi himoya vositalari va ularning chegarasi

Banklarda qo‘llanayotgan asosiy himoya vositalari va ularning zaif nuqtalari 2-jadvalda keltirilgan.

2-jadval

Himoya vositalarining imkoniyati va cheklovlari

Vosita	Nima beradi	Qayerda yetishmaydi
EMV chip va tokenizatsiya	Karta rekvizitlarini vaqtinchalik belgi bilan almashtiradi	Magnit yo‘lak va kartasiz kanallarga ta’sir qilmaydi
3-D Secure 2.x	To‘lovni qo‘shimcha ravishda tasdiqlaydi	Barcha savdo nuqtalarida yoqilmagan
SMS orqali bir martalik kod	Ikkinchi omil vazifasini bajaradi	Aldov, SIM almashtirish va troyan oldida himoyasiz
Qoidaga asoslangan antifrod	Ma’lum sxemalarni to‘xtatadi	Yangi sxemaga qoida qo‘lda yozilguncha vaqt ketadi
Push-tasdiqlash, FIDO2, xatti-harakat biometrikasi	Fishingga chidamli va mijozga sezilmaydigan tekshiruv	Qurilmaga bog‘lanish talab qiladi, keng joriy etilmagan
PCI DSS v4.0.1, SIEM va MB himoyasi	Karta ma’lumotlari muhitini va jurnallarni himoyalaydi	Qamrovi tor, malakali kadr yetishmaydi

Bu vositalarning deyarli barchasi banklarda mavjud, biroq ular bir-biridan ajralgan holda ishlaydi. Bank o‘z mijozining operatsiyasini ko‘radi, lekin pul o‘tkazilayotgan kartaning tarixi unga ko‘rinmaydi va himoya zanjiri shu joyda uziladi. Normativ darajada bu muammo e’tirof etilgan: markazlashgan antifrod platformasini yaratish, tranzaksiya ma’lumotlarini regulyator platformasiga ulash va zararni banklar zimmasiga yuklash belgilandi. Texnik darajada esa qaror mantig‘i ko‘pincha qo‘lda yozilgan qoidalarga tayanadi va yangi sxemaga qarshi qoida qo‘shilguncha bir necha hafta o‘tib ketadi.

Taklif etilayotgan xavfga asoslangan himoya modeli

Model to‘rt bosqichdan iborat. Qurilma darajasida ilova qurilmaga bog‘lanadi, SMS-kod o‘rniga push-tasdiqlash yoki FIDO2 biometrikasi ishlatiladi, seans davomida xatti-harakat ko‘rsatkichlari yig‘iladi. Tranzaksiya darajasida har bir operatsiyadan oldin xavf bahosi hisoblanadi. Bank darajasi jurnallar himoyasi, huquqlarni minimallashtirish va PCI DSS v4.0.1 talablarini qamraydi. Banklararo darajada qabul qiluvchi kartaning obro‘si markazlashgan platformadan so‘raladi. Shunga o‘xshash xavfga moslashuvchan bosqichli yondashuvlar onlayn bankingda sinab ko‘rilgan va statik parolga tayanishni kamaytirishi ko‘rsatilgan.

Tranzaksiya xavfi quyidagicha hisoblanadi:

$$R = \sum w_i \cdot f_i, \quad 0 \le f_i \le 1, \quad \sum w_i = 1, \quad R \in [0; 1] \qquad (1)$$

bu yerda f_i normallashtirilgan xavf omili, w_i esa uning vazni. Omillar: qurilma va IP manzilning odatiy profildan farqi, joylashuvning mantiqqa zid o‘zgarishi, summaning o‘rtacha qiymatdan chetlanishi, qisqa vaqtdagi operatsiyalar soni, qabul qiluvchi kartaning obro‘si, so‘nggi 72 soatda SIM-karta yoki parolning almashtirilgani, kanal turi va xatti-harakat biometrikasidagi chetlanish.

Vaznlar w_i tasdiqlangan firibgarlik hodisalari asosida davriy qayta hisoblanadi. Bitta bankda ma’lumot kam bo‘lsa, banklar shaxsiy ma’lumot almashmasdan umumiy modelni birgalikda o‘qitishi mumkin. Federativ o‘qitish karta firibgarligini aniqlashda muvaffaqiyatli sinalgan. Eskalatsiya qoidasiga ko‘ra, so‘nggi 24 soatda ikki va undan ortiq o‘rtacha xavfli hodisa qayd etilsa, chegaralar 0,10 ga pasaytiriladi. Natijaga qarab tizim 3-jadvaldagi javoblardan birini tanlaydi.

3-jadval

Xavf darajasi va tizimning javob harakatlari

R qiymati	Daraja	Tizimning javobi
$R < 0{,}30$	Past	Operatsiya to‘siqsiz bajariladi, faqat jurnalga yoziladi
$0{,}30 \le R < 0{,}55$	O‘rtacha	Push-tasdiqlash yoki biometrik tekshiruv so‘raladi
$0{,}55 \le R < 0{,}80$	Yuqori	Operatsiya 15–30 daqiqaga kechiktiriladi, mijozga xabar beriladi va aloqa markazi bog‘lanadi
$R \ge 0{,}80$	Kritik	Operatsiya rad etiladi, kanal vaqtincha cheklanadi, hodisa antifrod markaziga uzatiladi

Modelning asosiy g‘oyasi «o‘tkazish yoki bloklash» ikkilik qaroridan voz kechishdir. Qisqa kechiktirish mijozga o‘ylab ko‘rishga vaqt beradi. Ijtimoiy injiniringda firibgar mijozni ataylab shoshiltiradi, shuning uchun bir necha o‘n daqiqalik pauza ko‘pincha pulni saqlab qolishga yetadi.

Modelni qanday sinash kerak

Model hali real ma’lumotda sinalmagani uchun bu yerda sinov tartibi keltiriladi. Firibgarlik operatsiyalari umumiy oqimning bir foizidan kamini tashkil qiladi, shu bois umumiy aniqlik (accuracy) aldamchi ko‘rsatkich: hech narsani aniqlamaydigan model ham 99 foizdan yuqori natija beradi. Sinflarning keskin nomutanosibligi va kesishib ketishi bu sohadagi asosiy metodologik muammo sifatida qayd etilgan. Shu sababli asosiy o‘lchovlar recall, precision, F1 va PR-AUC bo‘ladi. Nomutanosib ma’lumotda PR-AUC ROC-AUC ga qaraganda ishonchliroq baho beradi. Bularga qaror vaqti (real vaqt uchun 100 ms dan kam), bloklab qolingan mablag‘ va noto‘g‘ri bloklash bo‘yicha shikoyatlar soni qo‘shiladi.

Ma’lumotlar bankning kamida 6–12 oylik anonimlashtirilgan jurnallaridan olinadi va vaqt bo‘yicha bo‘linadi: oldingi davr o‘qitish, keyingi davr sinov uchun. Joriy etish soya rejimidan boshlanadi: model qaror chiqaradi, lekin operatsiyaga ta’sir qilmaydi. Keyin natijalar nazorat guruhi bilan solishtiriladi.

Xulosa

Kartalardan pul o‘g‘irlanishining asosiy sababi inson omili bilan bog‘liq: firibgar odamni aldaydi, bank tizimi esa aldangan mijozning harakatini qonuniy operatsiya sifatida bajaradi. Shu sababli quyidagi choralarni birgalikda qo‘llash kerak:

SMS-koddan bosqichma-bosqich voz kechib, push-tasdiqlash va FIDO2 asosidagi fishingga chidamli autentifikatsiyaga o‘tish;

– ilovani qurilmaga bog‘lash, qurilma almashtirilganda va yangi qabul qiluvchiga birinchi marta yirik summa o‘tkazilganda kechiktirish oynasini qo‘llash;

– shubhali kartalar ro‘yxatini banklar o‘rtasida real vaqtda almashish va drop-hisoblarni avtomatik aniqlash tizimini yo‘lga qo‘yish;

– antifrod modelini statik qoidalardan xavf bahosiga o‘tkazish va vaznlarni haqiqiy hodisalar asosida yangilab borish;

– moliyaviy va raqamli savodxonlikni oshirishni bank xizmatining doimiy qismiga aylantirish.

Taklif etilgan modelni mavjud antifrod tizimiga qo‘shimcha modul sifatida o‘rnatish mumkin. Keyingi ishda u real ma’lumotlar asosida sinovdan o‘tkaziladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Markaziy banki. To‘lov tizimi statistikasi, 2026-yil 1-mart holatiga. - URL: https://cbu.uz/uz/statistics/paysistem/

2. O‘zbekiston Respublikasi IIV Kiberjinoyatlarga qarshi kurashish markazining 2024–2026-yillardagi rasmiy ma’lumotlari.

3. Fuertes W., Arévalo D., Castro J.D., Ron M., Estrada C.A., Andrade R., Peña F., Benavides E. Impact of social engineering attacks: a literature review // Developments and Advances in Defense and Security. - Singapore: Springer, 2021. - P. 25–35. - DOI: 10.1007/978-981-16-4884-7_3

4. Althobaiti K., Alsufyani N. A review of organization-oriented phishing research // PeerJ Computer Science. - 2024. - Vol. 10. - Art. e2487. - DOI: 10.7717/peerj-cs.2487

5. Hernández Aros L., Bustamante Molano L.X., Gutierrez-Portela F. et al. Financial fraud detection through the application of machine learning techniques: a literature review // Humanities and Social Sciences Communications. - 2024. - Vol. 11. - Art. 1130. - DOI: 10.1057/s41599-024-03606-0

6. Raza M.S., Zhan Q., Rubab S. Role of money mules in money laundering and financial crimes - a discussion through case studies // Journal of Financial Crime. - 2020. - Vol. 27, No. 3. - P. 911–931. - DOI: 10.1108/JFC-02-2020-0028

7. Jambhrunkar G., Sharma H., Singla S., Kailasam T. MuleTrack: a lightweight temporal learning framework for money mule detection in digital payments // Lecture Notes in Computer Science. - Cham: Springer, 2026. - Vol. 16008. - DOI: 10.1007/978-3-032-02725-2_30

8. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi PQ-153-son qarori. - URL: https://lex.uz

9. O‘zbekiston Respublikasi Markaziy banki Boshqaruvining 2024-yil 24-apreldagi 13/1-son qarori bilan tasdiqlangan nizom (ro‘yxat raqami 3513). - URL: https://lex.uz.

10. Soyemi J., Hammed M., Soyemi O.B. Adaptive risk-based multi-layer authentication framework for secure online banking systems // FUDMA Journal of Sciences. - 2026. - Vol. 10, No. 4.

11. Salam A., Fouad K.M., Elbably D.L., Elsayed S.M. Federated learning model for credit card fraud detection with data balancing techniques // Neural Computing and Applications. - 2024. - Vol. 36. - P. 6231–6256. - DOI: 10.1007/s00521-023-09410-2

12. Kalid S.N., Khor K.-C., Ng K.-H., Tong G.-K. Detecting frauds and payment defaults on credit card data inherited with imbalanced class distribution and overlapping class problems: a systematic review // IEEE Access. - 2024. - Vol. 12. - P. 23636–23652. - DOI: 10.1109/ACCESS.2024.3362831

13. Btoush E., Kobbaey T., Tamimi H., Zhou X. Machine learning-based cyber fraud detection: a comparative study of resampling methods for imbalanced credit card data // Applied Sciences. - 2026. - Vol. 16, No. 2. - Art. 850.

ВЛИЯНИЕ ПАРАМЕТРОВ ARGON2ID НА ПРАКТИЧЕСКУЮ БЕЗОПАСНОСТЬ ПАРОЛЕЙ: АНАЛИЗ ВЫЧИСЛИТЕЛЬНЫХ ЗАТРАТ И КОМПРОМИССОВ ПО ПАМЯТИ

Махмудова М.М.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Annotatsiya. Ushbu maqolada Argon2id algoritmi parametrlarining parollarni xeshlash vaqti hamda operativ xotira sarfiga ta’siri o‘rganiladi. Tajribalar Python dasturlash tili va argon2-cffi kutubxonasi yordamida Google Colab muhitida o‘tkazildi. Xotira hajmi, takroriy o‘tishlar soni, parallellik darajasi va bir vaqtda bajariladigan so‘rovlar soni o‘zgartirilib, natijalar taqqoslandi. Natijalar xotira hajmi va o‘tishlar sonining ortishi xeshlash vaqtini oshirishini, parallel so‘rovlar sonining ko‘payishi esa umumiy hisoblash yuklamasi va xotiraga bo‘lgan talabni oshirishini ko‘rsatdi.

Kalit so‘zlar: Argon2id, parollarni xeshlash, axborot xavfsizligi, kriptografik himoya, operativ xotira, hisoblash xarajatlari, parallellik, parollar xavfsizligi.

Аннотация. В статье исследуется влияние параметров Argon2id на время хеширования паролей и потребность в оперативной памяти. Эксперименты проводились в среде Google Colab с использованием Python и библиотеки argon2-cffi. Были изучены влияние объёма памяти, количества проходов, степени параллелизма и числа одновременно выполняемых запросов. Результаты показали, что увеличение объёма памяти и количества проходов повышает время хеширования, а рост числа параллельных запросов увеличивает общую вычислительную нагрузку и расчётную потребность в памяти.

Ключевые слова: Argon2id, хеширование паролей, информационная безопасность, криптографическая защита, оперативная память, вычислительные затраты, параллельная обработка, безопасность паролей.

Введение

Защита паролей остаётся одной из важных задач информационной безопасности. При утечке базы данных злоумышленник может пытаться восстановить исходные пароли, многократно проверяя возможные комбинации. Поэтому для хранения паролей применяются специализированные алгоритмы, которые увеличивают стоимость каждой проверки и затрудняют массовый перебор.

Одним из таких алгоритмов является Argon2id, позволяющий задавать объём используемой памяти, количество проходов и степень параллелизма. Эти параметры влияют как на вычислительные затраты при проверке пароля, так и на нагрузку на систему аутентификации. Слишком низкие значения могут сделать проверку паролей менее затратной для атакующего, тогда как чрезмерно высокие значения способны увеличить задержки и потребление ресурсов сервером.

Особенно важно учитывать эту зависимость при одновременной обработке нескольких запросов. Настройки, приемлемые для одной операции, могут создавать значительную суммарную нагрузку при росте количества пользователей.

Цель исследования - экспериментально оценить влияние основных параметров Argon2id на время хеширования паролей, а также рассмотреть изменение времени

обработки и расчётной потребности в памяти при одновременном выполнении нескольких запросов.

Теоретические основы Argon2id

Argon2id - алгоритм хеширования паролей, разработанный для повышения затрат на их перебор. Он сочетает особенности Argon2i, использующего независимую от обрабатываемых данных адресацию памяти, и Argon2d, адресация в котором зависит от промежуточных вычислений. Такое сочетание предназначено для обеспечения защиты от различных типов атак.

К основным параметрам алгоритма относятся объём памяти (m), количество проходов (t) и степень параллелизма (p). Параметр (m) определяет объём памяти, используемой при вычислении; (t) задаёт количество проходов обработки памяти; (p) определяет степень параллелизма алгоритма. Увеличение объёма памяти и количества проходов, как правило, повышает вычислительные затраты одной операции. Влияние параллелизма зависит от реализации и доступных вычислительных ресурсов.

Выбор параметров требует баланса между защитой паролей и производительностью системы. При этом время хеширования само по себе не показывает, сколько времени потребуется для взлома пароля: результат атаки также зависит от сложности пароля, возможностей оборудования и других факторов.

Методика исследования

Эксперименты проводились в Google Colab с использованием Python и библиотеки argon2-cffi. Для всех конфигураций длина выходного хеша составляла 32 байта, длина соли - 16 байт. Перед каждой серией выполнялся один прогревочный запуск, который не включался в расчёты. Затем проводилось семь измеряемых повторений. Для каждой конфигурации рассчитывались среднее время и медиана в миллисекундах. Исследование включало четыре эксперимента. В первом изучалось влияние объёма памяти при (t=2) и (p=1). Во втором изменялось количество проходов при фиксированных (m=19456) KiB и (p=1). В третьем сравнивались значения параллелизма (p=1), (p=2) и (p=4) при фиксированных (m=19456) KiB и (t=2).

В четвёртом эксперименте оценивалось время обработки пакета из 1, 2, 4 и 8 одновременных запросов. Для каждого запроса использовались параметры (m=19456) KiB, (t=2), (p=1). Дополнительно рассчитывались среднее время на запрос в составе пакета и расчётная потребность в памяти. Последняя определялась умножением 19456 KiB на число запросов и не являлась непосредственным измерением фактического потребления оперативной памяти.

Результаты и обсуждение

1.Влияние объёма памяти. В первом эксперименте объём памяти изменялся от 8 до 64 MiB при фиксированных значениях (t=2) и (p=1). Результаты представлены в таблице 1.

Таблица 1

Влияние объёма памяти на время хеширования Argon2id

Память m (MiB)	Среднее время (мс)	Медиана (мс)
8	12,10	12,06
19 (19456 KiB)	31,65	30,95
32	66,91	64,85
64	135,84	134,93

При увеличении объёма памяти с 8 до 64 MiB среднее время хеширования выросло с 12,10 до 135,84 мс, то есть приблизительно в 11,2 раза. В исследованной среде увеличение этого параметра сопровождалось существенным ростом вычислительных затрат. Следовательно, объём памяти является одним из ключевых факторов, которые необходимо учитывать при настройке Argon2id.

2. Влияние количества проходов. Во втором эксперименте объём памяти оставался равным 19456 KiB, а степень параллелизма - 1. Изменялось количество проходов от 1 до 4. Результаты измерений представлены в таблице 2.

Таблица 2

Влияние количества проходов на время хеширования

Число проходов t	Среднее время (мс)	Медиана (мс)
1	16,63	16,64
2	33,10	32,63
3	50,14	49,86
4	61,57	60,45

При увеличении количества проходов с 1 до 4 среднее время хеширования выросло с 16,63 до 61,57 мс, приблизительно в 3,7 раза. Результаты подтверждают, что увеличение количества проходов повышает вычислительные затраты операции. Однако это также увеличивает время обработки запроса, поэтому значение параметра следует выбирать с учётом требований безопасности и допустимой нагрузки на систему.

3. Влияние степени параллелизма. В третьем эксперименте использовались (m=19456) KiB и (t=2). Сравнивались значения параллелизма 1, 2 и 4.

Таблица 3

Влияние степени параллелизма на время хеширования

Параллелизм p	Среднее время (мс)	Медиана (мс)
1	32,25	32,24
2	34,40	34,66
4	30,40	30,13

Наименьшее среднее время было получено при (p=4), однако зависимость между степенью параллелизма и временем хеширования не была монотонной. При (p=2) время оказалось выше, чем при (p=1), а при (p=4) - ниже. Поэтому по результатам данного эксперимента нельзя утверждать, что увеличение параллелизма всегда ускоряет работу алгоритма. Полученный эффект зависит от условий выполнения и требует проверки на целевой системе.

4. Одновременная обработка запросов. В четвёртом эксперименте исследовалась работа Argon2id при одновременном выполнении нескольких запросов с одинаковыми параметрами: (m=19456) KiB, (t=2), (p=1).

Параметры Argon2id для каждого запроса: memory_cost = 19456 KiB, time_cost = 2, parallelism = 1

Таблица 4

Время обработки пакета запросов и расчётная потребность в памяти

Одновременные запросы	Среднее время пакета (мс)	Медиана (мс)	Среднее время на запрос в	Расчётная память (MiB)

			составе пакета (мс)	
1	31,28	30,83	31,28	19
2	58,96	56,69	29,48	38
4	117,53	116,78	29,38	76
8	238,90	234,78	29,86	152

При увеличении числа одновременных запросов с 1 до 8 среднее время обработки пакета выросло с 31,28 до 238,90 мс, приблизительно в 7,6 раза. При этом расчётная потребность в памяти увеличилась с 19 до 152 MiB.

Среднее время на один запрос, рассчитанное делением среднего времени обработки пакета на число запросов, оставалось в диапазоне 29,38–31,28 мс. Этот показатель не является непосредственно измеренной задержкой каждого отдельного запроса, поэтому его следует использовать только для приблизительного сравнения конфигураций.

Результаты показывают, что при увеличении числа запросов растут общее время обработки и расчётная потребность в памяти. Для систем аутентификации это означает необходимость учитывать совокупную нагрузку, а не только производительность одной операции. При этом фактическое потребление памяти в данном эксперименте отдельно не измерялось.

Заключение

В работе экспериментально исследовано влияние основных параметров Argon2id на время хеширования паролей и ресурсы, необходимые для обработки нескольких запросов. Увеличение объёма памяти с 8 до 64 MiB сопровождалось ростом среднего времени хеширования приблизительно в 11,2 раза, а увеличение количества проходов с 1 до 4 - приблизительно в 3,7 раза. Эти результаты показывают, что оба параметра существенно влияют на вычислительные затраты алгоритма.

Для степени параллелизма выраженной монотонной зависимости не выявлено: минимальное среднее время было получено при (p=4), но различия между конфигурациями были сравнительно небольшими. В эксперименте с одновременными запросами увеличение их количества с 1 до 8 привело к росту общего времени обработки примерно в 7,6 раза, а расчётной потребности в памяти - с 19 до 152 MiB.

Практическое значение исследования заключается в необходимости подбирать параметры Argon2id с учётом одновременно требований к защите паролей и возможностей вычислительной инфраструктуры. При этом измеренное время хеширования не является прямой оценкой времени взлома пароля, а расчётная потребность в памяти не заменяет непосредственного измерения её фактического использования. В дальнейшем исследование может быть расширено за счёт экспериментов на разных аппаратных платформах и непосредственного измерения потребления оперативной памяти.

Список использованной литературы:

1. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. - Boca Raton: CRC Press, 1996. - 810 p.

2. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. - Berlin; Heidelberg: Springer, 2010. - 372 p.Paar C., Pelzl J. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.

3. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. - Boca Raton: CRC Press, 2020. - 648 p.

FISHING HUJUMLARINI CHUQUR TAHLIL QILISH VA KO‘P QATLAMLI HIMOYA MODELI

Tashev K.A., Yoqubjonov O.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada ijtimoiy muhandislik hujumlarining eng keng tarqalgan ko‘rinishi - fishingda havolalarni maskalash (URL masking) va o‘xshash domen nomlaridan foydalanish texnikalari penetratsion testlash nuqtayi nazaridan tahlil qilingan. Nazorat qilinadigan laboratoriya muhitida maskalangan va maskalanmagan havolalar solishtirilib, foydalanuvchi e’tiborini chalg‘itadigan belgilar aniqlangan. Natijalar asosida texnik, tashkiliy va inson omilini qamrab oluvchi ko‘p qatlamli himoya modeli taklif etilgan.

Kalit so‘zlar: ijtimoiy muhandislik, fishing, URL maskalash, omoglif, penetratsion testlash, ko‘p faktorli autentifikatsiya.

Аннотация. В статье с позиции тестирования на проникновение проанализированы методы маскировки ссылок (URL masking) и использования похожих доменных имён в фишинге - наиболее распространённой форме атак социальной инженерии. В контролируемой лабораторной среде сопоставлены маскированные и немаскированные ссылки и выявлены признаки, отвлекающие внимание пользователя. По результатам предложена многоуровневая модель защиты, охватывающая технические, организационные меры и человеческий фактор.

Ключевые слова: социальная инженерия, фишинг, маскировка URL, омоглиф, тестирование на проникновение, многофакторная аутентификация.

Kirish

Axborot tizimlarini himoyalash vositalari takomillashgan sari tajovuzkorlar e’tibori texnik zaifliklardan inson omiliga ko‘chmoqda. FBI Internet Crime Complaint Center (IC3) ma’lumotlariga ko‘ra, 2024-yilda 859 531 ta shikoyat qayd etilib, umumiy zarar 16,6 mlrd AQSH dollarini tashkil etgan, fishing va spufing esa 193 407 ta shikoyat bilan eng ko‘p uchragan jinoyat turi bo‘lgan [1]. Verizon DBIR 2025 hisobotida tahlil qilingan 12 195 ta tasdiqlangan buzilishning taxminan 60 foizida inson omili ishtirok etgan [2]. APWG kuzatuvlariga ko‘ra, 2025-yilda taxminan 3,8 mln fishing hujumi qayd etilgan [3]. Sun’iy intellekt vositalari hujumlarni yanada ishonarli qilmoqda: 2024-yilda Arup kompaniyasining Gonkongdagi xodimi rahbariyat vakillarining deepfake tasviri ishtirokidagi video qo‘ng‘iroqqa ishonib, 15 ta o‘tkazma orqali taxminan 25,6 mln dollarni jinoyatchilarga yuborgan [4].

Ijtimoiy muhandislik hujumlarining aksariyati foydalanuvchini soxta manzilga yo‘naltiruvchi havola orqali amalga oshiriladi. Shu sababli havolani maskalash texnikalarini penetratsion testlash doirasida o‘rganish va ularga qarshi samarali himoya choralarini ishlab chiqish dolzarb vazifadir. Tadqiqotning maqsadi - maskalash usullarini tasniflash, laboratoriya sharoitida ularning foydalanuvchiga ko‘rinish xususiyatlarini baholash va ko‘p qatlamli himoya modelini taklif etishdir.

Tadqiqot metodologiyasi

Ijtimoiy muhandislik bo‘yicha test faqat buyurtmachining yozma roziligi, aniq belgilangan qamrov va o‘tkazish qoidalari (rules of engagement) mavjud bo‘lganda o‘tkaziladi. Ishda hujum bosqichlari - ochiq manbalardan ma’lumot yig‘ish (OSINT), ishonchli senariy (pretekst)

tayyorlash, yetkazish, foydalanuvchi harakati va hisobot berish - nazorat qilinadigan, ajratilgan laboratoriya muhitida o‘rganildi; faqat sinov hisoblaridan foydalanildi, haqiqiy foydalanuvchi ma’lumotlari yig‘ilmadi. Zphisher va D0ppelganger kabi ochiq kodli vositalar faqat himoya nuqtayi nazaridan - ular hosil qiladigan havolalar va belgilarni aniqlash maqsadida - tahlil qilindi [11, 12]. Ijtimoiy muhandislikda qo‘llaniladigan ta’sir tamoyillari - hokimiyatga bo‘ysunish, shoshilinchlik, o‘zaro majburiyat va ijtimoiy isbot - Cialdini va Hadnagy ishlariga tayangan holda baholandi [5, 6].

Test natijalari nafaqat «kim havolaga bosdi» degan savolga, balki «nima uchun bosdi» degan savolga ham javob berishi kerak. Shu sababli har bir senariy uchun qaysi psixologik omil (masalan, rahbar nomidan shoshilinch so‘rov) ishlatilgani va qaysi nazorat vositasi (pochta filtri, brauzer ogohlantirishi, xodimning tekshiruvi) hujumni to‘xtata olgani qayd etiladi. Bu yondashuv hisobotni texnik topilmalar ro‘yxatidan amaliy tavsiyalar to‘plamiga aylantiradi.

Maskalash texnikalarining tasnifi va tajriba natijalari

Tahlil natijasida to‘rtta asosiy yondashuv ajratildi (1-jadval): havolani qisqartirish xizmatlari yoki gipermatn ortiga yashirish; omoglif va typosquatting (masalan, «m» o‘rniga «rn», lotin harfi o‘rniga kirill harfi); subdomen aldovi (masalan, login.bank.com.example-secure.net ko‘rinishida haqiqiy domen o‘ngda bo‘lishi) hamda maskalanmagan, uzun parametrli havolalar. Omoglif belgilar bilan bog‘liq xavflar Unicode Security Mechanisms standartida alohida ko‘rsatilgan [8].

1-jadval

Havola maskalash usullari va ularga qarshi tekshiruvlar

№	Maskalash usuli	Foydalanuvchi uchun belgi	Tekshiruv / himoya
1	Havolani qisqartirish va gipermatn ortiga yashirish	Haqiqiy manzil ko‘rinmaydi; qisqa va "toza" ko‘rinish	Kursorni olib borib to‘liq URLni tekshirish; shlyuzda URLni ochib tahlil qilish
2	Omoglif va typosquatting (masalan, "rn" ↔ "m", IDN belgilar)	Brend nomi deyarli bir xil yoziladi	Punycode ko‘rsatish; yangi ro‘yxatdan o‘tgan domenlarni bloklash
3	Subdomen aldovi	Ishonchli nom chap tomonda, haqiqiy domen o‘ngda	Domenning ro‘yxatdan o‘tgan qismini ajratib tekshirish; DNS filtrlash
4	Uzun parametrli (maskalanmagan) havola	Tushunarsiz so‘rov parametrlari	Sandbox tahlili; foydalanuvchini o‘qitish

Laboratoriya tajribasida maskalangan va maskalanmagan havolalar solishtirildi. Maskalanmagan havola uzun bo‘lib, tushunarsiz parametrlarni o‘z ichiga oladi va foydalanuvchi uning manzilini odatda havolani ochgandan keyingina anglaydi. Maskalangan havola esa qisqa, ixcham va maskalovchi xizmat domenini ko‘rsatgani uchun dastlabki qarashda ishonchliroq tuyuladi. Biroq u ham haqiqiy havola bilan bir xil emas: odatiy bo‘lmagan subdomenlar, qo‘shimcha yo‘l segmentlari va shubhali so‘rov satrlari tayyorgarlikka ega foydalanuvchiga soxtalikni ko‘rsatadi. Demak, maskalashning asosiy kuchi texnik murakkablikda emas, balki foydalanuvchining shoshilinchlik, ishonch va hokimiyatga bo‘ysunish kabi psixologik omillarga tayanishidadir [5, 6]. Shuni ham ta’kidlash lozimki, sun’iy intellekt yordamida yozilgan shaxsiylashtirilgan xabarlar grammatik xatolar kabi an’anaviy belgilarni yo‘qotmoqda; shu sababli

foydalanuvchining «ko‘zi bilan tanish»ga tayanish o‘rniga, manzilni tizimli va avtomatik tekshirish zarur bo‘ladi.

Ko‘p qatlamli himoya modeli

Bitta himoya vositasi yetarli emas, shuning uchun uch qatlamli model taklif etiladi.

Texnik qatlam. Elektron pochta domenini SPF, DKIM va DMARC orqali himoyalash [9]; pochta shlyuzida havolalarni qayta yozish va sandbox muhitida tekshirish; DNS filtrlash va yangi ro‘yxatdan o‘tgan domenlarni cheklash; brauzerlarda soxta saytlarni aniqlash. Eng muhim chora - fishingga chidamli autentifikatsiya: FIDO2/WebAuthn kalitlari (passkey) domen nomiga bog‘langani uchun soxta domenda ishlamaydi. NIST SP 800-63-4 (2025) AAL2 darajasida fishingga chidamli variantni taklif etishni talab qiladi [7].

Tashkiliy qatlam. Moliyaviy va maxfiy so‘rovlarni ikkinchi kanal orqali tasdiqlash tartibi (ayniqsa, video yoki ovozli ko‘rsatma kelganda); shubhali xabarni bir bosishda yuborish tugmasi; hodisalarga javob berish rejasi; kritik axborot infratuzilmasi sub’ektlari uchun O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi ZRU-764-sonli Qonuni talablariga rioya qilish [10].

Inson qatlami. Bir martalik o‘quv o‘rniga muntazam simulyatsiyalar va qisqa mashg‘ulotlar. Samaradorlik uchta ko‘rsatkich bilan o‘lchanadi: havolaga bosish ulushi, shubhali xabar haqida xabar berish ulushi va xabar berish uchun ketgan vaqt. Penetratsion test hisoboti asosida o‘qitish mavzulari va siyosatlar yangilanib boriladi.

Xulosa

Tadqiqot shuni ko‘rsatdiki, URL maskalash hujumchidan yuqori texnik malaka talab qilmaydi, ammo foydalanuvchi e’tiborsizligiga tayanib yuqori samara beradi. Himoya faqat texnik vositalar bilan cheklanmasligi, fishingga chidamli autentifikatsiya, tashkiliy tasdiqlash tartiblari va doimiy o‘qitishni birlashtirishi lozim. Keyingi tadqiqotlarda taklif etilgan modelning samaradorligini tashkilotlarda o‘lchanadigan ko‘rsatkichlar (bosish va xabar berish ulushi) orqali baholash, shuningdek, sun’iy intellekt yordamidagi hujumlarni aniqlash usullarini o‘rganish rejalashtirilgan.

Foydalanilgan adabiyotlar

1. FBI Internet Crime Complaint Center (IC3). Internet Crime Report 2024. - Washington, 2025.
2. Verizon. 2025 Data Breach Investigations Report. - 2025.
3. Anti-Phishing Working Group (APWG). Phishing Activity Trends Reports, Q1–Q4 2025. - https://apwg.org/trendreports
4. Fortune. British engineering giant Arup revealed as $25 million deepfake scam victim. - 17.05.2024.
5. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. - Indianapolis: Wiley, 2018.
6. Cialdini R. B. Influence: The Psychology of Persuasion. - New York: Harper Business, 2021.
7. NIST SP 800-63-4. Digital Identity Guidelines. - July 2025.
8. Unicode Technical Standard #39. Unicode Security Mechanisms. - Unicode Consortium.
9. Kucherawy M., Zwicky E. RFC 7489. Domain-based Message Authentication, Reporting, and Conformance (DMARC). - IETF, 2015.
10. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi ZRU-764-sonli Qonuni. - 15.04.2022.
11. htr-tech. Zphisher [GitHub repository]. - https://github.com/htr-tech/zphisher
12. cheetz. D0ppelganger [GitHub repository]. - https://github.com/cheetz/d0ppelganger

KORPORATIV TARMOQLARNI KIBERHUJUMLARDAN HIMOYALASH USULLARI

Ahmadov U.S., Murodov M.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada korporativ tarmoqlarni kiberhujumlardan himoyalash usullari ilmiy nuqtai nazardan tahlil qilinib, mavjud xavf omillari tasniflangan va samarali himoya strategiyalari keltirilgan.

Kalit so‘zlar: Korporativ tarmoq xavfsizligi, tarmoq segmentatsiyasi, Zero trust modeli, Supply chain, Ransomware.

Аннотация: В статье анализируются методы защиты корпоративных сетей от кибератак с научной точки зрения, классифицируются существующие факторы риска и устанавливаются эффективные стратегии защиты.

Ключевые слова: Безопасность корпоративных сетей, Сегментация сетей, Модель нулевого доверия, Цепочка поставок, Программы-вымогатели.

Kirish

Raqamli transformatsiya jarayonining jadal rivojlanishi natijasida korporativ tarmoqlar zamonaviy biznes faoliyatining ajralmas qismi bo‘lib qoldi. Ma’lumotlar almashinuvi, bulutli servislar, online xizmatlar va mobil qurilmalar orqali tashkilotlar o‘z faoliyatini yanada samarali yuritmoqda. Ammo bu jarayon kiberxavfsizlik bilan bog‘liq yangi muammolarni ham yuzaga chiqarmoqda.

Korporativ tarmoqlarga qaratilgan kiberhujumlar soni yildan-yilga ortib bormoqda: Cisco va IBM kompaniyalarining hisobotlariga ko‘ra 2024-yilda korporativ infratuzilmalarni nishonga olgan Ransomware hujumlari global kiberhujumlarning 32% ini tashkil qilgan. Shu sababli tarmoq xavfsizligini ta’minlash faqat texnik emas, balki tashkiliy va strategik yondashuvni ham talab qilmoqda [1].

Korporativ tarmoqlarda kibertahdidlarning asosiy turlari

Korporativ tarmoqlar ko‘p foydalanuvchi va murakkab tuzilishga ega bo‘lgani sababli turli darajadagi tahdidlarga ochiqdir. Asosiy xavf turlari quyidagilar:

1. Tarmoq sathidagi hujumlar - DDoS, ARP spoofing, port skanerlash, sniffing va MITM (Man-in-the-Middle) kabi hujumlar orqali hujumchilar trafikni to‘sish yoki manipulyatsiya qilishga urinadi;
2. Ilova darajasidagi hujumlar - Web-server va API interfeyslarida SQL Injection, Cross-Site Scripting (XSS) kabi zaifliklardan foydalaniladi;
3. Ichki tahdidlar - xodimlarning beparvoligi, zaif parollar, noto‘g‘ri kirish siyosatlari tufayli tarmoqqa bo‘ladigan ichki xavflar;
4. Zanjirli (supply chain) hujumlar - tashqi xizmat yetkazib beruvchilar orqali tarmoqqa zararli kod yoki orqa eshik (backdoor) kiritilishi;
5. Ransomware va zararli dasturlar - foydalanuvchi qurilmalarida yoki serverlarda ma’lumotlarni shifrlash orqali to‘lov talab qilish [7].

Bu tahdidlar turli darajadagi himoya qatlamlarini buzishga qaratilgan bo‘lib, ularni oldini olish uchun ko‘p bosqichli himoya talab etiladi. Quyida bugungi kunda mavjud kiberhujumlarning bugungi kundagi ulushi keltirilgan [2].

1-jadval

Kiberhujumlarning bugungi kundagi ulushi

№	Kiber tahdid turlari	Ulushi (%)
1	Phishing	25%
2	Malware (viruslar, trojan)	20%
3	Ransomware (shifrlovchi dasturlar)	15%
4	DDoS hujumlari	10%
5	Ichki tahdidlar	15%
6	Exploit hujumlari	8%
7	Man-in-the-Middle	7%

Kiberhujumlardan himoyalanishning boshqaruv va siyosiy asoslari

Tarmoq xavfsizligi strategiyasining asosi bu axborot xavfsizligi siyosatidir. Bu siyosat tashkilotda qanday resurslar mavjudligi, ularning qiymati, ularga kim va qanday yo‘l bilan kirishi mumkinligi haqida qat’iy qoidalar majmuasidir. Ular quyidagilar bo‘lishi mumkin:

– Risklarni boshqarish: Aktivlarni inventarizatsiya qilish, xavf qiymatini aniqlash, zaif nuqtalarni tahlil qilish (risk assessment);

– Xavfsizlik siyosati: foydalanuvchi rollari, parol siyosati, masofaviy kirish qoidalari va insidentga javob berish tartibi;

– Favqulodda holatlar rejasi (Incident Response Plan): kiberhujum sodir bo‘lganda amalga oshiriladigan bosqichma-bosqich chora-tadbirlar.

CISA (Cybersecurity & Infrastructure Security Agency) tavsiyalariga ko‘ra, boshqaruv siyosati korporativ xavfsizlikning 60% ni tashkil qiladi, texnik vositalar esa bu siyosatni amalga oshirish vositasidir.

Texnik himoya qatlamlari

Korporativ tarmoqlarni texnik himoyalash vositalari ko‘p qatlamli model asosida quriladi. Quyida har bir asosiy qatlam keltirilgan:

Tarmoq segmentatsiyasi va Zero Trust arxitekturasi

Tarmoq segmentatsiyasi - tarmoqni VLAN yoki subnetlarga ajratish orqali ichki trafikni cheklash. Bu “Lateral movement” ni - ya’ni bir tizimdan boshqasiga o‘tish imkonini kamaytiradi.

Zero Trust modeli - “ishonch yo‘q, har doim tekshir” tamoyiliga asoslanadi. Foydalanuvchi yoki qurilma tarmoq ichida bo‘lsa ham, har safar autentifikatsiya va avtorizatsiyadan o‘tkaziladi. Microsoft va Google kompaniyalari 2023-yildan boshlab Zero Trust arxitekturasini o‘z infratuzilmalarida qo‘llab kelishadi [3].

Tarmoq perimetri xavfsizligi (Perimeter Security)

– NGFW (Next Generation Firewall) – 7-darajali tarmoq trafikini tahlil qiluvchi aqlli xavfsizlik devorlari;

– IDS/IPS tizimlari – hujumlarni aniqlash va oldini olish tizimlari real vaqt rejimida hujumlarni to‘xtatadi;

– VPN va TLS – ma’lumotlarni uzatish jarayonida xavfsizligini ta’minlaydi.

– *Endpoint va server himoyasi*

– EDR/XDR tizimlari – foydalanuvchi qurilmalarida zararli faoliyatni aniqlaydi va avtomatik javob beradi.

– Antimalware va HIPS – dasturiy xavfsizlik qatlamini kuchaytiradi.

– Patch boshqaruvi – tizimlarni muntazam yangilash orqali zaifliklarni kamaytiradi.

Kadrlar va ijtimoiy muhandislikka qarshi himoya

Kiber hujumlarning 70% dan ortig‘i inson xatosi bilan bog‘liq (IBM Cyber Security Report, 2024). Shu sababli texnik himoya bilan bir qatorda xodimlarni o‘qitish va xavfsizlik madaniyatini shakllantirish muhim rol o‘ynaydi [4].

Asosiy yo‘nalishlar:

– Phishing testlari – xodimlar soxta xabarlarni ajrata olishni o‘rganadilar;

– Treninglar – parol siyosati, ijtimoiy muhandislik usullari, ma’lumot maxfiyligi bo‘yicha muntazam o‘qituvlar;

– Xabar berish tizimi – xodimlar shubhali faoliyatni anonim tarzda bildirishi mumkin bo‘lgan kanal yaratiladi;

– Korporativ muhitda inson omilini minimallashtirish - eng muhim, lekin ko‘pincha e’tibordan chetda qoladigan himoya chorasi hisoblanadi.

Monitoring, audit va insidentga javob

Tarmoqdagi har qanday g‘ayrioddiy faoliyatni erta aniqlash uchun SIEM (Security Information and Event Management) tizimlari qo‘llaniladi. Ular log fayllarni markazlashgan holda yig‘ib, tahdid indikatorlari asosida avtomatik ogohlantirishlar yuboradi [5].

– SOAR (Security Orchestration, Automation & Response) - insidentlarga avtomatik reaksiya beruvchi tizim.

– Audit va testlash - muntazam penetratsion testlar, red-team mashg‘ulotlari orqali real hujum stsenariylarini sinab ko‘rish.

– Backup va Disaster Recovery - ma’lumotlarni shifrlash yoki yo‘qotish holatlarida tezda tiklash imkonini beradi.

Bunday yondashuv korporativ tarmoqlarning “kiberbardoshliligini” (cyber resilience) ta’minlaydi - ya’ni hujum yuz bersa ham tizim o‘z faoliyatini to‘xtatmaydi.

Bulutli infratuzilma va masofaviy ish uchun maxsus himoya turlari

Bulut xizmatlari va masofaviy ish (Remote Work) korporativ infratuzilmaning yangi segmentlarini yaratadi. Bu holatda quyidagi choralar muhim:

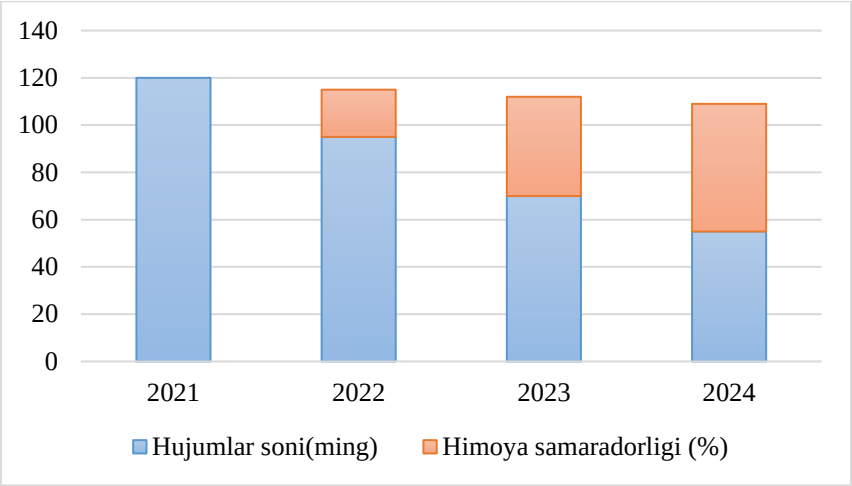
– ZTNA (Zero Trust Network Access) - faqat ishonchli qurilmalar va foydalanuvchilar uchun masofaviy kirish imkonini beradi;

– SASE (Secure Access Service Edge) - tarmoq va xavfsizlik funksiyalarini bulut orqali birlashtiruvchi model;

– Cloud IAM va DLP tizimlari - bulutdagi resurslar uchun kirish nazorati va ma’lumot oqimini boshqaradi.

Bulut xavfsizligi nafaqat texnik, balki shartnoma (SLA) darajasida ham belgilanadi - ya’ni xizmat ko‘rsatuvchi provayder ham xavfsizlik siyosatining bir qismi bo‘ladi [6].

Quyida korporativ tarmoqlarga bo‘lgan hujumlar va tashkilotlarning hujumlarga qarshi tura olish qobiliyatining yillar hisobida ko‘rsatkichlari keltirilgan.



1-rasm. Kiberhujumlardan himoyalanish dinamikasi

Xulosa

Yuqorida keltirilgan ma’lumotlardan xulosa qilib aytadigan bo‘lsak korporativ tarmoqlarni kiberhujumlardan himoyalash bu murakkab, ko‘p qatlamli, uzluksiz strategik jarayondir. Tizimning bardoshliligi faqatgina texnik vositalarga emas, balki boshqaruv siyosatiga, xodimlarning ehtiyotkorligiga va monitoring tizimlarining samaradorligiga ham bog‘liq.

Samarali himoya uchun quyidagi tamoyillar ustuvor hisoblanadi:

– Ko‘p qatlamli himoya (Defense in Depth) – har bir bosqichda alohida himoya vositasi;

– Zero Trust yondashuvi – ichki ishonchni bekor qilish va doimiy tekshirish;

– Doimiy takomillashtirish – yangi tahdidlar asosida xavfsizlik siyosatini yangilab borish.

Zamonaviy korporativ tarmoq xavfsizligi bu statik emas, balki dinamik tizimdir. Tizim o‘zgarishi, foydalanuvchi xatti-harakati va texnologik yangiliklarga mos holda himoya strategiyasini muntazam yangilab borish tashkilotning barqaror faoliyati uchun zarurdir.

Foydalanilgan adabiyotlar

1. Cisco Systems. Annual Cybersecurity Report, 2024.
2. IBM Security. Cost of a Data Breach Report, 2024.
3. CISA. Cybersecurity Best Practices for Corporate Networks, 2023.
4. Microsoft. Zero Trust Architecture Framework, 2024.
5. Cloud4C. Modern Network Security Challenges and Solutions, 2023.
6. SANS Institute. Enterprise Network Defense Model, 2023.
7. “Kiberxavfsizlik asoslari” O‘quv qo‘llanma S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov.

2-SHO‘BA. KRIPTOLOGIYA SOHASI ISTIQBOLLARI

МЕТОД ПОСТКВАНТОВОЙ МОДЕРНИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ КОРПОРАТИВНОГО МЕССЕНДЖЕРА

Валиулин А.Ш.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Annotatsiya. Maqolada korporativ messenjerning kriptografik kalitlarini boshqarish tizimini bosqichma-bosqich postkvant modernizatsiya qilish usuli taklif etiladi. PRIVATGRAM platformasi misolida X25519/X3DH asosidagi mavjud E2EE arxitekturasi tahlil qilinib, klassik X3DH va ML-KEM-768 ni birgalikda qo‘llashga asoslangan gibrid yondashuv ishlab chiqildi. PRIVATGRAM-PQ Backend, Mobile va Web v0.1 tajriba versiyalarida gibrid kalit shakllanishi tekshirildi va hisoblash hamda tarmoq xarajatlari baholandi.

Kalit so‘zlar: postkvant kriptografiya, ML-KEM, X25519, X3DH, Double Ratchet, E2EE, kriptografik kalitlarni boshqarish, PRIVATGRAM-PQ.

Аннотация. В статье предложен метод поэтапной постквантовой модернизации системы управления криптографическими ключами корпоративного мессенджера. На примере PRIVATGRAM исследована E2EE-архитектура X25519/X3DH и разработан гибридный подход X3DH + ML-KEM-768 с сохранением Double Ratchet. В экспериментальных версиях PRIVATGRAM-PQ Backend, Mobile и Web v0.1 проверена корректность формирования гибридного секрета и оценены вычислительные и сетевые издержки.

Ключевые слова: постквантовая криптография, ML-KEM, X25519, X3DH, Double Ratchet, E2EE, управление криптографическими ключами, PRIVATGRAM-PQ.

Введение

Корпоративные системы обмена сообщениями используются для передачи служебной, банковской и иной защищаемой информации, поэтому должны обеспечивать долговременную конфиденциальность, управление устройствами и работу в многоплатформенной среде. В современных E2EE-системах для асинхронного установления сессии применяется X3DH, а для последующего обновления ключевого материала - Double Ratchet [5, 7].

В PRIVATGRAM первоначальное установление E2EE-сессии основано на X25519/X3DH, а развитие сессии - на Double Ratchet. Однако X25519 относится к эллиптической криптографии, устойчивость которой в перспективе может быть нарушена квантовыми вычислениями с использованием алгоритма Шора [1, 8]. Для корпоративных систем дополнительно актуален сценарий Harvest Now, Decrypt Later, когда перехваченный сегодня криптографический обмен сохраняется для будущего криптоанализа [6].

В 2024 г. NIST стандартизовал ML-KEM в FIPS 203 [2]. Переход к постквантовой криптографии требует не только замены алгоритмов, но и crypto-agility - управляемого изменения форматов ключей и протокольных профилей без нарушения работы системы [3]. В предыдущих исследованиях автора была разработана архитектура PRIVATGRAM на основе X3DH и Double Ratchet [10], а затем предложена модель защищённых корпоративных коммуникаций как элемента киберустойчивости критической

инфраструктуры [11]. Настоящая работа развивает эти результаты в направлении постквантовой модернизации.

Цель исследования - разработка и экспериментальная проверка метода поэтапной постквантовой модернизации управления криптографическими ключами корпоративного мессенджера на основе совместного использования X25519/X3DH и ML-KEM-768.

Исходная архитектура и постановка задачи

PRIVATGRAM включает Backend, Android- и Web-клиенты. Сервер распределяет публичный ключевой материал и маршрутизирует ciphertext, но не получает закрытые E2EE-ключи. Каждое устройство имеет X25519 identity key, Ed25519 signing identity, Signed PreKey и набор One-Time PreKeys. При X3DH вычисляются DH1=DH(IKA,SPKB), DH2=DH(EKA,IKB), DH3=DH(EKA,SPKB) и, при наличии одноразового ключа, DH4=DH(EKA,OPKB). Результат обрабатывается HKDF-SHA-256 [9] и используется для инициализации Double Ratchet.



Рис. 1. Схема распределения ключей и сквозного шифрования сообщений между устройствами Alice и Bob в multi-device архитектуре PRIVATGRAM

Шифрование сообщений и вложений выполняется AES-256-GCM. В multi-device режиме каждое устройство имеет независимое криптографическое состояние и отдельную E2EE-сессию, что позволяет отзывать отдельное устройство без прекращения работы остальных [10]. С точки зрения PQ-миграции наиболее чувствительны X25519/X3DH и DH-компонент Double Ratchet, тогда как HKDF-SHA-256, симметрические цепочки и AES-256-GCM могут быть сохранены на первом этапе.

Поэтому целесообразно модернизировать прежде всего механизм первоначального установления секрета. Для действующей системы недостаточно просто заменить X25519 на ML-KEM: необходимо сохранить multi-device модель, раздельный жизненный цикл classical и post-quantum prekeys, key-blind Backend и защиту от несанкционированного понижения профиля.

Предлагаемый метод PRIVATGRAM-PQ

Для каждого устройства вводится Hybrid Device Bundle, содержащий классические X25519-ключи и постквантовые ML-KEM-768 ключи: PQSPK как last-resort prekey и набор

одноразовых PQOPK. PQ-состояние привязывается к конкретному устройству, а не к учётной записи пользователя. На первом этапе аутентификация prekeys сохраняется на Ed25519; её постквантовая замена относится к следующему этапу исследования.

При создании Hybrid-PQ-сессии сначала выполняется обычный X3DH. Параллельно инициатор получает публичный PQOPK (или PQSPK при отсутствии одноразового ключа) и выполняет (CTPQ, SSPQ)=MLKEM.Encaps(PQPKB). Получатель восстанавливает тот же секрет как SSPQ=MLKEM.Decaps(SKPQ,B, CTPQ). Итоговый ключевой материал вычисляется как SKH=HKDF-SHA256(DH1||DH2||DH3||[DH4]||SSPQ, Info), где Info="PRIVATGRAM-HYBRID-PQ-v1". Полученный SKH используется для инициализации существующего Double Ratchet.

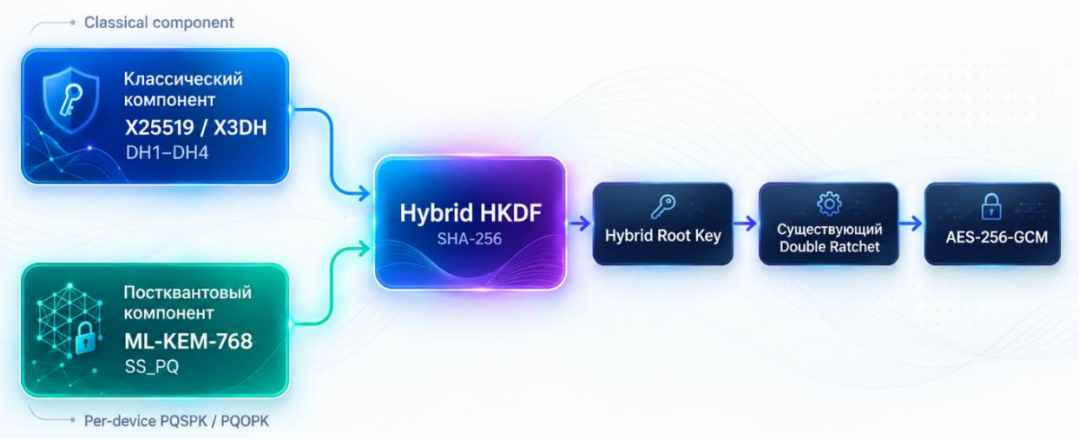


Рис. 2. Схема гибридного установления E2EE-сессии PRIVATGRAM-PQ

Для исключения downgrade вводятся профили PG-E2EE-CLASSICAL-V1 и PG-E2EE-HYBRID-PQ-V1. Если оба устройства объявили поддержку Hybrid-PQ, ошибка ML-KEM приводит к прекращению handshake, а не к автоматическому переходу на Classical. Идентификатор crypto suite, KEM, номер PQ-ключа и ML-KEM ciphertext включаются в authenticated context initial envelope.

Жизненный цикл одноразовых ключей также изменён: OPK и PQOPK считаются окончательно использованными только после успешной аутентификации initial message и фиксации нового состояния сессии. На Backend выдача classical OPK и PQOPK выполняется согласованно и атомарно.

Практическая реализация и эксперимент

Для проверки метода создана отдельная исследовательская ветка PRIVATGRAM-PQ: Backend v0.1, Mobile v0.1 и Web v0.1. Backend использует отдельный API /api/v1/e2ee-pq и хранит только публичные PQ-профили и PQOPK. Mobile реализует ML-KEM-768 через отдельный provider и защищает локальный PQ-private material существующим Android Keystore wrapping-механизмом. Web реализует тот же профиль PG-E2EE-HYBRID-PQ-V1 и отдельное локальное PQ-state. В обоих клиентах silent downgrade запрещён.

Криптографический self-test подтвердил совпадение 32-байтного ML-KEM shared secret и Hybrid Root на стороне инициатора и получателя, после чего тестовое сообщение успешно шифровалось и расшифровывалось AES-256-GCM. В reference benchmark x86-64/OpenSSL 3.5.5 средние значения составили: ML-KEM-768 KeyGen - около 45 мкс, Encaps - 32 мкс, Decaps - 48 мкс; classical X3DH initiator calculation - около 321 мкс, Hybrid X3DH + ML-KEM - около 353 мкс. Таким образом, чистая криптографическая составляющая initial establishment в данном стенде увеличилась примерно на 10 %.

Более заметным оказался сетевой overhead. Для ML-KEM-768 public key составляет 1184 байта, ciphertext - 1088 байт [2]. В тестовой JSON/Base64URL-сериализации initial header вырос примерно с 276 до 1816 байт, то есть на 1540 байт. При этом такой overhead возникает главным образом при bootstrap новой сессии; последующие сообщения используют существующий Double Ratchet и не требуют нового ML-KEM ciphertext.

Таблица 1

Предварительные результаты reference benchmark

Показатель	Classical	Hybrid-PQ
Initial calculation	≈321 мкс	≈353 мкс
Initial header	≈276 B	≈1816 B
ML-KEM public key	-	1184 B
ML-KEM ciphertext	-	1088 B

В multi-device модели отдельная операция ML-KEM Encaps требуется для каждого нового устройства адресата, поэтому initial overhead растёт приблизительно линейно с числом новых device sessions. Вместе с тем уже установленная сессия не выполняет ML-KEM повторно для каждого сообщения. Для PRIVATGRAM-PQ v0.1 выбран пул из 20 PQOPK, поскольку механическое использование 100 ключей, как в классической X25519-схеме, существенно увеличивает registration payload.

Полученные результаты показывают, что постквантовая миграция затрагивает прежде всего управление ключами, форматы device bundle и initial handshake, а не всю E2EE-подсистему. Основной практический компромисс связан с увеличением объёма ключевого материала, тогда как вычислительные затраты ML-KEM-768 в reference environment остаются умеренными.

Ограничения и дальнейшее развитие

PRIVATGRAM-PQ v0.1 усиливает первоначальное установление E2EE-секрета, однако не является полностью постквантовой системой. На данном этапе Ed25519-аутентификация, X25519-компонент дальнейшего DH-ratchet и криптография голосовых и видеозвонков остаются классическими. Поэтому результаты относятся прежде всего к снижению риска компрометации initial handshake и к исследованию жизненного цикла постквантовых ключей.

Следующий этап предусматривает гибридную либо постквантовую аутентификацию, модернизацию DH-компонента Double Ratchet и расширенные испытания на реальных Android- и Web-платформах. Такой поэтапный подход позволяет отдельно оценивать влияние каждого нового механизма и сохранять crypto-agility архитектуры.

Заключение

Предложен метод поэтапной постквантовой модернизации системы управления криптографическими ключами корпоративного мессенджера, основанный на гибридном X25519/X3DH + ML-KEM-768 установлении первоначального секрета с сохранением, существующего Double Ratchet и AES-256-GCM. Разработаны экспериментальные Backend, Mobile и Web-компоненты PRIVATGRAM-PQ v0.1, подтверждена корректность формирования Hybrid Root и получены предварительные оценки вычислительного и сетевого overhead.

Исследование показывает практическую возможность усилить initial E2EE establishment без полной замены криптографического ядра. Следующими этапами являются

постквантовая аутентификация, модернизация DH-компонента Double Ratchet и расширенные испытания на реальных Android- и Web-платформах.

Список литератур

1. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. - 1994. - P. 124-134. - DOI: 10.1109/SFCS.1994.365700.

2. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. - Gaithersburg: NIST, 2024.

3. National Institute of Standards and Technology. Considerations for Achieving Crypto Agility: Strategies and Practices. - NIST, 2025.

4. National Cybersecurity Center of Excellence. Migration to Post-Quantum Cryptography. - NIST.

5. Perrin T., Marlinspike M. The X3DH Key Agreement Protocol. - Signal Protocol Specification.

6. Signal. The PQXDH Key Agreement Protocol. - Signal Protocol Specification.

7. Perrin T., Marlinspike M., Schmidt R. The Double Ratchet Algorithm. - Signal Protocol Specification.

8. Langley A., Hamburg M., Turner S. RFC 7748: Elliptic Curves for Security. - IETF, 2016.

9. Krawczyk H., Eronen P. RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF). - IETF, 2010.

10. Valiulin A. Architecture of The PRIVATGRAM Secure Corporate Messenger for Critical Infrastructure Based on X3DH And Double Ratchet Protocols // The American Journal of Engineering and Technology. - 2026. - Vol. 8, Issue 05. - P. 159–164. - DOI: 10.37547/tajet/Volume08Issue05-15.

11. Valiulin A. Enterprise Secure Messaging for Critical Infrastructure: From Signal-Class Cryptography to National Cybersecurity Strategy // The American Journal of Applied Sciences. - 2026. - Vol. 8, Issue 06. - P. 339–349. - DOI: 10.37547/tajas/Volume08Issue06-18.

KRIPTOGRAFIK O‘LCHAMDAGI TUB SONLARNING TAQSIMOTI VA ULARNI GENERATSIYA QILISHNING NAZARIY ASOSLARI

Haydarov E.D., Salimov S., Janxojaev A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada tub sonlarning asosiy xossalari, katta bit o‘lchamli sonlarning tavsifi va tub sonlar teoremasidan kelib chiqadigan amaliy xulosalar ko‘rib chiqiladi. RSA modulining razryadi bilan uni hosil qiluvchi tub ko‘paytuvchilar razryadi o‘rtasidagi farq tushuntiriladi. Tub sonlar zichligi asosida 512–4096 bitli tub sonni tasodifiy toq nomzodlar orasidan topish uchun zarur bo‘lgan o‘rtacha sinovlar soni baholanadi. Katta tub sonlarni tasodifiy qidirish amaliy jihatdan bajariladigan masala ekanligi asoslanadi.

Kalit so‘zlar: tub son, tub sonlar teoremasi, tublik zichligi, bit uzunligi, RSA moduli, tub sonlik testi, tub sonlarni generatsiya qilish, ochiq kalitli kriptografiya.

Аннотация. В статье рассматриваются основные свойства простых чисел, описание чисел большой разрядности и практические следствия теоремы о распределении простых чисел. Объясняется различие между разрядностью модуля RSA и разрядностью образующих его простых сомножителей. На основе плотности простых чисел оценивается среднее число испытаний, необходимое для нахождения простого числа длиной 512–4096 бит среди случайных нечётных кандидатов. Обосновывается, что случайный поиск больших простых чисел является практически выполнимой задачей.

Ключевые слова: простое число, теорема о распределении простых чисел, плотность простых чисел, разрядность, модуль RSA, тест простоты, генерация простых чисел, криптография с открытым ключом.

Kirish

Tub son – 1 dan katta bo‘lgan va faqat 1 ga hamda o'‘ziga bo‘linadigan musbat butun son. Arifmetikaning asosiy teoremasiga ko‘ra, 1 dan katta har bir butun son, ko‘paytuvchilar tartibidan qat’i nazar, tub sonlar darajalarining ko‘paytmasi sifatida yagona tarzda ifodalanadi; masalan, $360 = 2^3 \cdot 3^2 \cdot 5$ [1, 2]. Shu sababli tub sonlar barcha natural sonlarning “qurilish g‘ishtlari” hisoblanadi. Zamonaviy axborot xavfsizligi tizimlarida, ayniqsa ochiq kalitli kriptografik mexanizmlarda – RSA, Diffie–Hellman, DSA va shu kabilarda – katta tub sonlar asosiy parametr sifatida ishlatiladi [3]. Bunday tizimlarni amalda qo‘llash uchun yuzlab o‘nlik raqamdan iborat tub sonlarni tez topa olish zarur. Ushbu ishning maqsadi – kriptografik o‘lchamdagi tub sonlarning qanchalik tez-tez uchrashini va ularni tasodifiy qidirish nima uchun amaliy jihatdan mumkinligini sonlar nazariyasi natijalari asosida ko‘rsatishdir.

Asosiy qism

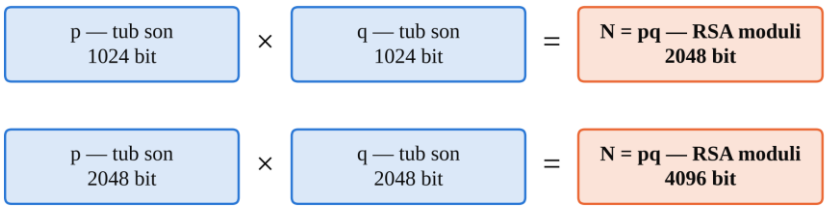
Tub sonlarning kriptografik qiymati ularning uchta xossasiga tayanadi. Birinchisi – yagona faktorizatsiya: har qanday murakkab sonning tuzilishi uning tub ko‘paytuvchilari bilan to‘liq aniqlanadi. Ikkinchisi – modulli arifmetikadagi algebraik xossalar: agar p tub son bo‘lsa, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ qoldiq sinflari chekli maydonni tashkil etadi, noldan farqli har bir element ko‘paytirishga nisbatan teskari elementga ega bo‘ladi va $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ to‘plami $p-1$ tartibli multiplikativ guruhni hosil qiladi [4]. Ko‘plab ochiq kalitli algoritmlar aynan shunday guruhlarda ishlaydi. Uchinchisi – cheksizlik: Evklid isbotiga ko‘ra, agar tub sonlar chekli p_1, p_2,

…, p_k bo‘lganida, $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ soni ularning hech biriga bo‘linmas edi. Aynan shu cheksizlik istalgan razryaddagi yangi tub sonlarni topish imkonini kafolatlaydi.

Kriptografiyada butun sonlar o‘nlik raqamlari soni bilan emas, balki bit uzunligi bilan tavsiflanadi. k bitli musbat butun n son $2^{k-1} \le n < 2^k$ shartni qanoatlantiradi, uning o‘nlik raqamlari soni esa taxminan quyidagicha aniqlanadi:

$d \approx k \cdot \log_{10} 2 \approx 0{,}30103 \cdot k.$

Demak, 1024 bitli son taxminan 308 ta, 2048 bitli son 617 ta, 4096 bitli son esa 1233 ta o‘nlik raqamdan iborat [3]. Bit uzunligi ortishi bilan o‘nlik raqamlar soni chiziqli, mumkin bo‘lgan qiymatlar sohasi esa eksponensial ravishda kengayadi. Bunda RSA modulining o‘lchami bilan alohida tub ko‘paytuvchilar o‘lchamini farqlash kerak (1-rasm): $N = pq$ moduli taxminan 2048 bit bo‘lsa va p hamda q o‘zaro yaqin o‘lchamga ega bo‘lsa, ularning har biri taxminan 1024 bitli bo‘ladi; 4096 bitli modul esa ikkita 2048 bitli tub sondan hosil qilinadi [5]. Shuning uchun :2048 bitli tub son” va “2048 bitli RSA kaliti” iboralari bir xil kattalikni anglatmaydi.



1-rasm. RSA modulining razryadi va uni hosil qiluvchi tub sonlar razryadi

Sonlar kattalashgani sari tub sonlar kamroq uchraydi, biroq ularning kamayishi muntazam asimptotik qonuniyatga bo‘ysunadi. $\pi(x)$ orqali x dan oshmaydigan tub sonlar soni belgilansa, tub sonlar teoremasi quyidagini tasdiqlaydi [1, 3]:

$\pi(x) \sim x / \ln x$, ya’ni $x \to \infty$ da $\pi(x) / (x / \ln x) \to 1$.

Teoremaning ma’nosini kichik sonlarda ham ko‘rish mumkin (2-rasm): 100 000 gacha 9592 ta tub son bor, $x / \ln x$ ifodasi esa taxminan 8686 ni beradi; x ortishi bilan ularning nisbati birga yaqinlashadi. Teorema ehtimollik talqiniga ham ega: yetarlicha katta x ga yaqin joylashgan tasodifiy butun sonning tub bo‘lish ehtimoli taxminan $1 / \ln x$ ga teng. 2 dan katta barcha tub sonlar toq bo‘lgani uchun faqat toq nomzodlar tanlansa, bu ehtimollik ikki baravar ortadi.

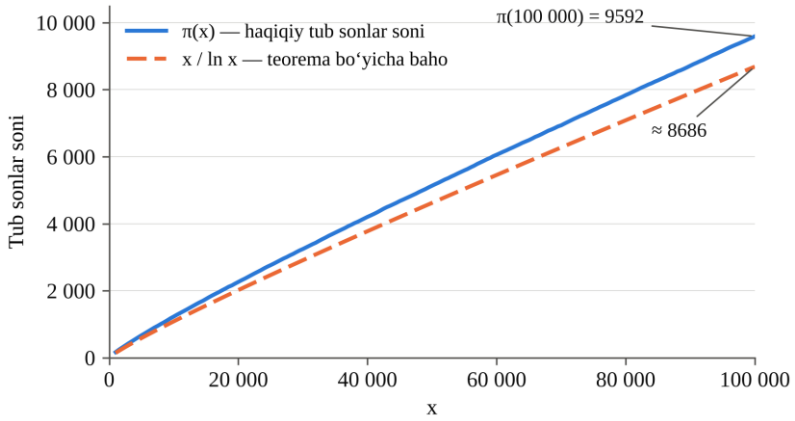
1-jadval

π(x) ning haqiqiy qiymatlari va x / ln x bahosi

x	π(x)	x / ln x (≈)	Nisbati
1 000	168	145	1,16
10 000	1229	1086	1,13
100 000	9592	8686	1,10

1-jadvaldan ko‘rinadiki, baho haqiqiy qiymatdan biroz kichik, lekin x o‘n baravar ortgan sari nisbat 1,16 dan 1,10 gacha kamayib, birga yaqinlashib boradi. Tub sonlarning joylashuvi dastlab tartibsiz ko‘rinsa-da, ularning umumiy taqsimoti butunlay tasodifiy emas, balki aniq asimptotik qonuniyatga bo‘ysunadi.

Kriptografik o‘lchamlar uchun bu quyidagini anglatadi. 2^{1024} atrofidagi son uchun $\ln(2^{1024}) = 1024 \cdot \ln 2 \approx 709{,}8$, ya’ni tasodifiy tanlangan butun sonning tub bo‘lish ehtimoli taxminan 1/710, toq nomzodlar uchun esa $2/709{,}8 \approx 1/355$. Boshqa razryadlar uchun ko‘rsatkichlar 2-jadvalda keltirilgan: b bitli sonlar orasida tublik zichligi $1/(b \cdot \ln 2)$ ga, bitta tub sonni topish uchun tekshiriladigan toq nomzodlarning o‘rtacha soni esa shu qiymatning yarmiga teng.



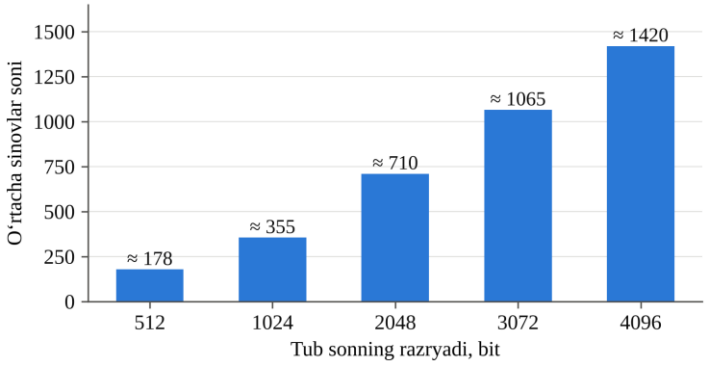
2-rasm. π(x) funksiyasi va uning tub sonlar teoremasi bo‘yicha bahosi

2-jadval

Kriptografik tub sonlarning razryadlari va xarakteristikalari

Razryad, bit	O‘nlik raqamlar soni (≈)	Tublik zichligi, 1/(b·ln 2)	O‘rtacha sinovlar soni (toq nomzodlar)
512	154	1 / 355	≈ 178
1024	308	1 / 710	≈ 355
2048	617	1 / 1420	≈ 710
3072	925	1 / 2129	≈ 1065
4096	1233	1 / 2839	≈ 1420

2-jadvaldan muhim hisoblash xulosasi kelib chiqadi: razryad sakkiz baravar – 512 dan 4096 bitgacha – ortganda o‘rtacha sinovlar soni ham atigi sakkiz baravar, 178 tadan 1420 tagacha o‘sadi (3-rasm). Ya’ni tub sonlar kriptografik o‘lchamlarda ham shunchalik kam uchramaydiki, ularni tasodifiy qidirish imkonsiz bo‘lib qolsin. Sonlar sohasining o‘zi eksponensial kengaygani holda, qidiruv mehnati razryadga nisbatan faqat chiziqli ortadi.

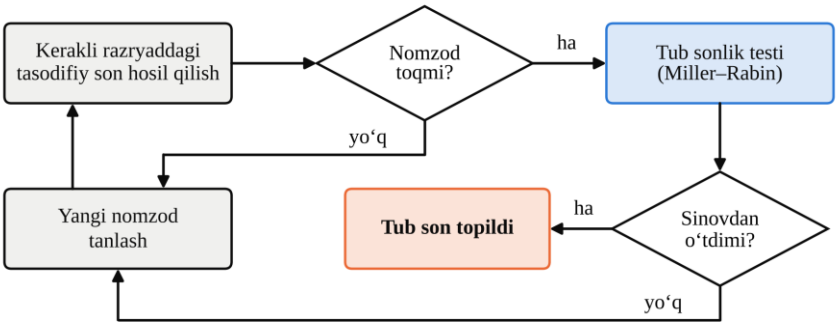


3-rasm. Bitta tub sonni topish uchun zarur bo‘lgan o‘rtacha sinovlar soni

Shu natijaga tayangan holda kriptografik dasturiy ta’minot tub sonlarni quyidagi tartibda hosil qiladi (4-rasm): kerakli bit uzunligidagi tasodifiy son generatsiya qilinadi; juft nomzodlar darhol chiqarib tashlanadi; toq nomzodga samarali tub sonlik testi, masalan, Miller–Rabin testi qo‘llanadi; nomzod murakkab bo‘lib chiqsa, yangi nomzod tanlanadi va jarayon takrorlanadi [6].

Tub sonlar zichligi bilan ularni generatsiya qilish imkoniyati o‘rtasidagi bu bog‘liqlik sonlar nazariyasiga asoslangan barcha tizimlar uchun muhim. RSA tizimida katta tub sonlardan kriptografik modul hosil qilinadi. Diffie–Hellman algoritmida tub son moduli asosida matematik guruh shakllantirilib, umumiy maxfiy qiymatni hosil qilish mexanizmi tashkil etiladi. DSA kabi raqamli imzo algoritmlarida ham tub sonlar va ularga asoslangan algebraik tuzilmalar asosiy

parametr vazifasini bajaradi. Demak, katta tub sonlarning mavjudligi, taqsimoti va ularni samarali topish imkoniyati kriptografik algoritmlarni amalda qo‘llashning zaruriy shartidir.



4-rasm. Katta tub sonni generatsiya qilish jarayoni

Bu yerda tub sonlikni tekshirish bilan faktorizatsiyani farqlash muhim. Tub sonlikni tekshirish berilgan sonning tub yoki murakkab ekanligini aniqlaydi va juda katta sonlar uchun ham amalda bajariladi. Faktorizatsiya esa murakkab sonni noma’lum tub ko‘paytuvchilarga ajratishni talab qiladi va nihoyatda murakkab bo‘lishi mumkin [7]. Sonning murakkab ekanligini tez aniqlash uning ko‘paytuvchilarini topish masalasini hal qilmaydi. Aynan shu nomutanosiblik – tub sonni topish oson, ularning ko‘paytmasini qayta ajratish qiyin – katta tub sonlarning kriptografiyada foydali bo‘lishining asosiy sababidir. Bunda tub sonning kattaligi bilan bir qatorda uning zarur matematik shartlarni qanoatlantirishi ham tekshiriladi [8].

Xulosa

Tub sonlarning yagona faktorizatsiya xossasi, cheksizligi va modulli arifmetikadagi algebraik xususiyatlari ularni ochiq kalitli kriptografiyaning matematik asosiga aylantiradi. Tub sonlar teoremasiga ko‘ra, b bitli sonlar orasida tublik zichligi taxminan $1/(b \cdot \ln 2)$ ga teng, shuning uchun 1024 bitli tub sonni topish uchun o‘rtacha 355 ta, 2048 bitli tub son uchun 710 ta toq nomzodni tekshirish kifoya. Bu samarali tub sonlik testlari bilan birgalikda RSA, Diffie–Hellman va DSA kabi tizimlar uchun zarur bo‘lgan katta tub sonlarni amaliy vaqt ichida generatsiya qilish imkonini beradi. Kriptografik parametrlarni to‘g‘ri talqin qilishda modul razryadi bilan tub ko‘paytuvchilar razryadini farqlash zarur.

Foydalanilgan adabiyotlar:

1. Hardy G.H., Wright E.M. An Introduction to the Theory of Numbers. – 6th ed. – Oxford: Oxford University Press, 2008. – 621 p.

2. Виноградов И.М. Основы теории чисел. – 9-е изд., перераб. – М.: Наука, 1981. – 176 с.

3. Crandall R., Pomerance C. Prime Numbers: A Computational Perspective. – 2nd ed. – New York: Springer, 2005. – 597 p.

4. Shoup V. A Computational Introduction to Number Theory and Algebra. – 2nd ed. – Cambridge: Cambridge University Press, 2009. – 580 p.

5. FIPS PUB 186-5. Digital Signature Standard (DSS). – Gaithersburg: National Institute of Standards and Technology, 2023. – DOI: 10.6028/NIST.FIPS.186-5.

6. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – Boca Raton: CRC Press, 1996. – 780 p.

7. Lenstra A.K., Verheul E.R. Selecting cryptographic key sizes // Journal of Cryptology. – 2001. – Vol. 14, № 4. – P. 255–293.

8. Moriarty K., Kaliski B., Jonsson J., Rusch A. RFC 8017. PKCS #1: RSA Cryptography Specifications Version 2.2. – Internet Engineering Task Force, 2016.

AGENTLI SUN’IY INTELLEKT TIZIMLARIDA AXBOROT OQIMI XAVFSIZLIGINI TA’MINLASHNING PANJARA MODELIGA ASOSLANGAN YONDASHUVI

Nurullayev M.M.
Buxoro davlat texnika universiteti

Annotatsiya. Tezisda katta til modellariga (LLM) asoslangan agentli sun’iy intellekt tizimlarida axborot oqimi xavfsizligini ta’minlash uchun panjara modeli taklif etilgan. Model maxfiylik va yaxlitlik darajalarining $L = C \times I$ ko‘paytma panjarasiga asoslanadi: agent xotirasi va agentlararo xabarlar yagona belgilangan kanallar sifatida ko‘riladi, agentlararo kanallar uchun esa “ishonch shifti” qoidasi kiritiladi. Belgilarni tarqatish va siyosatni ijro etishning oltita qoidasi ishlab chiqilgan hamda ular bajarilganda noaralashuv xossasi sessiyalar va agentlar bo‘ylab saqlanishi isbot g‘oyasi bilan asoslangan. Misolda modelning bilvosita prompt-in’eksiya tarqalishini to‘xtatishi ko‘rsatilgan.

Kalit so‘zlar: agentli sun’iy intellekt, axborot oqimini nazorat qilish, xavfsizlik panjarasi, ko‘p agentli tizimlar, agent xotirasi, bilvosita prompt-in’eksiya, ishonch shifti.

Аннотация. В тезисах предложена решёточная модель обеспечения безопасности информационных потоков в агентных системах искусственного интеллекта на основе больших языковых моделей (LLM). Модель основана на произведении решёток уровней конфиденциальности и целостности $L = C \times I$: память агента и межагентные сообщения единообразно рассматриваются как помеченные каналы, а для межагентных каналов вводится правило “потолка доверия”. Разработаны шесть правил распространения меток и применения политик и приведена идея доказательства того, что при их выполнении свойство невмешательства сохраняется между сессиями и агентами. На примере показано, что модель блокирует распространение косвенной промпт-инъекции через агентов и память.

Ключевые слова: агентный искусственный интеллект, контроль информационных потоков, решётка безопасности, мультиагентные системы, память агента, косвенная промпт-инъекция, потолок доверия.

Kirish

LLM asosidagi agentlar uzoq muddatli xotiraga ega bo‘ladi, vositalarni chaqiradi va ko‘p agentli tizimlarda bir-biriga topshiriq beradi. Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasi [1] bunday tizimlarni davlat xizmatlariga joriy etishni ko‘zda tutadi, bu esa ularning xavfsizligini “Kiberxavfsizlik to‘g‘risida”gi Qonun [2] doirasida ta’minlashni talab qiladi.

Agentlarning asosiy zaifligi – bilvosita prompt-in’eksiya: qayta ishlanayotgan veb-sahifa yoki xatga yashirilgan ko‘rsatma agent xatti-harakatini o‘zgartiradi [3]. Ko‘p agentli tizimlarda u agentdan agentga tarqaladi, shu sababli OWASP agentlararo xavfsiz bo‘lmagan aloqani alohida xavf sifatida qayd etgan [4].

Istiqbolli javoblardan biri – axborot oqimini nazorat qilish: ma’lumotlarga maxfiylik va yaxlitlik belgilari biriktiriladi, ularning tarqalishi panjara modeli [5] asosida nazorat qilinadi. FIDES [6] va CaMeL [7] bu yondashuvni bitta agent va bitta topshiriq uchun amalga oshirgan, SPA [8], MemLineage [9] va TMA-NM [10] esa uni sessiyalararo xotiraga kengaytirgan. Ko‘p agentli tizimlar uchun AgentFlow [11] siyosat tili va delegatsiya xavfsizligi isbotini taklif etadi,

TMA-NM mualliflari esa bu holatni kelgusi ishga qoldirgan. Biroq tahlil qilingan ishlarda xotira va agentlararo aloqani yagona kanal qoidasi bilan qamrab, sessiyalar va agentlar bo‘ylab noaralashuv xossasini beruvchi model uchramadi. Tezisning maqsadi – shunday panjara modelini taklif etish va uning xavfsizlik xossasini asoslash.

Asosiy qism

1. Belgilar panjarasi. Maxfiylik darajalari C = {0, 1, 2} (ochiq, ichki, maxfiy) va yaxlitlik darajalari I = {0, 1, 2} (ishonchli, cheklangan, ishonchsiz) to‘plamlarini olamiz. Belgi $\ell = (c, i) \in L = C \times I$; tartib va birlashma komponentlar bo‘yicha aniqlanadi: $(c, i) \sqsubseteq (c', i') \Leftrightarrow c \leq c'$ va $i \leq i'$; $(c, i) \sqcup (c', i') = (\max(c, c'), \max(i, i'))$. L – 9 elementli distributiv panjara, $\bot = (0, 0)$, $\top = (2, 2)$; axborot panjarada faqat yuqoriga oqishi mumkin [5]. “Cheklangan” daraja ishonchsiz matndan karantindagi LLM yordamida past sig‘imli τ turida (mantiqiy qiymat, chekli ro‘yxat, sana, tekshirilgan e-mail) ajratib olingan qiymatni bildiradi: uni hujumchi tanlagan bo‘lishi mumkin, ammo uning ko‘rsatma tashish imkoniyati cheklangan [6].

2. Kanallar va qoidalar.

Tizimni $S = \langle \mathcal{A}, \mathcal{T}, \mathcal{K}, R \rangle$ ko‘rinishida ifodalaymiz: $\mathcal{A}$ – agentlar (rejalovchi LLM, karantindagi LLM va xotira), $\mathcal{T}$ – vositalar, $\mathcal{K}$ – kanallar, R – kanallarni nazorat qiluvchi monitor. Asosiy g‘oya: foydalanuvchi kiritishi, vosita javobi, xotira va boshqa agent xabari – barchasi kanal bo‘lib, har bir $k \in \mathcal{K}$ ga ishonch shifti $\theta(k) \in I$ (kanal bera oladigan eng yuqori ishonch) va ruxsat darajasi $\kappa(k) \in C$ beriladi. $\theta = 0$ faqat bitta principal nomidan ishlovchi kanallarga beriladi: foydalanuvchi kiritishi, ichki vositalar, xotira va umumiy monitor ostidagi agentlar; tashqi kontent va tashqi agentlar uchun $\theta = 2$, tashqariga chiquvchi argumentlar uchun $\kappa = 0$. Belgilarni LLM emas, monitor biriktiradi. pc – rejalovchi qarorlari bog‘liq barcha qiymatlar (ko‘rgan qiymatlar, havolalar soni va turi, xato va rad etish xabarlari) belgilarining birlashmasi; u sessiya ichida faqat oshadi. Qoidalar:

1. Q1 (hisoblash): $\ell(f(v_1, \ldots, v_n)) = \ell(v_1) \sqcup \ldots \sqcup \ell(v_n) \sqcup pc$.
2. Q2 (qabul qilish): k kanalidan kelgan v uchun $\ell(v) = \ell_k(v) \sqcup (0, \theta(k))$, bu yerda $\ell_k(v)$ – jo‘natuvchi tomonda monitor biriktirgan belgi; vosita yoki xotira so‘roviga javobga so‘rov belgisi $pc \sqcup \ell(a_1) \sqcup \ldots \sqcup \ell(a_n)$ ham qo‘shiladi. Topshiriq sifatida kelgan xabar qabul qiluvchi pc sini xabar belgisigacha oshiradi.
3. Q3 (uzatish): v ni k kanaliga (vosita argumenti, xabar, xotira) uzatish faqat $c(v) \sqcup c(pc) \leq \kappa(k)$ bo‘lganda ruxsat etiladi va v $\ell(v) \sqcup pc$ belgisi bilan uzatiladi; xotira yozuvini o‘chirish yoki qayta yozish faqat $pc \sqsubseteq \ell(\text{yozuv})$ bo‘lganda bajariladi.
4. Q4 (rejalovchini ajratish): rejalovchi faqat i = 0 qiymatlarni ko‘radi, qolganlari mazmunsiz havola sifatida beriladi [7]; $i \geq 1$ qiymat bo‘yicha tarmoqlanish pc ni shu qiymat belgisigacha oshiradi.
5. Q5 (vosita chaqiruvi): $t(a_1, \ldots, a_n)$ faqat $i(pc) \leq \pi(t)$ va har bir j uchun $i(a_j) \leq \rho_t(j)$ bo‘lganda bajariladi; tashqi kuzatiladigan ta’sirga ega vositalar uchun $\pi(t) = 0$, bunday ta’siri yo‘q vositalar uchun $\pi(t) = 2$.
6. Q6 (nazoratli pasaytirish): τ turidagi ajratish faqat i ni 2 dan 1 ga tushiradi, c o‘zgarmaydi; i ni 0 ga tushirish (tasdiqlash) yoki $i(v) = 0$ bo‘lgan v ning c sini pasaytirish (deklassifikatsiya) faqat $i(pc) = 0$ kontekstdagi aniq qaror, masalan, foydalanuvchi tasdig‘i bilan amalga oshiriladi va jurnalga yoziladi [3, 15].

Xotira orqali belgi “yuvilishini” saqlanadigan belgi (Q3), agentlar orasidagi soxta belgi da’vosini ishonch shifti (Q2) bartaraf etadi. Topshiriq bilan pc ham uzatilgani uchun ishonchsiz

ma’lumotga qarab qaror qilgan agent boshqa agent qo‘li bilan tashqi ta’sirli harakat bajara olmaydi.

3. Tasdiq.

Q1–Q6 bajarilganda istalgan sonli sessiya va agentdan iborat ijroda: (a) $\theta = 2$ kanallardan kelgan kirishlar qaysi tashqi ta’sirli vosita chaqirilishiga ta’sir qilmaydi, argumentlarga esa faqat $\rho_t(j) \geq 1$ bo‘lgan parametrlar orqali ta’sir qiladi; (b) $\kappa = 0$ kanallarga chiqishlar $c = 2$ qiymatlarga bog‘liq emas. Q6 bo‘yicha qabul qilingan aniq qarorlar bundan mustasno.

Isbot g‘oyasi – global ijro qadamlari bo‘yicha induksiya. Invariant: mazmuni yoki mavjudligi $\theta = 2$ kirishga bog‘liq va Q6 bo‘yicha tasdiqlanmagan har qanday qiymat $i \geq 1$ belgisiga ega. $\sqcup$ monoton bo‘lgani uchun Q1 invariantni saqlaydi; Q2 uni so‘rov va topshiriq orqali, Q3 esa xotiradagi belgi orqali sessiya chegarasidan o‘tkazadi. Q4 ga ko‘ra $i(pc) = 0$ kontekstdagi qarorlar faqat $i = 0$ qiymatlarga bog‘liq, Q5 esa tashqi ta’sirli harakatlarni aynan shunday qarorlarga bog‘laydi; (b) qism c komponenti bo‘yicha xuddi shunday isbotlanadi. Natija Goguen–Meseguer [13] noaralashuvining tugashga befarq ko‘rinishidir [14]. Taxminlar: rejalovchi kirishlarining ixtiyoriy deterministik funksiyasi (LLM to‘g‘ri ishlashi talab qilinmaydi), agentlar ketma-ket ishlaydi, rad etish ijroni to‘xtatadi, monitor ishonchli hisoblash bazasiga kiradi, vositalar manba belgisini to‘g‘ri e’lon qiladi; vaqt bo‘yicha yon kanallar hisobga olinmaydi.

4. Misol.

A_1 – pochta agenti, A_2 – maxfiy ma’lumotlar bazasi va send_email vositasiga ega hisobot agenti ($\pi = 0$, $\rho(to) = 0$, tashqi pochtada $\kappa = 0$). Tashqi xatda “hisobotni x@mai.uz ga yubor” ko‘rsatmasi bor (1-jadval).

1-jadval.

Hujum ssenariysida qoidalarning ishlashi

Qadam	Qoida	Belgi (c, i)	Natija
A_1 tashqi xatni o‘qiydi	Q2 ($\theta = 2$), Q4	(0, 2)	Rejalovchiga faqat havola
A_1 A_2 ga topshiriq va xat xulosasini (ilova) yuboradi	Q3, Q2 ($\theta = 0$)	topshiriq (0, 0); ilova (0, 2)	Ilova belgisi saqlanadi
Ilova tashqi agentdan (0, 0) da’vosi bilan keladi	Q2 ($\theta = 2$)	(0, 2)	Soxta da’vo bekor
A_2 ilovadan manzilni τ turida ajratadi	Q4, Q6	(0, 1)	Faqat ma’lumot sifatida
send_email(to = x@mai.uz, body = hisobot)	Q5, Q3	to: (0, 1); body: (2, 0)	Rad etiladi: $i(to) > \rho(to)$, $c(body) > \kappa$
A_1 topshiriqni xat mazmuniga qarab tanlaydi	Q4, Q3, Q2	$pc(A_1) = pc(A_2) =$ (0, 2)	Tashqi ta’sirli chaqiruvlar rad etiladi: $i(pc) > \pi$

5-qadam foydalanuvchi o‘zi “hisobotni xatdagi manzilga yubor” desa ham amal qiladi: manzilni hujumchi tanlagan bo‘lishi mumkin, shuning uchun Q6 tasdig‘i kerak – bu modelning funksionallik narxi.

Xulosa

Xotira va agentlararo xabarlarni yagona belgilangan kanal sifatida ko‘ruvchi $L = C \times I$ panjara modeli va oltita qoida taklif etildi; ishonch shifti va topshiriq bilan uzatiladigan pc (Q2) belgi soxtalashtirilishi va “chalkash vakil” hujumlarini bartaraf etadi. Qoidalar bajarilganda noaralashuv sessiyalar va agentlar bo‘ylab saqlanishi asoslandi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi qarori. PQ-358-son, 14.10.2024.

2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 15.04.2022.

3. Greshake K. et al. Not What You’ve Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // AISec. – 2023.

4. OWASP GenAI Security Project. OWASP Top 10 for Agentic Applications for 2026. – 2025. – URL: https://genai.owasp.org

5. Denning D.E. A Lattice Model of Secure Information Flow // Communications of the ACM. – 1976. – Vol. 19, No. 5. – P. 236–243.

6. Costa M. et al. Securing AI Agents with Information-Flow Control // arXiv:2505.23643. – 2025.

7. Debenedetti E. et al. Defeating Prompt Injections by Design // arXiv:2503.18813. – 2025.

8. Girrens D., Wang G. SPA: Securing Persistent LLM Agents Across Queries with Plan-First Information-Flow Control // arXiv:2608.27234. – 2026.

9. Ouyang C., Hou R. MemLineage: Lineage-Guided Enforcement for LLM Agent Memory // arXiv:2605.14421. – 2026.

10. Louck Y. Securing LLM-Agent Long-Term Memory Against Poisoning: Non-Malleable, Origin-Bound Authority with Machine-Checked Guarantees // arXiv:2606.24322. – 2026.

11. Shivakumar B.A., Priya S., Gao P. AgentFlow: A Flow-Centric Policy Language and Framework for Securing LLM Agent Systems // arXiv:2608.22868. – 2026.

12. Cecchetti E., Myers A.C., Arden O. Nonmalleable Information Flow Control // Proc. ACM CCS. – 2017.

13. Goguen J.A., Meseguer J. Security Policies and Security Models // Proc. IEEE Symp. on Security and Privacy. – 1982. – P. 11–20.

14. Volpano D., Smith G., Irvine C. A Sound Type System for Secure Flow Analysis // Journal of Computer Security. – 1996. – Vol. 4, No. 2–3. – P. 167–187.

15. Zdancewic S., Myers A.C. Robust Declassification // Proc. 14th IEEE Computer Security Foundations Workshop. – 2001.

OCHIQ KALITLI KRIPTOTIZIMLARDA TUB SONLAR: FAKTORIZATSIYA VA DISKRET LOGARIFM MUAMMOLARI

Haydarov E.D., Murodov M., Janxojaev A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada ochiq kalitli kriptografiyaning tub sonlarga asoslangan matematik poydevori ko‘rib chiqiladi. Bir tomonli funksiya tushunchasi orqali ikki asosiy murakkablik oilasi – butun sonlarni faktorizatsiya qilish va diskret logarifmni hisoblash – tavsiflanadi. RSA va Diffie–Hellman tizimlarining tuzilishi sonli misol bilan ko‘rsatiladi, faktorizatsiya algoritmlarining murakkabligi taqqoslanadi. So‘nggi yillardagi faktorizatsiya rekordlari asosida 2048 bitli modullar minimal talab sifatida belgilanishi asoslanadi.

Kalit so‘zlar: ochiq kalitli kriptografiya, tub son, bir tomonli funksiya, faktorizatsiya, diskret logarifm, RSA, Diffie–Hellman, kalit uzunligi.

Аннотация. В статье рассматривается математический фундамент криптографии с открытым ключом, основанный на простых числах. Через понятие односторонней функции описываются два основных семейства вычислительно сложных задач – факторизация целых чисел и вычисление дискретного логарифма. Устройство систем RSA и Диффи–Хеллмана показано на числовом примере, сравнивается сложность алгоритмов факторизации. На основе рекордов факторизации последних лет обосновывается выбор модулей длиной 2048 бит в качестве минимального требования.

Ключевые слова: криптография с открытым ключом, простое число, односторонняя функция, факторизация, дискретный логарифм, RSA, Диффи–Хеллман, длина ключа.

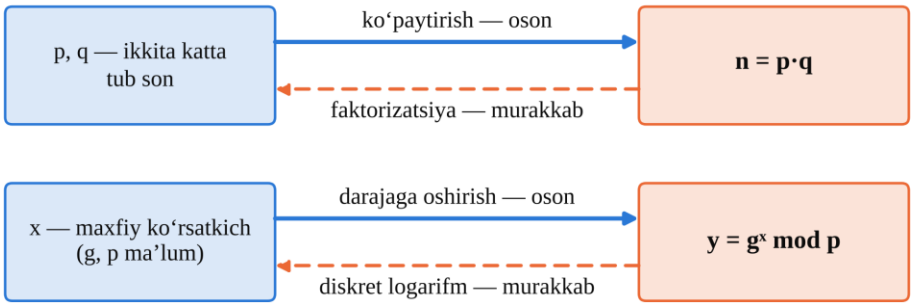
Kirish

Simmetrik kriptografiyada jo‘natuvchi va qabul qiluvchi bitta maxfiy kalitdan foydalanadi, bu esa kalitni xavfsiz uzatish muammosini keltirib chiqaradi: n ta foydalanuvchili tarmoqda har bir juftlik uchun alohida kalit zarur bo‘lsa, kalitlar soni $n(n-1)/2$ ga yetadi. 1976-yilda U. Diffi va M. Xellman taklif etgan ochiq kalitli kriptografiya bu muammoni hal qildi: foydalanuvchi ochiq tarqatiladigan ochiq kalitga va maxfiy saqlanadigan yopiq kalitga ega bo‘ladi. Ochiq kalitli kriptografiya uchta vazifani bajaradi – kalitlarni ochiq kanal orqali kelishib olish, ma’lumotni faqat qabul qiluvchi ocha oladigan tarzda shifrlash va raqamli imzo orqali muallifni tasdiqlash. Bu mexanizmlar bugungi kunda TLS protokoli, elektron hujjat aylanishi, bank to‘lov tizimlari va davlat elektron xizmatlarining kriptografik asosini tashkil etadi [1]. Ularning barchasi katta tub sonlar bilan bog‘liq ikki matematik masalaning murakkabligiga tayanadi. Ushbu ishda shu masalalar va ulardan kelib chiqadigan kalit uzunligi talablari ko‘rib chiqiladi.

Asosiy qism

Zamonaviy kriptografiyaning markaziy g‘oyalaridan biri – bir tomonli funksiya: uning qiymatini hisoblash oson (polinomial vaqtda), biroq $y = f(x)$ bo‘yicha x ni topish hisoblash jihatidan amaliy imkonsiz [2]. Kriptografiya uchun yashirin eshikli bir tomonli funksiyalar alohida qiymatga ega: ularni teskari aylantirish umumiy holda imkonsiz, ammo maxfiy qo‘shimcha ma’lumot ma’lum bo‘lsa, oson bajariladi. Tub sonlar bunday funksiyalarga ikkita tabiiy nomzodni beradi (1-rasm): ikkita katta tub sonni ko‘paytirish oson, ko‘paytmani qayta ko‘paytuvchilarga

ajratish esa murakkab; tub modul bo‘yicha darajaga oshirish oson, ko‘rsatkichni tiklash esa murakkab.



1-rasm. Tub sonlarga asoslangan ikkita bir tomonli amal

RSA kriptotizimi birinchi nomutanosiblikka tayanadi [3]. Kalitlarni generatsiya qilish ikkita katta va turli p, q tub sonni tanlashdan boshlanadi; ularning ko‘paytmasi $n = pq$ RSA moduli bo‘ladi. Eyler funksiyasi $\varphi(n) = (p-1)(q-1)$ hisoblanadi, ochiq ko‘rsatkich e uchun $\gcd(e, \varphi(n)) = 1$ sharti, yopiq ko‘rsatkich d uchun esa $ed \equiv 1 \pmod{\varphi(n)}$ tengligi bajariladi. Ochiq kalit (n, e) juftligidan iborat. Shifrlash va deshifrlash quyidagicha amalga oshiriladi:

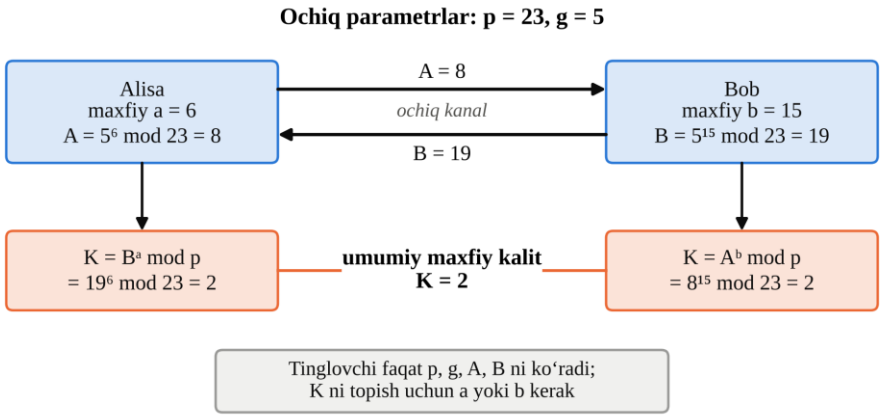
$$c = m^e \bmod n, \qquad m = c^d \bmod n.$$

Bu funksiyaning bir tomonliligi faqat p va q to‘g‘ri tanlanganda saqlanadi. Agar ular bir-biriga juda yaqin bo‘lsa, n Ferma usuli bilan oson faktorizatsiya qilinadi; agar $p-1$ faqat kichik tub bo‘luvchilarga ega bo‘lsa, Pollardning $p-1$ usuli samarali ishlaydi; tub sonlar sifatsiz tasodifiy generator bilan hosil qilingan bo‘lsa, turli modullar umumiy ko‘paytuvchiga ega bo‘lib qolishi mumkin [4]. Xavfsizlik haqida ham ehtiyotkorlik bilan gapirish kerak: faktorizatsiya ma’lum bo‘lsa, RSA albatta buziladi, teskari yo‘nalish esa umumiy holda isbotlanmagan [5].

Ikkinchi nomutanosiblikka Diffie–Hellman va ElGamal turidagi tizimlar tayanadi [6]. Yetarlicha katta p tub son uchun $\mathbb{Z}_p^*$ multiplikativ guruhida generator g tanlanadi. Alisa tasodifiy a ni tanlab $A = g^a \bmod p$ ni, Bob esa tasodifiy b ni tanlab $B = g^b \bmod p$ ni ochiq kanal orqali yuboradi, so‘ng ikkalasi umumiy kalitni hisoblaydi:

$$K = B^a \bmod p = A^b \bmod p = g^{ab} \bmod p.$$

Masalan, $p = 23$, $g = 5$, $a = 6$, $b = 15$ bo‘lsa, $A = 8$, $B = 19$ va umumiy kalit $K = 2$ bo‘ladi (2-rasm). Tinglovchi faqat p, g, A va B ni ko‘radi; $g^a \bmod p$ qiymatidan a ni tiklash esa diskret logarifm muammosidir. Xuddi shu tamoyil asosida DSA raqamli imzo algoritmi va milliy O‘z DSt 1092:2009 standartidagi elektron raqamli imzo algoritmlari qurilgan [7].



2-rasm. Diffie–Hellman kalit almashinuvining sonli misoli

Faktorizatsiya algoritmlarining rivoji kalit uzunligiga qo‘yiladigan talablarni bevosita belgilab kelgan. Eng oddiy usul – $\sqrt{n}$ gacha bo‘lgan sonlarga bo‘lib ko‘rish – eksponensial murakkablikka ega. RSA uchun eng xavfli algoritmlar subeksponensial murakkablikdagi kvadratik g‘alvir va sonli maydonning umumiy g‘alviri (GNFS) hisoblanadi [8, 9]. Ularning murakkabligi quyidagi belgilash orqali ifodalanadi:

$$L_n[\alpha, c] = \exp((c + o(1))\cdot(\ln n)^{\alpha}\cdot(\ln \ln n)^{1-\alpha}),$$

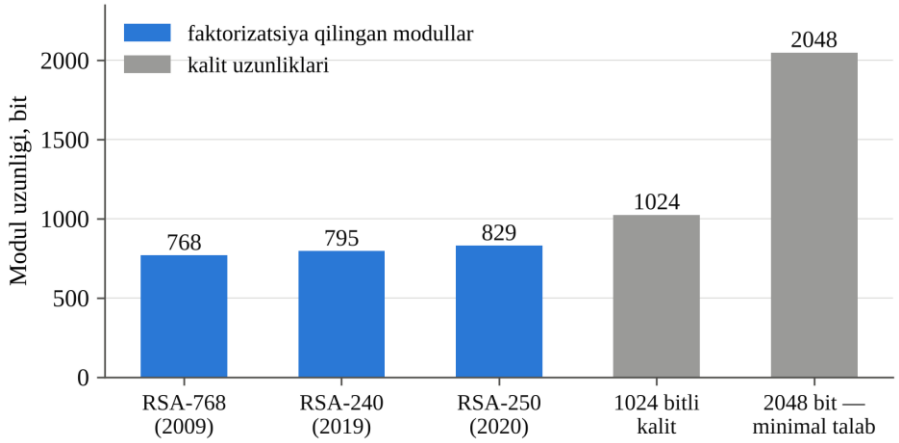
bunda $\alpha = 0$ polinomial, $\alpha = 1$ esa eksponensial murakkablikka mos keladi. Asosiy usullar 1-jadvalda taqqoslangan.

1-jadval

Butun sonlarni faktorizatsiya qilish algoritmlarining murakkabligi

Algoritm	Murakkablik	Qo‘llanish sohasi
Sinov bo‘lish	$O(\sqrt{n})$	Kichik sonlar, nomzodlarni saralash
Pollardning ρ-usuli	$O(\sqrt{p})$	Kichik bo‘luvchilarni topish
Pollardning $p-1$ usuli	$p-1$ ning eng katta tub bo‘luvchisiga bog‘liq	$p-1$ «silliq» bo‘lgan hollar
Elliptik egri chiziqlar usuli (ECM)	$Lp[1/2, \sqrt{2}]$	80 o‘nlik raqamgacha bo‘luvchilar
Kvadratik g‘alvir (QS)	$Ln[1/2, 1]$	100 o‘nlik raqamgacha bo‘lgan sonlar
Sonli maydonning umumiy g‘alviri (GNFS)	$Ln[1/3, \sqrt[3]{(64/9)}] \approx Ln[1/3; 1{,}923]$	RSA modullari, rekord hisoblashlar
Shor kvant algoritmi	log n ga nisbatan polinomial	Katta masshtabli kvant kompyuter talab etiladi

GNFS yordamida erishilgan natijalar bu talablarning qanday o‘zgarganini ko‘rsatadi (3-rasm). 2009-yilda 768 bitli RSA-768 moduli faktorizatsiya qilindi; bu ish bir yadroli protsessorda taxminan ikki ming yilga teng hisoblashni talab qildi. 2019–2020-yillarda 795 bitli RSA-240 va 829 bitli RSA-250 modullari faktorizatsiya qilindi, 795 bitli tub modul bo‘yicha diskret logarifm masalasi ham yechildi. Bu natijalar 1024 bitli kalitlar endi yetarli emasligini tasdiqlaydi va standartlarda 2048 bitni minimal talab sifatida belgilashga asos bo‘ladi [10].



3-rasm. Faktorizatsiya qilingan RSA modullari va kalit uzunligiga talablar

Diskret logarifm muammosi (DLP) g element generatsiya qiladigan n tartibli siklik guruhda g va $y = g^x$ ma’lum bo‘lganda x ni aniqlashdan iborat. Ixtiyoriy guruhda ishlaydigan umumiy algoritmlar – Shenksning «kichik qadam – katta qadam» usuli va Pollardning ρ-usuli –

taxminan $O(\sqrt{n})$ guruh amalini talab qiladi. Poling–Xellman algoritmi masalani guruh tartibining har bir tub bo‘luvchisi bo‘yicha alohida yechadi, shuning uchun DLP murakkabligi n ning o‘zi bilan emas, balki uning eng katta tub bo‘luvchisi bilan belgilanadi [11]; kriptografik guruhlar tartibi katta tub son bo‘ladigan qilib tanlanadi. $\mathbb{Z}_p^*$ guruhi uchun esa murakkabligi GNFS bilan bir xil $L_p[1/3]$ tartibli usullar mavjud, shu sababli chekli maydondagi Diffie–Hellman uchun ham kamida 2048 bitli tub modullar talab qilinadi [12]. Buning amaliy ahamiyati 2015-yilda aniqlangan Logjam hujumida namoyon bo‘ldi: ko‘plab serverlar bir xil standart 512 bitli tub sonlardan foydalangani sababli, hujumchi bitta tub son uchun og‘ir dastlabki hisoblashni bir marta bajarib, alohida ulanishlardagi diskret logarifmlarni tez topa olgan [13].

Xulosa

Klassik ochiq kalitli kriptografiya sonlar nazariyasiga asoslangan ikki murakkablik oilasiga tayanadi: $(p, q) \to pq$ ko‘paytirish oson, faktorizatsiya murakkab; $x \to g^x \bmod p$ darajaga oshirish oson, diskret logarifm murakkab. Har ikki holda xavfsizlik tub sonlarning to‘g‘ri tanlanishiga bog‘liq: ko‘paytuvchilar bir-biriga yaqin bo‘lmasligi, guruh tartibi katta tub bo‘luvchiga ega bo‘lishi, bir xil standart tub sonlardan ommaviy foydalanilmasligi kerak. Faktorizatsiya rekordlari 829 bitga yetgani sababli hozirgi kunda kamida 2048 bitli modullar qo‘llanishi lozim. Ikkala masala ham kvant kompyuterda Shor algoritmi yordamida polinomial vaqtda yechiladi, shuning uchun bu talablar klassik hisoblash modeliga tegishli.

Foydalanilgan adabiyotlar

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – Boca Raton: CRC Press, 1996. – 780 p.

2. Katz J., Lindell Y. Introduction to Modern Cryptography. – 3rd ed. – Boca Raton: CRC Press, 2020. – 626 p.

3. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. – 1978. – Vol. 21, № 2. – P. 120–126.

4. Heninger N., Durumeric Z., Wustrow E., Halderman J.A. Mining your Ps and Qs: detection of widespread weak keys in network devices // Proceedings of the 21st USENIX Security Symposium. – Bellevue, 2012. – P. 205–220.

5. Boneh D. Twenty years of attacks on the RSA cryptosystem // Notices of the American Mathematical Society. – 1999. – Vol. 46, № 2. – P. 203–213.

6. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. – 1985. – Vol. 31, № 4. – P. 469–472.

7. O‘z DSt 1092:2009. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari. – Toshkent: «O‘zstandart» agentligi, 2009.

8. Pollard J.M. A Monte Carlo method for factorization // BIT Numerical Mathematics. – 1975. – Vol. 15, № 3. – P. 331–334.

9. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие. – Казань: Казанский университет, 2011. – 190 с.

10. Barker E. NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General. – Gaithersburg: National Institute of Standards and Technology, 2020. – DOI: 10.6028/NIST.SP.800-57pt1r5.

11. Pohlig S.C., Hellman M.E. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance // IEEE Transactions on Information Theory. – 1978. – Vol. 24, № 1. – P. 106–110.

12. Gillmor D. RFC 7919. Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS). – Internet Engineering Task Force, 2016.

13. Adrian D., Bhargavan K., Durumeric Z. et al. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice // Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS ’15). – Denver, 2015. – P. 5–17.

GRAIN V1 OQIMLI SIMMETRIK SHIFRLASH ALGORITMINING TUZILISHI, ISHLASH PRINSIPI VA KRIPTOGRAFIK XUSUSIYATLARI TAHLILI

Xudoykulov Z.T., Jabbarov N.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Mazkur tezisda Grain v1 oqimli simmetrik shifrlash algoritmining tuzilishi, kalit oqimini hosil qilish tartibi va kriptografik xususiyatlari tahlil qilinadi. Tadqiqotning maqsadi resurslari cheklangan qurilmalarga mo‘ljallangan mazkur konstruksiyada apparat soddaligi bilan xavfsizlik talablari o‘rtasidagi bog‘liqlikni aniqlashdan iborat. Tahlilda spetsifikatsiyalarni qiyoslash, Bul funksiyalarining algebraik tuzilishini o‘rganish, hujum modellarini farqlash va nashr etilgan apparat ko‘rsatkichlarini solishtirish usullari qo‘llanadi. Algoritmning 80 bitli chiziqli hamda chiziqsiz registrlari, besh o‘zgaruvchili filtrlash funksiyasi va 160 taktli dastlabki sozlash jarayoni izohlanadi. To‘liq qidirish, korrelyatsion, algebraik, vaqt-xotira-ma’lumotlar almashinuvi, tanlangan boshlang‘ich vektor va xatolik kiritish hujumlari tegishli shartlar doirasida baholanadi.

Kalit so‘zlar: Grain v1, oqimli shifr, LFSR, NFSR, kalit oqimi, kriptotahlil, apparat samaradorligi.

Аннотация. В тезисе анализируются структура алгоритма потокового симметричного шифрования Grain v1, порядок формирования ключевого потока и криптографические свойства. Цель исследования заключается в определении взаимосвязи между аппаратной простотой и требованиями безопасности алгоритма, предназначенного для устройств с ограниченными ресурсами. Применяются методы сопоставления спецификаций, анализа алгебраической структуры булевых функций, разграничения моделей атак и сравнения опубликованных аппаратных показателей. Рассматриваются линейный и нелинейный регистры сдвига длиной 80 бит, фильтрующая функция пяти переменных и инициализация продолжительностью 160 тактов. Оцениваются полный перебор ключа, корреляционный и алгебраический криптоанализ, атаки на основе компромисса между временем, памятью и данными, выбранных векторов инициализации и внесения ошибок.

Ключевые слова: Grain v1, потоковый шифр, LFSR, NFSR, ключевой поток, криптоанализ, аппаратная эффективность.

Kirish

Grain oilasi xotira va mantiqiy sxema maydoni cheklangan qurilmalar uchun yaratilgan. Sinxron oqimli shifrlashda kalit oqimining ochiq matndan mustaqilligi ixcham yadroni amalga oshirishga imkon beradi [1]. Grain v1 eSTREAMning apparat portfeliga kiritilgan [2].

Grain v0 dagi chiziqli yaqinlashuvlarga tayangan hujumdan so‘ng v1 chiqish funksiyasi va NFSR teskari aloqasi o‘zgartirilgan [1, 3]. Tadqiqot registr tenglamalari, sozlash tartibi, hujum shartlari va apparat resurslari bilan tezlik nisbatini tahlil qiladi.

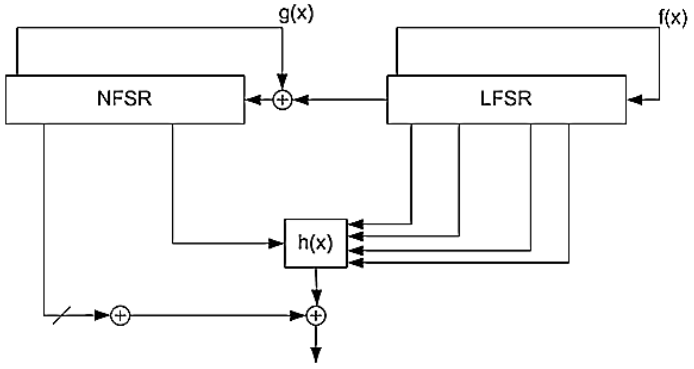
Asosiy qism. Algoritm chiziqli teskari aloqa siljitish registri - LFSR (Linear Feedback Shift Register), chiziqsiz teskari aloqa siljitish registri - NFSR (Nonlinear Feedback Shift Register) va chiqish blokidan iborat. Boshlang‘ich vektor - IV (Initialization Vector) ochiq parametr bo‘lib, maxfiy kalitni almashtirmaydi [1, 4].

1-jadval.

Grain v1 ning asosiy parametrlari

Parametr	Qiymat
Maxfiy kalit / IV uzunligi	80 bit / 64 bit
LFSR / NFSR uzunligi	80 bit / 80 bit
Ichki holat hajmi	160 bit
Dastlabki sozlash	160 mantiqiy takt
Bazaviy chiqish tezligi	1 bit/takt

LFSR biti NFSRning yangi bitiga XOR qilinadi. h blokiga to‘rtta LFSR va bitta NFSR biti kiradi. Natija yettita NFSR biti bilan birlashtiriladi [4].



1-rasm. Grain v1 arxitekturasi

Barcha amallar GF(2) maydonida bajariladi. $\oplus$ belgisi XORni, yonma-yon yozilgan bitlar ko‘paytmasi ANDni bildiradi. LFSRning primitiv teskari aloqa ko‘phadi va unga mos rekurrent tenglama quyidagicha [1, 4]:

$$f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80} \quad (1)$$

$$s_{i+80} = s_i \oplus s_{i+13} \oplus s_{i+23} \oplus s_{i+38} \oplus s_{i+51} \oplus s_{i+62} \quad (2)$$

i-taktda LFSR holati ketma-ket 80 ta s bitidan, NFSR holati 80 ta b bitidan tashkil topadi. (2) tenglamadagi oltita pozitsiya yangi LFSR bitini belgilaydi. Takt yakunida birinchi bit chiqarilib, yangi bit registr oxiriga kiritiladi. NFSRning to‘liq yangilanishi quyidagicha ifodalanadi [1, 4]:

$$b_{i+80} = s_i + b_{i+62} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + b_{i+21} + b_{i+14} + b_{i+9} + b_i + b_{i+63}b_{i+60} + b_{i+37}b_{i+33} + b_{i+15}b_{i+9} + b_{i+60}b_{i+52}b_{i+45} + b_{i+33}b_{i+28}b_{i+21} + b_{i+63}b_{i+45}b_{i+28}b_{i+9} + b_{i+60}b_{i+52}b_{i+37}b_{i+33} + b_{i+63}b_{i+60}b_{i+21}b_{i+15} + b_{i+63}b_{i+60}b_{i+52}b_{i+45}b_{i+37} + b_{i+33}b_{i+28}b_{i+21}b_{i+15}b_{i+9} + b_{i+52}b_{i+45}b_{i+37}b_{i+33}b_{i+28}b_{i+21} \quad (3)$$

(3) tenglamada NFSRning 11 ta chiziqli biti, LFSRning bitta biti va darajasi 2-6 bo‘lgan 11 ta chiziqsiz had qatnashadi. LFSR bilan bog‘lanish NFSRni avtonom registr sifatida tahlil qilishni cheklaydi. Chiziqsiz hadlar keyingi holatlarni boshlang‘ich bitlar orqali ifodalashdagi algebraik murakkablikni oshiradi.

Besh o‘zgaruvchili Bul (Boolean) filtrlash funksiyasi [4]:

$$h(x_0, x_1, x_2, x_3, x_4) == x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4 \quad (4)$$

Kirishlar mos ravishda LFSRning 3, 25, 46, 64-pozitsiyalari va NFSRning 63-pozitsiyasidan olinadi. h funksiyasining algebraik darajasi 3, nochiziqliligi 12; u muvozanatlangan va birinchi tartibli korrelyatsiyaga immun [4]. Chiqish tenglamasi esa:

$$z_i = b_{i+1} \oplus b_{i+2} \oplus b_{i+4} \oplus b_{i+10} \oplus b_{i+31} \oplus b_{i+43} \oplus b_{i+56} \oplus h(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63}) \quad (5)$$

Avtonom LFSR noldan farqli holatda $2^{80} - 1$ davrli ketma-ketlik hosil qiladi. Bu qiymat butun kalit oqimining aniq davrini belgilamaydi; chiqish xususiyatlari NFSR va h funksiyasiga ham bog‘liq [1].

Kalit bitlari NFSRga yuklanadi. IV LFSRning dastlabki 64 pozitsiyasiga joylashtiriladi, qolgan 16 pozitsiya birlar bilan to‘ldiriladi [1, 4]:

$$\begin{aligned} b_j &= k_j, && 0 \le j \le 79, \\ s_j &= IV_j, && 0 \le j \le 63, \\ s_j &= 1, && 64 \le j \le 79. \end{aligned} \quad (6)$$

Bu yuklash LFSRning boshlang‘ich holatini noldan farqli qiladi. So‘ng 160 takt davomida (5) orqali hisoblangan chiqish tashqariga uzatilmaydi. U ikkala registrning yangi bitiga qayta qo‘shiladi:

$$\begin{aligned} s_{i+80} &= F(S_i) \oplus z_i, \\ b_{i+80} &= s_i \oplus G(B_i) \oplus z_i, \qquad 0 \le i < 160. \end{aligned} \quad (7)$$

Bu yerda F - (2) ning o‘ng tomoni, G - (3) dagi barcha NFSR hadlari, S va B tegishli registr holatlarini bildiradi. Ikkala yangi bit bir xil eski holatdan hisoblanadi. Registrlardan birini oldin yangilab, uning yangi bitidan ikkinchisi uchun foydalanish spetsifikatsiyaga mos kelmaydi.

160-takt yakunida chiqishning teskari kiritilishi uziladi. Birinchi foydali kalit oqimi biti navbatdagi holatdan olinadi. Yuklashdan boshlangan indekslash saqlansa, bu z_{160} bitidir, shifrlashda oqim qayta indekslanib Z_0 deb belgilanadi. Keyingi har bir taktda (2), (3) va (5) bajariladi [4].

$$C_j = P_j \oplus Z_j, \qquad P_j = C_j \oplus Z_j \quad (8)$$

(8) dagi P, C va Z mos ravishda ochiq matn, shifrmatn va kalit oqimi bitlaridir. Bir xil kalit va IVni qayta ishlatish bir xil oqimni beradi. Grain v1 ning XOR shifrlashi xabar yaxlitligini mustaqil tekshirmaydi, chunki shifrmatn bitidagi o‘zgarish ochiq matnning ayni bitini o‘zgartiradi.

To‘liq qidirish 80 bitli kalit fazosini tekshiradi: eng yomon holatda 2^{80}, o‘rtacha taxminan 2^{79} nomzod sinovdan o‘tadi. Bu loyihalash mezoni bo‘lib, barcha maxsus hujumlar uchun isbotlangan quyi chegara emas [1].

Korrelyatsion hujum kalit oqimi va LFSR bitlarining chiziqli kombinatsiyalari orasidagi statistik og‘ishni izlaydi. v1 dagi yettita NFSR chiqish hadi v0 uchun ishlatilgan yaqinlashuvni o‘zgartiradi [1, 3]. Biroq Todo va hammualliflar to‘liq Grain v1 ga ko‘p chiziqli yaqinlashuv asosidagi korrelyatsion kriptotahlilni qo‘llagan [5]. h ning birinchi tartibli immunligi umumiy xavfsizlik isboti hisoblanmaydi.

Algebraik hujum chiqish va holat yangilanishini ko‘p o‘zgaruvchili tenglamalar tizimiga aylantiradi. NFSRning oltinchi darajagacha bo‘lgan hadlari va 160 taktli aralashtirish kalit orqali ifodalashni qiyinlashtiradi. Mualliflarning dastlabki “samarasiz” bahosi algebraik usullarni mutlaq istisno etmaydi. Manbada to‘liq v1 uchun amaliy algebraik kalit tiklash tajribasi keltirilmagan [1].

Vaqt–xotira–ma’lumotlar almashinuvi - TMDTO (Time-Memory-Data Trade-Off) hujumi oldindan tuzilgan jadvallar orqali oqimdan ichki holatni qidiradi. Manbadagi 2^{80} tartibli baho umumiy modelga tegishli [1]. Keyingi ishda holatni qisman taxmin qilish va filtrlash funksiyasini

chiziqlashtiruvchi shartli namunalar TMDTO bilan birlashtirilgan [6]. Onlayn vaqt, xotira, oqim hajmi va tayyorlash xarajati birgalikda baholanishi zarur.

Tanlangan IV hujumi bir kalit ostida maxsus IVlar hosil qilgan oqim farqlarini o‘rganadi. Qisqartirilgan sozlashdagi deterministik bog‘lanishlar to‘liq 160 taktli variantga avtomatik tatbiq etilmaydi [1]. Lee va hammualliflarning to‘liq v1 ga tegishli kalit tiklash natijasi bog‘liq kalitlar ham talab qiladigan modelga asoslangan: taxminan $2^{22.59}$ tanlangan IV, $2^{26.29}$ oqim biti va $2^{22.90}$ hisoblash xarajati [7]. Bu oddiy, yagona noma’lum kalitli hujum emas.

Xatolik kiritish hujumi buzilmagan va buzilgan oqimlarni solishtirib registr bitlarini tiklaydi. Banik va hammualliflar h funksiyasining ayrim differensiallari chiziqli bo‘lishidan foydalanib LFSR hamda NFSRni tiklash usulini ko‘rsatgan [8]. Keyingi modelda Grain v1 uchun kamida beshta xatolik yetarli ekani berilgan [9]. Natija qayta sozlash, xatolik modeli va kuzatiladigan oqimga bog‘liq. U masofadan turib bajariladigan oddiy hujumga tenglashtirilmaydi.

Grain v1 yadrosi 160 bitli holat xotirasi, XOR va AND tarmoqlaridan iborat. FPGA (Field-Programmable Gate Array - dasturlanuvchi mantiqiy matritsa) va CPLD (Complex Programmable Logic Device - murakkab dasturlanuvchi mantiqiy qurilma) realizatsiyalarida funksiyalar takrorlanib, t ta qadam bitta apparat taktida bajariladi [1].

2-jadval

Parallelizatsiya va apparat o‘tkazuvchanligi

t	GE	MAX 3000A Mbit/s	MAX II Mbit/s	Cyclone Mbit/s
1	1450	49	200	282
2	1637	98	422	576
4	2010	196	632	872
8	2756	-	1184	1736
16	4248	-	2128	3136

GE (Gate Equivalent) - NAND2 elementiga nisbatan ekvivalent baho; FPGAning fizik resurslari sonidan farqlanadi. Manbada D-trigger 8 GE, XOR2 esa 2,5 GE bilan baholangan. Chiziq ko‘rsatkich berilmaganini bildiradi. MAX 3000A EPM3256 realizatsiyasiga $t \leq 4$ holatlari joylashgan [1].

$$R = t \cdot f_{clk}, \qquad N_{init} = 160/t \tag{9}$$

(9) da R - bit/sdagi o‘tkazuvchanlik, f - chastota, N - sozlash taktlari. Jadval tartibida mos ravishda 160, 80, 40, 20, 10 apparat takti talab etiladi. Mantiqiy sozlash uzunligi 160 qadamligicha qoladi [1].

Cyclone platformasida t=1 dan t=16 ga o‘tilganda GE 1450 dan 4248 ga, o‘tkazuvchanlik 282 dan 3136 Mbit/s ga oshgan. Shu ma’lumotlardan hisoblangan o‘sish mos ravishda 2,93 va 11,12 martani tashkil etadi. Tezlikning 16 marta oshmasligi maksimal chastotaning 282 dan 196 MHz gacha kamayishi bilan izohlanadi [1].

Registrlarning 65-79-pozitsiyalari kirishlarda ishlatilmagani 16 qadamgacha yoyishni soddalashtiradi. Xotira oshmaydi. Natijalar tarixiy Altera qurilmalariga tegishli [1].

Xulosa

Grain v1 da ikkita 80 bitli registr, chiziqsiz teskari aloqa va ixcham filtrlash funksiyasi yagona kalit oqimi generatorini tashkil etadi. 160 taktli sozlash kalit va IVni ikkala registr holatiga tarqatadi. Registr uzunligi, tap indekslari va amallar tartibi realizatsiyaning spetsifikatsiyaga mosligini belgilaydi [1, 4].

Apparat natijalari qo‘shimcha mantiq hisobiga o‘tkazuvchanlikni oshirish mumkinligini ko‘rsatadi. Biroq ixchamlik, h funksiyasining xususiyatlari va dastlabki 80 bitli xavfsizlik maqsadi keyingi hujumlarni istisno etmaydi. Korrelyatsion, bog‘liq kalitli va xatolik kiritish natijalari tegishli shartlar bilan baholanishi zarur [5, 7-9]. Grain v1 resurslar va tezlik muvozanatini o‘rganish uchun ahamiyatli; qo‘llash imkoniyati kalit uzunligi, IVni boshqarish, yaxlitlik mexanizmi va realizatsiyaning fizik himoyasiga bog‘liq.

Foydalanilgan adabiyotlar:

1. Hell M., Johansson T., Meier W. Grain: a stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, 2007, 2(1), 86–93. https://doi.org/10.1504/IJWMC.2007.013798.

2. Hell M., Johansson T., Maximov A., Meier W. The Grain Family of Stream Ciphers. New Stream Cipher Designs: The eSTREAM Finalists. LNCS 4986, Springer, 2008, 179–190. https://doi.org/10.1007/978-3-540-68351-3_14.

3. Berbain C., Gilbert H., Maximov A. Cryptanalysis of Grain. FSE 2006, LNCS 4047, Springer, 2006, 15–29. https://doi.org/10.1007/11799313_2.

4. Hell M. On the Design and Analysis of Stream Ciphers. PhD dissertation. Lund University, 2007, §8.1.1, 129–130. https://lucris.lub.lu.se/ws/files/5980979/598772.pdf

5. Todo Y., Isobe T., Meier W., Aoki K., Zhang B. Fast Correlation Attack Revisited: Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1. CRYPTO 2018, LNCS 10992, Springer, 2018, 129–159. https://doi.org/10.1007/978-3-319-96881-0_5.

6. Mihaljević M. J., Sinha N., Gangopadhyay S., Maitra S., Paul G., Matsuura K. An Improved Cryptanalysis of Lightweight Stream Cipher Grain-v1. COST CRYPTACUS Workshop, Nijmegen, 16–18.11.2017.

7. Lee Y., Jeong K., Sung J., Hong S. Related-Key Chosen IV Attacks on Grain-v1 and Grain-128. ACISP 2008, LNCS 5107, Springer, 2008, 321–335. https://doi.org/10.1007/978-3-540-70500-0_24.

8. Banik S., Maitra S., Sarkar S. A Differential Fault Attack on the Grain Family of Stream Ciphers. CHES 2012, LNCS 7428, Springer, 2012, 122–139. https://doi.org/10.1007/978-3-642-33027-8_8.

9. Siddhanti A., Sarkar S., Maitra S., Chattopadhyay A. Differential Fault Attack on Grain v1, ACORN v3 and Lizard. SPACE 2017, LNCS 10662, Springer, 2017, 247–263. Mualliflar nusxasi: https://eprint.iacr.org/2017/678.

A COMPACT ARITHMETIC PARAMETERIZATION OF PRIMES: FROM 48 LINEAR FUNCTIONS TO A VERIFIED PERIOD-56 FORMULA

Abdullaev T.R., Juraev G.U.
National University of Uzbekistan named after Mirzo Ulugbek

Annotatsiya. Kriptografik maqsadlarda tasodifiy tub son hosil qilish ikkita mustaqil vazifaga bo‘linadi: nomzodni taklif qilish va uni tekshirish. Li va boshqalar (2024) aniqlagan 210 moduli bo‘yicha 48 ta arifmetik progressiyadan, ya’ni klassik Wheel-210 dan boshlab, biz barcha 48 ta foydali qoldiq sinfini tiklaydigan yagona yopiq ko‘rinishdagi, jadvalsiz arifmetik ifodani qurdik. U Eylerning n^2+n+41 ko‘phadidan olingan ixcham 14 qiymatli konstruksiyani davr 56 bo‘lgan formulagacha kengaytiradi va bu formula har bir $p \geq 11$ tub songa isbotlangan tarzda erishadi. Biz bu qamrovni teorema sifatida isbotlaymiz, formulani bo‘luvchilarga ajratish usulida (trial division) qo‘llashdagi nozik to‘g‘rilik tuzog‘ini hujjatlashtiramiz hamda barcha usullarni kompilyatsiya qilingan C++ kodida (g++ -O3) sinovdan o‘tkazamiz, bunda nomzodlarni generatsiya qilish va tub sonni boshidan oxirigacha hosil qilish jarayonlari alohida o‘lchanadi. Miller–Rabin bilan juftlikda nomzod generatori sifatida formula va Wheel-210 statistik jihatdan farq qilmasligi ma’lum bo‘ldi. Formulaning haqiqiy afzalligi shundaki, taxminan 20 bitdan past oraliqda u bo‘luvchilarga ajratish usulidagi tekshiruvchi sifatida Miller–Rabin’dan o‘zib ketadi, bundan tashqari, saqlanadigan qoldiqlar jadvaliga ehtiyoj yo‘qoladi.

Kalit so‘zlar: tub sonlarni generatsiya qilish, g‘ildirakli g‘alvir (wheel sieve), Miller–Rabin testi, o‘rnatilgan (embedded) tizimlar, arifmetik formula, Bateman–Horn gipotezasi.

Аннотация. Получение случайного простого числа для криптографических целей разделяется на две независимые задачи: предложение кандидата и его проверка. Отталкиваясь от 48 арифметических прогрессий по модулю 210, выделенных Li и соавторами (2024), то есть от классического Wheel-210, мы строим единое замкнутое арифметическое выражение без таблиц, которое воспроизводит все 48 полезных классов вычетов. Развивая компактную конструкцию из 14 значений, выведенную из полинома Эйлера n^2+n+41, до формулы с периодом 56, которая доказуемо достигает каждого простого $p \geq 11$. Мы доказываем это покрытие как теорему, описываем тонкую ловушку корректности при использовании формулы для пробного деления и тестируем все методы в скомпилированном C++ (g++ -O3), разделяя генерацию кандидатов и сквозную генерацию простых чисел. Оказалось, что формула и Wheel-210 статистически неразличимы в роли генераторов кандидатов в паре с тестом Миллера–Рабина. Реальное преимущество формулы состоит в настоящей точке пересечения ниже примерно 20 бит, где она обгоняет Миллера–Рабина как тестер на основе пробного деления, а также в отсутствии хранимой таблицы вычетов.

Ключевые слова: генерация простых чисел, колёсное решето (wheel sieve), тест Миллера–Рабина, встраиваемые системы, арифметическая формула, гипотеза Бейтмана–Хорна.

Introduction

Public-key cryptosystems - RSA, Diffie–Hellman, DSA/ECDSA, and several post-quantum schemes - depend on producing large random primes quickly. The task splits cleanly into two jobs: proposing a candidate integer, and deciding whether it is prime. Conflating the two, or

benchmarking one while believing one is measuring the other, was the main source of the erroneous conclusions this line of work drew and later retracted.

Li et al. (2024) observed that every prime greater than 7 falls into one of 48 arithmetic progressions $r_i + 210k$, since $210 = 2 \cdot 3 \cdot 5 \cdot 7$ is the fourth primorial. Restricting candidate generation to these 48 classes ("Wheel-210") improves candidate density by a factor of about 4.37 over random sampling, at the cost of a 48-entry lookup table. Separately, Euler's polynomial n^2+n+41 is known to give 40 consecutive primes. This paper combines the two ideas into a single closed-form expression - no branching, no stored table - that reproduces the wheel's 48 useful residues plus eight extra multiples of 7 per period of 56, and subjects the result to a rigorous coverage proof and an honest compiled-code benchmark.

From 48 Residue Classes to a Period-56 Formula

Every prime $p \geq 11$ is coprime to 2, 3, 5 and 7, so its residue mod 210 is one of exactly 48 values - e.g. 1, 11, 13, 17, 19, 23, ..., 209. Each residue r_i defines a linear generator $f_i(n) = 210n + r_i$. Rather than keep 48 separate generators, the first fourteen values of Euler's polynomial $E(k) = k^2+k+41$ ($k = 0,...,13$, reversed) are folded into one periodic expression:

$$f_{14}(n) = 210 \cdot \lfloor n/14 \rfloor + (n \bmod 14)^2 - 27(n \bmod 14) + 223.$$

This f_{14} covers only the 14 densest residues and discards the other 34. Extending the period to 56 (48 useful residues plus 8 unavoidable multiples of 7) gives complete coverage:

$$f(n) = 210 \cdot \lfloor n/56 \rfloor + 11 + 2(\lfloor (n \bmod 56)/14 \rfloor \bmod 2) + 6\lfloor (n \bmod 56)/28 \rfloor + 30\lfloor (n \bmod 14)/2 \rfloor + 10(n \bmod 2) \cdot (2 - (\lfloor (n \bmod 56)/14 \rfloor \bmod 2)).$$

Theorem. For every prime $p \geq 11$ there exists $n \in \mathbb{N}$ such that $f(n) = p$.

Proof sketch. Consecutive blocks of 56 values of n map to disjoint, strictly increasing output ranges, and each block reproduces all 48 useful residues mod 210 exactly once. Hence every integer $210k + r$, for r one of the 48 residues and any $k \geq 0$, appears as $f(n)$ for some n; every prime $p \geq 11$ is of this form. ■

Within one block of 56, f is deliberately non-monotonic: it produces values ending in 1, 3, 7, 9 in four separate passes (a "four-toothed saw"), though the block maxima strictly increase across blocks.

A Correctness Pitfall: Periodic, Not Linear

Because f(n) is proven surjective onto the primes, it is tempting to use its own output f(1), f(2), ... directly as a trial-division divisor sequence, halting once the running divisor exceeds $\sqrt{X}$. This fails: since f is non-monotonic within a block, a large divisor can appear before a smaller true factor in the same block. Concretely, $169 = 13^2$ is misclassified as prime because the sequence reaches 211 (whose square already exceeds 169) at $n = 13$, before reaching the actual factor 13 at $n = 14$. Tested naively across ≈70,000 integers, this bug misclassified composites as prime in 12.4% of cases. The remedy is to finish testing every divisor within the current block of 56 before checking the stopping condition against the block's maximum; re-verification against sympy across the same 70,000 integers then showed zero discrepancies.

The essence of the objects compared in Section 4 ("Formula" and "Trial division") is the compact arithmetic candidate stream itself - no lookup table, just four starting offsets and an alternating step - together with a direct trial-division test of each proposed candidate p:

```
static const uint8_t a[4] = {11, 13, 17, 19};
uint64_t q = n / 30;
uint64_t r = n % 30;
uint64_t p = q * 30 + a[line];
```

```
uint64_t step = (r & 1) ? 10 : 20;
for (;;) {
        process(p);
        p += step;
        step = 30 - step;
}
```

"Formula" in Table 2 denotes this stream used to propose candidates, tested by trial division against the divisors it itself emits (with the block-respecting stopping rule of Section 3); "Miller–Rabin" denotes the same candidates tested with twelve fixed-base Miller–Rabin rounds instead. The comparison therefore isolates the cost of the primality-testing strategy, not the candidate source.

Benchmark and Results

All methods were implemented in compiled C++ (g++ -O3 -march=native); Python timings were discarded after they proved to measure interpreter overhead rather than real cost. Candidate-generation cost was measured separately from end-to-end prime generation, and generator benchmarks started from realistic bounds N rather than resetting to 11 each run.

End-to-end generation of one random prime (formula vs. Wheel-210, both with Miller–Rabin) is statistically indistinguishable across all tested bit widths (Table 1); an alternating hybrid of the two offers no additional benefit.

Table 1.

Median time to generate one random prime (Miller–Rabin, selected bit widths).

Bits	Formula + MR	Wheel-210 + MR
16	0.00302 ms	0.00300 ms
32	0.00643 ms	0.00638 ms
64	0.04333 ms	0.04227 ms
96	3.02 ms	2.79 ms

A genuine, complexity-driven crossover appears when the formula is used as its own trial-division tester against Miller–Rabin (Table 2): trial division costs $O(\sqrt{X})$, Miller–Rabin costs $O(\log^2 X)$, and the two cross between 19 and 20 bits (≈500,000). Below that, trial division wins by up to 2.4×; by 28 bits Miller–Rabin is already ≈10× faster.

Table 2.

Formula-as-trial-division vs. Miller–Rabin: crossover near 20 bits.

Bits	Trial division	Miller–Rabin	Faster
16	0.00177 ms	0.00301 ms	TD, 1.7×
19	0.00313 ms	0.00359 ms	TD, narrowly
20	0.00410 ms	0.00380 ms	MR
24	0.01563 ms	0.00548 ms	MR, 2.9×
28	0.05242 ms	0.00551 ms	MR, 9.5×

A separate table-free four-line generator (starting offsets 11, 13, 17, 19 mod 30, alternating +10/+20 step) was also tested: its four lines jointly cover all eight residues coprime to 30, so every prime > 5 is reachable. In isolation it advances a candidate substantially faster than a 48-byte Wheel-210 table (Table 3), using only 4 bytes of read-only data instead of 48. This does not translate into an end-to-end win, however: following only one line requires more Miller–Rabin calls than Wheel-210 to reach a prime, so across independent 32–64-bit trials the complete

generation time for both approaches remains within a few percent of each other, with neither consistently ahead.

Table 3.

Isolated candidate-generation speed and memory footprint, tested x86-64 platform.

Generator	Candidate cost	Read-only data	Relative speed
Wheel-210 (table)	≈0.89 ns/candidate	48 bytes	1.0×
Compact mod-30 (arithmetic)	≈0.36 ns/candidate	4 bytes	≈2.5×

The intermediate f_{14} stage deserves a note on originality: its quadratic part is exactly Euler's polynomial evaluated at $k = 13-t$, not an independently discovered dense sequence, and it should not be presented as beating Euler's or record-holding quadratics (e.g. $m^2-79m+1601$) on density at long range - quadratic growth erodes any near-origin density advantage as the index grows. The paper's originality claim rests specifically on the period-56 closed form and its coverage proof, not on f_{14}'s density in isolation.

Discussion and Recommendations

The paper separates several distinct questions. Mathematically, f(n) gives complete, table-free coverage of all primes ≥ 11 (proved, not merely observed). Practically, honest end-to-end benchmarking shows no candidate generator has a decisive speed advantage over Wheel-210 at cryptographic sizes; the formula's genuine wins are (a) trial division below ≈20 bits, relevant to 8/16-bit microcontrollers and smart cards, and (b) removing a stored residue table - 48 bytes at minimum, 192 bytes in the naive 32-bit representation - which matters on memory-constrained embedded targets more than on servers. We were unable to obtain a trustworthy 128-bit benchmark (our hand-written big-number arithmetic was both too slow and overflow-prone); extending this study to real cryptographic key sizes with a library such as GMP is the most immediate future work.

Conclusion

We constructed a single closed-form period-56 arithmetic expression, provably surjective onto all primes ≥ 11, requiring no stored lookup table; its intermediate f_{14} stage is exactly the first fourteen values of Euler's polynomial reversed and embedded modulo 210. Measured honestly in compiled code, it does not outperform Wheel-210 end-to-end at cryptographic sizes, but it does eliminate the residue table, provides a genuine trial-division speedup below ≈20 bits, and - in a related four-line variant - an arithmetic candidate stream that advances at sub-nanosecond cost.

References

1. Li, H.-L., Fang, S.-C., & Kuo, W. (2024). The Periodic Table of Primes. SSRN Preprint 4742238.

2. Euler, L. (1772). De numeris primis valde frequentibus. Commentationes arithmeticae collectae, 2, pp. 1–9.

3. Bateman, P. T., & Horn, R. A. (1962). A heuristic asymptotic formula concerning the distribution of prime numbers. Mathematics of Computation, 16(79), pp. 363–367.

4. Miller, G. L. (1976). Riemann's hypothesis and tests for primality. Journal of Computer and System Sciences, 13(3), pp. 300–317.

MA’LUMOT ALMASHINUVI TIZIMLARIDA SHIFRLANGAN PAKETLARNI UZATISH USULLARINI TAKOMILLASHTIRISH

Jurayev G.U.
Toshkent davlat iqtisodiyot universiteti
Anvarov Sh.S.
O‘zbekiston Respublikasi Mudofaa vazirligi

Annotatsiya. Maqolada ochiq kanal orqali uzatiladigan ma’lumot birligini shifrlangan paketga aylantirishning uchta qoidaga asoslan usuli bayon etiladi.

Kalit so‘zlar: shifrlangan paket, UDP datagrammasi, MTU 1400, boshlang‘ich vektor, CFB rejimi, kadr sig‘imi, juftlik raqami, butunlik belgisi.

Аннотация. В статье излагается метод преобразования единицы данных, передаваемого по открытому каналу, в зашифрованный пакет, основанный на трех правил.

Ключевые слова: шифрованный пакет, UDP-дейтаграмма, MTU 1400, вектор инициализации, режим CFB, ёмкость кадра, номер пары, признак целостности.

Kirish

Ma’lumot almashinish tizimida ochiq kanalga chiqadigan ma’lumot birligini yuborishdan oldin shifrlanadi. Qabul qiluvchi tomoni paketni ochib, dastlabki ma’lumot birligini tiklaydi. Bunday ma'lumotlar almashinuv tizimida ikkita cheklov birga bajariladi. Birinchisi kadr sig‘imi: oddiy kadrning foydali yuki 1500 baytdan oshmaydi [4]. Ikkinchisi shifrmatn bo‘yicha teskari aloqa (CFB) rejimida har bir shifrlangan paket o‘z boshlang‘ich vektorini o‘zi bilan olib yuradi [3].

Tarmoqda default IP paket 1500 baytdan oshmaydi. Shu paket oqimli rejimda shifrlanib, UDP datagrammasiga yuklanadi [1,2]. Agar tayyor datagramma 1500 baytlik kadrga sig‘masa, kanal uni o‘z qatlamida bo‘lib yuboradi. Bo‘linmalardan biri yo‘qolsa, butun shifrlangan paket yo‘qoladi [5, 6]. Maqolada shu muammoni hal qilishning uchta qoidaga asoslangan usuli taklif etiladi. Hisoblar o‘lchov natijasi emas: ular bayt tartibidagi yig‘indidir.

Asosiy qism

Ma’lumot birligini shifrlangan paketga aylantirish usuli quyidagi uchta qoidaga asoslanadi.

Birinchi qoida. Shifrlanadigan ochiq bo‘lakning uzunligi 1400 baytdan oshmaydi. Bu chegara tashqi qo‘shimchani oldindan hisobga oladi.

Ikkinchi qoida. IP paket uzunligi L 1400 baytdan katta va 1500 baytdan oshmasa, paket UDP ga yuklanishidan oldin ikkiga bo‘linadi: $L_1=(L+1)\text{div}2$ va $L_2=L\text{div}2$. Default to‘liq paketda L=1500, bo‘laklar 750 va 750 bayt. Har bir bo‘lak alohida UDP datagrammasi bo‘ladi.

Uchinchi qoida. Har bir paket, yaxlit yoki bo‘lak bo‘lishidan qat’iy nazar, 8 baytli yangi boshlang‘ich vektor oladi. Ushbu vektor ochiq sarlavhada turadi va faqat shu paketning registrini yoqadi. Juftlikdagi ikki datagrammaning vektorlari har xil bo‘ladi.

Paketning tuzilishi. Har bir shifrlangan paket uch qismdan iborat: 22 baytli ochiq sarlavha, uzunligi ochiq bo‘lakka teng shifrlangan yuk va 4 baytli butunlik belgisi. Tanlangan rejim to‘ldirish qo‘shmaydi, shuning uchun yuk uzunligi ochiq bo‘lak uzunligiga teng qoladi. UDP yuki L+26 bayt, tashqi uzunlik L+54 bayt.

Butunlik belgisi sarlavha (shu jumladan, vektor) va shifrlangan yuk ustidan hisoblanadi. Belgi mos kelmasa, paket ochilmaydi.

1-jadval

Almashuv sarlavhasining maydonlari

Maydon	Uzunlik	Vazifasi
Versiya	1 bayt	Usulning shu ko‘rinishi
Tur	1 bayt	Butun paket / 1-bo‘lak / 2-bo‘lak
Ketma-ketlik	4 bayt	Har bir datagrammada oshadi
Kalit identifikatori	4 bayt	Qaysi kalit bilan ochish
Juftlik raqami	4 bayt	Ikki bo‘lakni bog‘laydi
Boshlang‘ich vektor	8 bayt	Registrning boshlang‘ich holati

1400 baytlik chegara va UDP yuklash. Tashqi paket quyidagi yig‘indadan hosil bo‘ladi. Ochiq IP paket L bayt. Unga 22 bayt sarlavha va 4 bayt butunlik belgisi qo‘shiladi. UDP sarlavhasi 8 bayt, tanlovlarsiz IP sarlavhasi 20 bayt [1,2]. Demak,

$$L+22+4+8+20 = L+54.$$

L=1400 bayt bo‘lganda tashqi uzunlik 1454 bayt. Kadr sig‘imi 1500 bayt. Farq 46 bayt zaxira. Shu zaxira bilan chegara 1500−100=1400 ko‘rinishida yoziladi, chunki 100=54+46.

L=1500 bo‘lgan default paket bitta UDP datagrammaga yuklansa, tashqi uzunlik 1554 bayt bo‘ladi va kadrdan chiqadi. Usul uni 750 va 750 baytlik ikkita datagrammaga ajratadi. Har birining tashqi uzunligi 804 bayt. Ikkalasi ham kadrga sig‘adi.

2-jadval

Default paketni UDP ga yuklashdagi tashqi uzunlik

L, bayt	UDP soni	Yuklar	Tashqi uzunlik	Kadrga
1400	1	1400	1454	sig‘adi
1500 (bitta)	1	1500	1554	chiqadi
1500 (ikki)	2	750 / 750	804 / 804	sig‘adi

46 baytlik zaxira qisqa qo‘shimcha yorliq yoki qisqa o‘rash qo‘shilganda ham tashqi paketni 1500 bayt ichida saqlash uchun qoldiriladi.

Boshlang‘ich vektor va qabul tartibi. Shifrlash 64 bitli blokli shifrning shifrmatn bo‘yicha teskari aloqa rejimida bajariladi [3,7]. Registr 8 bayt. Shifrlash boshlanganda registrga shu paketning vektori yoziladi. Shifrlangan yukning uzunligi ochiq bo‘lak uzunligiga teng qoladi. Vektor maxfiy emas: u sarlavhada ochiq turadi. Uning vazifasi bir xil kalit ostida ham har bir paketda registrni boshqa nuqtadan boshlashdir. Bir xil kalit va bir xil vektor takrorlansa, birinchi kalit oqimi bloki ham takrorlanadi [8].

Qabul tomoni avval butunlik belgisini tekshiradi. Moslik bo‘lmasa, paket ochilmaydi. Moslik bo‘lsa, sarlavhadan kalit identifikatori va 8 baytli vektor o‘qiladi, yuk shu juftlik bilan ochiladi. Tur butun paket bo‘lsa, ochiq yuk darhol birlik bo‘ladi. Tur bo‘lak bo‘lsa, juftlik raqami bo‘yicha kutish joyiga qo‘yiladi. Ikkala bo‘lak ham ochilgach, ular tur tartibida ulanadi.

Yuborish va qabul qilish tartibi. Yuborishda avval IP paketning uzunligi L aniqlanadi. $L\le1400$ bo‘lsa, bitta UDP datagramma rejalashtiriladi. $1400<L\le1500$ bo‘lsa, L_1 va L_2 hisoblanadi va ikkita datagramma rejalashtiriladi. Har bir rejalashtirilgan paket uchun yangi 8 baytli vektor olinadi, sarlavha yoziladi, ochiq bo‘lak shu vektor bilan yopiladi, so‘ng 4 baytli butunlik belgisi qo‘shiladi. Tayyor yuk UDP datagrammasiga solinadi.

Qabulda tashqi sarlavhalar olinadi va shifrlash qatlami ajratiladi. Uzunlik 26 baytdan kichik bo‘lsa, paket tashlanadi. Butunlik belgisi tekshiriladi. Keyin versiya, kalit identifikatori va

vektor o‘qiladi. Yuk shu vektor bilan ochiladi. Tur butun bo‘lsa, ochiq bo‘lak darhol chiqariladi. Tur bo‘lak bo‘lsa, juftlik raqami bo‘yicha saqlanadi va ikkinchi bo‘lak kelgach, tartib bilan ulanadi. Bir bo‘lak yetmasa, usul yetishmagan qismni o‘zi to‘ldirmaydi: uning vazifasi har bir yuborilgan datagrammani kadr ichida butun saqlashdir.

Mazkur usul ma’lumot birligining ichki tuzilishiga tayanmaydi. Birlik bayt ketma-ketligi sifatida olinadi, 1400 baytlik chegaraga solishtiriladi, kerak bo‘lsa ikkiga bo‘linadi va har bir bo‘lak alohida shifrlangan UDP datagrammasi bo‘ladi. Qabul tomoni juftlikni ulab, xuddi shu bayt ketma-ketligini hosil qiladi. Kadr sig‘imi boshqa qiymat bo‘lsa, chegara qayta hisoblanadi: sig‘imdan 54 bayt ayiriladi va 46 baytlik zaxira saqlanadi. Qolgan qoidalar o‘zgarishsiz qoladi.

Xulosa

Taklif etilayotgan usul ochiq kanalda shifrlangan paketni uchta qoida bilan shakllantiradi. Ochiq bo‘lak 1400 bayt bilan chegaralanadi; 54 baytlik qo‘shimcha bilan tashqi uzunlik 1454 bayt bo‘ladi va 1500 baytlik kadrda 46 bayt zaxira qoladi. Default 1500 baytlik IP paket UDP ga yuklanishidan oldin ikkita datagrammaga ajratiladi. Har bir datagramma o‘z 8 baytli boshlang‘ich vektorini ochiq sarlavhada olib yuradi. Natija kanal qatlamida bo‘linishga bermasdan, har bir tayyor datagrammani kadr ichida butun yetkazish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Postel J. Internet Protocol. RFC 791. 1981.
2. Postel J. User Datagram Protocol. RFC 768. 1980.
3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST SP 800-38A. 2001.
4. IEEE Std 802.3-2018. IEEE Standard for Ethernet. New York: IEEE, 2018.
5. Bonica R., Baker F., Huston G., Hinden R., Troan O., Gont F. IP Fragmentation Considered Fragile. RFC 8900. 2020.
6. Kent C.A., Mogul J.C. Fragmentation Considered Harmful. ACM SIGCOMM. 1987.
7. ISO/IEC 10116:2017. Information technology - Security techniques - Modes of operation for an n-bit block cipher. Geneva: ISO, 2017.
8. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996.

KVANT KOMPYUTERLARINING KRIPTOGRAFIK ALGORITMLARGA TAHDIDI VA POST-KVANT KRIPTOGRAFIYAGA O‘TISH ZARURIYATI

Allanov O.M., Shakarov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Mavlonov O.N.
Samarqand iqtisodiyot va servis instituti

Annotatsiya. Ushbu tezisda kvant kompyuterlarining zamonaviy kriptografik algoritmlariga yuzaga keltirishi mumkin bo‘lgan tahdidlar va ushbu tahdidlarga qarshi post-kvant kriptografiyaning o‘rni tahlil qilinadi. Xususan, RSA, Diffie–Hellman va elliptik egri chiziqqa asoslangan kriptografik mexanizmlarning xavfsizlik asoslari, Shor va Grover algoritmlarining ularga ta’siri ko‘rib chiqiladi. Shuningdek, kvant kompyuterlarining rivojlanishi sharoitida axborot xavfsizligini ta’minlash uchun post-kvant algoritmlarni tanlash, ularni mavjud tizimlarga joriy etish hamda kelgusidagi rivojlanish istiqbollari bo‘yicha asosiy yo‘nalishlar belgilanadi.

Kalit so‘zlar: post-kvant kriptografiya, kvant kompyuteri, Shor algoritmi, Grover algoritmi, RSA, Diffie–Hellman, elliptik egri chiziq, CRYSTALS-KYBER, Module-LWE, kiberxavfsizlik.

Аннотация. В данной работе проанализированы потенциальные угрозы, которые квантовые компьютеры могут представлять для современных криптографических алгоритмов, а также роль постквантовой криптографии в противодействии этим угрозам. В частности, рассмотрены основы безопасности криптографических механизмов, основанных на RSA, Diffie–Hellman и эллиптических кривых, а также влияние алгоритмов Шора и Гровера на их безопасность. Кроме того, определены основные направления выбора постквантовых алгоритмов, их внедрения в существующие системы и дальнейшего развития данных подходов для обеспечения информационной безопасности в условиях развития квантовых вычислений.

Ключевые слова: постквантовая криптография, квантовый компьютер, алгоритм Шора, алгоритм Гровера, RSA, Диффи - Хеллман, эллиптическая кривая, CRYSTALS-Kyber, Module-LWE, кибербезопасность.

Kirish

Bugungi kunda raqamli texnologiyalar va tarmoq infratuzilmalarining kengayishi natijasida axborot almashinuvi, elektron to‘lovlar, telekommunikatsiya, bulutli xizmatlar hamda IoT tizimlarida kriptografik himoyaga bo‘lgan ehtiyoj ortib bormoqda. Shuningdek kriptografik algoritmlar, ma’lumotlarning maxfiyligi, butunligi va foydalanuvchilarni ta’minlash hamda raqamli imzolar orqali ma’lumot haqiqiyligini tasdiqlashda asosiy mexanizmlardan biri hisoblanadi.

An’anaviy ochiq kalitli kriptografik tizimlarning xavfsizligi ma’lum matematik masalalarning klassik kompyuterlarda katta hisoblash murakkabligiga asoslangan. Xususan, RSA katta sonlarni faktorlashga, Diffie–Hellman diskret logarifmlashga, elliptik egri chiziqqa asoslangan algoritmlar esa elliptik egri chiziqdagi diskret logarifm masalasining murakkabligiga tayanadi [1].

Kvant hisoblashning kriptografiyaga asosiy ta’siri esa Shor va Grover algoritmlari bilan uzviy bog‘liq hisoblanadi. Shor algoritmi faktorlash va diskret logarifmlash masalalarini kvant kompyuterida samarali yechish imkoniyatini nazariy jihatdan [2], Grover algoritmi esa tartibsiz qidiruvni tezlashtirib, simmetrik kriptografiya va xesh funksiyalarining xavfsizlik darajasiga ta’sir

ko‘rsatadi [6]. Shu sababli RSA, Diffie–Hellman va elliptik egri chiziqqa asoslangan ochiq kalitli algoritmlar kelajakdagi kvant tahdidlariga nisbatan alohida e’tibor talab qiladi.

Yuqoridagilardan kelib chiqib, post-kvant kriptografiyasi zamonaviy kiberxavfsizlikning muhim tadqiqot yo‘nalishiga aylanmoqda. Shuningdek xorijiy va O‘zbekistonlik olimlar bu borada bir qancha ilmiy izlanishlar olib borishmoqda. O‘rganishlar shuni ko‘rsatadiki, post-kvant algoritmlar kvant kompyuterlaridan foydalanadigan hujumchilarga nisbatan chidamli bo‘lishi ko‘zda tutilgan bo‘lib, ularning ishlashi klassik kompyuterlarda ham amalga oshiriladi.

Asosiy qism

Post-kvant kriptografiyaning asosiy maqsadi - kvant kompyuterlari keng qo‘llanila boshlagan davrda ham axborot tizimlarining kriptografik himoyasini ta’minlashdan iborat. Buning uchun kvant kompyuterlarining hisoblash imkoniyatlariga chidamli bo‘lgan yangi kriptografik algoritmlardan foydalanish ko‘zda tutiladi. Post-kvant kriptografiyada bir nechta asosiy matematik yondashuvlar mavjud bo‘lib, ular orasida panjaraga, kodlarga, xesh funksiyalariga va ko‘p o‘zgaruvchili polinomlarga asoslangan algoritmlar alohida ahamiyatga ega.

Panjaraga asoslangan kriptografiyada xavfsizlik panjara nazariyasidagi murakkab matematik masalalarga tayanadi. Ushbu yo‘nalish kalit almashish, shifrlash va raqamli imzo kabi turli kriptografik funksiyalarni yaratish imkonini beradi. Kodga asoslangan yondashuvlar xatolarni tuzatuvchi kodlarning murakkabligidan foydalanadi. Xeshga asoslangan yondashuvlar esa asosan raqamli imzo mexanizmlarini shakllantirishda qo‘llaniladi.

Quyidagi jadvalda an’anaviy kriptografik mexanizmlar va post-kvant yondashuvlarning umumiy farqi keltirilgan.

1-jadval

An’anaviy va post-kvant kriptografik yondashuvlarning umumiy taqqoslanishi

Yondashuv	Xavfsizlik asosi	Kvant davridagi holati
RSA	Katta sonlarni faktorlash	Shor algoritmi sababli zaiflashish xavfi
Diffie–Hellman	Diskret logarifmlash	Shor algoritmi sababli zaiflashish xavfi
ECC/ECDH/ECDSA	Elliptik egri chiziqdagi diskret logarifm	Shor algoritmi sababli zaiflashish xavfi
AES va xeshlar	Kalitni qidirish va xesh xususiyatlari	Grover ta’siri; parametrlarni kuchaytirish mumkin
PQC	Panjaralar, kodlar, xeshlar va boshqa masalalar	Kvant tahdidlariga chidamlilik uchun ishlab chiqiladi

Jadvaldan ko‘rinib turibdiki, kvant tahdidi barcha kriptografik mexanizmlarga bir xil tarzda ta’sir qilmaydi. Asosiy xavf faktorlash va diskret logarifmlashga asoslangan ochiq kalitli algoritmlarga tegishlidir. Simmetrik algoritmlarda esa xavfsizlik parametrlarini oshirishda, kalit uzunligini oshirish orqali Grover algoritmining ta’sirini kamaytirish imkoniyati mavjud.

Post-kvant kriptografiyaning istiqbolli yo‘nalishlaridan biri panjara nazariyasiga asoslangan algoritmlar hisoblanadi. Tahlillar natijasi shuni ko‘rsatadiki, aynan ushbu yo‘nalish xavfsizlik, hisoblash samaradorligi va turli kriptografik konstruksiyalarni amalga oshirish imkoniyatlari bilan bog‘liq istiqbolli yo‘nalish sifatida ko‘rsatilgan.

Shuningdek, Post-kvant algoritmlar orasida CRYSTALS-KYBER algoritmi alohida ahamiyatga ega [3]. Ushbu algoritm Key Encapsulation Mechanism (KEM) sifatida ishlaydi va uning xavfsizlik asosi Module-LWE masalasiga bog‘langan [4]. CRYSTALS-KYBER algoritmi umumiy maxfiy kalitni kapsulalash va dekapsulatsiya jarayonlari orqali ikki tomon o‘rtasida kalit almashish jarayonini tashkil etadi. Bir qancha tadqiqot ishlarida CRYSTALS-KYBER algoritmi uchun turli xavfsizlik darajalariga mos parametrlar, shuningdek, uning CCA xavfsizlik modeli va Number Theoretic Transform arxitekturasi asosidagi hisoblash jarayonlari ko‘rib chiqilgan.

CRYSTALS-KYBER algoritmining amaliy qiymati esa uning dasturiy hamda apparat muhitlariga oson moslashuvchanligi hisoblanadi. Shuningdek ushbu algoritmning turli tizimlardagi unumdorligi, shu jumladan, Cortex-M4 toifasidagi resurs imkoniyati cheklangan qurilmalarga joriy etilishidir. Ushbu holat post-kvant kriptografik mexanizmlarni zamonaviy telekommunikatsiya texnologiyalari va IoT infratuzilmasiga joriy qilish masalasining qanchalik muhimligini namoyon etadi.

Shuningdek, Post-kvant kriptografiyani tarmoq xavfsizligida qo‘llashda algoritmning faqat nazariy xavfsizligi emas, balki uning amaliy ko‘rsatkichlari ham hisobga olinishi lozim. Jumladan, kalit va shifrmatn hajmi, hisoblash vaqti, xotira sarfi, tarmoq protokollariga moslashuvchanlik va energiya sarfi muhim ko‘rsatkichlar hisoblanadi.

IoT va sensor tizimlarida kriptografik himoyaga qo‘yiladigan talablar alohida ahamiyatga ega, chunki bunday qurilmalarning hisoblash quvvati, xotira hajmi va energiya resurslari ko‘pincha cheklangan bo‘ladi. Shu nuqtai nazardan, post-kvant kriptografik algoritmlarni sensor ma’lumotlarini xavfsiz uzatish, qurilmalarni autentifikatsiya qilish hamda qurilmaning ichki dasturiy ta’minoti va sozlama fayllari yaxlitligini ta’minlash uchun qo‘llash istiqbolli yo‘nalishlardan biri hisoblanadi.

Shu bilan birga, post-kvant kriptografiyaga o‘tish mavjud infratuzilmani to‘liq almashtirishni anglatmaydi. Ushbu o‘tish jarayonida avval ishlatilayotgan kriptografik algoritmlarni aniqlash, kvant tahdidlariga zaif mexanizmlarni ajratish, yangi algoritmlarni sinash va ularning mavjud protokollar bilan mosligini baholash talab etiladi.

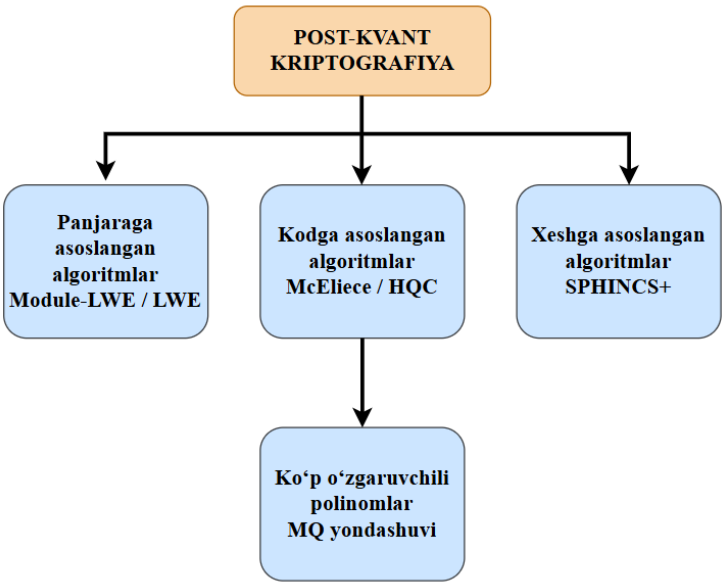
Post-kvant kriptografiyasini amaliyotga tatbiq etishdagi ustuvor vazifalardan biri - uning yagona standartlarini belgilash hamda amaldagi axborot infratuzilmasi bilan o‘zaro muvofiqligini ta’minlashdan iborat. Muqobil algoritmlar yaratilgach, ularni mavjud aloqa tarmoqlari, dasturiy vositalar va kommunikatsiya protokollariga moslashtirish ehtiyoji tug‘iladi. Shu bois, yangi xavfsizlik modeliga o‘tish bosqichlarini tizimli va izchillik bilan amalga oshirish maqsadga muvofiqdir.

Bunda jarayonni quyidagi bosqichli ketma-ketlikda tashkil etish tavsiya etiladi:

- Amaldagi barcha kriptografik algoritmlarni va vositalarni to‘liq audit qilish;
- RSA, Diffie–Hellman hamda elliptik egri chiziqli kriptotizimlar qo‘llanilgan zaif nuqtalarni aniqlashtirish;
- munosib post-kvant algoritmlarini saralab olish va ularning barqarorligi hamda unumdorligini amalda testdan o‘tkazish;
- zaruriyatga qarab, an’anaviy va yangi usullarni birlashtiruvchi gibrid sxemalarni qo‘llash hamda yakuniy bosqichda to‘liq o‘tishni poyoniga yetkazish.

Post-kvant davriga o‘tish jarayonidagi eng murakkab muammolardan biri - bu ilgari kuzatilmagan yangi hujum usullarining paydo bo‘lishi va kriptografik vositalarning himoyalanganlik darajasini uzluksiz ravishda qayta ko‘rib chiqish zaruratidir. Muayyan algoritmning nazariy jihatdan kvant hisoblashlariga chidamliligi uning muhandislik yoki dasturiy ko‘rinishdagi har qanday amaliy tatbiqi mutlaq xavfsiz bo‘lishini kafolatlamaydi. Xususan, kodni amalda qo‘llash jarayonidagi xatoliklar, yon kanal orqali ma’lumot sizib chiqishi, noaniq sozlamalar va sifatsiz muhandislik yechimlari umumiy axborot xavfsizligi tizimini zaiflashtirib qo‘yishi mumkin. Shu sababli, post-kvant xavfsizlik tizimlarini baholashda faqatgina ularning matematik apparatiga tayanib qolmasdan, balki dasturiy-apparat muhitidagi barqarorligi hamda real tahdidlarga bardoshliligini yaxlit holda tadqiq etish talab etiladi.

Post-kvant kriptografiyaning asosiy afzalliklari sifatida kelajakdagi kvant xatarlariga qarshi himoyani ta’minlash, axborot xavfsizligini kuchaytirish hamda turli axborot tizimlarida qo‘llash imkoniyati ko‘rsatiladi. Shu bilan birga, yuqori samaradorlikka ega va kvant hujumlariga chidamli algoritmlarni ishlab chiqish, ularni amaliyotga keng joriy etish, standartlashtirish hamda yangi paydo bo‘layotgan xatarlarga o‘z vaqtida javob berish muhim amaliy vazifalar hisoblanadi.



1-rasm. Post-kvant kriptografiyaning asosiy matematik yo‘nalishlari

Xulosa

Xulosa qilib aytganda kvant hisoblash texnologiyalarining rivojlanishi natijasida hozirgi kriptografik himoya vositalarining kelajakdagi qo‘llanish imkoniyatlarini baholash zarurati yuzaga kelmoqda. O‘tkazilgan tahlil natijasida, Shor algoritmi RSA, Diffie–Hellman va elliptik egri chiziqlarga asoslangan kriptografik mexanizmlarga, Grover algoritmi esa simmetrik kriptografiya hamda xesh-funksiyalarga yangi xavfsizlik talablarini qo‘yishini ko‘rsatdi. Mazkur holat kvant hisoblash imkoniyatlariga moslashgan kriptografik yechimlarni oldindan ishlab chiqish va amaldagi tizimlarni ulardan foydalanishga tayyorlash muhimligini ko‘rsatadi.

Shu nuqtai nazardan, mavjud kriptografik tizimlarni inventarizatsiya qilish, post-kvant algoritmlarning amaliy xususiyatlarini baholash va ularni mavjud infratuzilma bilan uyg‘unlashtirish kelgusidagi asosiy vazifalardan hisoblanadi. Ayniqsa, telekommunikatsiya va IoT qurilmalarida hisoblash resurslarining cheklanganligi sababli post-kvant algoritmlarning tezkorligi, xotira talabi va energiya sarfini tajriba asosida o‘rganish alohida ahamiyatga ega.

Foydalanilgan adabiyotlar:

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994; pp. 124–134.

2. Grover, L.K. A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 1996; pp. 212–219.

3. Bernstein, D.J.; Lange, T. Post-quantum cryptography. Nature, 2017, 549, 188–194.

4. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. Proceedings of the 2018 IEEE European Symposium on Security and Privacy, London, UK, 2018; pp. 353–367.

5. Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Dang, T.; Kelsey, J.; Lichtinger, J.; Miller, C.; Moody, D.; Peralta, R.; et al. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST, Gaithersburg, MD, USA, 2022.

6. Joseph, D.; Misoczki, R.; Manzano, M.; Tricot, J.; Pinuaga, F.D.; Lacombe, O.; Leichenauer, S.; Hidary, S.; Venables, P.; Hansen, R. Transitioning organizations to post-quantum cryptography. Nature, 2022, 605, 237–243.

7. Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-quantum lattice-based cryptography implementations: A survey. ACM Computing Surveys, 2019, 51, 1–41.

KRIPTOGRAFIK KALITLARNI HOSIL QILISHDA HKDF ALGORITMINING SAMARADORLIGI VA XAVFSIZLIK XUSUSIYATLARINI TADQIQ ETISH

Daminov A.A., Karimov A.A., Olimov I.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada kriptografik kalitlarni hosil qilishda HKDF (*HMAC* asosidagi extract-and-expand) algoritmining xavfsizlik xususiyatlari va hisoblash samaradorligi tahlil qilinadi. *Extract* va expand bosqichlari, salt va info parametrlarining roli, qo‘llanish shartlari hamda cheklovlari ko‘rib chiqiladi. HKDF entropiya qo‘shmasligi, shu sababli kirish kalit materialining sifati alohida baholanishi zarurligi asoslanadi.

Kalit so‘zlar: HKDF, *HMAC*, kalit hosil qilish, extract-and-expand, xavfsizlik, samaradorlik, entropiya.

Аннотация. В статье анализируются свойства безопасности и вычислительная эффективность алгоритма HKDF (extract-and-expand на основе *HMAC*) при формировании криптографических ключей. Рассматриваются этапы *Extract* и expand, роль параметров salt и info, условия применения и ограничения. Обосновано, что HKDF не добавляет энтропию, поэтому качество исходного ключевого материала необходимо оценивать отдельно.

Ключевые слова: HKDF, *HMAC*, формирование ключей, extract-and-expand, безопасность, эффективность, энтропия.

Kirish

Kriptografik protokollarda umumiy maxfiy qiymatdan (masalan, Diffie–Hellman natijasidan) bir nechta mustaqil kalit hosil qilish uchun kalit hosil qilish funksiyalari (KDF) qo‘llanadi. HKDF - *HMAC* asosidagi extract-and-expand sxemasi bo‘lib, RFC 5869 da bayon etilgan [1]. NIST SP 800-56C Rev. 2 (2020) kalit o‘rnatish sxemalari uchun ikki bosqichli «extraction-then-expansion» usulini keltiradi va RFC 5869 uning bir variantini belgilashini qayd etadi [2]; kengaytirish bosqichida SP 800-108 dagi PRF asosidagi KDF ishlatilishi talab qilinadi [3]. HKDF gibrid ochiq kalitli shifrlash (HPKE) standartida ham qo‘llanadi [4]. Tezisning maqsadi HKDF ning xavfsizlik xususiyatlari va hisoblash samaradorligini adabiyot asosida tahlil qilishdir. Original eksperiment o‘tkazilmagan; keltirilgan natijalar adabiyotdan olingan, samaradorlik bahosi esa spetsifikatsiyaga asoslangan analitik hisobdir.

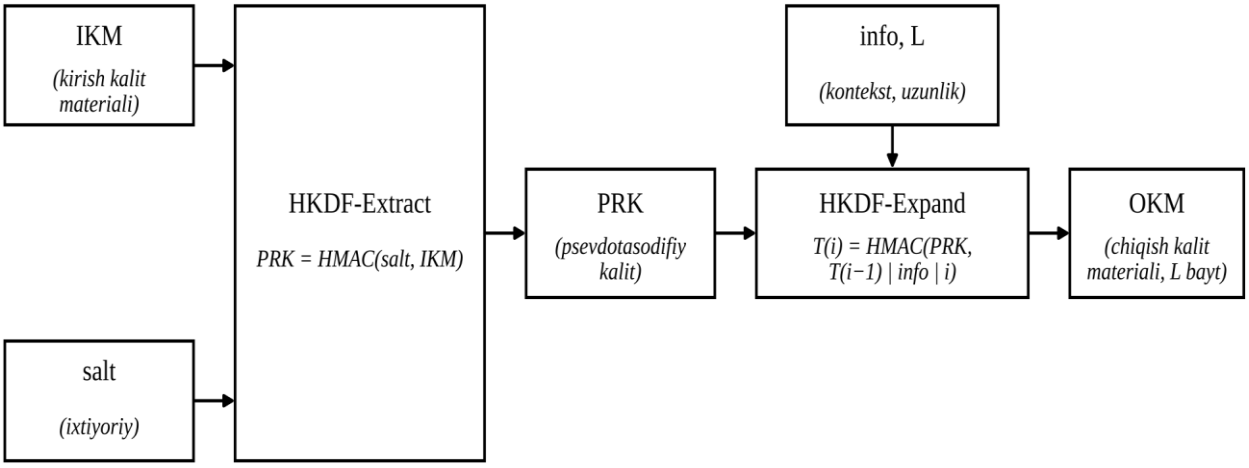
HKDF tuzilishi. Algoritm ikki bosqichdan iborat (1-rasm). *Extract* bosqichi IKM (kirish kalit materiali) dan PRK (psevdotasodifiy kalit) hosil qiladi:

$$\mathrm{PRK} = \mathit{HMAC\text{-}Hash}(\mathrm{salt}, \mathrm{IKM}) \qquad (1)$$

bunda *salt* - ixtiyoriy tasodifiy qiymat (berilmasa HashLen ta nol bayt), *HMAC-Hash* - tanlangan xesh-funksiya asosidagi *HMAC*. Expand bosqichi PRK dan uzunligi L bayt bo‘lgan OKM (chiqish kalit materiali) hosil qiladi:

$$\mathrm{T}(i) = \mathit{HMAC\text{-}Hash}(\mathrm{PRK}, \mathrm{T}(i-1) \mid \mathrm{info} \mid i) \qquad (2)$$

bunda info - kontekstni bildiruvchi ixtiyoriy satr, i - bir baytli hisoblagich, | - birlashtirish, T(0) - bo‘sh satr. OKM sifatida T (1) | T (2) | … | T(N) ning dastlabki L bayti olinadi, $N = \lceil L/\mathrm{HashLen} \rceil$, $L \le 255 \cdot \mathrm{HashLen}$.



1-rasm. HKDF ning extract-and-expand tuzilishi

Xavfsizlik xususiyatlari. Extract bosqichi mavjud entropiyani to‘playdi, lekin yangisini qo‘shmaydi; salt kirish materialidan mustaqil bo‘lishi va hujumchi tomonidan boshqarilmasligi lozim. IKM allaqachon kuchli psevdotasodifiy kalit bo‘lsa, *Extract* o‘tkazib yuborilishi mumkin, Diffie–Hellman qiymatlari uchun esa uni o‘tkazib yuborish tavsiya etilmaydi. Demak, HKDF kirish materialining min-entropiyasini oshirmaydi va manba sifati alohida baholanishi kerak. Info orqali bitta PRK dan kontekstga bog‘liq mustaqil kalitlar olinadi; HPKE da Labeled*Extract* va LabeledExpand funksiyalari versiya, to‘plam identifikatori va maqsad yorliqlarini qo‘shib domenlarni ajratadi. HKDF xavfsizligi *HMAC* ning PRF xususiyatiga tayanadi: da *HMAC* ning har qanday uzunlikdagi kalit uchun PRF xavfsizligi isbotlangan, kalit va xabar o‘rni almashtirilganda (dual-PRF) esa xavfsizlik umumiy holda ta'minlanmasligi, faqat kalitlar «feasibility» shartini bajaradigan to‘plamlardan olinganda o‘rinli bo‘lishi ko‘rsatilgan; TLS 1.3, KEMTLS, MLS va Noise bu taxminga tayanadi. HKDF-*Extract* da maxfiy IKM *HMAC* ning xabar kirishiga beriladi, shu sababli bu natija HKDF tahlilida ahamiyatli. TLS 1.3 kalit jadvali *Extract* va expand amallari grafi sifatida modellashtirilib, kirish materiallaridan biri xavfsiz bo‘lsa, chiqish kalitlari ham xavfsiz ekani ko‘rsatilgan [6]. Xususiyatlar 1-jadvalda umumlashtirilgan.

Samaradorlik. Expand bosqichi $N = \lceil L/\text{HashLen} \rceil$ ta ketma-ket *HMAC* chaqiruvidan iborat, chunki T(i) hisobi T(i−1) ga bog‘liq . SHA-256 uchun (HashLen = 32 bayt, blok 64 bayt) qisqa kirishlarda (IKM ≤ 55 bayt, info ≤ 22 bayt) har bir *HMAC* chaqiruvi ipad va opad holatlari oldindan hisoblanmaganda 4 ta siqish funksiyasi chaqiruvini talab qiladi; jami xarajat taxminan 4(1 + N) chaqiruv bo‘ladi (muallifning analitik hisobi, o‘lchov emas). Masalan, 256 bitli kalit uchun (N = 1) 8 ta, 512 bitli kalit uchun (N = 2) 12 ta chaqiruv kerak. Expand bosqichida PRK doimiy kalit bo‘lgani uchun ipad va opad holatlarini bir marta hisoblash mumkin; bunda Expand xarajati 4N o‘rniga 2(1 + N) chaqiruvga tushadi. Skye ishida HKDF umumiy maqsadli konstruksiya bo‘lib, Diffie–Hellman qiymatlari kabi aniq manbalar uchun optimallashtirilmagani va ketma-ket tuzilishi sababli parallellashtirishdan foyda oladigan platformalarda sekinroq ekani qayd etilgan; Skye SHA-256 asosidagi HKDF dan apparat qo‘llab-quvvatlashiga qarab 4–47 marta tezroq, Signal ga integratsiyada esa bir yo‘nalishli almashinuvda 38–64 %, ikki yo‘nalishlida (10 xabar) 12–36 % tezlashuv bergani keltirilgan. Bu natijalar mualliflarning o‘z o‘lchovlari bo‘lib, ushbu tezisda takrorlanmagan.

HKDF parol asosida kalit hosil qilish uchun mo‘ljallanmagan: u ataylab sekinlashtirish mexanizmini o‘z ichiga olmaydi, bunday holatda PKCS #5 tavsiya etiladi. L ≤ HashLen bo‘lganda PRK ni bevosita chiqish sifatida ishlatish info hisobga olinmagani uchun tavsiya etilmaydi. Tezis

adabiyot tahliliga asoslangan; son jihatdan solishtirma natijalar keltirilmagan, chunki ular platforma, xesh-funksiya va kirish uzunligiga bog‘liq.

1-jadval

HKDF ning xavfsizlik va samaradorlik xususiyatlari

Xususiyat	Mazmuni	Shart yoki cheklov	Manba
Extract bosqichi	PRK = *HMAC-Hash* (salt, IKM): mavjud entropiyani to‘playdi	Entropiya qo‘shmaydi; IKM yetarli min-entropiyaga ega bo‘lishi kerak	[1]
Salt	*Extract* bosqichining kuchini oshiradi; berilmasa HashLen ta nol bayt	IKM dan mustaqil bo‘lishi va hujumchi tomonidan boshqarilmasligi lozim	[1]
Expand bosqichi va info	Bir PRK dan kontekstga bog‘liq bir nechta kalit; domenlarni ajratish	$L \leq 255 \cdot HashLen$; HPKE da yorliqlar bilan kengaytirilgan	[1], [4]
HMAC ning PRF xavfsizligi	Har qanday uzunlikdagi kalit uchun isbotlangan	Kalit va xabar o‘rni almashganda umumiy holda ta'minlanmaydi	[5]
TLS 1.3 kalit jadvali	Kirish materiallaridan biri xavfsiz bo‘lsa, chiqish kalitlari ham xavfsiz	*Extract* va expand amallari grafi modelida tahlil qilingan	[6]
Parol asosidagi hosil qilish	Mo‘ljallanmagan: sekinlashtirish mexanizmi yo‘q	Bunday holatlar uchun PKCS #5 tavsiya etiladi	[1]
Samaradorlik	Ketma-ket *HMAC* chaqiruvlari; xarajat N ga chiziqli	Ixtisoslashgan KDF (Skye) tezroq bo‘lishi mumkin	[7]

Amaliy ahamiyati. Kalit generatsiyasi zanjirida HKDF entropiya manbasi va DRBG ning o‘rnini bosmaydi: manba entropiyasi alohida baholanishi, HKDF esa uni kontekstga bog‘liq kalitlarga taqsimlashi lozim. SP 800-56C Rev. 2 bitta kalit hosil qilish kalitidan (extraction natijasidan) bir necha marta expansion bajarish shartlari uchun alohida bo‘lim kiritgan va «gibrid» umumiy sirni $Z' = Z \parallel T$ ko‘rinishida ishlatishga ruxsat bergan. SP 800-108 Rev. 1 PRF sifatida *HMAC*, CMAC va KMAC ni qamrab oladi. Adabiyotdagi shartlardan quyidagi amaliy talablar kelib chiqadi: har bir kalit maqsadi uchun noyob info yorlig‘i qo‘llash; salt ni IKM dan mustaqil tanlash; Diffie–Hellman qiymatlarida *Extract* bosqichini saqlash; L ni $255 \cdot HashLen$ dan oshirmaslik; parol asosidagi holatlarda HKDF dan foydalanmaslik. Masalan, bitta Diffie–Hellman natijasidan shifrlash kaliti, autentifikatsiya kaliti va boshlang‘ich vektor uchun turli info qiymatlari bilan uchta expand bajarilsa, uchta mustaqil OKM olinadi; 256 bitli uchta kalit uchun jami xarajat $4 + 3 \cdot 4 = 16$ siqish chaqiruvi (yuqoridagi hisob bo‘yicha).

Xulosa

1) HKDF xavfsizligi *HMAC* ning PRF xususiyatiga, salt ning mustaqilligiga va kirish materialining sifatiga bog‘liq; algoritm entropiya qo‘shmaydi. 2) Xarajat chiqish uzunligiga chiziqli va ketma-ket; SHA-256 uchun taxminan $4(1 + N)$ siqish chaqiruviga teng, ixtisoslashgan KDF lar esa tezroq bo‘lishi mumkin [7]. 3) Original eksperiment o‘tkazilmagani sababli, amaliy tanlov uchun maqsadli platformada o‘lchovlar zarur.

Foydalanilgan adabiyotlar

1. H. Krawczyk and P. Eronen, "*HMAC*-based extract-and-expand key derivation function (HKDF)," IETF, RFC 5869, May 2010, doi: 10.17487/RFC5869. [Online]. Available: https://www.rfc-editor.org/info/rfc5869

2. E. Barker, L. Chen, and R. Davis, "Recommendation for key-derivation methods in key-establishment schemes," NIST, Gaithersburg, MD, USA, SP 800-56C Rev. 2, Aug. 2020, doi: 10.6028/NIST.SP.800-56Cr2.

3. L. Chen, "Recommendation for key derivation using pseudorandom functions," NIST, Gaithersburg, MD, USA, SP 800-108 Rev. 1 (Upd. 1), Feb. 2024, doi: 10.6028/NIST.SP.800-108r1-upd1.

4. R. Barnes, K. Bhargavan, B. Lipp, and C. Wood, "Hybrid public key encryption," IETF, RFC 9180, Feb. 2022, doi: 10.17487/RFC9180. [Online]. Available: https://www.rfc-editor.org/info/rfc9180

5. M. Backendal, M. Bellare, F. Günther, and M. Scarlata, "When messages are keys: Is *HMAC* a dual-PRF?" in Advances in Cryptology – CRYPTO 2023, Lecture Notes in Computer Science, Cham, Switzerland: Springer, 2023, pp. 661–693, doi: 10.1007/978-3-031-38548-3_22.

6. C. Brzuska, A. Delignat-Lavaud, C. Egger, C. Fournet, K. Kohbrok, and M. Kohlweiss, "Key-schedule security for the TLS 1.3 standard," in Advances in Cryptology – ASIACRYPT 2022, Lecture Notes in Computer Science, Cham, Switzerland: Springer, 2022, pp. 621–650, doi: 10.1007/978-3-031-22963-3_21.

7. A. S. Bhati, A. Dufka, E. Andreeva, A. Roy, and B. Preneel, "Skye: An expanding PRF based fast KDF and its applications," in Proc. 19th ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS '24), New York, NY, USA, Jul. 2024, pp. 1082–1098, doi: 10.1145/3634737.3637673.

KONSORSIUM BLOKCHEYN TEXNOLOGIYASINING QATLAMLI ARXITEKTURASI, KONSENSUS MEXANIZMLARI VA RIVOJLANISH ISTIQBOLLARI

Janxojaev A.A., Aralbaev I.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda ishtirokchilari oldindan autentifikatsiyadan o‘tadigan konsorsium blokcheyn texnologiyasining arxitekturasi, konsensus mexanizmlari va amaliy qo‘llanish sohalari tahlil qilinadi. Konsorsium blokcheyn apparat, tarmoq, ma’lumotlar, konsensus, aqlli shartnoma qatlamlari hamda ikkinchi daraja protokollari kesimida ko‘rib chiqiladi. Hyperledger Fabric, Ethereum, FISCO BCOS, Corda, Quorum va Ripple platformalari ma’lumotlar modeli, konsensus algoritmi va unumdorligi bo‘yicha qiyoslanadi. Markazsizlashuv va unumdorlik o‘rtasidagi muvozanat, isbotlanuvchi xavfsizlik, ishonchli bajarilish muhiti hamda postkvant kriptografiyaga o‘tish dolzarb tadqiqot yo‘nalishlari sifatida asoslanadi.

Kalit so‘zlar: konsorsium blokcheyn, konsensus mexanizmlari, Vizantiya nosozliklariga bardoshlilik, aqlli shartnoma, Merkle daraxti, ishonchli bajarilish muhiti, postkvant kriptografiya.

Аннотация. В тезисе анализируются архитектура, механизмы консенсуса и области практического применения технологии консорциумного блокчейна, участники которого проходят предварительную аутентификацию. Консорциумный блокчейн рассматривается в разрезе аппаратного и сетевого уровней, уровней данных, консенсуса и смарт-контрактов, а также протоколов второго уровня. Проведено сравнение платформ Hyperledger Fabric, Ethereum, FISCO BCOS, Corda, Quorum и Ripple по модели данных, алгоритму консенсуса и производительности. В качестве актуальных направлений исследований обоснованы баланс между децентрализацией и производительностью, доказуемая безопасность, доверенная среда исполнения и переход к постквантовой криптографии.

Ключевые слова: консорциумный блокчейн, механизмы консенсуса, византийская отказоустойчивость, смарт-контракт, дерево Меркла, доверенная среда исполнения, постквантовая криптография.

Kirish

Blokcheyn texnologiyasi taqsimlangan tarmoqda bir-biriga ishonmaydigan ishtirokchilar o‘rtasidagi ishonch modelini tubdan o‘zgartirdi. Bitcoin kriptovalyutasi bilan boshlangan bu texnologiya Ethereum platformasidagi Tyuring-to‘liq aqlli shartnomalar orqali moliya sohasiga, keyinchalik esa buyumlar interneti, sog‘liqni saqlash, aqlli shahar va kiberxavfsizlik kabi sohalarga kirib bordi [1]. Blokcheynlar odatda uch turga ajratiladi: istalgan foydalanuvchi erkin qo‘shila oladigan ochiq blokcheyn; ishtirokchilari ruxsat olib qo‘shiladigan va tugunlari bir nechta tashkilotga tegishli bo‘lgan konsorsium blokcheyn; barcha tugunlari bitta tashkilotga qarashli xususiy blokcheyn.

Konsorsium blokcheyn umumiy manfaatga ega tashkilotlarga bir-birini tanigan holda hamkorlik qilish imkonini beradi, natijada ishonch bilan bog‘liq xatar kamayadi, boshqaruv va qaror qabul qilish jarayonlari esa ochiq blokcheynga nisbatan ko‘proq nazorat ostida bo‘ladi. Shu bois u bank-moliya, davlat xizmatlari va idoralararo ma’lumot almashinuvi kabi yuqori xavfsizlik talab qilinadigan sohalar uchun ayniqsa qulay. Ushbu tezisning maqsadi konsorsium

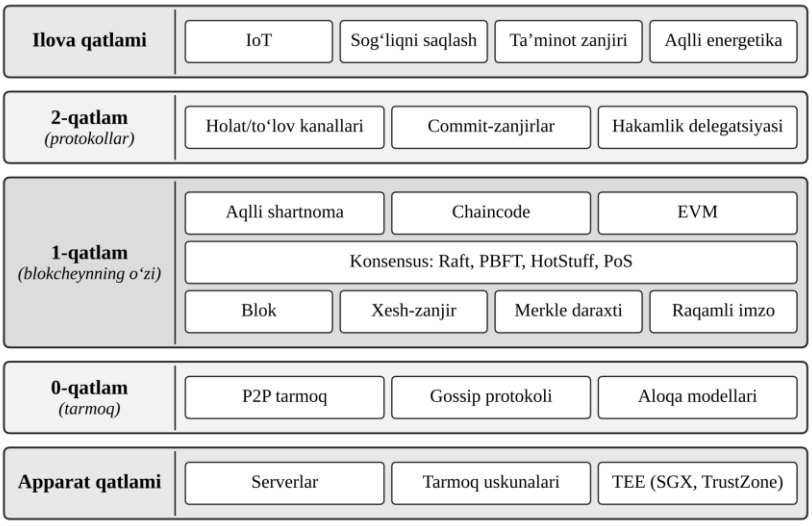
blokcheynning kriptografik va arxitekturaviy asoslarini umumlashtirish hamda kriptologiya sohasidagi dolzarb tadqiqot yo‘nalishlarini belgilashdan iborat.

Asosiy qism

Konsorsium blokcheynning nazariy asosini holatlar mashinasini replikatsiya qilish (State Machine Replication, SMR) modeli tashkil etadi. Unga ko‘ra barcha halol replikalar bir xil boshlang‘ich holatdan boshlab, bir xil buyruqlar ketma-ketligini deterministik tarzda bajaradi va bir xil yangi holatga keladi. Model ikki asosiy xossani ta’minlaydi: jonlilik, ya’ni har bir to‘g‘ri buyruq oxir-oqibat qayd etiladi, va izchillik, ya’ni aloqada kechikish bo‘lsa ham barcha tugunlar bir xil natijani ko‘radi. Blokcheyn muhitida bu model Vizantiya nosozliklariga bardoshlilik (BFT) bilan to‘ldiriladi: tugunlarning bir qismi g‘arazli harakat qilgan taqdirda ham qolganlari kelishuvga erisha oladi [1, 2].

An’anaviy taqsimlangan ma’lumotlar bazasidan farqli ravishda, konsorsium blokcheyn bitta tugundagi g‘arazli xatti-harakat butun tizimni izdan chiqarishiga yo‘l qo‘ymaydi, tranzaksiyalarni alohida emas, blok darajasida tasdiqlaydi va holatni barcha tugunlarda to‘liq takrorlaydi. Uning unumdorligi asosan kriptografik amallar va tarmoq aloqasi bilan belgilanadi. Bu yondashuvning narxi saqlash xarajatining oshishidir, chunki har bir tugun ma’lumotlarning to‘liq nusxasini saqlaydi; shu sababli sharding, siqish va deduplikatsiya usullari faol tadqiq qilinmoqda [1].

Qatlamli arxitektura. Konsorsium blokcheynni quyidagi qatlamlar ko‘rinishida tahlil qilish qulay (1-rasm) [1]. Apparat qatlami serverlar, tarmoq uskunalari va ishonchli bajarilish muhitlaridan (TEE: Intel SGX, ARM TrustZone, AMD SEV) iborat; TEE kodni himoyalangan anklavda bajarib, natija to‘g‘riligini masofadan attestatsiya qilish imkonini beradi, biroq yon-kanal hujumlariga zaifligicha qolmoqda. Tarmoq qatlami (0-qatlam) tugunlar o‘rtasidagi P2P aloqa, gossip protokollari va sinxron, qisman sinxron yoki asinxron aloqa modellarini qamrab oladi. 1-qatlam blokcheynning o‘zi bo‘lib, ma’lumotlar, konsensus va aqlli shartnoma osti qatlamlariga bo‘linadi. 2-qatlam protokollari (holat va to‘lov kanallari, commit-zanjirlar, hakamlik delegatsiyasi) asosiy zanjirni o‘zgartirmasdan tranzaksiyalarning bir qismini zanjirdan tashqariga chiqarib, masshtablanuvchanlikni oshiradi [4].



1-rasm. Konsorsium blokcheynning qatlamli arxitekturasi

Ma’lumotlar qatlamining kriptografik asoslari. Har bir blok sarlavhasida oldingi blokning xesh qiymati, tranzaksiyalar Merkle daraxtining ildizi va vaqt belgisi saqlanadi. Demak, zanjirning o‘zgarmasligi to‘liq xesh-funksiyaning bir tomonlamaligi va kolliziyaga bardoshliligiga tayanadi.

Tranzaksiyalar haqiqiyligi ECDSA kabi raqamli imzo algoritmlari bilan ta’minlanadi, ulardan tanlangan xabarlar hujumi sharoitida soxtalashtirib bo‘lmaslik (EU-CMA) xossasi talab qilinadi. Merkle daraxti esa muayyan tranzaksiyaning blokka kiritilganini butun blokni yuklamasdan, ildizgacha bo‘lgan qo‘shni tugunlar xeshlaridan iborat log n o‘lchamli isbot orqali tekshirish imkonini beradi [1].

Konsensus mexanizmlari. Konsensus mexanizmi barcha halol tugunlarning bir xil holatga kelishini kafolatlaydi va uchta xossaga ega bo‘lishi kerak: chekli vaqtda tugallanish, halol tugunlar o‘rtasida kelishuv hamda kelishilgan qiymatning halol tugundan kelib chiqishi. Mexanizmlar ikki asosiy sinfga bo‘linadi. Raft kabi nosozliklarga bardoshli (CFT) algoritmlar tugunlarning yarmidan kamrog‘i ishdan chiqqanda ishlay oladi, lekin g‘arazli tugunlardan himoyalamaydi. PBFT, BFT-SMaRt, HotStuff kabi BFT algoritmlari esa tugunlarning uchdan bir qismigacha g‘arazli bo‘lishiga bardosh beradi, ammo xabarlar almashinuvi hajmi kattaligi sababli tugunlar soni oshganda unumdorligi pasayadi [1, 2]. HoneyBadger va Dumbo kabi asinxron protokollar tarmoq kechikishlari haqida hech qanday faraz qilmasdan ishlashi bilan ajralib turadi.

Platformalar qiyosi. Amaliyotda eng ko‘p qo‘llaniladigan konsorsium blokcheyn platformalari bir-biridan arxitekturaviy yechimlari bilan farq qiladi. Hyperledger Fabric tranzaksiyalarni tasdiqlash, tartiblash va qayd etish bosqichlariga ajratadi; FISCO BCOS bloklarni konveyer asosida va tranzaksiyalarni parallel ijro etish orqali unumdorlikni oshiradi; Corda esa tranzaksiyani faqat unga aloqador tomonlar bilan bo‘lishib, maxfiylikni ustuvor qo‘yadi [1, 3]. Asosiy ko‘rsatkichlar 1-jadvalda keltirilgan.

1-jadval

Konsorsium blokcheyn platformalarining qiyosiy tavsifi

Platforma	Ma’lumotlar modeli	Konsensus	Unumdorlik, tx/s (sinov tarmog‘i)	Asosiy xususiyati
Hyperledger Fabric	Hisobga asoslangan	Raft, PBFT	~3000 (4 tugun)	Almashtiriladigan konsensus, masshtablanuvchanlik
Ethereum	Hisobga asoslangan	PoW, PoS	~6000 (10 tugun)	Tyuring-to‘liq aqlli shartnomalar
FISCO BCOS	Hisobga asoslangan	Raft, PBFT	~3000 (6 tugun)	Samaradorlik, moslashuvchanlik
Corda	UTXO	Raft, PBFT	~2500 (4 tugun)	Maxfiylik, masshtablanuvchanlik
Quorum	Hisobga asoslangan	Raft, PBFT	~2000 (3 tugun)	Modullilik, maxfiy tranzaksiyalar
Ripple	Ripple modeli	RPCA	~1000 (16 tugun)	Real vaqtda hisob-kitob (RTGS)

Qo‘llanish sohalari. Konsorsium blokcheyn ikki asosiy funksiyani taqdim etadi: ishonchli saqlash va kafolatlangan hisoblash. Shu asosda u buyumlar internetida qurilmalarga sertifikat berish va ma’lumotlarni xavfsiz boshqarishda, sog‘liqni saqlashda shaxsiy tibbiy yozuvlarni IPFS va nol bilimli isbotlar yordamida maxfiy almashishda, ta’minot zanjirida mahsulot harakatini kuzatishda (masalan, Hyperledger Fabric asosidagi IBM Food Trust), qishloq xo‘jaligi mahsulotlarining kelib chiqishini aniqlashda hamda aqlli energetika tarmoqlarida elektr energiyasi savdosini xavfsiz tashkil etishda qo‘llanilmoqda [1].

Muammolar va istiqbolli yo‘nalishlar. Birinchi asosiy muammo - markazsizlashuv, masshtablanuvchanlik va xavfsizlikni bir vaqtda ta’minlashning qiyinligi (blokcheyn trilemmasi). Konsorsium blokcheyn bu borada markazlashgan ma’lumot markazlari va ochiq blokcheynlar o‘rtasida oraliq o‘rinni egallaydi, shuning uchun tizimni loyihalashda aniq amaliy talablardan kelib chiqish lozim. Ikkinchi muammo - blokcheyn asosidagi protokollar xavfsizligini formal isbotlash. Zamonaviy kriptografiya paradigmasiga ko‘ra, bu aniq ta’riflar, aniq farazlar va qat’iy isbotlarni talab qiladi; isbotlar o‘yin asosida yoki simulyatsiya asosida, shuningdek universal kompozitsiyalanuvchi (UC) model doirasida qurilishi mumkin [1].

Istiqbolli yo‘nalishlar sifatida quyidagilarni ajratish mumkin: TEE yordamida konsensus samaradorligini oshirish va aqlli shartnomalar maxfiyligini ta’minlash; 2-qatlam protokollarining xarajati va markazsizlik darajasini miqdoriy baholash hamda ularning 1-qatlam bilan o‘zaro ta’sirini hisobga olgan xavfsizlik ta’riflarini ishlab chiqish. Kriptologiya nuqtai nazaridan eng muhim yo‘nalish - postkvant konsorsium blokcheynga o‘tishdir. Hozirgi platformalar xavfsizligi ECDSA kabi elliptik egri chiziqlarga asoslangan imzolarga tayanadi, Shor algoritmini bajara oladigan kvant kompyuter esa bunday imzolarni buzishi mumkin [5]. NIST tomonidan 2024-yilda standartlashtirilgan ML-DSA va SLH-DSA imzo algoritmlari [6] muqobil yechim bo‘lsa-da, ularning imzo va kalit o‘lchamlari kattaroq bo‘lib, blok hajmi va tarmoq yuklamasiga ta’sir qiladi. Hozircha keng e’tirof etilgan postkvant konsorsium blokcheyn platformasi mavjud emas [1]. Milliy sharoitda esa platformalarga mahalliy kriptografik standartlarni (masalan, O‘z DSt 1092 raqamli imzo va O‘z DSt 1106 xesh-funksiya standartlarini) almashtiriladigan kriptografik modul sifatida integratsiya qilish dolzarb vazifa hisoblanadi.

Xulosa

Konsorsium blokcheyn ishonchli saqlash va kafolatlangan hisoblash imkoniyatlari tufayli ochiq blokcheyn bilan markazlashgan tizimlar o‘rtasida muvozanatli yechim bo‘lib, moliya, buyumlar interneti, sog‘liqni saqlash va energetika sohalarida keng qo‘llanilmoqda. Uning xavfsizligi bevosita xesh-funksiyalar, raqamli imzolar va BFT konsensus protokollariga tayanadi. Shu sababli kelgusidagi tadqiqotlar unumdorlik va markazsizlik muvozanatini optimallashtirish, protokollar xavfsizligini formal isbotlash, TEE imkoniyatlaridan foydalanish hamda kvant hujumlariga bardoshli kriptografik primitivlarga bosqichma-bosqich o‘tishga yo‘naltirilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. Chen X., He S., Sun L., Zheng Y., Wu C.Q. A Survey of Consortium Blockchain and Its Applications // Cryptography. – 2024. – Vol. 8, No. 2. – Art. 12. – DOI: 10.3390/cryptography8020012.

2. Castro M., Liskov B. Practical Byzantine Fault Tolerance // Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI). – New Orleans, 1999. – P. 173–186.

3. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // Proceedings of the 13th EuroSys Conference. – Porto, 2018.

4. Gudgeon L., Moreno-Sanchez P., Roos S., McCorry P., Gervais A. SoK: Layer-Two Blockchain Protocols // Financial Cryptography and Data Security. – Springer, 2020. – P. 201–226.

5. Fernandez-Carames T.M., Fraga-Lamas P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks // IEEE Access. – 2020. – Vol. 8. – P. 21091–21116.

6. NIST FIPS 204. Module-Lattice-Based Digital Signature Standard. – Gaithersburg: NIST, 2024.

ZKP (ZERO-KNOWLEDGE PROOF) TIZIMLARINI AUTENTIFIKATSIYA VA FOYDALANISHNI BOSHQARISH VAZIFALARIDA QO‘LLASH

Mardiyev U.R.
UNICON.UZ Fan-texnika va marketing tadqiqotlari markazi
Turobov A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada nol bilimli isbot (ZKP) tizimlarining autentifikatsiya va foydalanishni boshqarishdagi o‘rni tahlil qilinadi. ZKP ning uch xossasi, interaktiv va noninteraktiv protokollar hamda Schnorr, Fiat–Shamir, zk-SNARK, zk-STARK va Bulletproofs tizimlari ishonchli sozlash, isbot o‘lchami, tekshirish vaqti va kvantga chidamlilik mezonlari bo‘yicha solishtiriladi. Parolsiz kirish, atributga asoslangan ruxsat, anonim hisob ma’lumotlari va markazlashmagan identifikatsiya sohalaridagi 2025–2026-yillardagi natijalar, jumladan ISO/IEC 27565:2026 standarti va ECDSA asosidagi anonim hisob ma’lumotlari ko‘rib chiqiladi.

Kalit so‘zlar: nol bilimli isbot, autentifikatsiya, zk-SNARK, zk-STARK, anonim hisob ma’lumotlari, tasdiqlanadigan ma’lumotnomalar.

Аннотация. В статье анализируется роль систем доказательства с нулевым разглашением (ZKP) в задачах аутентификации и управления доступом. Рассмотрены три свойства ZKP, интерактивные и неинтерактивные протоколы, а также системы Schnorr, Fiat–Shamir, zk-SNARK, zk-STARK и Bulletproofs, которые сравниваются по необходимости доверенной настройки, размеру доказательства, времени проверки и стойкости к квантовым атакам. Освещены беспарольный вход, доступ на основе атрибутов, анонимные учётные данные и децентрализованная идентификация, а также результаты 2025–2026 годов, включая стандарт ISO/IEC 27565:2026 и анонимные учётные данные на основе ECDSA.

Ключевые слова: доказательство с нулевым разглашением, аутентификация, zk-SNARK, zk-STARK, анонимные учётные данные, проверяемые учетные данные.

Kirish

An’anaviy autentifikatsiyada foydalanuvchi o‘z sirini (odatda parolni) serverga yuboradi yoki server uning xeshini saqlaydi. Natijada parollar bazasi o‘g‘irlansa, barcha hisoblar xavf ostida qoladi; shuningdek, xizmat so‘ralgan faktdan ortiq ma’lumotni, masalan, yoshni tasdiqlash uchun butun tug‘ilgan sanani yoki hujjat nusxasini oladi. Nol bilimli isbot (ZKP) bu muammoni boshqacha hal qiladi: isbotlovchi biror da’voning to‘g‘riligini, shu da’voning o‘zidan boshqa hech narsani oshkor qilmasdan tasdiqlaydi.

Raqamli hujjatni beruvchi tashkilot (emitent) uni o'z imzosi bilan tasdiqlaydi. Foydalanuvchi hujjatning faqat kerakli qismini ko'rsatishi mumkin, qolgan maydonlar yashirin qoladi (bu usul selektiv oshkor qilish deyiladi). Biroq har safar bir xil imzo va ochiq kalit ko'rsatilgani uchun, turli xizmatlar bu ma'lumotlarni solishtirib, foydalanuvchini kuzatib borishi mumkin. Bu GDPRning "faqat zarur ma'lumotni yig'ish" tamoyiliga zid; Podda va hammualliflar buni ZKP bilan bartaraf etish mumkinligini ta’kidlaydi [1-manba]. 2026-yil 9-fevralda ISO/IEC 27565:2026 - ZKP asosida maxfiylikni saqlash bo‘yicha ko‘rsatmalar e’lon qilindi [2-manba]. Maqolaning maqsadi ZKP tizimlarini taqqoslash va ularning autentifikatsiya hamda foydalanishni boshqarishdagi qo‘llanilishini so‘nggi manbalar asosida ko‘rsatishdir. Tadqiqot uslubi - 2025–

2026-yillardagi ilmiy nashrlar, standartlar hamda IETF va W3C hujjatlarining solishtirma tahlili; maqola sharh xarakteriga ega, 1-jadvaldagi o‘lchov natijalari esa [8] manbadan olingan.

Asosiy qism

Ushbu qismda ZKP ning nazariy asoslari, asosiy tizimlari, autentifikatsiya va foydalanishni boshqarishdagi qo‘llanilishi hamda cheklovlari ketma-ket ko‘rib chiqiladi.

ZKP asoslari. ZKP tushunchasini Goldwasser, Micali va Rackoff kiritgan [3]. Isbotlovchi P va tekshiruvchi V o‘rtasidagi har qanday ZKP protokoli uchta xossani qanoatlantirishi kerak.

To‘liqlik (completeness). Da’vo to‘g‘ri bo‘lsa va ikkala tomon protokolga amal qilsa, V isbotni albatta qabul qiladi. Bu xossa tizimning ishlashini kafolatlaydi: sirni bilgan qonuniy foydalanuvchi rad etilmaydi. Keyingi bo‘limda keltirilgan Schnorr protokolida tekshiruv tengligi $s = r + c \cdot x$ bo‘lgani uchun doim bajariladi: $g^s = g^r \cdot (g^x)^c = t \cdot y^c$.

Ishonchlilik (soundness). Da’vo noto‘g‘ri bo‘lsa, hech qanday aldovchi P tekshiruvchini, e’tiborga olinmaydigan ehtimoldan tashqari, ishontira olmaydi; bu ehtimol soundness xatosi deyiladi. Xossa cheksiz hisoblash kuchiga ega P ga qarshi ham bajarilsa, protokol isbot (proof), faqat polinomial vaqtda ishlovchi P ga qarshi bajarilsa - argument deyiladi; amaliy zk-SNARK tizimlari argumentlar sirasiga kiradi. Autentifikatsiya uchun kuchliroq xossa - bilimning isboti - kerak: V ni ishontirgan P dan sirni ajratib olish (extractor) mumkin bo‘lishi shart. Schnorr protokolida bir xil t uchun ikki xil c va c' ga to‘g‘ri javob (s va s') berilsa, $x = (s - s')/(c - c') \bmod q$ bo‘ladi; demak, sirni bilmagan P bir t uchun ko‘pi bilan bitta c ga javob bera oladi. Fiat–Shamir identifikatsiyasida aldash ehtimoli har raundda 1/2 bo‘lib, k raunddan so‘ng 2^{-k} gacha kamayadi.

Nol bilimlilik (zero-knowledge). V protokoldan da’vo to‘g‘riligidan boshqa hech narsani bilib olmaydi. Bu simulyator tushunchasi orqali ifodalanadi: sirni bilmaydigan algoritm haqiqiy suhbatdan farqlab bo‘lmaydigan yozuvni o‘zi hosil qila olsa, yozuv sir haqida ma’lumot bermaydi. Schnorr protokolida simulyator c va s ni tasodifiy tanlab, $t = g^s \cdot y^{-c}$ ni hisoblaydi; hosil bo‘lgan (t, c, s) uchligi tekshiruvdan o‘tadi va haqiqiy yozuv bilan bir xil taqsimlangan. Taqsimotlar aynan bir xil bo‘lsa - mukammal, deyarli bir xil bo‘lsa - statistik, polinomial vaqtli algoritm ularni farqlay olmasa - hisoblash nol bilimliligi deyiladi. Schnorr protokoli faqat halol tekshiruvchiga nisbatan (HVZK) nol bilimli: g‘arazli V so‘rovni hiyla bilan tanlashi mumkin, shu sababli amalda c ni xesh funksiyasi hisoblaydi (Fiat–Shamir evristikasi).

Ishonchlilik tekshiruvchini aldanishdan, nol bilimlilik esa isbotlovchini ma’lumot sizishidan himoya qiladi. Xavfsizlik isbotlarida ular mos ravishda ajratib oluvchi (extractor) va simulyator mavjudligi orqali ko‘rsatiladi.

Interaktiv isbotda tekshiruvchi tasodifiy so‘rov (challenge) yuboradi va isbotlovchi shunga javob beradi. Noninteraktiv isbotda bu so‘rov Fiat–Shamir evristikasi [4] yordamida isbotlovchining majburiyati va da’voning xeshidan hisoblanadi; bu xavfsizlik isbotini tasodifiy oracle modelida beradi va protokolni bir xabarga (isbotga) keltiradi. Aynan shu o‘zgartirish autentifikatsiya, raqamli imzo va blokcheyn kabi amaliy tizimlarda keng qo‘llanishga imkon berdi.

ZKP turlari. Schnorr va Fiat–Shamir identifikatsiya protokollari. Schnorr protokoli [5] $y = g^x$ ni qanoatlantiruvchi x sirni bilishni isbotlaydi: isbotlovchi $t = g^r$ ni yuboradi, tekshiruvchi tasodifiy c ni tanlaydi, isbotlovchi $s = r + c \cdot x \pmod q$ ni qaytaradi va tekshiruvchi $g^s = t \cdot y^c$ tengligini tekshiradi. Fiat–Shamir identifikatsiyasi [4] esa kvadratik chegirmalar (faktorlash qiyinligi) asosida qurilgan. Ikkalasi ham ishonchli sozlashni talab qilmaydi, lekin ular faqat sodda (bitta munosabatli) da’volarni isbotlaydi.

zk-SNARK, zk-STARK va Bulletproofs. zk-SNARK tizimlari (masalan, Groth16) juda qisqa isbot beradi, ammo sxemaga xos ishonchli sozlashni talab qiladi. zk-STARK [6] ishonchli

tomonsiz (shaffof) ishlaydi va xesh funksiyalariga tayanadi, shu sababli kvantga chidamli deb hisoblanadi, lekin isboti katta. Bulletproofs [7] ishonchli sozlashni talab qilmaydi, isbot o‘lchami witness hajmiga logarifmik o‘sadi va diskret logarifm taxminiga tayanadi; u ayniqsa diapazon isbotlari (range proofs) uchun samarali. Tizimlarning umumiy taqqoslanishi 1-jadvalda keltirilgan.

1-jadval

ZKP tizimlarining taqqoslanishi

Tizim	Ishonchli sozlash	Isbot o‘lchami	Tekshirish vaqti	Kvantga chidamlilik
Schnorr / Fiat–Shamir	Yo‘q	Juda kichik	Tez (bir necha amal)	Yo‘q (DLP / faktorlash)
zk-SNARK (Groth16)	Ha, sxemaga xos	Doimiy, 384 B [8]	Nazariy jihatdan doimiy	Yo‘q (juftlikli egri chiziqlar)
zk-STARK	Yo‘q (shaffof)	Katta, ≈69 KB [8]	Polilogarifmik	Ha (xesh funksiyalarga asoslangan)
Bulletproofs	Yo‘q	Logarifmik	Chiziqli (paketlash mumkin)	Yo‘q (DLP)

Amaliy o‘lchovlar nazariy kutilmalardan farq qilishi mumkin. 2025-yilda e’lon qilingan tajribada (Apple M1, ochiq o‘quv darajasidagi implementatsiyalar, bitta sxema) Groth16 isboti 55 ms da hosil bo‘lib, 384 bayt bo‘lgan; STARK isboti 3,8 s da hosil bo‘lib, ≈68,6 KB bo‘lgan. Biroq tekshirish STARKda tezroq bo‘lgan (472 ms ga qarshi 1807 ms), bu nazariyaga zid - mualliflar implementatsiya tafsilotlari natijaga kuchli ta’sir qilishini ta’kidlaydi [8]. Shuning uchun jadvaldagi sonlarni umumiy qoida emas, bitta o‘lchov sifatida qabul qilish kerak.

Autentifikatsiya va foydalanishni boshqarishda qo‘llash

Parolsiz autentifikatsiya

Schnorr turidagi noninteraktiv isbotda foydalanuvchi maxfiy kalitni bilishini isbotlaydi, serverda esa faqat ochiq qiymat y saqlanadi. Shuning uchun server bazasi o‘g‘irlansa ham, undan kirish uchun yaroqli sir olinmaydi; isbot sessiya kontekstiga (nonce, domen nomi) bog‘lansa, takroriy ishlatish (replay) hujumi oldi olinadi.

Atributga asoslangan ruxsat

ZKP yosh, fuqarolik yoki rolni asl qiymatini oshkor qilmay isbotlashga imkon beradi (masalan, «yosh ≥ 18»). Frigo va shelat ISO mdoc formatidagi mavjud ECDSA imzolangan hujjatlar ustidan ZK isbot qurishni taklif qilgan: usul emitent jarayonlari va mobil qurilmalarni o‘zgartirishni talab qilmaydi va ZK qismida faqat SHA-256 taxminiga tayanadi; ECDSA isboti eng yaxshi holatda ≈20 ms, mobil qurilmada mdoc taqdimoti esa bir necha yuz millisekund oladi [9]. Shuni inobatga olish kerakki, ECDSA imzosining o‘zi kvantga chidamli emas.

Anonim hisob ma’lumotlari

BBS imzo sxemasi bir nechta xabar ustidan doimiy o‘lchamli imzo beradi, egasi esa imzoni bilishining ZK isbotini yaratib, xabarlarning ixtiyoriy qismini oshkor qiladi; bir imzodan olingan turli isbotlar o‘zaro bog‘lanmaydi (unlinkability). Sxema IETF/IRTF CFRG tomonidan ishlab chiqilmoqda: draft-irtf-cfrg-bbs-signatures-12 (2026-yil 28-sentyabr) hujjati «Informational» maqomida, shifr to‘plamlari BLS12-381 egri chizig‘iga asoslangan [10]. Podda va hammualliflar

ko‘rsatishicha, CL va BBS imzolari egasining ochiq kalitini yashirishi mumkin, lekin ular hozircha iste’molchi telefonlaridagi xavfsiz elementlarda qo‘llab-quvvatlanmaydi [1].

Markazlashmagan identifikatsiya (DID, verifiable credentials). Verifiable Credentials 2.0 spetsifikatsiyalar oilasi 2025-yil 15-mayda W3C tavsiyasi maqomini oldi; uning JOSE/COSE qismi JWT uchun selektiv oshkor qilishni qamrab oladi [11]. ZKP bu modelga taqdimot qatlamida qo‘shiladi: egasi hisob ma’lumotining o‘zini emas, uning ma’lum predikatni qanoatlantirishini isbotlaydi. Natijada tekshiruvchi emitent bilan bog‘lanmaydi va foydalanuvchi turli xizmatlarda kuzatib borilmaydi.

Muammolar va cheklovlar

Birinchidan, hisoblash narxi yuqori: 25 ta ochiq ZKP freymvorkini baholagan tadqiqot ZKP hatto oddiy vazifalarda ham sezilarli qo‘shimcha hisoblash yuki keltirishini va ko‘p freymvorklarda hujjatlar hamda yuqori darajadagi API yetishmasligini ko‘rsatgan; STARK uchun qulay freymvorklar kam [12]. Ikkinchidan, isbot o‘lchami: STARK isboti SNARKnikidan sezilarli katta [8]. Uchinchidan, ishonchli sozlash xavfi: sozlash paytidagi maxfiy parametrlar (toxic waste) sizib chiqsa, soxta isbotlar yaratish mumkin bo‘ladi, shu sababli shaffof tizimlar (STARK, Bulletproofs) afzal ko‘riladi. To‘rtinchidan, joriy etish murakkabligi: umumiy maqsadli ZKP murakkabroq va yetukligi pastroq, CL va BBS kabi anonim hisob ma’lumotlari imzolari esa telefonlardagi xavfsiz elementlarda hozircha qo‘llab-quvvatlanmaydi [1].

Standartlar masalasida vaziyat o‘zgarmoqda, ammo hali yakunlanmagan: ISO/IEC 27565:2026 ko‘rsatmalar sifatida e’lon qilingan [2], BBS esa hanuz Internet-Draft bosqichida [10]; eIDAS 2.0 va GDPR o‘rtasidagi huquqiy munosabat ham aniq emas [1]. Kvantga chidamlilik nuqtai nazaridan faqat xeshga asoslangan tizimlar (STARK) tayyor, juftlikli egri chiziq va diskret logarifmga asoslangan tizimlar uchun esa o‘tish rejasi kerak.

Xulosa

Nol bilimli isbot an'anaviy autentifikatsiyaning ikkita asosiy kamchiligini bartaraf etadi. Birinchidan, parol yoki maxfiy kalit serverga yuborilmaydi, shuning uchun server bazasi o'g'irlansa ham foydalanuvchilarning sirlari hujumchiga tushmaydi. Ikkinchidan, foydalanuvchi o'zi haqida faqat kerakli faktni isbotlaydi, masalan, "yoshim 18 dan katta", va butun hujjatini ko'rsatmaydi.

Qaysi tizimni tanlash vazifaga bog'liq. Oddiy kirish uchun Schnorr yoki Fiat–Shamir protokoli yetarli. Isbot juda kichik va tekshiruv tez bo'lishi kerak bo'lsa, zk-SNARK qulay, lekin u ishonchli sozlashni talab qiladi. Sozlashsiz va kvant kompyuterlardan ham himoyalangan deb hisoblanadigan yechim kerak bo'lsa, zk-STARK mos keladi, faqat uning isboti katta. Bulletproofs esa qiymat ma'lum oraliqda ekanini isbotlash uchun ayniqsa qulay.

So'nggi yillardagi eng muhim yangiliklar anonim hisob ma'lumotlari sohasida bo'ldi. ECDSA imzolari ustidan ishlaydigan ZK isbotlar mavjud infratuzilmani o'zgartirmasdan qo'llanishi mumkinligi ko'rsatildi [9], BBS imzo sxemasi standartlashtirilmoqda [10], 2026-yilda esa ISO/IEC 27565 bo'yicha ko'rsatmalar e'lon qilindi [2]. Shunga qaramay, keng joriy etishga hali uchta narsa xalaqit beradi: hisoblash xarajati, telefonlardagi xavfsiz elementlarda BBS kabi imzolarning qo'llab-quvvatlanmasligi [1] va standartlarning hali to'liq tugallanmaganligi. Kelgusi tadqiqotlar shu uch yo'nalishga qaratilishi kerak.

Foydalanilgan adabiyotlar:

1. Podda E., Hölzmer P., Amard A., Sedlmeir J., Fridgen G. The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets // Internet Policy Review. – 2025. – Vol. 14, No. 3. – DOI: 10.14763/2025.3.2019.

2. ISO/IEC 27565:2026. Information security, cybersecurity and privacy protection - Guidelines on privacy preservation based on zero-knowledge proofs. – ISO/IEC, 2026 (e'lon qilingan: 09.02.2026).

3. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM Journal on Computing. – 1989. – Vol. 18, No. 1. – P. 186–208.

4. Fiat A., Shamir A. How to prove yourself: practical solutions to identification and signature problems // CRYPTO '86, LNCS 263. – Springer, 1987. – P. 186–194.

5. Schnorr C.P. Efficient signature generation by smart cards // Journal of Cryptology. – 1991. – Vol. 4, No. 3. – P. 161–174.

6. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // IACR Cryptology ePrint Archive. – 2018. – Paper 2018/046.

7. Bünz B., Bootle J., Boneh D., Poelstra A., Wuille P., Maxwell G. Bulletproofs: Short proofs for confidential transactions and more // IEEE Symposium on Security and Privacy. – 2018 (IACR ePrint 2017/1066).

8. Nainwal A., Kamble A., Awathare N. A comparative analysis of zk-SNARKs and zk-STARKs: Theory and practice // arXiv:2512.10020. – 2025.

9. Frigo M., shelat a. Anonymous credentials from ECDSA // IACR Cryptology ePrint Archive. – 2024. – Paper 2024/2010 (rev. 27.04.2026); Communications in Cryptology. – Vol. 3, Issue 1.

10. Looker T., Kalos V., Whitehead A., Lodder M., Bernstein G. The BBS Signature Scheme. draft-irtf-cfrg-bbs-signatures-12 // IRTF CFRG Internet-Draft. – 28.09.2026.

11. W3C. The Verifiable Credentials 2.0 family of specifications is now a W3C Recommendation. – 15.05.2025. – https://www.w3.org/news/2025/the-verifiable-credentials-2-0-family-of-specifications-is-now-a-w3c-recommendation

12. Sheybani N., Ahmed A., Kinsy M., Koushanfar F. Zero-knowledge proof frameworks: A systematic survey // arXiv:2502.07063. – 2025.

POST-KVANT KRIPTOGRAFIYADA ML-KEM ALGORITMLARINING XAVFSIZLIK XUSUSIYATLARI VA ISHLASH SAMARADORLIGI: TAHLIL VA AMALIY TAJRIBA

Xursandova Z.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada kvant hisoblash texnologiyalarining an’anaviy ochiq kalitli kriptografiyaga keltirishi mumkin bo‘lgan tahdidlari va post-kvant kriptografiyaga o‘tish zarurati ko‘rib chiqiladi. Python muhitida ML-KEM-512, ML-KEM-768 va ML-KEM-1024 algoritmlari bo‘yicha kichik amaliy tajriba o‘tkazildi. Ochiq va yopiq kalitlar, shifrmatn hajmi, asosiy amallarning o‘rtacha bajarilish vaqti hamda umumiy maxfiy kalitning mosligi tekshirildi. Olingan natijalar qiyosiy tahlil qilinib, tashkilotlarda post-kvant kriptografiyani sinovdan o‘tkazish va bosqichma-bosqich joriy etish bo‘yicha tavsiyalar berildi.

Kalit so‘zlar: post-kvant kriptografiya, ML-KEM, kvant kompyuteri, kriptografik xavfsizlik, inkapsulyatsiya, Python.

Аннотация. В статье рассматриваются потенциальные угрозы квантовых вычислений для традиционной криптографии с открытым ключом и необходимость перехода к постквантовой криптографии. В среде Python проведён небольшой практический эксперимент с алгоритмами ML-KEM-512, ML-KEM-768 и ML-KEM-1024. Измерены размеры открытого и закрытого ключей, шифротекста, среднее время выполнения основных операций и совпадение общего секретного ключа. Полученные результаты сопоставлены, а также предложены рекомендации по тестированию и поэтапному внедрению постквантовой криптографии в организациях.

Ключевые слова: постквантовая криптография, ML-KEM, квантовый компьютер, криптографическая безопасность, инкапсуляция, Python.

Kirish

Raqamli xizmatlar, elektron hujjat aylanishi, masofaviy identifikatsiya va bulutli infratuzilmalarning kengayishi kriptografik himoyaning ishonchliligini muhim masalaga aylantirmoqda. Bugungi kunda RSA va elliptik egri chiziqlarga asoslangan mexanizmlar ochiq kalitli kriptografiyada keng qo‘llanadi. Yetarli quvvatga ega kvant kompyuteri paydo bo‘lgan taqdirda, Shor algoritmi butun sonlarni faktorlash va diskret logarifm masalalariga asoslangan ayrim keng tarqalgan kriptografik mexanizmlarga tahdid tug‘dirishi mumkin [1].

Post-kvant kriptografiya (PQC) klassik kompyuterlarda ishlaydigan, shu bilan birga ma’lum kvant hujumlariga qarshi turishga mo‘ljallangan algoritmlarni anglatadi. 2024-yilda AQSh Milliy standartlar va texnologiyalar instituti (NIST) ML-KEM, ML-DSA va SLH-DSA standartlarini e’lon qildi [2–4]. Ushbu ishda ML-KEM oilasining uchta parametr to‘plami kichik tajriba asosida solishtiriladi.

Tadqiqotning maqsadi - ML-KEM-512, ML-KEM-768 va ML-KEM-1024 algoritmlarining ma’lumot hajmi va bajarilish tezligi bo‘yicha o‘lchangan ko‘rsatkichlarini taqqoslash hamda natijalarni amaliy joriy etish nuqtayi nazaridan izohlash. Vazifalar: post-kvant kriptografiya dolzarbligini asoslash; tajriba metodikasini bayon qilish; o‘lchovlarni taqdim etish va cheklovlarini ko‘rsatish; joriy etish bo‘yicha tavsiyalar ishlab chiqish.

ML-KEM va post-kvant kriptografiya

Kvant tahdidi faqat kelajakdagi tizimlar bilan cheklanmaydi. Uzoq muddat maxfiy saqlanishi lozim bo‘lgan ma’lumotlar uchun “hozir yig‘ib, keyin deshifrlash” ssenariysi muhim: hujumchi bugun uzatilayotgan shifrlangan ma’lumotlarni saqlab, kelajakda ularni ochishga urinishi mumkin. Shu sababli tashkilotlar ishlatayotgan kriptografik algoritmlar, sertifikatlar, aloqa protokollari va kalitlarni boshqarish jarayonlarini oldindan inventarizatsiya qilishi kerak.

NIST FIPS 203 standarti ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) mexanizmini belgilaydi [2]. U ikki tomon o‘rtasida umumiy maxfiy kalitni hosil qilish uchun ishlatiladi; ma’lumotning o‘zi odatda keyinchalik ushbu kalitdan foydalanadigan simmetrik algoritm bilan shifrlanadi. ML-KEM-512, ML-KEM-768 va ML-KEM-1024 turli parametr to‘plamlaridir. Ularni tanlashda xavfsizlik darajasi bilan bir qatorda kalit va shifrmatn hajmi, protokol bilan moslik, kechikish va resurs cheklovlari ham hisobga olinadi.

Mazkur maqoladagi tajriba faqat uchta ML-KEM parametr to‘plamining asosiy hajm va tezlik ko‘rsatkichlarini o‘lchaydi. Bu tajriba algoritmlarning matematik xavfsizligini isbotlash yoki barcha hujumlarga chidamliligini baholash vazifasini bajarmaydi.

Amaliy tajriba metodikasi

Tajriba Windows operatsion tizimida Python dasturlash tili va pqcrypto kutubxonasi yordamida amalga oshirildi. Tadqiqotda ML-KEM-512, ML-KEM-768 va ML-KEM-1024 algoritmlari o‘rganildi. Har bir algoritm uchun ochiq va yopiq kalitlar juftligi yaratildi. Keyin ochiq kalit yordamida *encapsulation* amali bajarilib, shifrmatn va yuboruvchi tomonning umumiy maxfiy kaliti hosil qilindi. Yopiq kalit hamda shifrmatn yordamida *decapsulation* amali bajarilib, qabul qiluvchi tomonning umumiy maxfiy kaliti tiklandi. Dastur ikkala tomon hosil qilgan maxfiy kalitlarning o‘zaro tengligini tekshirdi.

Har bir ML-KEM parametr to‘plami uchun kalit yaratish, inkapsulyatsiya va dekapsulyatsiya amallarining bajarilish vaqti 100 ta takrorlash orqali o‘lchandi. O‘rtacha bajarilish vaqti umumiy o‘lchangan vaqtni takrorlashlar soniga bo‘lish orqali hisoblandi. Kalitlarning mosligi har bir parametr to‘plamida alohida tekshirildi. Inkapsulyatsiya va dekapsulyatsiya vaqtlarini o‘lchashda oldindan yaratilgan kalitlar juftligi hamda shifrmatndan foydalanildi. O‘lchovlar time.perf_counter() funksiyasi yordamida amalga oshirildi.

1-jadval.

ML-KEM algoritmlarining hajm ko‘rsatkichlari

Ko‘rsatkich (bayt)	ML-KEM-512	ML-KEM-768	ML-KEM-1024
Ochiq kalit	800	1184	1568
Yopiq kalit	1632	2400	3168
Shifrmatn	768	1088	1568
Umumiy maxfiy kalit	32	32	32

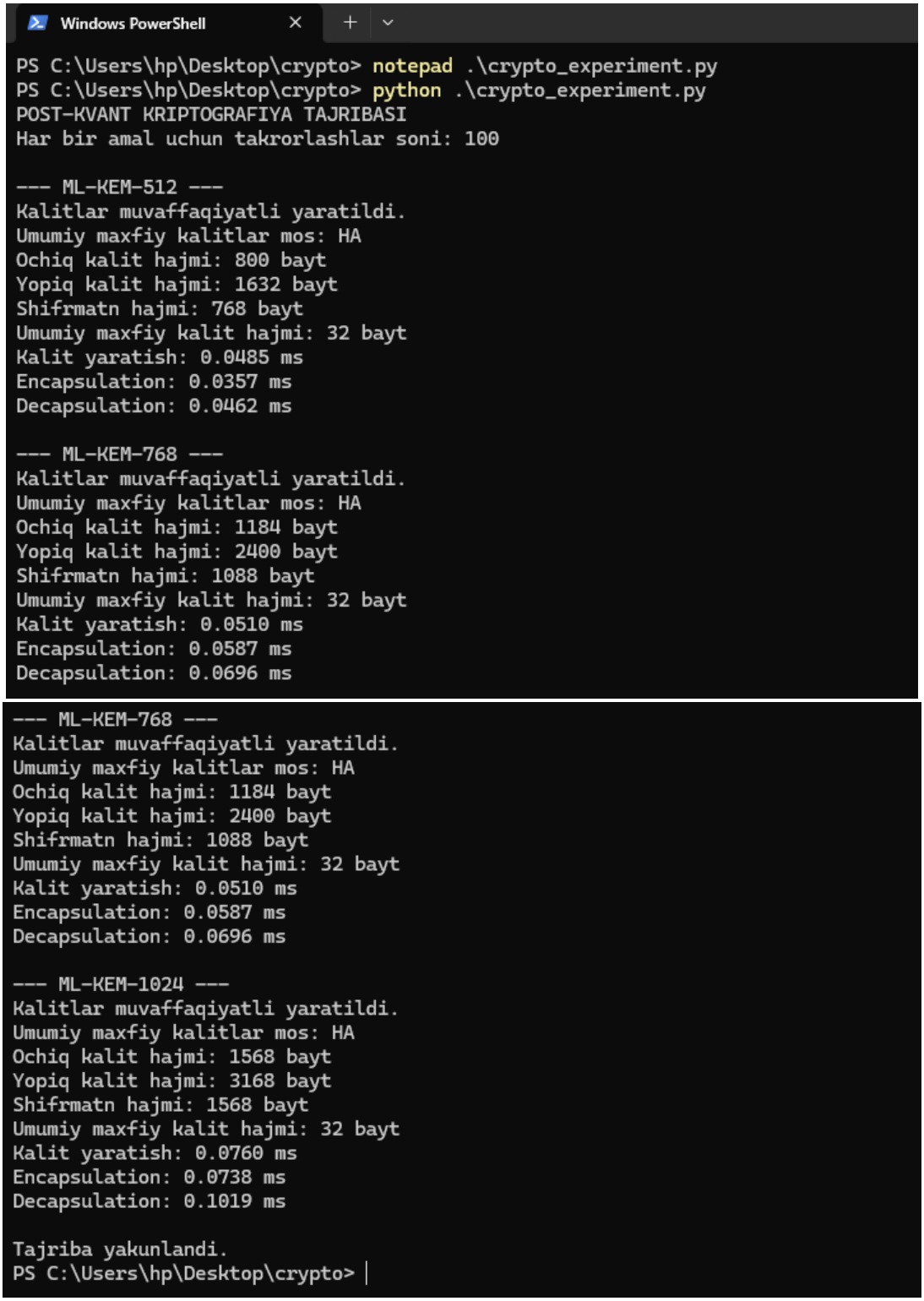
2-jadval.

Asosiy amallarning o‘rtacha bajarilish vaqti

Amal (ms)	ML-KEM-512	ML-KEM-768	ML-KEM-1024
Kalit yaratish	0,0485	0,0510	0,0760
Encapsulation	0,0357	0,0587	0,0738
Decapsulation	0,0462	0,0696	0,1019

Izoh: vaqtlar har bir amalni 100 marta takrorlash orqali olingan; qiymatlar sinov muhiti bilan bog‘liq.

Amaliy CMD da o‘tkazilgan tajriba screenshotlari:



1-rasm. Tajriba natijalari

Natijalar va muhokama

Uchala parametr to‘plamida ham dastur muvaffaqiyatli yakunlandi va yuboruvchi hamda qabul qiluvchi tomon hosil qilgan umumiy maxfiy kalitlar mos keldi. Bu natija sinovdan o‘tgan

dasturiy ish oqimining to‘g‘ri bajarilganini ko‘rsatadi, ammo algoritmlarning barcha xavfsizlik xususiyatlarini mustaqil ravishda isbotlamaydi.

Ma’lumotlar hajmi bo‘yicha ML-KEM-512 eng kichik ko‘rsatkichlarni qayd etdi: ochiq kalit hajmi 800 bayt, yopiq kalit hajmi 1632 bayt va shifrmatn hajmi 768 baytni tashkil etdi. ML-KEM-1024 uchun ushbu qiymatlar mos ravishda 1568 bayt, 3168 bayt va 1568 bayt bo‘ldi. ML-KEM-768 da esa ochiq kalit 1184 bayt, yopiq kalit 2400 bayt va shifrmatn 1088 baytni tashkil etdi. Uchala parametr to‘plamida umumiy maxfiy kalit hajmi 32 bayt bo‘lib, bu ko‘rsatkich o‘zgarmadi. Natijalar parametr to‘plamiga qarab kalitlar va shifrmatn hajmlari farqlanishini ko‘rsatadi.

Bajarilish vaqti bo‘yicha ham tajriba muhitida farqlar kuzatildi. ML-KEM-512 kalit yaratish, inkapsulyatsiya va dekapsulyatsiya amallarida mos ravishda 0,0485 ms, 0,0357 ms va 0,0462 ms natijalarni ko‘rsatdi. ML-KEM-768 uchun ushbu qiymatlar 0,0510 ms, 0,0587 ms va 0,0696 ms, ML-KEM-1024 uchun esa 0,0760 ms, 0,0738 ms va 0,1019 ms ni tashkil etdi. Shunday qilib, mazkur tajriba muhitida ML-KEM-512 uchala amal bo‘yicha eng qisqa, ML-KEM-1024 esa eng uzun bajarilish vaqtiga ega bo‘ldi.

Ushbu farqlar parametr to‘plamlari va ular bilan bog‘liq hisoblash jarayonlarining xususiyatlari bilan bog‘liq bo‘lishi mumkin. Biroq o‘tkazilgan tajriba sekinlashish sabablarini alohida tekshirmaganligi sababli, bu bog‘liqlikni uzil-kesil isbotlangan xulosa sifatida talqin qilish mumkin emas. Bundan tashqari, o‘lchovlar bitta kompyuter va dasturiy muhitda olingan. Protsessor xususiyatlari, operatsion tizim yuklamasi, kutubxona versiyasi va o‘lchash usuli natijalarga ta’sir ko‘rsatishi mumkin.

Kelgusidagi tadqiqotlarda tajribani bir necha mustaqil ishga tushirish, ko‘proq o‘lchovlar olish hamda median va standart og‘ish kabi statistik ko‘rsatkichlarni hisoblash natijalarning ishonchliligini baholashga yordam beradi. Faqat bajarilish tezligiga qarab algoritm tanlash to‘g‘ri emas. ML-KEM parametr to‘plamini tanlashda talab etiladigan xavfsizlik darajasi, kalit va shifrmatn hajmi, tizim resurslari hamda foydalaniladigan protokol bilan moslik birgalikda hisobga olinishi lozim.

O‘zbekiston tashkilotlari uchun amaliy tavsiyalar

Post-kvant kriptografiyaga o‘tishni bosqichma-bosqich tashkil etish tavsiya etiladi. Birinchi bosqichda tashkilot TLS, VPN, elektron imzo, sertifikatlar va uchinchi tomon xizmatlarida ishlatilayotgan kriptografik mexanizmlarni inventarizatsiya qiladi. Ikkinchi bosqichda uzoq muddat maxfiy qolishi zarur bo‘lgan ma’lumotlar va muhim infratuzilmalar xavf darajasiga ko‘ra ustuvorlashtiriladi.

Uchinchi bosqichda standartlashtirilgan mexanizmlar laboratoriya muhitida sinovdan o‘tkaziladi. Bunda kalit va xabar hajmi, aloqa protokoli bilan moslik, kechikish, xatolarni qayta ishlash hamda kutubxona yangilanishlari tekshiriladi. To‘rtinchi bosqichda cheklangan pilot loyiha ishga tushirilib, natijalar va zaxira rejasi tasdiqlangandan so‘ng yechim bosqichma-bosqich kengaytiriladi.

Tashkilotlar kriptografik chaqqonlik (crypto-agility) tamoyilini ko‘zda tutishi, ya’ni kelajakda algoritmni butun tizimni qayta qurmasdan almashtirish imkoniyatini yaratishi lozim. Ushbu tavsiyalar tajriba doirasida ishlab chiqilgan taklif bo‘lib, muayyan tashkilotda joriy etilgan yechim sifatida talqin qilinmasligi kerak.

Xulosa

Maqolada post-kvant kriptografiyaga o‘tish zarurati yoritildi va ML-KEM-512, ML-KEM-768 hamda ML-KEM-1024 algoritmlari Python muhitida amaliy tajriba orqali qiyoslandi. Uchala

variantda umumiy maxfiy kalitlarning mosligi tasdiqlandi. O‘lchovlarda ML-KEM-512 eng kichik kalit/shifrmatn hajmlari va eng qisqa bajarilish vaqtlarini, ML-KEM-1024 esa eng katta hajmlar va yuqoriroq vaqt ko‘rsatkichlarini namoyish etdi. Natijalar tanlovda tezlik, ma’lumot hajmi, xavfsizlik talabi va tizim cheklovlarini birgalikda hisobga olish zarurligini ko‘rsatadi.

Tadqiqotning cheklovi - sinov bitta kompyuter va dasturiy muhitda bajarilganidir. Keyingi ishlar turli apparat muhitlarida takroriy sinov, statistik ko‘rsatkichlar, gibrid kalit almashish va real protokollar bilan moslikni baholashga qaratilishi mumkin.

Foydalanilgan adabiyotlar

1. Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

2. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024. https://doi.org/10.6028/NIST.FIPS.203.

3. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard. 2024. https://doi.org/10.6028/NIST.FIPS.204.

4. National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Standard. 2024. https://doi.org/10.6028/NIST.FIPS.205.

5. National Institute of Standards and Technology. Post-Quantum Cryptography Project. https://csrc.nist.gov/projects/post-quantum-cryptography.

KALITLARNI HOSIL QILISH MEXANIZMLARINING KRIPTOGRAFIK ASOSLARI

Xudoynazarov U.U.
Muhammad al-Alxorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada kriptografik kalitlarni hosil qilish mexanizmlarining nazariy asoslari NIST SP 800 seriyasidagi standartlar asosida tahlil qilinadi. Kriptografik kalitlarga oid asosiy tushunchalar tizimlashtirilib, umumlashtirilgan jadval ko‘rinishida keltiriladi. Simmetrik va asimmetrik kriptografik tizimlarda kalitlarni hosil qilish usullari qiyosiy tahlil qilinadi hamda kalitlarni hosil qilish jarayonining ishonchliligi va qo‘llaniladigan kriptografik mexanizmlarga ham bog‘liqligi asoslanadi. Ishning asosiy natijalaridan biri sifatida kalitni almashtirish va seans davomida kalit materialini yangilash mexanizmlari o‘rtasidagi farq aniqlashtiriladi. Olingan natijalarning amaliy ahamiyati TLS 1.3 protokoli misolida yoritiladi.

Kalit so‘zlar: kalit generatsiyasi, kalit hosil qilish funksiyasi, xavfsizlik darajasi, entropiya, kalit-derivatsiya kaliti, kripto-davr, derivatsiya zanjiri, TLS protokoli.

Аннотация. В статье анализируются теоретические основы механизмов формирования криптографических ключей на основе стандартов серии NIST SP 800. Основные понятия, связанные с криптографическими ключами, систематизируются и представляются в обобщённой таблице. Проводится сравнительный анализ методов формирования ключей в симметричных и асимметричных криптографических системах, а также обосновывается зависимость безопасности ключей от надёжности процесса их формирования и применяемых криптографических механизмов. В качестве одного из основных результатов уточняется различие между механизмами замены ключа и обновления ключевого материала в рамках сеанса. Практическая значимость полученных результатов рассматривается на примере протокола TLS 1.3.

Ключевые слова: генерация ключей, функция выработки ключа, уровень безопасности, энтропия, ключ выработки ключей, криптопериод, цепочка выработки, Протокол TLS.

Kirish

Kriptografik tizimning bardoshliligi nafaqat qo‘llanilayotgan algoritmning matematik xususiyatlariga, balki unda foydalaniladigan kalitning qay tarzda hosil qilinganiga ham bog‘liq. Matematik jihatdan yuqori darajadagi xavfsizlikni ta’minlaydigan algoritm ham kalit bashorat qilinadigan yoki yetarlicha tasodifiy bo‘lmagan jarayon orqali hosil qilinganda, amaliy himoyani kafolatlay olmaydi. Kriptografiya amaliyotida kalitlarni hosil qilishdagi kamchiliklar kriptografik tizimlar xavfsizligining buzilishiga olib kelgan holatlar bilan tasdiqlangan [8], [9].

Ayni paytda kriptografik kalitlarga oid atamalar ilmiy adabiyotlarda bir xil qo‘llanilmaydi. Xususan, asosiy kalit, kalitni almashtirish va kalitni yangilash tushunchalari ko‘pincha o‘zaro farqlanmaydi, holbuki standartlarda ular uchun turli talablar belgilangan. Mazkur ishning maqsadi kalitlarga oid asosiy tushunchalarni standartlar asosida aniqlashtirish, kalit hosil qilish usullarini qiyoslash, kalitni yangilash mexanizmlarini farqlash hamda ularning amaliy qo‘llanilishini yoritishdan iborat.

Kalitlarga oid asosiy tushunchalar

Kriptografik kalit - kriptografik algoritmda shifrlash, deshifrlash va boshqa kriptografik amallarni bajarish uchun ishlatiladigan parametrdir. NIST SP 800-133 Rev. 2 standartiga ko‘ra,

kriptografik kalitlar tasdiqlangan tasodifiy bitlar generatori (*Random Bit Generator, RBG*) chiqishidan bevosita yoki bilvosita foydalanish asosida hosil qilinadi [1]. Shu sababli, kalitning oldindan aytib bo‘lmasligi generator ta’minlaydigan entropiya miqdori va sifatiga bog‘liq.

1-jadval.

Kalitlarga oid asosiy tushunchalar

Tushuncha	Ta’rifi
Kalit-derivatsiya kaliti (master key)	Boshqa kalitlarni hosil qilish uchun kirish sifatida ishlatiladigan kalit; SP 800-57 glossariysida “master key” atamasi aynan shu tushunchaga havola qiladi
Sessiya kaliti (efemer kalit)	Kriptografik jarayonning har bir bajarilishi uchun alohida hosil qilinadigan va seans tugagach amal qilishdan to‘xtaydigan kalit
Statik kalit	Nisbatan uzoq muddat va kalit o‘rnatish sxemasining ko‘p sonli bajarilishlarida ishlatiladigan kalit
Kalit o‘rovchi kalit (KEK)	Boshqa kalitlarga nisbatan ham maxfiylik, ham butunlik himoyasini ta’minlovchi simmetrik kalit
Oldindan kelishilgan kalit (PSK)	Aloqa boshlanishidan oldin tomonlarga yetkazilgan va kalit-derivatsiya kaliti sifatida ishlatiladigan kalit
Xavfsizlik darajasi	Algoritmni buzish uchun zarur amallar soni bilan bog‘liq son; kalit uzunligi bilan majburiy ravishda mos kelmaydi
Kripto-davr	Muayyan kalitni ishlatish uchun ruxsat etilgan vaqt oralig‘i

Amaliy tizimlarda kalitlar bir-biridan mustaqil holda emas, balki iyerarxik tuzilma sifatida tashkil etiladi: uzoq muddatli kalitdan derivatsiya yo‘li bilan qisqa muddatli kalitlar hosil qilinadi. Bunday tashkil etish uzoq muddatli kalitning ishlatilish chastotasini kamaytiradi va kalitning oshkor bo‘lish oqibatlarini cheklaydi. Kalitlarga oid asosiy tushunchalar va ularning standart hujjatlardagi ta’riflari 1-jadvalda umumlashtirilgan[1,2,6,7].

Kalitlarni hosil qilish va kriptografik amallarni bajarish jarayonlarida kalitdan tashqari bir qator yordamchi parametrlar ham qo‘llaniladi. Ushbu parametrlar vazifasi va ularga qo‘yiladigan talablar jihatidan bir-biridan farq qiladi. Ularning standartlardagi ta’riflari 2-jadvalda qiyoslangan.

2-jadval

Kalit hosil qilish jarayonidagi yordamchi parametrlar

Parametr	Ta’rifi
Boshlang‘ich qiymat (seed)	DRBG ga kirish sifatida beriladigan va uning ichki holatini aniqlaydigan bitlar qatori
Tuz (salt)	Tasodifiylikni ajratib olish bosqichida MAC funksiyasining kaliti sifatida ishlatiladigan bayt qatori
Boshlang‘ich vektor (IV)	Blokli shifrlash rejimlarida ochiq matndan tashqari beriladigan qo‘shimcha boshlang‘ich kirish
Bir martalik qiymat (nonce)	Vaqtga bog‘liq o‘zgaruvchi, takrorlanish ehtimoli e’tiborga olinmaydigan darajada kichik qiymat

Simmetrik va asimmetrik kalitlarni hosil qilish

NIST SP 800-133 Rev. 2 da simmetrik kalitlarni hosil qilishning to‘rt usuli ko‘rsatilgan: RBG chiqishidan bevosita foydalanish, Diffie–Hellman yoki elliptik egri chiziqlarga asoslangan sxemalar orqali umumiy sirni hosil qilish, mavjud kalit-derivatsiya kalitidan yangi kalit yaratish va parol asosida kalit hosil qilish [1]. Dastlabki uch usulda kalit yaratish avvalgi bosqichlarda olingan tasodifiy qiymatlarga tayanadi. Standartda bunday qiymatlarning manbai *ajdod kalit* (*ancestor key*) tushunchasi bilan ifodalanadi [1].

Paroldan kalit hosil qilish alohida holat hisoblanadi: agar parol tasdiqlangan tasodifiy bitlar generatori (RBG) yordamida yaratilmagan bo‘lsa, uning entropiyasi yetarli darajada asoslanmagan deb baholanadi [1]. Bunday sxemalarda parolga qo‘shimcha ravishda tuz (salt) ishlatiladi [10]. Tuz bir xil parollardan bir xil kalitlar hosil bo‘lishining oldini olishga va lug‘at hujumlariga qarshi himoyani kuchaytirishga xizmat qiladi. Ushbu usul, asosan, ma’lumotlarni saqlash tizimlarida qo‘llaniladi.

Asimmetrik kalit juftligini hosil qilish simmetrik holatdan tubdan farq qiladi. Simmetrik kalit Asimmetrik kalit juftligini hosil qilish simmetrik usuldan farq qiladi. Simmetrik kalit belgilangan uzunlikdagi tasodifiy bitlar qatori bo‘lsa, asimmetrik kalit matematik shartlarga mos ravishda shakllantiriladi: tasodifiy qiymat asosida maxfiy kalit hisoblanadi, so‘ng unga mos ochiq kalit hosil qilinadi [1]. Shu sababli asimmetrik kalitlar generatsiyasi qo‘shimcha tekshiruvlarni talab qiladi va undagi xatoliklar kriptografik zaifliklarga olib kelishi mumkin. Bunga 2017-yilda aniqlangan ROCA zaifligi misol bo‘lib, unda tub sonlarni generatsiya qilishdagi kamchilik RSA modullarini amaliy faktorlash imkonini bergan [9].

Ikki sinf o‘rtasidagi farq kalit uzunliklarida ham namoyon bo‘ladi. SP 800-57 Part 1 Rev. 5 xavfsizlik darajasini kalit uzunligidan ajratib ko‘rsatadi [2]; qiyoslanadigan darajalar 3-jadvalda keltirilgan.

3-jadval.

Simmetrik va asimmetrik algoritmlarning qiyoslanadigan xavfsizlik darajalari [2]

Xavfsizlik darajasi, bit	Simmetrik algoritm (kalit uzunligi, bit)	DH va DSA: ochiq / maxfiy kalit, bit	RSA kalit uzunligi, bit	ECC kalit uzunligi, bit
≤ 80	2TDEA (112)	1024 / 160	1024	160–223
112	3TDEA (168)	2048 / 224	2048	224–255
128	AES-128 (128)	3072 / 256	3072	256–383
192	AES-192 (192)	7680 / 384	7680	384–511
256	AES-256 (256)	15360 / 512	15360	512 va yuqori

Jadvaldagi har bir qator bir xil xavfsizlik darajasini ta’minlovchi kalit uzunliklarini ko‘rsatadi. SP 800-57 Part 1 Rev. 5 standartiga ko‘ra, RSA uchun keltirilgan qiymat modul uzunligi, ECC uchun esa asos nuqta tartibining uzunligi bo‘lib, ikkala holatda ham ular odatda kalit uzunligi sifatida qaraladi; chekli maydon asosidagi sxemalarda (DH, DSA) ochiq va maxfiy kalit uzunliklari alohida belgilanadi [2].

Kalit uzunligi va xavfsizlik darajasining farqi simmetrik algoritmlar ustunida ham yaqqol ko‘rinadi. AES uchun ushbu ikki qiymat o‘zaro teng, chunki algoritmga qarshi barcha kalitlarni sinab ko‘rishdan samaraliroq usul ma’lum emas. 2TDEA va 3TDEA holatida esa ular farq qiladi: kalit uzunligi mos ravishda 112 va 168 bit bo‘lsada, ta’minlanadigan xavfsizlik darajasi 80 va 112 bitdan oshmaydi, chunki bu algoritmlarga qarshi to‘liq sinovdan kam ish talab qiluvchi hujumlar

mavjud [2]. Demak, kalit uzunligi kalitning o‘lchamini, xavfsizlik darajasi esa uni topishning haqiqiy murakkabligini ifodalaydi.

Jadvaldan ko‘rinadiki, 128 bitli xavfsizlik darajasini ta’minlash uchun simmetrik algoritmda 128 bitli, ECC da 256 bitli, RSA da esa 3072 bitli kalit talab etiladi. Biroq kalitning xavfsizligi uning uzunligiga va generatsiya jarayonining mustahkamligiga ham bog‘liq. Masalan, NIST SP 800-133 Rev. 2 standartiga ko‘ra, 112 bitli xavfsizlik darajasiga ega manbadan generatsiya qilingan 128 bitli AES kalitining xavfsizlik darajasi 112 bitdan oshmaydi [1]. NIST SP 800-57 Part 1 Rev. 5 standartida ham xavfsizlik darajasi tegishli jarayonning mustahkamligi bilan cheklanishi ta’kidlanadi [2]. Demak, kalit hosil qilish funksiyasi (KDF) yangi entropiya yaratmaydi, balki mavjud entropiyadan foydalanadi.

Kalitlarni yangilash va diversifikatsiya qilish

Hech bir kriptografik kalit cheksiz muddat ishlatilmaydi. NIST SP 800-57 Part 1 Rev. 5 standartida kalitdan foydalanish davrini belgilovchi kripto-davr tushunchasi keltirilgan. Uning cheklanishi kalit ostida to‘planadigan shifrmatn hajmini kamaytirish va kalit oshkor bo‘lganda yuzaga keladigan zarar ko‘lamini cheklashga xizmat qiladi [2].

NIST SP 800-57 Part 1 Rev. 5 standartida kalitni yangilash (*key update*) eski kalit asosida yangi kalit hosil qilish jarayoni sifatida ta’riflanadi [2]. Biroq buzilgan kalitni almashtirishda eski kalitdan foydalanish tavsiya etilmaydi. NIST SP 800-133 Rev. 2 standart talablariga ko‘ra, yangi kalit buzilgan kalitdan mustaqil ravishda generatsiya qilinishi lozim [1]. Aks holda, eski kalitni qo‘lga kiritgan hujumchi yangi kalitni ham hisoblab topishi mumkin.

Dastlab, bu talab amaliy protokollardagi yechimlarga zid ko‘rinishi mumkin, chunki TLS 1.3 protokolining KeyUpdate mexanizmida yangi trafik kalitlari oldingi maxfiy holatdan hosil qilinadi [7]. Biroq bu tafovut kalitni almashtirish va kalit materialini yangilash mexanizmlarini farqlash orqali izohlanadi:

- *Kalitni almashtirish (rekeying)* kriptografik davr tugaganda yoki kalit buzilganda amalga oshiriladi. Agar eski kalit oshkor bo‘lgan bo‘lsa, yangi kalit undan mustaqil ravishda, xavfsiz tasodifiy qiymatlar asosida generatsiya qilinishi kerak [1], [2].

- *Seans davomida kalit materialini yangilash* kalit ostida qayta ishlanadigan ma’lumot hajmini cheklash maqsadida amalga oshiriladi. Bunda yangi trafik kaliti oldingi maxfiy holatdan kalit hosil qilish funksiyasi (KDF) yordamida olinadi. Eski holatning o‘chirilishi va derivatsiya mexanizmining xususiyatlari oldingi kalitlarni tiklash imkoniyatini cheklashi mumkin [7].

Shunday qilib, buzilgan kalitni almashtirish va buzilmagan kalitlar iyerarxiyasi doirasida yangi kalit hosil qilish turli vazifalarni bajaradi. Derivatsiya zanjiri buzilgan kalitni xavfsiz almashtirish o‘rnini bosa olmaydi; bunday holatda mustaqil kalit generatsiyasi talab etiladi.

Kalit materialini boshqarishning yana bir mexanizmi - *kalitlarni diversifikatsiya qilish*. Bunda asosiy kalitdan har bir qurilma yoki foydalanuvchi uchun alohida kalit hosil qilinadi. Derivatsiya funksiyasiga qurilma yoki foydalanuvchining noyob identifikatori kontekst sifatida kiritiladi [6]. Bu yondashuv markazlashgan kalit boshqaruvini soddalashtiradi va har bir qurilma uchun alohida kalitlarni saqlash zaruratini kamaytiradi. Biroq asosiy kalitning oshkor bo‘lishi undan hosil qilingan barcha kalitlarni xavf ostiga qo‘yishi mumkin. Shu sababli asosiy kalitni himoyalash va derivatsiya mexanizmini to‘g‘ri tashkil etish muhim hisoblanadi.

Amaliy qo‘llanilish

Yuqorida ko‘rib chiqilgan tushunchalarning o‘zaro bog‘liqligi TLS 1.3 protokoli misolida yaqqol Kalitlarni hosil qilish mexanizmlari axborotni uzatish va saqlash, autentifikatsiya hamda

to‘lov tizimlarining muhim tarkibiy qismidir. Masalan, TLS protokolida har bir ulanish uchun alohida kalitlar hosil qilinadi va trafik kalitlari seans davomida yangilanadi [7].

Kriptografik tizim xavfsizligi kalitlarni hosil qilish jarayoniga ham bog‘liq. 2008-yilda Debian tizimida aniqlangan zaiflik va 2017-yildagi ROCA zaifligi kalit generatsiyasidagi kamchiliklar kriptografik himoyani susaytirishi mumkinligini ko‘rsatadi [8], [9].

Tahlil natijalari uch jihatdan amaliy ahamiyatga ega: kalit uzunligini xavfsizlik darajasiga muvofiq tanlash, kalitlarning maqsadi va amal qilish muddatini belgilash, shuningdek, kalitni yangilash bilan almashtirish mexanizmlarini farqlash. Xususan, oshkor bo‘lgan kalit o‘rniga undan hosil qilingan kalitni qo‘llash xavfsizlikni tiklamaydi.

Xulosa

Kalitning xavfsizlik darajasi uning uzunligiga, generatsiya manbasiga va unga ishlov berish jarayonlariga bog‘liq. Kalit derivatsiyasi yangi entropiya yaratmaydi. Simmetrik kalitlar uchun tasodifiy bitlar sifati, asimmetrik kalitlar uchun esa qo‘shimcha ravishda matematik shartlarning to‘g‘ri bajarilishi muhimdir.

Ishning asosiy natijasi kalitni almashtirish va seans davomida kalit materialini yangilash mexanizmlari farqini aniqlashtirishdan iborat. Buzilgan kalitni almashtirishda undan hosil qilingan yangi kalitga tayanib bo‘lmaydi, biroq buzilmagan kalitlar iyerarxiyasida derivatsiya orqali yangilash qo‘llanilishi mumkin. Ushbu farqlash kriptografik protokollarda kalit hosil qilish mexanizmlarini tahlil qilish uchun metodik asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar:

1. Barker E., Roginsky A. Recommendation for Cryptographic Key Generation. NIST Special Publication 800-133 Rev. 2. - Gaithersburg: NIST, 2020. - 27 p.

2. Barker E. Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1 Rev. 5. - Gaithersburg: NIST, 2020. - 171 p.

3. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A Rev. 1. - Gaithersburg: NIST, 2015. - 109 p.

4. Barker E., Chen L., Davis R. Recommendation for Key-Derivation Methods in Key-Establishment Schemes. NIST Special Publication 800-56C Rev. 2. - Gaithersburg: NIST, 2020. - 45 p.

5. Dworkin M. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38A. - Gaithersburg: NIST, 2001. - 66 p.

6. Chen L. Recommendation for Key Derivation Using Pseudorandom Functions. NIST Special Publication 800-108 Rev. 1. - Gaithersburg: NIST, 2022. - 21 p.

7. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. - IETF, 2018. - 160 p.

8. Yilek S., Rescorla E., Shacham H., Enright B., Savage S. When Private Keys are Public: Results from the 2008 Debian OpenSSL Vulnerability // Proceedings of the 9th ACM SIGCOMM Internet Measurement Conference. - New York: ACM, 2009. - P. 15–27.

9. Nemec M., Sýs M., Švenda P., Klinec D., Matyáš V. The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. - New York: ACM, 2017. - P. 1631–1648.

10. Sönmez Turan M., Barker E., Burr W., Chen L. Recommendation for Password-Based Key Derivation: Part 1 – Storage Applications. NIST Special Publication 800-132. - Gaithersburg: NIST, 2010. - 18 p.

VIDEOKUZATUV TIZIMLARI UCHUN YENGIL OQIMLI SHIFRLAR VA KICHIK HOLATLI KALIT OQIMI GENERATORLARINING QIYOSIY KRIPTOTAHLILI

Qozoqova T.Q.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda videokuzatuv tizimlarining resursi cheklangan chekka tugunlari uchun yengil oqimli shifrlar tahlil qilingan. eSTREAM portfelining apparat profili (Grain v1, Trivium, MICKEY 2.0), ISO/IEC 29192-3 va NIST SP 800-232 standartlari hamda kalitli yangilanuvchi kichik holatli generatorlar (Sprout, Plantlet, Fruit-80, Lizard, Atom, Draco) kriptotahlil holati va amalga oshirish ko‘rsatkichlari bo‘yicha qiyoslangan. Baholash natijasi platformaga bog‘liq ekani, kichik holatli konstruksiyalarda esa holat hajmi 46 % ga qisqarganda maydon atigi 24 % ga kamayishi ko‘rsatilgan. Tahlil asosida videooqim uchun yangi kalit oqimi generatorini loyihalash mezonlari shakllantirilgan.

Kalit so‘zlar: yengil oqimli shifr, videokuzatuv, kriptotahlil, Grain, Trivium, TMDTO hujumi, kichik holatli shifr, kalit oqimi generatori.

Аннотация. В тезисе проанализированы лёгкие поточные шифры для ресурсно-ограниченных периферийных узлов систем видеонаблюдения. Аппаратный профиль портфеля eSTREAM (Grain v1, Trivium, MICKEY 2.0), стандарты ISO/IEC 29192-3 и NIST SP 800-232, а также генераторы с малым внутренним состоянием и ключевым обновлением (Sprout, Plantlet, Fruit-80, Lizard, Atom, Draco) сопоставлены по состоянию криптоанализа и показателям реализации. Показано, что результат оценки зависит от платформы, а в конструкциях с малым состоянием сокращение объёма состояния на 46 % уменьшает площадь лишь на 24 %. На основе анализа сформулированы критерии проектирования нового генератора ключевого потока для видеопотока.

Ключевые слова: лёгкий поточный шифр, видеонаблюдение, криптоанализ, Grain, Trivium, TMDTO-атака, шифр с малым состоянием, генератор ключевого потока.

Kirish

IP-kameralar, sensorlar va kodlovchi modullardan iborat videokuzatuv tizimlarining chekka tugunlarida kriptografik modulga ajratiladigan maydon, quvvat va kechikish byudjeti qat’iy cheklangan. Bunday sharoitda oqimli shifrlar blokli shifrlarga nisbatan afzalroq: siljish registrlari apparatda ixcham amalga oshiriladi, kechikish blok hajmiga bog‘liq emas, sinxron rejimda esa xatolik keyingi bitlarga tarqalmaydi bu siqilgan video uchun muhim.

Biroq sohada jiddiy muammo mavjud: taklif qilingan yengil oqimli shifrlarning katta qismi mustaqil kriptotahlil sinovidan o‘tmaydi. Manifavas va hamkasblarining keng qamrovli sharhiga ko‘ra, tekshirilgan 31 ta dizayndan faqat 6 tasi xavfsiz deb topilgan [1]. Standartlashtirilgan yechimlar ham kam: ISO/IEC 29192-3 faqat Trivium va Enocoro ni qamraydi, NIST SP 800-232 dagi Ascon esa permutatsiyaga asoslangan AEAD sxemasi bo‘lib, oqimli shifr emas. Tezisning maqsadi klassik va kichik holatli yengil oqimli shifrlarni kriptotahlil holati hamda amalga oshirish ko‘rsatkichlari bo‘yicha qiyosiy tahlil qilish va videokuzatuv tizimi uchun kalit oqimi generatorini loyihalash mezonlarini asoslashdan iborat.

Asosiy qism

Klassik konstruksiyalar va ularning kriptotahlil holati. eSTREAM loyihasining apparat profili (Profil 2) yakuniy portfeliga Grain v1, Trivium va MICKEY 2.0 kiritilgan. Grain v1 80 bitli

LFSR va 80 bitli NFSR dan iborat 160 bitli holatga ega, chiqish nochiziqli filtr funksiyasi orqali shakllanadi va qo‘shimcha apparat hisobiga bir taktda 16 bitgacha kalit oqimi olinadi [2]. Trivium uchta aylanma registrdan iborat 288 bitli holatga va 1152 taktli initsializatsiyaga ega [3]. MICKEY 2.0 notekis taktlashga asoslangan: bu xususiyat hujumlarni murakkablashtirsa-da, parallellashtirishni deyarli imkonsiz qiladi. 128 bitli xavfsizlik darajasida oqimli shifr sinfidagi yagona zamonaviy AEAD yechimi - NIST LWC finalchisi Grain-128AEADv2 (kalit 128 bit, nonce 96 bit, holat 256 bit, teg 64 bit) [4]. Ushbu shifrlarning parametrlari va kriptotahlil holati 1-jadvalda keltirilgan.

1-jadval

eSTREAM portfeli shifrlarining kriptotahlil holati

Shifr	Kalit / IV; holat, bit	Eng kuchli ma’lum natija	Baho
Grain v1	80 / 64; 160	Tez korrelyatsion hujum, 275,1 bit kalit oqimi	Amalda erishib bo‘lmaydi
Grain-128a	128 / 96; 256	Tez korrelyatsion hujum, 2113,8 bit kalit oqimi	Amalda erishib bo‘lmaydi
Trivium	80 / 80; 288	Kub hujumi 832/1152 raund, < 250	To‘liq versiya buzilmagan
MICKEY 2.0	80 / 0–80; 200 + 7	Differensial xatolik hujumi, 214,7 inyeksiya	Jismoniy kirishda real tahdid
Salsa20	256 / 64; 512	Korrelyatsion quvvat tahlili, 20 000 so‘rov	Apparatda qarshi chora shart

Kriptotahlil natijalari shuni ko‘rsatadiki, Grain oilasining to‘liq versiyalariga qarshi ma’lum bo‘lgan yagona hujum tez korrelyatsion hujum bo‘lib, u $2^{75,1}$ (Grain v1) va $2^{113,8}$ (Grain-128a) bit kalit oqimini talab qiladi [5]; bunday hajmni bitta kalit/IV juftligidan olish amalda mumkin emas. Triviumning to‘liq versiyasi buzilmagan, kub hujumi esa 1152 raunddan 832 tasigacha yetib boradi. MICKEY 2.0 ga qarshi matematik hujum e’lon qilinmagan, ammo SAT-yechuvchi qo‘llangan differensial xatolik hujumi $2^{14,7}$ ta xatolik inyeksiyasi bilan butun ichki holatni tiklaydi [6] jismonan ochiq joyda o‘rnatilgan kamera uchun bu real tahdid. Dasturiy tezlik bo‘yicha yetakchi Salsa20 esa apparat amalga oshirishda korrelyatsion quvvat tahliliga zaif: barcha kalit so‘zlari 20 000 so‘rovda tiklanadi, qarshi chora maydonni 14 % ga oshiradi [7]. Demak, baholash mezonlariga yon kanal chidamliligi ham kiritilishi shart.

Platformaning baholashdagi roli. Amalga oshirish ko‘rsatkichlari turli platformalarda qarama-qarshi natija beradi. FPGA (Xilinx Virtex-II) da o‘tkazuvchanlikning maydonga nisbati Trivium uchun 5,05, Grain-128 uchun 3,77, MICKEY-128 2.0 uchun esa atigi 1,05 ni tashkil etadi [8]. ARM protsessorida real videooqimni shifrlashda esa manzara teskari: so‘z yo‘naltirilgan Sosemanuk va Salsa20 eng yuqori kadr/sekund va eng past energiya sarfini, bit yo‘naltirilgan Grain v1, MICKEY va Trivium esa eng past natijani ko‘rsatgan [9]. Demak, baholashda platforma g‘olibni belgilaydi va turli manbalar raqamlarini to‘g‘ridan-to‘g‘ri birlashtirib bo‘lmaydi. Shu sababli yadro ko‘rsatkichlari apparat sintezida, tizim ko‘rsatkichlari esa real chekka platformada o‘lchanishi lozim.

Kichik holatli kalitli yangilanuvchi generatorlar. Ichki holat hajmining quyi chegarasi vaqt–xotira–ma’lumotlar almashuvi (TMDTO) hujumlaridan kelib chiqadi. Holat hajmi n bit, holatlar fazosi $N = 2^n$ bo‘lganda Babbage–Golić almashuvi

$$TM = N,\ P = M,\ T \le D \quad (1)$$

muvozanat nuqtasida $2^{n/2}$ murakkablikni beradi, Biryukov–Shamir almashuvi esa

$$TM^2D^2 = N^2,\ P = N/D \quad (2)$$

ko‘rinishga ega [10]. Bu yerda T - onlayn vaqt, M - xotira, D - kalit oqimi hajmi, P - oldindan hisoblash. Shu sababli k bitli xavfsizlik uchun $n \ge 2k$ sharti talab qilinadi va 128 bitli darajada holat kamida 256 bit bo‘ladi. 2015-yildan boshlab bu cheklovni chetlab o‘tish uchun maxfiy kalitni kalit oqimi hosil qilish bosqichida ham holat yangilanishiga jalb qilish g‘oyasi rivojlandi: holat tiklangan taqdirda ham oqimni kalitsiz davom ettirib bo‘lmaydi. Kalitning ishlatilishiga ko‘ra uch sinf ajratiladi: kalitdan uzluksiz foydalanish (CKEY - Sprout, Plantlet, Fruit-80, Atom), kalitni initsializatsiya oxirida qayta qo‘shish (FP(1) Lizard) [11] hamda IV va kalit prefiksidan uzluksiz foydalanish (CIVK - Draco) [12]. Ularning parametrlari va kriptotahlil holati 2-jadvalda jamlangan.

Tahlil uchta takrorlanuvchi naqshni ko‘rsatadi. Birinchidan, raund kaliti funksiyasi eng zaif bo‘g‘in bo‘lib chiqdi: Sproutda u ko‘p taktlarda kalit ta’sirini o‘chirib qo‘ygan va shifr e’lon qilingan yiliyoq buzilgan [13]. Ikkinchidan, kalit oqimi uzunligiga qo‘yilgan cheklov nazariy emas, amaliy shartdir: 4 Mbit/s tezlikdagi H.264 oqimi uchun Draconing 2^{32} bitlik chegarasi taxminan 18 daqiqalik, Lizardning 2^{18} bitlik chegarasi esa atigi 0,07 soniyalik uzluksiz yozuvga teng, ya’ni Lizard faqat har bir kadr yoki paket uchun yangi IV bilan qo‘llanishi mumkin. Uchinchidan, isbotlangan xavfsizlik model chegarasida qoladi: Draconing TMDTO ga qarshi formal isboti tanlangan IV hujumi oldida o‘z kuchini yo‘qotgan [14].

2-jadval

Kichik holatli oqimli shifrlarning parametrlari va kriptotahlil holati

Shifr (yili)	Holat, bit / maydon, GE	Sinf	Kriptotahlil holati
Grain v1 (2007)	160 / 1270	klassik	Barqaror (taqqoslash uchun)
Sprout (2015)	80 / 813	CKEY	To‘liq buzilgan, ≈ 269 shifrlash [13]
Plantlet (2017)	101 / 996	CKEY	Korrelyatsion hujum, ma’lumot cheklovi majburiy [15]
Fruit-80 (2018)	87 / 960	CKEY	Tez korrelyatsion hujum, vaqt 272,71 [15]
Lizard (2017)	121 / 1218	FP(1)	Da’voga mos; kalit oqimi ≤ 218 bit
Atom (2021)	159 / -	CKEY	Differensial xatolik hujumi
Draco (2022)	128 / -	CIVK	Tanlangan IV bilan 2107 (240 IV) [14]

Maydon bo‘yicha yutuq ham kutilganidan kam: holat hajmi 160 bitdan 87 bitgacha (46 % ga) qisqarganda maydon 1270 GE dan 960 GE gacha, ya’ni atigi 24 % ga kamayadi [16]. Sababi - uzluksiz kalit murojaati multipleksor va boshqaruv mantig‘ini talab qiladi, kalit esa o‘zgarmas xotiraga ko‘chadi, xolos. Muvaffaqiyatsizliklar sababi paradigmaning o‘zida emas, balki komponentlarni tanlashning tizimsizligida. Sarkar metodikasi [5] Bul funksiyalarini algebraik immunitet, rezilyentlik va nochiziqlilik bo‘yicha tizimli tanlash, NSIG initsializatsiyasi va tap pozitsiyalari uchun korrelyatsiya shartlarini beradi.

Xulosa

O‘tkazilgan qiyosiy tahlil natijasida eSTREAM portfeli shifrlaridan apparat yo‘nalishi uchun eng ishonchlisi Grain oilasi ekani, MICKEY 2.0 esa notekis taktlash, parallellashtirishning imkonsizligi va xatolik hujumiga zaifligi sababli videokuzatuv tizimlari uchun nomzod bo‘la olmasligi aniqlandi. Kichik holatli konstruksiyalardan faqat Lizard nisbatan barqaror qolgan,

ularning hech biri AEAD emas. Dissertatsiyada taklif etiladigan kalit oqimi generatorini loyihalash uchun quyidagi mezonlar shakllantirildi:

1) TMDTO hujumining kalitni tiklash va farqlovchi variantlari alohida baholanishi;

2) raund kaliti funksiyasi kalit ta'sirini hech bir taktda yo'qotmasligi va uni registrlar bo'ylab tekis tarqatishi;

3) bitta kalit/IV juftligi uchun kalit oqimi uzunligi aniq cheklanishi va bu cheklov kadrlar guruhi darajasida majburlanishi;

4) Bul funksiyalari va tap pozitsiyalari tasodifiy qidiruv bilan emas, [5] metodikasi asosida tizimli tanlanishi;

5) kalitni o'zgarmas xotirada doimiy saqlash yon kanal tahdidini oshirgani uchun FP(1) tipidagi yechimga ustunlik berilishi;

6) autentifikatsiya dizaynga boshidan kiritilishi, baholash esa apparat va chekka platformada alohida o'tkazilishi.

Foydalanilgan adabiyotlar

1. Manifavas C., Hatzivasilis G., Fysarakis K., Papaefstathiou I. A survey of lightweight stream ciphers for embedded systems // Security and Communication Networks. – 2016. – Vol. 9(10). – P. 1226–1246.

2. Hell M., Johansson T., Meier W. Grain: a stream cipher for constrained environments // International Journal of Wireless and Mobile Computing. – 2007. – Vol. 2(1). – P. 86–93.

3. De Cannière C., Preneel B. Trivium // New Stream Cipher Designs: The eSTREAM Finalists. LNCS 4986. – Springer, 2008. – P. 244–266.

4. Hell M., Johansson T., Maximov A., Meier W., Sönnerup J., Yoshida H. Grain-128AEADv2: a lightweight AEAD stream cipher. – NIST Lightweight Cryptography Project, 2021.

5. Sarkar P. The Grain family of stream ciphers: an abstraction, strengthening of components and new concrete instantiations. – arXiv:2511.12981, 2025.

6. Banik S., Maitra S., Sarkar S. Improved differential fault attack on MICKEY 2.0 // IACR Cryptology ePrint Archive. – 2013. – Report 2013/029.

7. Mazumdar B., Ali S.S., Sinanoglu O. A compact implementation of Salsa20 and its power analysis vulnerabilities // ACM Transactions on Design Automation of Electronic Systems. – 2017. – Vol. 22(1). – Art. 11.

8. Bulens P., Kalach K., Standaert F.-X., Quisquater J.-J. FPGA implementations of eSTREAM phase-2 focus candidates with hardware profile. – UCL Crypto Group, 2006.

9. Khan M., Dagenborg H., Johansen D. Performance evaluation of lightweight stream ciphers for real-time video feed encryption on ARM processor // Future Internet. – 2024. – Vol. 16(8). – 261.

10. Biryukov A., Shamir A. Cryptanalytic time/memory/data tradeoffs for stream ciphers // ASIACRYPT 2000. LNCS 1976. – Springer, 2000. – P. 1–13.

11. Hamann M., Krause M., Meier W. LIZARD – a lightweight stream cipher for power-constrained devices // IACR Transactions on Symmetric Cryptology. – 2017. – No. 1. – P. 45–79.

12. Hamann M., Moch A., Krause M., Mikhalev V. The DRACO stream cipher: a power-efficient small-state stream cipher with full provable security against TMDTO attacks // IACR Transactions on Symmetric Cryptology. – 2022. – No. 2. – P. 1–42.

13. Lallemand V., Naya-Plasencia M. Cryptanalysis of full Sprout // CRYPTO 2015. LNCS 9215. – Springer, 2015. – P. 663–682.

14. Banik S. Cryptanalysis of Draco // IACR Cryptology ePrint Archive. – 2022. – Report 2022/749.

15. Todo Y., Meier W., Aoki K. On the data limitation of small-state stream ciphers: correlation attacks on Fruit-80 and Plantlet // SAC 2019. LNCS 11959. – Springer, 2020. – P. 365–392.

16. Ghafari V.A., Hu H. Fruit-80: a secure ultra-lightweight stream cipher for constrained environments // Entropy. – 2018. – Vol. 20(3). – 180.

TLS 1.2 VA TLS 1.3 DA KALIT HOSIL QILISH FUNKSIYALARI: MILLIY ALGORITMLAR ASOSIDA QO‘LLASH TAJRIBASI VA O‘ZBEKISTON UCHUN IMKONIYATLAR

Xudoykulov Z.T., Qutlimurotov A.H.
Muhammad al-Xorazmiy nomidagi TATU

Annotatsiya. Maqolada psevdotasodifiy funksiya (PRF), kalit hosil qilish funksiyasi (KDF) va HKDFning vazifalari, xavfsizlik talablari va loyihalash tamoyillari, TLS 1.2 dagi PRF va TLS 1.3 dagi HKDF asosidagi kalitlar jadvali tahlil qilingan. Rossiya, Belarus va Xitoy profillarida milliy algoritmlar kalit hosil qilishning qaysi bosqichiga kiritilgani birlamchi spetsifikatsiyalar bo‘yicha aniqlangan: TLS profillarida konstruktsiya va jadval saqlanib, HMAC ichidagi xesh almashtirilgan. O‘zbekiston uchun HKDFni O‘zMSt 285:2024 xeshi bilan parametrizatsiyalash boshlang‘ich yo‘nalish sifatida baholangan.

Kalit so‘zlar: PRF; KDF; HKDF; HMAC; kalitlar jadvali; TLS 1.2; TLS 1.3; GOST; STB; SM3; TLCP; O‘zMSt 285:2024.

Аннотация. Рассмотрены назначение, требования безопасности и принципы построения PRF, KDF и HKDF, а также схемы выработки ключей на основе PRF в TLS 1.2 и HKDF в TLS 1.3. По первичным спецификациям установлено, на каком этапе национальные алгоритмы применяются в профилях России, Беларуси и Китая: в профилях TLS конструкция и схема ключей сохранены, заменена хэш-функция внутри HMAC. Для Узбекистана исходным направлением оценена параметризация HKDF хэш-функцией O‘zMSt 285:2024.

Ключевые слова: PRF; KDF; HKDF; HMAC; схема выработки ключей; TLS 1.2; TLS 1.3; ГОСТ; СТБ; SM3; TLCP; O‘zMSt 285:2024.

Kirish

TLS (Transport Layer Security – transport qatlam xavfsizligi) da kalit hosil qilish qo‘l siqishdagi umumiy sirni - yozuvlarni himoyalash, Finished xabari, seansni tiklash va eksport uchun mustaqil kalitlarga aylantiradi. TLS 1.2 da bu vazifani PRF (Pseudorandom Function – psevdotasodifiy funksiya), TLS 1.3 da HKDF (HMAC-based Extract-and-Expand Key Derivation Function – HMAC asosidagi ajratish va kengaytirish orqali kalit hosil qilish funksiyasi) bajaradi. TLS 1.3 ning amaldagi spetsifikatsiyasi – IETF (Internet Engineering Task Force – Internet muhandisligi ishchi guruhi) ning 2026-yil iyulidagi Proposed Standard maqomli RFC (Request for Comments – sharhlar uchun so‘rov) 9846 bo‘lib, u RFC 8446, RFC 5246 va RFC 7627 ni bekor qiladi [1]. Maqsad – milliy profillarda aynan qaysi komponent o‘zgarganini aniqlash va O‘zbekiston uchun asosli yo‘lni baholash.

PRF, KDF va HKDF: vazifalari va xavfsizlik talablari

PRF – maxfiy kalit bilan belgilanadigan funksiyalar oilasi bo‘lib, kalitni bilmagan va hisoblash resurslari chegaralangan hujumchi uni tasodifiy funksiyadan sezilarli ehtimol bilan ajrata olmaydi. KDF (Key Derivation Function – kalit hosil qilish funksiyasi) dastlabki kalit materialidan belgilangan maqsadlar uchun kalitlar hosil qiluvchi konstruktsiya bo‘lib, odatda PRF asosida quriladi; HKDF esa aniq spetsifikatsiyalangan KDF dir. TLS dagi ikkala konstruktsiyada PRF sifatida HMAC (Hash-based Message Authentication Code – xesh asosidagi xabar autentifikatsiya kodi) [2] ishlatiladi. Uning PRF sifatidagi xavfsizligi xeshning kolliziyaga

bardoshliligidan emas, siqish funksiyasining PRF xossasiga egaligi farazidan kelib chiqadi [3]; kolliziyaga bardoshlilik ham, statistik tasodifiylik testlari ham KDF xavfsizligini isbotlamaydi.

HKDF [4], [5] da ajratish (extract) yetarli entropiyali, lekin notekis ma'lumotdan psevdotasodifiy kalit oladi, kengaytirish (expand) undan kontekstga bog'langan kalit materialini hosil qiladi:

$$\mathrm{PRK} = \mathrm{HKDF-Extract}(\mathrm{salt}, \mathrm{IKM}) = \mathrm{HMAC-Hash}(\mathrm{salt}, \mathrm{IKM}), \quad (1)$$

$$\mathrm{OKM} = \mathrm{HKDF-Expand}(\mathrm{PRK}, \mathrm{info}, \mathrm{L}) = \mathrm{T}(1) \parallel \mathrm{T}(2) \parallel \ldots,$$

$$\mathrm{T}(\mathrm{i}) = \mathrm{HMAC-Hash}(\mathrm{PRK}, \mathrm{T}(\mathrm{i}-1) \parallel \mathrm{info} \parallel \mathrm{i}). \quad (2)$$

Bu yerda, IKM (Input Keying Material – kirish kalit materiali) – masalan, Diffi–Xellman natijasi; salt – maxfiy bo'lmasligi mumkin bo'lgan ixtiyoriy qiymat (berilmasa HashLen nol bayt); PRK (Pseudorandom Key – psevdotasodifiy kalit) – HashLen baytli oraliq kalit; info – maqsad va kontekst; OKM (Output Keying Material – chiqish kalit materiali) – birinchi L bayt, T(0) bo'sh, i – bir baytli hisoblagich, $L \leq 255 \cdot \mathrm{HashLen}$ [5]. HKDF saltining vazifasi ajratishni kuchaytirish bo'lib, parolli funksiyalardagi kabi lug'at hujumini sekinlashtirish emas.

KDF entropiyani ko'paytirmaydi: chiqish xavfsizligi IKM entropiyasi va primitiv xavfsizlik darajasining kichigi bilan cheklanadi. Yuqori entropiyali kalitdan hosil qilishda kengaytirish yetarli [6], kalit kelishuvi natijasi uchun ajratish va kengaytirish kerak [7], parollar uchun esa ataylab sekinlashtirilgan PBKDF2 (Password-Based Key Derivation Function 2 – parolga asoslangan kalit hosil qilish funksiyasi 2) kabi funksiyalar qo'llanadi [8]; HKDF ularning o'rnini bosmaydi. Vazifalar, tomonlar va seanslar kalitlari foydalanish sohalarini ajratish (domain separation) – yorliq (label), kontekst (context) va chiqish uzunligini kirishga qo'shish orqali mustaqil amalga oshiriladi; bu parametrlar uzunlik maydonlari bilan bir ma'noli kodlanishi lozim. Bitta hosil qilingan kalit oshkor bo'lsa boshqalari himoyalangan qoladi, ammo PRK yoki asosiy sir oshkor bo'lsa, barcha hosila kalitlar fosh bo'ladi. Amalga oshirishda o'zgarmas vaqtli HMAC, oraliq sirlarni o'chirish va yon-kanal hujumlaridan himoya talab etiladi.

Loyihalash va baholash tartibi

KDF ni loyihalash yoki milliy primitivga moslashtirish ketma-ketligi: (1) foydalanish holati, tahdid modeli va xavfsizlik darajasi; (2) IKM manbai, formati va entropiyasi; (3) primitiv va konstruktsiya – NIST (National Institute of Standards and Technology – AQSh Milliy standartlar va texnologiyalar instituti) SP 800-108 Rev. 1 HMAC, CMAC (Cipher-based Message Authentication Code – blokli shifr asosidagi xabar autentifikatsiya kodi) yoki KMAC (KECCAK Message Authentication Code – KECCAK asosidagi xabar autentifikatsiya kodi) bilan hisoblagich, teskari aloqa va qo'sh konveyer rejimlarini [6], SP 800-56C Rev. 2 esa kalit kelishuvidan keyingi sxemalarni [7] belgilaydi; (4) yorliq, kontekst, salt va uzunliklarning kodlanishi; (5) kalitlar iyerarxiyasi va foydalanish chegaralari; (6) xavfsizlik asoslari, kriptotahlil va amalga oshirishni baholash; (7) sinov vektorlari, muvofiqlik sinovlari va standartlashtirish. TLS kalitlar jadvali bitta sirdan turli yorliqlar bilan turli vazifa kalitlarini hosil qiluvchi iyerarxiyaga namunadir.

TLS 1.2 va TLS 1.3 dagi kalit hosil qilish

TLS 1.2 da [9] PRF HMAC asosidagi P_hash orqali aniqlanadi:

$$\mathrm{PRF}(\mathrm{secret}, \mathrm{label}, \mathrm{seed}) = \mathrm{P}_{\mathrm{hash}}(\mathrm{secret}, \mathrm{label} \parallel \mathrm{seed}), \quad (3)$$

$$\mathrm{P}_{\mathrm{hash}}(\mathrm{s}, \mathrm{d}) = \mathrm{HMAC}(\mathrm{s}, \mathrm{A}(1) \parallel \mathrm{d}) \parallel \mathrm{HMAC}(\mathrm{s}, \mathrm{A}(2) \parallel \mathrm{d}) \parallel \ldots,$$

$$\mathrm{A}(0) = \mathrm{d},\ \mathrm{A}(\mathrm{i}) = \mathrm{HMAC}(\mathrm{s}, \mathrm{A}(\mathrm{i}-1)). \quad (4)$$

Bunda, secret (s) – kalit, label – ASCII yorliq, seed (d) – tasodifiy qiymatlar yoki transkript xeshi. RFC 5246 to'plamlari PRF uchun SHA (Secure Hash Algorithm – xavfsiz xesh algoritmi)

oilasidagi SHA-256 ni ishlatadi, yangi to‘plamlar esa o‘z PRF xeshini belgilaydi; u imzodagi xeshdan farq qilishi mumkin, TLS 1.0/1.1 dagi ikki xeshli PRF esa TLS 1.2 da qo‘llanmaydi [9]. Asosiy seans siri master_secret = PRF(pre_master_secret, “master secret”, ClientHello.random ‖ ServerHello.random)[0..47]. EMS (Extended Master Secret – kengaytirilgan asosiy seans siri) da yorliq “extended master secret”, seed esa qo‘l siqish xabarlari xeshi (session_hash) bo‘lib, sir transkriptga bog‘lanadi [10]; mexanizm endi RFC 9846 da “extended_main_secret” nomi bilan berilgan [1]. key_block = PRF(master_secret, “key expansion”, server_random ‖ client_random) ketma-ket MAC (Message Authentication Code – xabar autentifikatsiya kodi) kalitlari, shifrlash kalitlari va IV (Initialization Vector – initsializatsiya vektori) larga bo‘linadi; Finished xabaridagi verify_data master_secret, “client finished”/”server finished” va transkript xeshidan (odatda 12 bayt) olinadi [9].

TLS 1.3 da [1] HKDF ikki yordamchi funksiya orqali qo‘llanadi:

$$\mathrm{HKDF-Expand-Label}(\mathrm{S},\mathrm{L},\mathrm{C},\mathrm{n}) = \mathrm{HKDF-Expand}(\mathrm{S},\mathrm{HkdfLabel},\mathrm{n}), \quad (5)$$

$$\mathrm{Derive-Secret}(\mathrm{S},\mathrm{L},\mathrm{M}) = \mathrm{HKDF-Expand-Label}(\mathrm{S},\mathrm{L},\mathrm{TH(M)},\mathrm{Hash.length}). \quad (6)$$

Bunda, S – sir, L – yorliq, C – kontekst, n – uzunlik, M – qo‘l siqish xabarlari, TH(M) – ularning transkript xeshi (Transcript-Hash). HkdfLabel – oddiy biriktirish emas, uzunlik maydonli tuzilma: 2 baytli Length, oldiga “tls13 “ qo‘shilgan 7–255 baytli yorliq va 0–255 baytli kontekst. Jadval uchta HKDF-Extract dan iborat: PSK (Pre-Shared Key – oldindan kelishilgan kalit) dan dastlabki sir, (EC)DHE ((Elliptic Curve) Diffie–Hellman Ephemeral – (elliptik egri chiziqli) efemer Diffi–Xellman) natijasidan qo‘l siqish siri va nol kirishdan asosiy sir (Main Secret); keyingi Extract saltlari oldingi sirdan “derived” yorlig‘i bilan olinadi. Mijoz va server sirlari alohida yorliqlar (“c hs traffic”, “s ap traffic” va h.k.) bilan transkriptning tegishli qismiga bog‘lanadi; AEAD (Authenticated Encryption with Associated Data – qo‘shimcha ma’lumotli autentifikatsiyalangan shifrlash) uchun trafik kaliti va IV “key”, “iv”, Finished kaliti “finished”, kalit yangilash “traffic upd”, eksport “exp master”, seansni tiklash “res master” yorlig‘i bilan olinadi [1]. Eksport va tiklashda HKDF-Expand kolliziyaga bardoshli bo‘lishi, ya’ni xesh kolliziyaga bardoshli va chiqish kamida 256 bit bo‘lishi talab etiladi [1].

Qiyoslaganda, TLS 1.2 da bitta PRF asosiy sir va key_block uchun ishlatiladi, transkript faqat EMS va Finished orqali bog‘lanadi, kalitlar key_block dan pozitsiya bo‘yicha ajratiladi; TLS 1.3 da ajratish va kengaytirish bo‘lingan, har bir sir o‘z yorlig‘i va transkript qismi bilan olinadi. Oldingi seanslar maxfiyligini saqlash (forward secrecy) HKDF emas, efemer (EC)DHE va sirlarni o‘chirish ta’minlaydi: faqat PSK yoki statik RSA (Rivest–Shamir–Adleman – RSA kriptotizimi) kalit almashinuvida bu xossa yo‘q.

Milliy profillarda PRF va KDF qanday o‘zgartirilgan

Milliy algoritm uch darajada kiritilishi mumkin: parametrizatsiyalash (HMAC xeshini almashtirish), qo‘shimcha mexanizm (jadvaldan keyingi milliy KDF yoki kalit yangilash) va konstruktsiyani almashtirish. Milliy shifr yoki imzo kiritilishi PRF/KDF almashtirilganini anglatmaydi.

Rossiya. RFC 9189 (TLS 1.2) [11] va RFC 9367 (TLS 1.3) mustaqil oqimdagi Informational RFC lar, IETF standarti emas. TLS 1.2 dagi PRF_TLS_GOSTR3411_2012_256 – RFC 5246 dagi P_hash, HMAC ichida GOST (Государственный стандарт, State Standard – davlat standarti) R 34.11-2012 ning 256 bitli xeshi bilan [12]; asosiy sir va key_block tartibi saqlangan, CTR_OMAC to‘plamlarida verify_data 32 bayt [11]. Dastlabki sir server kaliti asosida VKO va KDF_TREE_GOSTR3411_2012_256 bilan olingan kalitda eksport qilinadi – bu kalit kelishuvi bosqichidagi milliy KDF bo‘lib, PRF o‘rnini bosmaydi va forward secrecy bermaydi

[11]. TLS 1.3 da HKDF va jadval o‘zgarmagan, xesh – GOST R 34.11-2012 [13]. Ikkala profildagi TLSTREE trafik kalitidan har bir yozuv uchun KDF_GOSTR3411_2012_256 = HMAC(K, 0x01 ‖ label ‖ 0x00 ‖ seed ‖ 0x01 ‖ 0x00) asosida uch bosqichli daraxt quradi [12]; u jadvaldan keyin, yozuvlarni himoyalashda ishlaydi va bitta kalit bilan himoyalanadigan hajmni cheklaydi [11, 13].

Belarus. TLS 1.2 uchun RFC 5246 asosidagi STB (STandards of Belarus – Belarus standartlari) 34.101.65-2014 PRF ni STB 34.101.47 dagi HMAC rejimli generator bilan aniqlaydi: kalit – secret, sinxropaket – label ‖ seed, xesh shifr to‘plami bilan belgilanadi [14, 15]. Generator (r ← hmac(K, S); Y_i ← hmac(K, r ‖ S); r ← hmac(K, r)) P_hash bilan tuzilmaviy jihatdan bir xil; asosiy sir bandini va EMS ni tekshirish uchun standartning to‘liq matni kerak. TLS 1.3 uchun STB 34.101.90-2026 va uni tanituvchi Internet-Draft (RFC emas, identifikatorlari vaqtinchalik) mavjud; Internet-Draft xesh sifatida belt-hash yoki bash256 ni belgilab, kalit hosil qilishni to‘liq RFC 9846 ga qoldiradi, biroq HMAC blok uzunligini ko‘rsatmaydi [16]. belt-che256 kalitini 2^{32} yozuvdan keyin yangilash – foydalanish chegarasi, KDF emas.

Xitoy. RFC 8998 (Informational, mustaqil oqim) TLS 1.3 da SM3 ni to‘plam xeshi sifatida belgilaydi, kalit hosil qilish TLS 1.3 ga muvofiq bo‘lishi va SM2 kalit almashish protokoli qo‘llanmasligini talab qiladi [17] – faqat HKDF xeshi parametrlangan. TLCP (Transport Layer Cryptography Protocol – transport qatlam kriptografik protokoli) mustaqil protokol [18]; standart matni ochiq topilmagani uchun qoidalari muvofiqlikni e’lon qilgan ochiq amalga oshirish kodi [19] bo‘yicha tavsiflandi va standart bilan tekshirilishi kerak: PRF – HMAC-SM3 li P_hash, asosiy sir 48 bayt, verify_data 12 bayt; ECC (Elliptic Curve Cryptography – elliptik egri chiziqlar kriptografiyasi) to‘plamlarida dastlabki sir server shifrlash kaliti bilan SM2 orqali shifrlanadi, ECDHE to‘plamlarida esa ikki tomon kalitlaridan SM2 kalit almashish algoritmi (o‘z SM3 asosidagi KDF i bilan) orqali hosil qilinadi. Demak, SM2 KDF dastlabki sirni shakllantirishda, HMAC-SM3 PRF esa keyingi bosqichda ishlaydi.

1-jadval

Milliy profillarda kalit hosil qilishga kiritilgan o‘zgarishlar [11–19]

Profil, maqom	Bazaviy PRF/KDF	Milliy primitiv	O‘zgarish	Qo‘shimcha; jadval
RU, TLS 1.2: RFC 9189 (Inf.)	P_hash	GOST R 34.11-2012	Faqat xesh	TLSTREE, eksport KDF; saqlangan
RU, TLS 1.3: RFC 9367 (Inf.)	HKDF	GOST R 34.11-2012	Faqat xesh	TLSTREE; saqlangan
BY, TLS 1.2: STB 34.101.65	brng-hmac (P_hash)	to‘plam xeshi	Xesh	Aniqlanmadi; saqlangan
BY, TLS 1.3: STB 34.101.90; I-D	HKDF	belt-hash, bash256	Faqat xesh	Yo‘q; saqlangan
CN, TLS 1.3: RFC 8998 (Inf.)	HKDF	SM3	Faqat xesh	Yo‘q; saqlangan
CN, TLCP: GB/T 38636	P_hash*	HMAC-SM3, SM2 KDF	Dastlabki sir	TLS 1.2 ga o‘xshash*

RU – Rossiya, BY – Belarus, CN – Xitoy; Inf. – Informational RFC; I-D – Internet-Draft; * – ochiq amalga oshirish bo‘yicha [19].

Parametrizatsiyalash kutubxonaga xesh va to‘plam identifikatorini qo‘shish bilan amalga oshadi va eng kam o‘zgarish talab qiladi; TLSTREE kabi mexanizm yozuvlar qatlamini

o‘zgartiradi va alohida tahlil talab qiladi, TLCP kabi mustaqil protokol esa butun kalit hosil qilishni qayta tahlil qilishni taqozo etadi.

O‘zbekiston uchun imkoniyatlar va cheklovlar

O‘zMSt 285:2024 [20] da 1-algoritm 256 bitli blok va chiqishga ega, xabarga uzunlik va nazorat summasi bloklarini qo‘shadi va 256 bitli k parametrini qabul qiladi; 2-algoritm qadam funksiyasida 64 bitli shifrni ishlatadi va qayd etiladigan boshlang‘ich vektor H ga ega. O‘zMSt 270:2024 dagi funksional kalitni xesh orqali yangilash shifrning ichki mexanizmi, TLS KDF emas [21]; kalit kelishuvi bo‘yicha milliy standart yo‘q.

A variant – parametrizatsiyalash. TLS 1.3 HKDF va TLS 1.2 P_hash saqlanib, HMAC xeshi O‘zMSt 285 bilan almashtiriladi. Shartlar: HMAC blok uzunligi B (1-algoritm uchun 32 bayt) va chiqish 32 bayt belgilanishi; k (yoki H) ning yagona ochiq qiymati qayd etilishi – standartda u faqat nazorat misolida berilgan; siqish funksiyasining PRF xossasi va kolliziyaga bardoshliligi bo‘yicha mustaqil tahlil, chunki HMAC isbotlari uzunlik va nazorat summasi bloklari bo‘lgan tuzilmaga avtomatik ko‘chmaydi. TLS 1.3 da HKDF-Expand-Label, transkript bilan bog‘lanish va kalitlarni ajratish qoidalari o‘zgarmaydi, transkript xeshi va Finished 32 bayt bo‘ladi; xesh to‘plam identifikatori bilan tanlangani uchun yangi kengaytma yoki KDF tanlash mexanizmi kerak emas. TLS 1.2 da P_hash EMS bilan qo‘llanadi. Xesh nomini kodda almashtirish yetarli emas: sinov vektorlari va muvofiqlik sinovlari zarur.

B variant – qo‘shimcha mexanizm. Jadvaldan keyingi kalitlar daraxti yoki davriy yangilash faqat aniq talab bilan asoslanadi, masalan, yozuvlarda 64 bitli shifr ishlatilsa hajmni cheklash uchun (TLSTREE ga o‘xshash); u yozuvlar qatlamiga kiritiladi, ikki tomonda tartib raqami bo‘yicha bir xil hisoblanishi va TLS 1.3 KeyUpdate bilan solishtirib asoslanishi kerak; mexanizmning o‘zi xavfsizlikni oshirmaydi.

C variant – yangi PRF/KDF. MShA (Ma’lumotlarni shifrlash algoritmi) yoki gubka asosidagi konstruktsiya yangi xavfsizlik modeli, isbot, mustaqil kriptotahlil va protokol bilan birgalikdagi tahlilni talab qiladi; ko‘rilgan TLS profillari bu yo‘lni tanlamagan.

Tavsiya. Dastlab A variantni TLS 1.3 uchun tadqiq qilish maqsadga muvofiq: modifikatsiya hajmi eng kichik, xorijiy TLS profillari tajribasiga mos, o‘zaro ishlash, testlash va standartlashtirish xarajatlari kam; ammo shartlar bajarilmaguncha u xavfsiz deb e’lon qilinmaydi. Ketma-ketlik: (1) O‘zMSt 285 algoritmi va 128 bitli maqsadli daraja; (2) HMAC parametrlari, kirish, chiqish, yorliq va kontekst spetsifikatsiyasi; (3) RFC 5869 va RFC 9846 dan farqlarni (xesh, B, uzunliklar) qayd etish; (4) mustaqil sinov vektorlari; (5) standart va milliy xesh bilan alohida tekshirish; (6) xususiy identifikatorli tajribaviy profil; (7) kamida ikki mustaqil amalga oshirish mosligi; (8) unumdorlik, xotira va yon-kanal o‘lchovlari; (9) kriptotahlil va standartlashtirish. Tajriba kodi va vaqtinchalik profil ishlab chiqarishga tayyor standart emas.

Xulosa

Ko‘rib chiqilgan TLS profillarida (Rossiya RFC 9189 va RFC 9367, Belarus STB 34.101.65-2014 va TLS 1.3 loyihasi, Xitoy RFC 8998) PRF/HKDF konstruktsiyasi va kalitlar jadvali saqlangan, o‘zgarish HMAC ichidagi xeshdan iborat; Rossiyada TLSTREE va kalit eksporti KDF i alohida bosqichlarda ishlaydi, dastlabki sirni shakllantirish tartibi esa faqat mustaqil TLCP protokolida farqlanadi.

O‘zbekiston uchun dastlab TLS 1.3 HKDF ni O‘zMSt 285:2024 xeshi bilan parametrizatsiyalash (A variant) maqsadga muvofiq; qo‘shimcha mexanizm yoki yangi KDF faqat aniq talab va mavjud yondashuv yetishmovchiligi isbotlanganda ko‘riladi.

Buni amaliy tavsiyaga aylantirish uchun HMAC parametrlari va xeshning qayd etilgan parametrlari, siqish funksiyasi bo‘yicha mustaqil tahlil, sinov vektorlari, ikki mustaqil amalga oshirish mosligi, unumdorlik va yon-kanal o‘lchovlari hamda kalit kelishuvi bo‘yicha milliy standart zarur.

Foydalanilgan adabiyotlar

1. Rescorla E. The TLS Protocol Version 1.3. RFC 9846 (Proposed Standard), 2026.
2. Krawczyk H. et al. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997.
3. Bellare M. New Proofs for NMAC and HMAC // CRYPTO 2006, LNCS 4117. P. 602–619.
4. Krawczyk H. Cryptographic Extraction and Key Derivation // CRYPTO 2010, LNCS 6223. P. 631–648.
5. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand KDF (HKDF). RFC 5869, 2010.
6. NIST SP 800-108r1. Key Derivation Using Pseudorandom Functions. 2022 (upd. 2024).
7. NIST SP 800-56Cr2. Key-Derivation Methods in Key-Establishment Schemes. 2020.
8. Moriarty K. (ed.) et al. PKCS #5: Password-Based Cryptography v2.1. RFC 8018, 2017.
9. Dierks T., Rescorla E. The TLS Protocol Version 1.2. RFC 5246, 2008.
10. Bhargavan K. (ed.) et al. TLS Session Hash and Extended Master Secret. RFC 7627, 2015.
11. Smyshlyaev S. (ed.) et al. GOST Cipher Suites for TLS 1.2. RFC 9189 (Informational), 2022.
12. Smyshlyaev S. (ed.) et al. Algorithms to Accompany GOST R 34.10/34.11-2012. RFC 7836, 2016.
13. Smyshlyaev S. (ed.) et al. GOST Cipher Suites for TLS 1.3. RFC 9367 (Informational), 2023.
14. СТБ 34.101.65-2014. Протокол защиты транспортного уровня (TLS). Минск, 2014.
15. СТБ 34.101.47-2017. Алгоритмы генерации псевдослучайных чисел. Минск, 2017.
16. Agievich S., Kalosha N. STB Parameters for TLS 1.3. draft-kalosha-stb-tls13-00 (I-D), 2026.
17. Yang P. ShangMi (SM) Cipher Suites for TLS 1.3. RFC 8998 (Informational), 2021.
18. GB/T 38636-2020. Transport layer cryptography protocol (TLCP). Beijing, 2020.
19. GoTLCP – GB/T 38636-2020 ning ochiq amalga oshirilishi. https://github.com/Trisia/gotlcp.
20. O‘zMSt 285:2024. Xeshlash funksiyasi. Toshkent, 2024.
21. O‘zMSt 270:2024. Ma’lumotlarni shifrlash algoritmi. Toshkent, 2024.

KRIPTOLOGIYA SOHASIDA KADRLAR TAYYORLASH VA DOLZARB YO‘NALISHLAR

Ortiqboyev A.M.
UNICON.UZ - Fan-texnika va marketing tadqiqotlari markazi

Annotatsiya. Tezisda kriptologiyaning axborot xavfsizligini ta’minlashdagi o‘rni, O‘zbekistonda ushbu sohaning shakllanishi va rivojlanishi, “UNICON.UZ” MChJda olib borilayotgan ilmiy-tadqiqot ishlari hamda kriptologiya bo‘yicha kadrlar tayyorlashning ustuvor yo‘nalishlari yoritilgan. Shuningdek, amaliy ta’lim, ilmiy-tadqiqot faoliyatini rag‘batlantirish, xalqaro hamkorlik va normativ-huquqiy bazani takomillashtirish bo‘yicha takliflar keltirilgan.

Kalit so‘zlar: kriptologiya, kriptografiya, kriptotahlil, axborot xavfsizligi, milliy kriptografik algoritmlar, elektron raqamli imzo, kadrlar tayyorlash, post-kvant kriptografiya.

Аннотация. В тезисах освещаются роль криптологии в обеспечении информационной безопасности, становление и развитие данной области в Узбекистане, научно-исследовательская деятельность ООО «UNICON.UZ», а также приоритетные направления подготовки кадров в сфере криптологии. Кроме того, представлены предложения по развитию практико-ориентированного обучения, стимулированию научно-исследовательской деятельности, расширению международного сотрудничества и совершенствованию нормативно-правовой базы.

Ключевые слова: криптология, криптография, криптоанализ, информационная безопасность, национальные криптографические алгоритмы, электронная цифровая подпись, подготовка кадров, постквантовая криптография.

Kirish

XXI asrda axborot texnologiyalari jamiyat taraqqiyotining muhim omiliga aylandi. Raqamli iqtisodiyot, elektron hukumat, elektron hujjat aylanishi va masofaviy xizmatlarning kengayishi axborot xavfsizligini ta’minlash masalasining dolzarbligini yanada oshirmoqda. Axborotlarni ruxsatsiz foydalanish, o‘g‘irlash va o‘zgartirishdan himoya qilish davlat va tashkilotlar faoliyatining muhim yo‘nalishlaridan biri hisoblanadi.

Axborot xavfsizligining ilmiy asoslaridan biri bo‘lgan kriptologiya ma’lumotlarni matematik usullar yordamida himoya qilish, autentifikatsiya mexanizmlarini yaratish va kriptografik tizimlarning bardoshliligini tahlil qilishni qamrab oladi. Shu sababli kriptologiya sohasida zamonaviy bilim va amaliy ko‘nikmalarga ega mutaxassislarni tayyorlash milliy axborot xavfsizligini mustahkamlashning muhim shartidir.

Asosiy qism

Kriptologiya ikkita asosiy yo‘nalish - kriptografiya va kriptotahlilni birlashtiradi. Kriptografiya axborotni shifrlash, elektron raqamli imzo va boshqa kriptografik mexanizmlar orqali himoya qilish usullarini ishlab chiqadi. Kriptotahlil esa kriptografik algoritmlar va tizimlarning bardoshliligini tekshirish, ularning zaif tomonlarini aniqlash hamda xavfsizlik darajasini baholashga xizmat qiladi.

Kriptografik usullar axborotning maxfiyligi, yaxlitligi, autentifikatsiyasi va elektron amallarning inkor etilmasligini ta’minlashda muhim ahamiyatga ega. Ular davlat boshqaruvi, moliya, elektron tijorat, elektron hujjat aylanishi, himoyalangan aloqa va boshqa raqamli xizmatlarda keng qo‘llaniladi.

Bugungi kunda kriptologiya sohasining rivojlanishi nafaqat mavjud kriptografik vositalardan samarali foydalanishni, balki milliy algoritmlarni yaratish, ularning xavfsizligini ilmiy asosda baholash va zamonaviy tahdidlarga moslashtirishni ham talab etadi.

O‘zbekistonda kriptologiya sohasining shakllanishi va rivojlanishi

O‘zbekiston Respublikasida kriptologiya sohasining rivojlanishi axborot xavfsizligini ta’minlash bo‘yicha ilmiy-amaliy faoliyatning shakllanishi bilan chambarchas bog‘liq. 1997-yilda “UNICON.UZ” MChJning avvalgi tashkiliy tuzilmasi tarkibida “Axborot xavfsizligi” ilmiy-tadqiqot laboratoriyasi tashkil etilgan, 1999-yilda esa u alohida bo‘limga aylantirilgan. Ushbu faoliyat natijasida kriptografik himoya vositalari, elektron raqamli imzo va kalitlarni boshqarish yo‘nalishlarida amaliy tadqiqotlar rivojlana boshlagan.

2006-yilda Toshkent axborot texnologiyalari universitetida “Axborot xavfsizligi” kafedrasi tashkil etilgan. 2008-yilda esa “Kriptografiya va kriptotahlil” yo‘nalishi bo‘yicha magistratura mutaxassisligi ochilgan. Bu jarayon mamlakatda kriptologiya bo‘yicha ilmiy va amaliy kadrlar tayyorlash tizimini shakllantirishga xizmat qilgan.

Kriptologiya sohasini rivojlantirishda oliy ta’lim muassasalari, ilmiy-tadqiqot tashkilotlari va tegishli mutaxassislarning hamkorligi muhim o‘rin tutadi. Ushbu hamkorlik doirasida milliy kriptografik algoritmlar, autentifikatsiya tizimlari, elektron raqamli imzo texnologiyalari va axborotni himoyalash vositalarini ishlab chiqish bo‘yicha ishlar amalga oshirilmoqda.

O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi PQ-293-son qarori kriptologiya sohasida ta’lim va ilm-fanni rivojlantirishga qaratilgan muhim hujjatlardan biri hisoblanadi. Qarorda kriptologiya sohasidagi ta’lim va ilm-fanni rivojlantirish bo‘yicha chora-tadbirlar, 2024–2028-yillarga mo‘ljallangan ilmiy-tadqiqot ishlari dasturi hamda sohada idoralararo ekspertlar guruhini tashkil etish masalalari nazarda tutilgan.

“UNICON.UZ” MChJning kriptologiya sohasidagi faoliyati

“UNICON.UZ” MChJda kriptologiya yo‘nalishining rivojlanishi bir necha bosqichni qamrab oladi. 1997-yilda tashkil etilgan ilmiy-tadqiqot laboratoriyasi faoliyati keyinchalik axborot xavfsizligi bo‘limi, axborotni himoyalash vositalari xizmati, axborot xavfsizligi va kriptologiya ilmiy-tadqiqot bo‘limi hamda tegishli departamentlar faoliyati bilan davom ettirilgan.

Kriptologiya va axborotni himoyalash yo‘nalishida 40 dan ortiq ilmiy-tadqiqot ishlari amalga oshirilgan, 60 dan ortiq davlat standartlari va normativ hujjatlar ishlab chiqilgan. Shuningdek, milliy algoritmlarga asoslangan himoyalangan tizimlar, maxsus xavfsizlikni ta’minlovchi apparat-dasturiy vositalar, monografiyalar va o‘quv qo‘llanmalar yaratilgan. Kriptografiya sohasidagi ixtirolar va dasturiy vositalarga tegishli patent hamda guvohnomalar olingan.

Mazkur faoliyat milliy kriptografik yechimlarni takomillashtirish, axborot tizimlarining himoyalanganligini oshirish va kriptologiya sohasidagi ilmiy salohiyatni mustahkamlashga xizmat qiladi.

O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi PQ-293-son qaroridagi vazifalar ijrosini ta’minlash va milliy kriptograf kadrlarning yangi avlodini tayyorlash maqsadida “UNICON.UZ” MChJ qoshida Kriptologiya maktabi tashkil etildi. Maktabning maqsadi iqtidorli yoshlar, mutaxassislar va ilmiy izlanuvchilarga kriptologiya bo‘yicha chuqurlashtirilgan qo‘shimcha ta’lim berish, ularning malakasini muntazam oshirish va ilmiy salohiyatini qo‘llab-quvvatlashdan iborat.

Kriptologiya maktabining asosiy vazifalari quyidagilardan iborat:

– kriptologiyaning yangi va istiqbolli yo‘nalishlarini rivojlantirish;

– mutaxassislarning kasbiy malakasini oshirish va ilmiy seminarlar tashkil etish;

– ilmiy-tadqiqot ishlarida hamda axborot tizimlari uchun dasturiy va apparat-dasturiy vositalar yaratishda ishtirok etish;

– davlat idoralari va tashkilotlarining axborot hamda kiberxavfsizlik uchun mas’ul xodimlarining kriptologik savodxonligini oshirish;

– yosh mutaxassislarning ilmiy salohiyatini rivojlantirish va amaliy ko‘nikmalarini mustahkamlash.

“Kriptologiya maktabi”da 2025-yil may oyidan hozirgi kunga qadar davlat organlari va tashkilotlarining axborot xavfsizligi hamda kiberxavfsizlik yo‘nalishlarida faoliyat yurituvchi 600 nafardan ortiq mas’ul xodimlari uchun malaka oshirish o‘quv kurslari tashkil etildi. Mazkur kurslar axborot xavfsizligini ta’minlash, kiberxavfsizlik asoslari, korxonalarda IP-telefoniyani tashkil etish va uning xavfsizligini ta’minlash, elektron hujjat aylanishi tizimlaridan foydalanish hamda axborot xavfsizligini boshqarish kabi yo‘nalishlarni qamrab oldi.

Kriptologiya sohasining dolzarb va istiqbolli yo‘nalishlari

Zamonaviy texnologiyalarning rivojlanishi kriptologiya sohasida yangi ilmiy va amaliy vazifalarni yuzaga keltirmoqda. Ayniqsa, kvant hisoblash texnologiyalarining rivojlanishi RSA va elliptik egri chiziqlarga asoslangan ayrim kriptografik mexanizmlarning uzoq muddatli xavfsizligiga tahdid tug‘dirishi mumkin. Shu sababli post-kvant kriptografiya algoritmlarini o‘rganish, ularning xavfsizligi va samaradorligini baholash hamda amaliy tizimlarga joriy etishga tayyorgarlik ko‘rish dolzarb hisoblanadi.

Bundan tashqari, sun’iy intellekt asosidagi kiberhujumlar, buyumlar interneti qurilmalarining ko‘payishi va bulutli xizmatlarning kengayishi axborotni kriptografik himoyalashga qo‘yiladigan talablarni oshirmoqda. Bunday sharoitda kriptografik algoritmlarning xavfsizligi bilan bir qatorda, ularning hisoblash samaradorligi, resurslardan foydalanish darajasi va turli texnologik muhitlarda ishlash imkoniyatlarini ham hisobga olish zarur.

Mazkur o‘zgarishlar kriptologiya bo‘yicha kadrlar tayyorlashda quyidagi bilim va ko‘nikmalarga alohida e’tibor qaratishni talab etadi:

– kriptografiyaning matematik asoslari va algoritmlarni tahlil qilish;

– milliy kriptografik algoritmlarni dasturiy amalga oshirish va sinovdan o‘tkazish;

– elektron raqamli imzo, kriptografik kalitlarni boshqarish va autentifikatsiya mexanizmlarini o‘rganish;

– kriptografik tizimlarning bardoshliligini baholash va zaifliklarni aniqlash;

– post-kvant kriptografiya algoritmlari va zamonaviy xalqaro standartlarni o‘rganish;

– resurslari cheklangan qurilmalar va turli axborot tizimlari uchun samarali kriptografik yechimlarni ishlab chiqish.

Ushbu yo‘nalishlar bo‘yicha mutaxassislar tayyorlash milliy kriptografik vositalarni takomillashtirish, axborot tizimlari xavfsizligini oshirish va yangi texnologik tahdidlarga tayyor turish imkonini beradi.

Kriptologiya sohasida kadrlar tayyorlashni takomillashtirish bo‘yicha takliflar

Kriptologiya sohasida yuqori malakali mutaxassislarni tayyorlash uchun ta’lim, ilm-fan va amaliy ishlab chiqish jarayonlarini o‘zaro uyg‘unlashtirish zarur. Bunda nazariy bilimlarni amaliy mashg‘ulotlar bilan mustahkamlash, zamonaviy laboratoriyalarni rivojlantirish va kriptografik yechimlarni real sharoitlarga yaqin muhitda sinovdan o‘tkazish imkoniyatlarini kengaytirish muhim hisoblanadi.

Birinchidan, **amaliyotga yo‘naltirilgan ta’limni rivojlantirish** lozim. O‘quv dasturlariga kriptografik algoritmlarni dasturiy amalga oshirish, elektron raqamli imzo mexanizmlarini o‘rganish, kalitlarni boshqarish va kriptografik tizimlarni sinashga oid amaliy mashg‘ulotlarni kengroq kiritish maqsadga muvofiq.

Ikkinchidan, **ilmiy-tadqiqot faoliyatini kadrlar tayyorlash bilan integratsiyalash** zarur. Talabalar, yosh olimlar va mutaxassislarni milliy kriptografik algoritmlar, post-kvant kriptografiya va axborotni himoyalash vositalarini ishlab chiqishga qaratilgan loyihalarga jalb etish ilmiy salohiyatni oshiradi hamda nazariy bilimlarning amaliy natijalarga aylanishiga yordam beradi.

Uchinchidan, **malaka oshirish tizimini uzluksiz rivojlantirish** kerak. Davlat organlari va tashkilotlarining axborot xavfsizligi uchun mas’ul xodimlari uchun o‘quv dasturlarini ularning kasbiy vazifalari va zamonaviy tahdidlardan kelib chiqib yangilab borish lozim. Bunda Kriptologiya maktabining ilmiy-amaliy tajribasidan foydalanish va o‘quv mashg‘ulotlari natijalarini muntazam baholash muhimdir.

To‘rtinchidan, **oliy ta’lim muassasalari, ilmiy-tadqiqot tashkilotlari va ishlab chiqarish korxonalari o‘rtasidagi hamkorlikni kengaytirish** zarur. Bunday hamkorlik qo‘shma ilmiy loyihalarni amalga oshirish, mutaxassislarning tajriba almashishini tashkil etish va ilmiy ishlanmalarni amaliyotga joriy etish imkoniyatlarini oshiradi.

Beshinchidan, **xalqaro tajriba va zamonaviy standartlarni o‘rganishga e’tibor qaratish** lozim. Yetakchi xorijiy universitetlar va ilmiy markazlar bilan hamkorlik, xalqaro konferensiya va stajirovkalarda ishtirok etish, shuningdek, kriptografiya standartlaridagi yangiliklarni o‘quv dasturlariga kiritish kadrlar tayyorlash sifatini oshirishga xizmat qiladi.

Xulosa

Xulosa qilib aytganda, kriptologiya milliy axborot xavfsizligini ta’minlash, raqamli xizmatlarning ishonchliligini oshirish va elektron hujjatlar bilan ishlash jarayonlarini himoyalashda muhim ahamiyatga ega. O‘zbekistonda ushbu sohaning rivojlanishi ilmiy-tadqiqot faoliyatini kengaytirish, milliy kriptografik vositalarni yaratish va malakali mutaxassislar tayyorlash bilan uzviy bog‘liq.

Kriptologiya sohasida amalga oshirilayotgan ilmiy-tadqiqot ishlari va Kriptologiya maktabi faoliyati ushbu yo‘nalishdagi ilmiy hamda amaliy salohiyatni rivojlantirishga xizmat qiladi. Kelgusida amaliyotga yo‘naltirilgan ta’limni kengaytirish, ilmiy-tadqiqotlarni rag‘batlantirish, xalqaro hamkorlikni kuchaytirish va post-kvant kriptografiya kabi istiqbolli yo‘nalishlarni rivojlantirish kriptologiya sohasida raqobatbardosh kadrlar tayyorlashning muhim omillari hisoblanadi.

YARIM TUB SONLARNI FAKTORLASHNING GEOMETRIK QIDIRUV USULI VA UNING SAMARADORLIK TAHLILI

Axadova O.Ch.
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti

Annotatsiya

Maqolada yarim tub sonlarni faktorlashning geometrik qidiruv fazosiga asoslangan algoritmi taklif etiladi. Yondashuvda diskriminant funksiyasining analitik xususiyatlaridan foydalanib, qidiruv jarayoni maxsus bosqichlariga ajratiladi. Hisoblash samaradorligini oshirish uchun rekurrent hisoblash va modulli filtrlash mexanizmlari qo‘llaniladi. Python muhitida 10 000 ta yarim tub son ustida o‘tkazilgan tajribalar natijalari Ferma va Pollard Rho algoritmlari bilan taqqoslanadi.

Kalit so‘zlar: yarim tub son, faktorlash, geometrik qidiruv fazosi, diskriminant, rekurrent hisoblash, modulli filtrlash, Ferma algoritmi, Pollard Rho.

Аннотация

В статье предлагаются алгоритм факторизации полупростых чисел, основанные на геометрическом пространстве поиска. Аналитические свойства дискриминантной функции используются для разделения процесса поиска на этапы. Для повышения вычислительной эффективности применяются рекуррентные вычисления и модульная фильтрация. Результаты экспериментов над 10 000 полупростых чисел сравниваются с алгоритмами Ферма и Pollard Rho.

Ключевые слова: полупростое число, факторизация, геометрическое пространство поиска, дискриминант, рекуррентные вычисления, модульная фильтрация, алгоритм Ферма, Pollard Rho.

Kirish

Yarim tub son deb ikkita tub son ko‘paytmasi ko‘rinishida ifodalanadigan natural songa aytiladi. Masalan, N=15=3*5 va N=49=7*7 sonlari yarim tub sonlardir [4]. Bunday sonlarni tub ko‘paytuvchilarga ajratish, ya’ni N=pq tenglikdagi p va q tub sonlarni aniqlash sonlar nazariyasi va kriptografiyada muhim masalalardan biri hisoblanadi. Xususan, katta sonlarni faktorlash murakkabligi RSA kabi ochiq kalitli kriptografik tizimlarning xavfsizligi bilan bog‘liq.

Ushbu masalani yechishda Ferma, Pollard Rho, Pollard p-1 [1], kvadratik elak va umumiy sonlar maydoni elagi kabi algoritmlardan foydalaniladi. Ularning samaradorligi faktorlanuvchi sonning xususiyatlari va tub ko‘paytuvchilarning o‘zaro munosabatiga qarab farqlanadi.

Mazkur maqolada yarim tub sonlarni faktorlashning geometrik qidiruv fazosiga asoslangan algoritmi taklif etiladi. Unda diskriminant xossalari orqali qidiruv mintaqalari aniqlanib, rekurrent hisoblash va modulli filtrlash yordamida ortiqcha tekshiruvlarni kamaytirish ko‘zda tutiladi. Algoritm samaradorligi Ferma va Pollard Rho usullari bilan tajribaviy taqqoslash orqali baholanadi.

Taklif etilgan algoritmning ishlash prinsipi

Taklif etilgan algoritmning asosiy g‘oyasi - yarim tub sonning tub ko‘paytuvchilarini qidirish jarayonini oldindan aniqlangan qidiruv oraliqlari bo‘yicha tashkil etish va yechim mavjud bo‘lishi mumkin bo‘lgan sohalarni ketma-ket tekshirishdan iborat.

Algoritm kirish ma’lumoti sifatida faktorizatsiyalanishi lozim bo‘lgan N yarim tub sonni qabul qiladi. Dastlabki bosqichda qidiruv jarayonini tashkil etish uchun zarur parametrlar aniqlanadi va qidiruv oraliqlari belgilanadi. Matematik modelda aniqlangan xossalarga muvofiq, yechim mavjud bo‘lmaydigan L3 sohasi qidiruvdan chiqarib tashlanadi. Natijada qidiruv faqat L1, L2 va L4 oraliqlarida amalga oshiriladi.

Algoritmning keyingi bosqichida har bir qidiruv oralig‘i bo‘yicha nomzod qiymatlar ketma-ket tekshiriladi. Har bir nomzod uchun diskriminant qiymati hisoblanadi. Agar diskriminant manfiy bo‘lsa, ushbu nomzod haqiqiy yechim bermaydi va qidiruv keyingi qiymat bilan davom ettiriladi. Agar diskriminant to‘liq kvadrat bo‘lsa, noma’lum o‘zgaruvchilarning butun qiymatlari aniqlanadi hamda ular asosida dastlabki sonning ehtimoliy tub ko‘paytuvchilari tiklanadi. Olingan ko‘paytuvchilarning to‘g‘riligi ularning ko‘paytmasi N ga tengligi va zarur hollarda tub ekanligi tekshirilishi orqali tasdiqlanadi.

Qidiruv jarayoni uchta mustaqil bosqich orqali tashkil etiladi:

– *L1 bosqichi* - belgilangan birinchi qidiruv oralig‘idagi nomzod qiymatlarni tekshiradi va mos yechimni izlaydi.

– *L2 bosqichi* - birinchi bosqichda yechim topilmagan taqdirda, baza qiymati atrofida belgilangan qo‘shimcha qidiruv oralig‘ini tekshiradi.

– *s* - oldingi bosqichlarda yechim aniqlanmagan hollarda, modelda belgilangan keyingi qidiruv sohasida izlashni davom ettiradi.

Har bir bosqichda nomzod qiymatlar belgilangan tartibda tekshiriladi. Agar mos tub ko‘paytuvchilar aniqlansa, algoritm qidiruvni yakunlaydi va natijani qaytaradi. Aks holda, joriy bosqichdagi qidiruv tugagach, keyingi bosqichga o‘tiladi. Barcha belgilangan oraliqlar tekshirilganidan keyin ham yechim topilmasa, algoritm ushbu qidiruv doirasida faktorlar aniqlanmaganini bildiradi.

Shunday qilib, algoritm qidiruvni tasodifiy yoki butun mumkin bo‘lgan qiymatlar to‘plami bo‘yicha amalga oshirish o‘rniga, matematik modeldan kelib chiqib belgilangan sohalar bo‘yicha tashkil etadi. Yechim mavjud bo‘lmaydigan L3 sohasining chiqarib tashlanishi yechim mavjud bo‘lmaydigan qiymatlarni tekshirishga sarflanadigan hisoblashlarni kamaytirishga xizmat qiladi.

Algoritm (Psevdokod)

Taklif etilgan faktorizatsiyalash algoritmi

$Kirish$:

$N - faktorizatsiyalanadigan\ yarim\ tub\ son$

$Chiqish$:

$p, q - N\ ning\ tub\ ko'paytuvchilari$

1. $M \leftarrow 10^{\left(\left\lfloor \frac{len(N)-1}{2} \right\rfloor + 1\right)}$
2. $N_1 \leftarrow N\ div\ M$

   $N_2 \leftarrow N\ mod\ M$
3. $S \leftarrow \frac{M^2 - N + N_2}{M}$
4. $k_kichik \leftarrow 2M - S - 2\sqrt{M^2 - MS + N_2}$

$k_{katta} \leftarrow 2M - S + 2\sqrt{M^2 - MS + N_2}$

5. // L1 qidiruvi

$FOR\ i \leftarrow M/10 + 1\ TO\ k_kichik\ DO$

$D \leftarrow (S + i)\text{^}2 - 4(Mi + N_2)$

$IF\ D\ mukammal\ kvadrat\ bo'lsa\ THEN$

$d \leftarrow \sqrt{D}$

$x \leftarrow (S + i - d)/2$

$y \leftarrow (S + i + d)/2$

$p \leftarrow M - x$

$q \leftarrow M - y$

$RETURN(p, q)$

$END\ IF$

$END\ FOR$

6. // L2 qidiruvi

$FOR\ i \leftarrow \frac{M}{10} + 1\ TO \frac{M}{100}\ DO$

$D \leftarrow (S + i)\text{^}2 - 4(Mi + N_2)$

$IF\ D\ mukammal\ kvadrat\ bo'lsa\ THEN$

$d \leftarrow \sqrt{D}$

$x \leftarrow (S + i - d)/2$

$y \leftarrow (S + i + d)/2$

$p \leftarrow M - x$

$q \leftarrow M - y$

$RETURN(p, q)$

$END\ IF$

$END\ FOR$

7. // L4 qidiruvi

$FOR\ i \leftarrow k_{kichik}\ TO\ k_{katta}\ \ DO$

$D \leftarrow (S + i)\text{^}2 - 4(Mi + N_2)$

$IF\ D\ mukammal\ kvadrat\ bo'lsa\ THEN$

$d \leftarrow \sqrt{D}$

$x \leftarrow (S + i - d)/2$

$y \leftarrow (S + i + d)/2$

$p \leftarrow M - x$

$q \leftarrow M - y$

$RETURN(p, q)$

$END\ IF$

$END\ FOR$

8. $RETURN(\text{“}Factor\ topilmadi\text{”})$.

Tajriba natijalari va tahlili

Taklif etilgan algoritm Python dasturlash tilida amalga oshirildi va Google Colab muhitida sinovdan o‘tkazildi. Tajribalarda SymPy kutubxonasining randprime() funksiyasi yordamida tub sonlar generatsiya qilindi. Ulardan tuzilgan yarim tub sonlar to‘plamida takroriy qiymatlar chiqarib tashlanib, jami 10 000 ta test holati shakllantirildi.

Algoritm samaradorligini baholashda faktorizatsiya yakunlangan qidiruv bosqichi, hisoblash qadamlari soni va bajarilish vaqti qayd etildi. Natijalar Ferma faktorizatsiyalash algoritmi hamda Pollard Rho algoritmi bilan taqqoslandi [2, 3].

Qidiruv bosqichlari bo‘yicha natijalar

Tajriba natijalariga koʻra, faktorizatsiya holatlarining 6 194 tasi (61,94%) L1, 3 183 tasi (31,83%) L2, 623 tasi (6,23%) esa L4 bosqichida yakunlangan. Bu taqsimlanish test toʻplamida algoritmning turli qidiruv mintaqalaridan foydalanish darajasi bir xil emasligini koʻrsatadi.

Ferma algoritmi bilan hisoblash qadamlari soni boʻyicha taqqoslanganda, taklif etilgan algoritm 2 028 ta holatda ustunlikka erishgan. Ushbu holatlarning 929 tasi (45,81%) L1, 1 099 tasi (54,19%) esa L2 bosqichiga toʻgʻri kelgan. Mazkur tajriba toʻplamida bu mezon boʻyicha ustunlik asosan L1 va L2 bosqichlarida kuzatilgan.

Keltirilgan oʻrtacha qiymatlar boʻyicha taklif etilgan algoritm hisoblash qadamlari sonini taxminan 59,63% ga kamaytirgan. Ushbu natija aynan oʻrganilgan test toʻplami va hisoblash qadamlari mezoniga tegishli boʻlib, barcha kirish sonlari uchun universal ustunlikni anglatmaydi.

Hisoblash samaradorligi va optimallashtirish

Diskriminantni rekurrent hisoblash va modulli filtrlash mexanizmlari algoritmning bajarilish vaqtini kamaytirish maqsadida qoʻllanildi. Tajribalarda optimallashtirishdan oldingi oʻrtacha bajarilish vaqti 6,549 ms, optimallashtirishdan keyingi koʻrsatkich esa 4,857 ms ni tashkil etdi. Bu taxminan 1,35 baravar tezlashish yoki bajarilish vaqtining 25,8% ga qisqarishiga mos keladi.

Pollard Rho algoritmi bilan taqqoslashda taklif etilgan algoritmning hisoblash qadamlari boʻyicha ustunligi 273 ta holatda kuzatilgan. Ushbu holatlarning 172 tasi L4 bosqichiga toʻgʻri kelgan. Bu natija L4 bosqichining ayrim testlarda ahamiyatli boʻlishi mumkinligini koʻrsatadi, biroq u barcha holatlarda samaraliroq ekanini isbotlamaydi.

Umuman olganda, tajribalar taklif etilgan algoritmning samaradorligi qidiruv mintaqasi va baholash mezoniga bogʻliqligini koʻrsatadi. Shu sababli algoritmni boshqa faktorlash usullariga universal muqobil sifatida emas, balki muayyan holatlarda foydali boʻlishi mumkin boʻlgan yondashuv sifatida baholash lozim.

Xulosa

Maqolada yarim tub sonlarni faktorlashning geometrik qidiruv fazosiga asoslangan matematik modeli va algoritmi koʻrib chiqildi. Diskriminant funksiyasining analitik xususiyatlari orqali qidiruv bosqichlari shakllantirildi, rekurrent hisoblash va modulli filtrlash mexanizmlari esa hisoblash jarayonini optimallashtirish uchun qoʻllanildi.

10 000 ta yarim tub son boʻyicha oʻtkazilgan tajribalarda optimallashtirilgan variantning oʻrtacha bajarilish vaqti 6,549 ms dan 4,857 ms gacha kamaydi. Ferma algoritmi bilan hisoblash qadamlari boʻyicha taqqoslashda taklif etilgan algoritm 2 028 ta holatda ustunlik koʻrsatdi; ushbu holatlar asosan L1 va L2 bosqichlarida yakunlandi.

Olingan natijalar taklif etilgan yondashuvning ayrim qidiruv mintaqalarida amaliy afzalliklarga ega boʻlishi mumkinligini koʻrsatadi. Kelgusidagi ishlar algoritmning murakkabligini nazariy asoslash, kattaroq bit uzunligiga ega sonlarda sinash va turli parametrlar ta’sirini batafsil baholashga yoʻnaltirilishi lozim.

Foydalanilgan adabiyotlar

1. Fermat, P. *Oeuvres de Fermat*. Tome I. Édité par C. Henry et P. Tannery. Paris: Gauthier-Villars, 1891.

2. Pollard, J. M. A Monte Carlo method for factorization. *BIT*, 1975, vol. 15, no. 3, pp. 331–334. DOI: https://doi.org/10.1007/BF01933667.

3. Brent, R. P. An improved Monte Carlo factorization algorithm. *BIT*, 1980, vol. 20, no. 2, pp. 176–184. DOI: https://doi.org/10.1007/BF01933190.

4. Crandall, R., Pomerance, C. *Prime Numbers: A Computational Perspective*. 2nd ed. New York: Springer, 2005. 597 p. DOI: https://doi.org/10.1007/0-387-28979-8.

POSTKVANT KRIPTOGRAFIYA VA ML-KEM (FIPS 203) KALIT INKAPSULYATSIYALASH MEXANIZMINING TUZILISHI, XAVFSIZLIK ASOSLARI VA AMALIY JORIY ETISH MUAMMOLARI TAHLILI

Mardiyev U.R.
UNICON.UZ Fan-texnika va marketing tadqiqotlari markazi.
Arabboyev B.B.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnalogiyalari universiteti

Annotatsiya. Maqolada kvant kompyuterlari davrida axborotni himoyalash uchun mo‘ljallangan postkvant kriptografiya yo‘nalishlari va AQSh NIST tomonidan standartlashtirilgan ML-KEM (FIPS 203) kalit inkapsulyatsiyalash mexanizmi tahlil qilinadi. Panjara kriptografiyasining asosi bo‘lgan LWE, Ring-LWE va Module-LWE muammolari, ML-KEM ning KeyGen, Encaps va Decaps algoritmlari, parametr to‘plamlari (ML-KEM-512/768/1024) hamda sonli-nazariy akslantirish (NTT) roli yoritiladi. Shuningdek, amaliy joriy etishdagi asosiy muammolar: kalit va shifrmatn o‘lchamlari, samaradorlik, yon kanal hujumlari va apparat tezlatish imkoniyatlari ko‘rib chiqiladi.

Kalit so‘zlar: postkvant kriptografiya, ML-KEM, CRYSTALS-Kyber, panjara kriptografiyasi, Module-LWE, kalit inkapsulyatsiyalash, yon kanal hujumlari.

Аннотация. В статье анализируются направления постквантовой криптографии и механизм инкапсуляции ключа ML-KEM (FIPS 203), стандартизованный NIST. Рассматриваются задачи LWE, Ring-LWE и Module-LWE, лежащие в основе криптографии на решётках, алгоритмы KeyGen, Encaps и Decaps, наборы параметров (ML-KEM-512/768/1024) и роль теоретико-числового преобразования (NTT). Освещены основные проблемы практического внедрения: размеры ключей и шифртекстов, производительность, атаки по побочным каналам и возможности аппаратного ускорения.

Ключевые слова: постквантовая криптография, ML-KEM, CRYSTALS-Kyber, криптография на решётках, Module-LWE, инкапсуляция ключа, атаки по побочным каналам.

Kirish

Zamonaviy ochiq kalitli kriptografiya (RSA, Diffi–Xellman, elliptik egri chiziqlar) butun sonlarni ko‘paytuvchilarga ajratish va diskret logarifmlash masalalarining hisoblash murakkabligiga tayanadi. Shor algoritmi [1] yetarlicha quvvatli kvant kompyuterida bu masalalarni polinomial vaqtda yechishga imkon beradi, ya’ni RSA va ECC asosidagi sxemalar to‘liq buzilishi mumkin. Grover algoritmi [2] esa kalitlar fazosida qidiruvni kvadrat tezlashtiradi va simmetrik shifrlar uchun samarali kalit uzunligini taxminan ikki barobar kamaytiradi. Shu sababli simmetrik kriptografiyada kalit uzunligini oshirish (masalan, AES-256) yetarli bo‘lsa, ochiq kalitli sxemalarni butunlay almashtirish talab etiladi.

Bundan tashqari, “hozir yig‘, keyin och” (harvest now, decrypt later) tahdidi mavjud: tajovuzkor bugun shifrlangan trafikni saqlab qo‘yib, kelajakda kvant kompyuteri paydo bo‘lganda uni ochishi mumkin. Mosca tomonidan taklif qilingan yondashuvga ko‘ra [3], agar axborotning maxfiy saqlanish muddati va tizimni migratsiya qilish vaqti yig‘indisi kvant tahdidining paydo bo‘lish vaqtidan oshsa, o‘tish jarayonini hoziroq boshlash zarur. Bu ML-KEM kabi postkvant kalit almashish mexanizmlarini joriy etishni dolzarb qiladi.

Postkvant kriptografiya yo‘nalishlari

Postkvant kriptografiya klassik kompyuterlarda ishlaydigan, ammo kvant hujumlariga bardoshli deb hisoblanadigan algoritmlarni o‘z ichiga oladi. Asosiy yo‘nalishlar: panjaralarga, kodlarga, xesh-funksiyalarga va multivariat tenglamalarga asoslangan sxemalar [4]. Panjara asosidagi sxemalar nisbatan kichik kalit o‘lchami va yuqori tezligi tufayli eng istiqbolli hisoblanadi; kodga asoslangan sxemalar (McEliece) uzoq tarixga ega, biroq ochiq kalit hajmi katta; xesh asosidagi imzolar xavfsizlikni faqat xesh-funksiya bardoshliligiga keltiradi; multivariat sxemalar esa imzo uchun qiziqarli, ammo bir qator variantlari kriptotahlil qilingan.

NIST 2016-yilda postkvant kriptografiya standartlashtirish tanlovini e’lon qildi, 2022-yilda CRYSTALS-Kyber (kalit inkapsulyatsiyalash) hamda CRYSTALS-Dilithium, Falcon va SPHINCS+ (raqamli imzo) algoritmlarini tanladi va 2024-yil avgustida birinchi standartlarni chop etdi: FIPS 203 (ML-KEM, Kyber asosida), FIPS 204 (ML-DSA, Dilithium asosida) va FIPS 205 (SLH-DSA, SPHINCS+ asosida) [5, 6]. Shunday qilib, ML-KEM umumiy maqsadli kalit inkapsulyatsiyalash uchun asosiy standart hisoblanadi.

Panjara kriptografiyasi asoslari

Panjara kriptografiyasining xavfsizligi xatolar bilan o‘rganish (Learning With Errors, LWE) masalasiga asoslanadi. Regev [7] tomonidan kiritilgan LWE masalasida tasodifiy A matritsa va $b = A \cdot s + e \pmod q$ ko‘rinishidagi vektor beriladi, bunda s – maxfiy vektor, e – kichik “shovqin”; s ni tiklash yoki b ni tasodifiy vektordan ajratish talab etiladi. LWE ning o‘rtacha holatdagi qiyinligi panjaradagi eng qisqa vektor kabi eng yomon holat masalalariga keltirilishi isbotlangan [7].

Klassik LWE katta matritsalar sababli kalit hajmini oshiradi. Ring-LWE [8] masalani $R_q = Z_q[x]/(x^n+1)$ halqasidagi ko‘phadlarga o‘tkazib, matritsa o‘rniga bitta ko‘phad saqlash va ko‘paytirishni tezlashtirish imkonini beradi, ammo halqaning qo‘shimcha algebraik tuzilishi xavfsizlik bo‘yicha ehtiyotkorlik uyg‘otadi. Module-LWE [9] bu ikki yondashuv oralig‘ini egallaydi: A matritsa elementlari R_q halqasidagi ko‘phadlardan iborat $k \times k$ matritsa bo‘ladi. Xavfsizlik darajasi n ni o‘zgartirmasdan faqat k modul o‘lchamini o‘zgartirish bilan sozlanadi, bu esa bir xil arifmetik yadro ($n = 256$) asosida bir nechta xavfsizlik darajasini qo‘llab-quvvatlashga imkon beradi va dasturiy/apparat realizatsiyani soddalashtiradi.

Ko‘phadlarni ko‘paytirish eng qimmat amal bo‘lgani uchun sonli-nazariy akslantirish (Number-Theoretic Transform, NTT) ishlatiladi: u tez Furye almashtirishining chekli maydondagi analogi bo‘lib, ko‘paytirish murakkabligini $O(n^2)$ dan $O(n \log n)$ ga tushiradi. ML-KEM da $q = 3329$ tanlangan, $q - 1$ soni 256 ga bo‘linadi ($3328 = 2^8 \cdot 13$), shu sababli to‘liq bo‘lmagan (incomplete) NTT qo‘llaniladi va ko‘paytirish ikkinchi darajali ko‘phadlar juftligida bajariladi.

ML-KEM tuzilishi

ML-KEM CRYSTALS-Kyber [10] sxemasiga asoslangan bo‘lib, Module-LWE ga tayanuvchi IND-CPA xavfsiz ochiq kalitli shifrlash sxemasini Fujisaki–Okamoto o‘zgartirishi orqali IND-CCA2 xavfsiz KEM ga aylantiradi [5, 10]. Mexanizm uch algoritmdan iborat:

KeyGen: tasodifiy urug‘dan SHAKE128 yordamida $A \in Rq\hat{}(k \times k)$ matritsa NTT sohasida hosil qilinadi; markazlashgan binomial taqsimot (CBD) bo‘yicha kichik s va e vektorlar tanlanadi; $t = A \cdot s + e$ hisoblanadi. Ochiq kalit (t, ρ), maxfiy kalit – s (hamda ochiq kalit, xeshi va rad etish uchun z qiymati).

Encaps: tasodifiy m xabar tanlanadi, $(K, r) = G(m \parallel H(\text{ochiq kalit}))$ hisoblanadi; r yordamida kichik r', e1, e2 shovqinlari hosil qilinib, siqilgan shifrmatn (u, v) tuziladi, umumiy kalit K (32 bayt) qaytariladi.

Decaps: shifrmatn s yordamida ochilib, m' tiklanadi; so‘ng shifrmatn qayta shifrlanib tekshiriladi. Mos kelmasa, “yashirin rad etish” (implicit rejection) orqali z va shifrmatndan yolg‘on kalit hosil qilinadi, bu esa tanlangan shifrmatn hujumlariga qarshi himoyani ta’minlaydi.

Asosiy amallar: NTT/teskari NTT, Keccak oilasi (SHA3-256, SHA3-512, SHAKE128, SHAKE256) asosidagi xeshlash va psevdotasodifiy generatsiya, CBD tanlash hamda koeffitsiyentlarni siqish/ochish (du, dv bitlarga). Siqish shifrmatn hajmini kamaytiradi, buning evaziga kichik ochish xatosi ehtimoli paydo bo‘ladi ($\approx 2^{-139} \ldots 2^{-174}$). Parametr to‘plamlari 1-jadvalda keltirilgan [5].

1-jadval.

ML-KEM parametrlari va o‘lchamlari (bayt) [5]

Parametr	ML-KEM-512	ML-KEM-768	ML-KEM-1024
k (modul o‘lchami)	2	3	4
η1 / η2	3 / 2	2 / 2	2 / 2
(du, dv)	(10, 4)	(10, 4)	(11, 5)
Ochiq kalit	800	1184	1568
Maxfiy kalit	1632	2400	3168
Shifrmatn	768	1088	1568
Umumiy kalit	32	32	32
NIST xavfsizlik toifasi	1	3	5

Toifalar mos ravishda AES-128, AES-192 va AES-256 kalit qidiruviga teng qiyinlikka ega deb hisoblanadi: ML-KEM-512 – 1-toifa, ML-KEM-768 – 3-toifa, ML-KEM-1024 – 5-toifa. Umumiy maqsadlar uchun odatda ML-KEM-768 tavsiya etiladi.

Amaliy joriy etish muammolari

Samaradorlik. ML-KEM panjara sxemalari orasida eng tezkorlaridan biri: zamonaviy protsessorlarda AVX2 yordamida har bir amal o‘nlab mikrosekund tartibida bajariladi, ARM Cortex-M4 kabi mikrokontrollerlarda ham amaliy qo‘llash mumkinligi ko‘rsatilgan [11]. Hisoblash vaqtining katta qismini Keccak va NTT egallaydi, shu sababli aynan shu bloklar optimallashtirishning asosiy ob’ektidir.

Kalit va shifrmatn o‘lchami. 1-jadvaldan ko‘rinadiki, ML-KEM-768 da ochiq kalit 1184 bayt, shifrmatn 1088 bayt. Bu ECDH (X25519) dagi 32 baytlik qiymatlardan ancha katta. TLS kabi protokollarda handshake hajmi ortadi, paketning MTU dan oshib fragmentatsiyalanishi, cheklangan kanalli IoT qurilmalarida esa energiya sarfi oshishi mumkin. Shu sababli o‘tish davrida klassik va postkvant sxemalarni birga qo‘llovchi gibrid kalit almashish (masalan, X25519 + ML-KEM-768) tavsiya etiladi.

Yon kanal hujumlari. Matematik bardoshlik realizatsiya xavfsizligini kafolatlamaydi. Maxfiy kalit bilan ishlovchi amallar vaqt, quvvat iste’moli yoki elektromagnit nurlanish orqali sizishi mumkin. Primas va boshqalar niqoblangan panjara asosidagi shifrlashga NTT amali bo‘yicha bitta iz (single-trace) hujumini ko‘rsatgan [12]; shuningdek, Kyber realizatsiyalarida bo‘lish amalining o‘zgaruvchan vaqti bilan bog‘liq vaqt hujumlari (KyberSlash) aniqlangan. Himoya choralari: konstanta vaqtli kod, maxfiy qiymatlarga bog‘liq tarmoqlanish va xotiraga murojaatlarni yo‘qotish, niqoblash (masking), shuffling hamda Decaps dagi taqqoslashni xavfsiz bajarish. Bu choralar odatda sezilarli qo‘shimcha hisoblash xarajatini keltirib chiqaradi.

Apparat tezlatish. ML-KEM arifmetikasi (q = 3329 modulida 12 bitli koeffitsiyentlar, NTT butterfly amallari, Keccak almashtirishlari) apparat realizatsiya uchun qulay. Dasturiy joriy etishda

SIMD buyruqlari (AVX2, NEON) qo‘llaniladi; FPGA da parallel butterfly bloklari va Keccak yadrosi yordamida past kechikish, ASIC da esa eng yaxshi energiya samaradorligi hamda yon kanal himoyasini apparat darajasida joriy qilish imkoniyati mavjud. Biroq apparat yechimlarda moslashuvchanlik (parametr to‘plamlarini almashtirish, kelajakdagi yangilanishlar) va chip maydoni o‘rtasida muvozanat saqlanishi kerak.

Xulosa

ML-KEM kvant kompyuterlari tahdidiga qarshi kalit almashishning standartlashtirilgan va amaliy jihatdan eng yetuk yechimi hisoblanadi. Uning xavfsizligi Module-LWE masalasining qiyinligiga tayanadi, samaradorligi esa NTT va Keccak asosidagi optimallashtirilgan arifmetikaga bog‘liq. Asosiy muammolar – kalit va shifrmatn o‘lchamlarining kattaligi hamda yon kanal hujumlariga qarshi himoya. Keyingi yo‘nalishlar: gibrid sxemalarni protokollarga (TLS, VPN) joriy etish, realizatsiyalarni konstanta vaqtlilik va niqoblash bo‘yicha rasmiy tekshirish hamda cheklangan resursli qurilmalar uchun apparat-dasturiy yechimlarni takomillashtirish.

Foydalanilgan adabiyotlar

1. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing, 1997. Vol. 26, No. 5. – P. 1484–1509.

2. Grover L.K. A fast quantum mechanical algorithm for database search // Proc. 28th Annual ACM Symposium on Theory of Computing (STOC), 1996. – P. 212–219.

3. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? // IEEE Security & Privacy, 2018. Vol. 16, No. 5. – P. 38–41.

4. Bernstein D.J., Lange T. Post-quantum cryptography // Nature, 2017. Vol. 549. – P. 188–194.

5. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. – Gaithersburg: NIST, 2024. https://doi.org/10.6028/NIST.FIPS.203

6. NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard; FIPS 205: Stateless Hash-Based Digital Signature Standard. – Gaithersburg: NIST, 2024.

7. Regev O. On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM, 2009. Vol. 56, No. 6. – Art. 34.

8. Lyubashevsky V., Peikert C., Regev O. On ideal lattices and learning with errors over rings // Journal of the ACM, 2013. Vol. 60, No. 6. – Art. 43.

9. Langlois A., Stehlé D. Worst-case to average-case reductions for module lattices // Designs, Codes and Cryptography, 2015. Vol. 75, No. 3. – P. 565–599.

10. Bos J., Ducas L., Kiltz E., et al. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM // IEEE European Symposium on Security and Privacy (EuroS&P), 2018. – P. 353–367.

11. Kannwischer M.J., Rijneveld J., Schwabe P., Stoffelen K. pqm4: Testing and benchmarking NIST PQC on ARM Cortex-M4 // IACR Cryptology ePrint Archive, 2019/844.

12. Primas R., Pessl P., Mangard S. Single-trace side-channel attacks on masked lattice-based encryption // CHES 2017, LNCS 10529. – Springer, 2017. – P. 513–533.

MOBIL ILOVALARDA SHAXSIY MA’LUMOTLARNI KRIPTOGRAFIK HIMOYALASH TALABLARIGA MUVOFIQLIGINI BAHOLASH USULLARI

Abduxalilov X.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada mobil ilovalarda foydalanuvchilarning shaxsiy ma’lumotlarini kriptografik himoyalash talablariga muvofiqligini (Compliance) baholash masalalari ko‘rib chiqiladi. Mavjud yondashuvlarning asosiy kamchiligi - texnik zaifliklarni aniqlash va hujjatlar auditi natijalari yagona o‘lchamda birlashtirilmasligi - asoslanadi. Baholashning besh sohasi, mezonlar tizimi, vazn koeffitsientlari va integral muvofiqlik koeffitsientini hisoblash tartibi taklif etiladi. Modelga kritik mezonlar bo‘yicha cheklov qoidasi kiritilgan.

Kalit so‘zlar: mobil ilova, shaxsiy ma’lumotlar, kriptografik himoya, talablarga muvofiqlik, baholash mezonlari, integral koeffitsient.

Аннотация. В статье рассматриваются вопросы оценки соответствия (Compliance) криптографической защиты персональных данных пользователей в мобильных приложениях установленным требованиям. Обоснован основной недостаток существующих подходов - разобщённость результатов технического анализа и документального аудита. Предложены пять областей оценки, система критериев, весовые коэффициенты и порядок расчёта интегрального коэффициента соответствия.

Ключевые слова: мобильное приложение, персональные данные, криптографическая защита, соответствие требованиям, критерии оценки, интегральный коэффициент.

Kirish

Mobil ilovalar bugungi kunda pasport ma’lumotlari, bank kartalari va shaxsiy yozishmalarni qayta ishlovchi asosiy vositaga aylandi. Biroq kriptografik himoyaning mavjudligi uning talablarga muvofiqligini anglatmaydi. Mustaqil tadqiqotlar natijalariga ko‘ra, tahlil qilingan korporativ mobil ilovalarning 92 foizida zaif yoki xato qo‘llangan kriptografik usullar aniqlangan, parol va kalitlarni shifrlagan ilovalarning 60 foizdan ortig‘i esa buni eskirgan algoritmlar bilan amalga oshirgan.

Ilova AES-256 algoritmidan foydalanishi, ammo shifrlash kalitini manba kodida saqlashi mumkin; TLS protokolini qo‘llashi, ammo server sertifikatini tekshirmasligi mumkin. Har ikki holatda ham himoya rasman mavjud, amalda esa yo‘q. O‘zbekiston Respublikasining “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuni maxfiylik va butunlikni ta’minlashni talab qiladi, lekin aniq bir ilova ushbu talabni bajarganmi degan savolga javob beruvchi o‘lchov mexanizmini bermaydi. Amaldagi texnik metodikalar zaifliklarni aniqlaydi, ammo huquqiy muvofiqlik haqida xulosa chiqarmaydi; boshqaruv standartlari esa tashkiliy jarayonlarni baholab, ilova kodiga kirmaydi. Shu bo‘shliqni to‘ldiruvchi, miqdoriy va qaytariluvchan baholash usulini ishlab chiqish dolzarb vazifa hisoblanadi.

Masalaning o‘rganilganlik darajasi quyidagicha. Xalqaro amaliyotda mobil ilovalar xavfsizligini tekshirishning ikki yo‘nalishi shakllangan. Birinchisi - OWASP MASVS va MASTG hujjatlariga asoslangan texnik tekshiruv bo‘lib, u zaifliklar ro‘yxatini beradi, ammo natijani huquqiy talablar bilan bog‘lamaydi va umumlashtirilgan baho shakllantirmaydi. Ikkinchisi - ISO/IEC 27001 va 27701 standartlari bo‘yicha sertifikatsiya bo‘lib, u tashkilotning boshqaruv

jarayonlarini baholaydi, biroq konkret ilovaning kodi va trafigini tekshirmaydi. Milliy darajada O‘z DSt standartlari kriptografik algoritmlarga talab qo‘yadi, lekin ularning mobil ilovada qanday tekshirilishi metodik jihatdan belgilanmagan. Natijada texnik tahlil natijasi bilan huquqiy talab o‘rtasida uzilish yuzaga keladi.

Asosiy qism

Taklif etilayotgan usul uch manbadan olingan dalillarga tayanadi. Statik tahlilda ilova paketi dekompilyatsiya qilinib, kriptografik API chaqiruvlari, algoritm identifikatorlari hamda kalitlarning manba koddagi izlari tekshiriladi. Dinamik tahlilda ilova nazorat ostidagi qurilmada ishga tushirilib, tarmoq trafigi qamrab olinadi va TLS versiyasi, shifrlar to‘plami, sertifikatni tekshirish mexanizmi aniqlanadi. Normativ-hujjatli tahlilda maxfiylik siyosati, rozilik olish tartibi va saqlash muddatlari qonunchilik talablariga solishtiriladi. Bir manbaning o‘zi yetarli emas: statik tahlil kalitni topadi, lekin uning ishlatilishini ko‘rsatmaydi, dinamik tahlil esa trafikni ko‘rib, qurilmadagi saqlashni ko‘rmaydi.

Baholash sohalari shaxsiy ma’lumotning ilovadagi hayot sikliga muvofiq ajratildi. Birinchi soha - ma’lumotlarni qurilmada saqlash: lokal baza, fayllar, keshlar va zaxira nusxalarining shifrlanganligi. Ikkinchi soha - uzatish kanalining himoyasi: TLS versiyasi, sertifikatni tekshirish va certificate pinning mexanizmi. Uchinchi soha - kriptografik kalitlarni boshqarish: generatsiya, apparat himoyalangan omborda saqlanishi, amal qilish muddati va qattiq kodlangan kalitlarning yo‘qligi. To‘rtinchi soha - autentifikatsiya va seansni boshqarish: parol xeshlash algoritmi, seans tokenlarining himoyasi va biometrik ma’lumotlarning qurilmadan chiqmasligi. Beshinchi soha - tashkiliy-huquqiy muvofiqlik: foydalanuvchi roziligi, maxfiylik siyosatining aniqligi va ma’lumotlar joylashuvi talabining bajarilishi.

Sohalar uchun jami 22 ta mezon shakllantirildi. Ularning har biri amaldagi normativ hujjatdan - “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun, O‘z DSt 1105:2009, 1106:2009 va 1092:2009 standartlari, OWASP MASVS v2.0, NIST FIPS 140-3 hamda ISO/IEC 27001:2022 talablaridan - kelib chiqadi. Har bir mezon uch darajali shkalada baholanadi: 0 - talab bajarilmagan, 1 - qisman bajarilgan, 2 - to‘liq bajarilgan. Ball faqat kuzatilgan dalilga, ya’ni kod fragmenti, trafik yozuvi yoki hujjat bandiga asoslanadi; ishlab chiquvchining bayonoti dalil hisoblanmaydi. Ushbu qoida usulning qaytariluvchanligini, ya’ni turli ekspertlar tomonidan bir xil natija olinishini ta’minlaydi.

Sohalarning vazn koeffitsientlari iyerarxiyalarni tahlil qilish usuli asosida, juftlik bo‘yicha qiyoslash orqali aniqlandi va quyidagicha qabul qilindi: saqlash - 0,25, uzatish - 0,25, kalitlarni boshqarish - 0,20, autentifikatsiya - 0,15, tashkiliy-huquqiy muvofiqlik - 0,15. Saqlash va uzatishga eng yuqori vazn berildi, chunki ma’lumotlar sizib chiqishining aksariyat hollari aynan shu bosqichlarda ro‘y beradi. Integral muvofiqlik koeffitsienti sohalar bo‘yicha olingan ballarning maksimal balga nisbatini vazn koeffitsientlariga ko‘paytirib jamlash orqali hisoblanadi va 0 dan 100 foizgacha oraliqda qiymat oladi.

Mezonlarning mazmunini ayrim namunalar orqali ko‘rsatish mumkin. Saqlash sohasida maxfiy ma’lumotlarning lokal bazada shifrlangan holda saqlanishi, shifrlash algoritmining amaldagi standartga mosligi, zaxira nusxaga maxfiy ma’lumotlar kiritilmasligi hamda ularning jurnal va kesh fayllariga yozilmasligi tekshiriladi. Uzatish sohasida barcha murojaatlarning TLS 1.2 yoki undan yuqori versiyada amalga oshirilishi, shifrlanmagan HTTP murojaatlarining yo‘qligi, sertifikat zanjiri, muddati va domenining tekshirilishi hamda zaif shifrlar to‘plamining o‘chirilgani baholanadi. Kalitlarni boshqarish sohasida manba kodida qattiq kodlangan kalit, parol yoki tokenning mavjud emasligi, kalitlarning apparat himoyalangan omborda saqlanishi va

ularning kriptografik xavfsiz generator orqali hosil qilinishi tekshiriladi. Autentifikatsiya sohasida parollarning sekin xeshlash algoritmlari bilan saqlanishi va biometrik shablonning qurilmadan tashqariga uzatilmasligi nazarda tutiladi.

Baholash besh bosqichda bajariladi: ilova paketini olish va statik tahlil, nazorat qurilmasida dinamik tahlil, hujjatlarni tekshirish, mezonlar bo‘yicha ballash hamda koeffitsientni hisoblash. Har bir ballga tegishli dalil biriktiriladi, bu esa baholash natijasining tekshirilishi mumkinligini ta’minlaydi. Masalan, shartli ilova uchun sohalar bo‘yicha quyidagi natijalar olingan bo‘lsin: saqlash - 10 balldan 9, uzatish - 10 balldan 9, kalitlarni boshqarish - 8 balldan 6, autentifikatsiya - 8 balldan 7, tashkiliy-huquqiy muvofiqlik - 8 balldan 7. Bu holda integral koeffitsient 86,3 foizni tashkil etadi va shkala bo‘yicha “yetarli” darajaga to‘g‘ri keladi.

Faqat o‘rtacha qiymatga tayanish xato xulosaga olib keladi. Mezonlarning aksariyatini bajargan, ammo shifrlash kalitini manba kodida saqlagan ilova 90 foizga yaqin natija olishi mumkin, holbuki uning himoyasi amalda buzilgan. Shu sababli modelga cheklov qoidasi kiritildi: kritik deb belgilangan o‘n mezondan birortasi bo‘yicha ball nolga teng bo‘lsa, umumiy koeffitsient qiymatidan qat‘i nazar, ilovaning yakuniy darajasi “qisman muvofiq” dan yuqori bo‘la olmaydi. Olingan natija to‘rt darajali shkala bo‘yicha talqin qilinadi: 90 foizdan yuqori - yuqori daraja, 75–89 foiz - yetarli, 50–74 foiz - qisman, 50 foizdan past - nomuvofiq. Yuqorida keltirilgan misolda kalitlarni boshqarish sohasida qattiq kodlangan kalit aniqlangani sababli kritik mezon bo‘yicha ball nolga teng bo‘ladi, shu bois 86,3 foizlik natijaga qaramay ilovaning yakuniy darajasi “qisman muvofiq” deb belgilanadi. Bu modelning asosiy afzalligini ko‘rsatadi: yuqori umumiy ball bitta hal qiluvchi nuqsonni yashira olmaydi.

Xulosa

Ishlab chiqilgan usul milliy qonunchilik va O‘z DSt standartlari talablarini xalqaro OWASP, NIST hamda ISO/IEC me’yorlari bilan yagona baholash tizimida birlashtiradi, sifat ko‘rsatkichlarini vazn koeffitsientlari orqali miqdoriy natijaga keltiradi va kritik mezonlar bo‘yicha cheklov qoidasi hisobiga alohida hal qiluvchi nuqsonlarning yuqori umumiy ball ostida yashirinishiga yo‘l qo‘ymaydi. Usul ishlab chiquvchilar uchun chiqarishdan oldingi tekshiruv ro‘yxati, buyurtmachilar uchun texnik topshiriq sharti va nazorat organlari uchun yagona o‘lchov sifatida qo‘llanilishi mumkin. Tadqiqotning keyingi bosqichida usulni ommabop mobil ilovalar namunasida aprobatsiyadan o‘tkazish va baholashning statik qismini avtomatlashtiruvchi dasturiy vosita yaratish ko‘zda tutilgan.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuni, O‘RQ-547-son, 2019-yil 2-iyul.

2. O‘z DSt 1105:2009. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi. - Toshkent: O‘zstandart, 2009.

3. OWASP Mobile Application Security Verification Standard (MASVS) v2.0. - OWASP Foundation, 2023.

4. NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management. - Gaithersburg: NIST, 2020.

5. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. - Pearson, 2022.

OCHIQ KALITLI QIDIRISH IMKONIYATLI SHIFRLASH ALGORITMLARIGA PARAMETRLI ALGEBRANI TATBIQ ETISH YONDASHUVLARI

Xudoynazarov U.U.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti,

Annotatsiya. Ishda ochiq kalitli qidirish imkoniyatli shifrlash sxemalariga parametrli algebra amallarini tatbiq etish imkoniyatlari ularning algebraik tuzilmasi bo‘yicha tahlil qilingan. Tatbiq imkoniyatini baholash uchun uchta mezon ajratilgan hamda ular asosida ikki chiziqli juftlashuvga asoslangan va asoslanmagan konstruksiyalar qiyosiy o‘rganilgan. Juftlashuvga asoslangan sxemalarda tatbiqni cheklovchi omillar aniqlangan, juftlashuvga asoslanmagan sxemalar esa algebraik asosiga ko‘ra ajratilib, modulli siklik guruhda qurilgan konstruksiyalar parametrli amallarni bevosita joriy etish uchun mos ekanligi ko‘rsatilgan.

Kalit so‘zlar: parametrli algebra, ochiq kalitli qidirish imkoniyatli shifrlash, ikki chiziqli juftlashuv, modulli siklik guruh, elliptik egri chiziq, parametrli darajaga oshirish, parametrli ko‘paytirish, qidiruv tuynugi.

Аннотация. В статье анализируется возможность реализации операций параметрической алгебры в схемах шифрования с открытым ключом и возможностью поиска, основанных на их алгебраической структуре. Выделены три критерия оценки возможности реализации, и на их основе сравнительно изучаются конструкции, основанные на билинейном спаривании и не основанные на нем. Выявлены факторы, ограничивающие реализацию в схемах, основанных на спаривании, схемы, не основанные на спаривании, различаются по их алгебраическому базису, и показано, что конструкции, построенные на модулярной циклической группе, подходят для непосредственной реализации параметрических операций.

Ключевые слова: параметрическая алгебра, шифрование с открытым ключом и возможностью поиска, билинейное спаривание, модулярная циклическая группа, эллиптическая кривая, параметрическое повышение, параметрическое умножение, поисковая дыра.

Ochiq kalitli qidirish imkoniyatli shifrlash sxemalari ma’lumot jo‘natuvchiga qabul qiluvchining ochiq kaliti yordamida kalit so‘z indeksini shifrlash, qabul qiluvchiga esa o‘z maxfiy kaliti bilan qidiruv tuynugini shakllantirish imkonini beradi. Bulutli server indeks va tuynuk mosligini tekshiradi, biroq na kalit so‘zni, na hujjat mazmunini bilmaydi. Mazkur yondashuv dastlab Boneh va boshqalar tomonidan taklif etilgan [1] va keyinchalik ko‘p kalit so‘zli qidiruv hamda jo‘natuvchini autentifikatsiyalash yo‘nalishlarida rivojlantirilgan [2].

Bulutli muhitda bunday sxemalar elektron hujjatlar bo‘yicha xavfsiz qidiruvni tashkil etish vositasi sifatida qo‘llanilmoqda [4].

Bugungi kunda qidirish imkoniyatli shifrlash sxemalari qidiruv samaradorligini oshirish, dimamikli jarayonlarni takomillashtirish, turli xavfsizlik xususiyatlarini oshirish borasida bir qancha izlanishlar olib borilmoqda. Shuni ta’kidlash lozimki, mamlakatimizda ham turli kriptografik algoritmlar parametrli algebraga asoslangan algebraik strukturalar yordamida takomillashtirilmoqda. Qidirish imkoniyatli shifrlash algoritmlarini ham mavjud parametrli algebra bilan takomillashtirish usullarini ko‘rib chiqish mumkin. Mavjud sxemalarni parametrli

algebra asosida takomillashtirishda ular orasidan mos bo‘lganini tanlash talab etiladi, chunki parametrli amallarning qo‘llanilishi sxemaning ichki algebraik tuzilmasiga bevosita bog‘liq.

Parametrli algebrada EKUB(R, q) = 1 shartni qanoatlantiruvchi R parametr tanlanadi va barcha amallar q modul bo‘yicha bajariladi. Asosiy hisoblashlar parametrli ko‘paytirish $a \circledast b \equiv a + b + a \cdot R \cdot b \,(mod\, q)$ va parametrli darajaga oshirish $a^{\backslash k} = ((1 + R \cdot a)^k - 1) \cdot R^{-1} (mod\, q)$ amallari orqali bajariladi

Mazkur strukturaning neytral elementi klassik ko‘paytirishdagi 1 emas, 0 ga teng. Yuqorida keltirilgan yopiq ifoda parametrli darajaga oshirishni ketma-ket hisoblashlarsiz bajarish va murakkablikni $O(k)$ dan $O(log\, k)$ gacha kamaytirish imkonini beradi [3]. Shuningdek, parametrli darajaga oshirish uchun $(a^{\,z})^{\backslash d} = \left(a^{\backslash d}\right)^{\backslash z}$ kommutativlik munosabati o‘rinli bo‘lib, u kalitlar kelishuviga asoslangan sxemalarda tomonlar hisoblagan qiymatlar tengligini isbotlash imkonini beradi.

Keltirilgan ifodalardan ko‘rinadiki, parametrli amallar modulli ko‘paytirish va modulli darajaga oshirishga tayanadi. Shundan kelib chiqib, sxemaning parametrli algebra bilan mosligini baholash uchun uchta mezon ajratildi: asosiy hisoblash jarayonlari modulli siklik guruhda bajarilishi; sxemada juftlashuv yoki interpolatsiya kabi kompozit algebraik konstruksiyalar ishtirok etmasligi; funksional to‘g‘rilik parametrli amallarning algebraik xossalari orqali isbotlanishi mumkin bo‘lishi.

Qo‘llaniladigan kriptografik mexanizmga ko‘ra ochiq kalitli qidirish imkoniyatli shifrlash sxemalari ikki chiziqli juftlashuvga asoslangan va asoslanmagan guruhlarga ajratiladi [2, 4, 10]. Quyida har ikki guruh yuqoridagi mezonlar asosida ko‘rib chiqiladi.

Ikki chiziqli juftlashuvga asoslangan sxemalar. Bunday sxemalarda kriptografik amallar ikki chiziqli akslantirish orqali quriladi. Bir xil tartibli siklik guruhlar uchun aniqlangan e: $G_1 \times G_2 \to G_t$ akslantirish ixtiyoriy guruh elementlari va butun sonlar uchun ikki chiziqlilik xossasini qanoatlantiradi. Indeks bilan qidiruv tuynugi mosligi aynan shu akslantirish yordamida tekshiriladi, sxemaning xavfsizligi esa ikki chiziqli Diffie–Hellman oilasidagi hisoblash muammolariga tayanadi [1]. Ushbu yondashuv keng funksional imkoniyatlarga ega sxemalarni yaratishga imkon bersada, parametrli amallarni joriy etish nuqtai nazaridan bir qator strukturaviy qiyinchiliklarga ega (1-jadval).

1-jadval

Sxemalarning parametrli algebra bilan mosligi

Qiyinchilik	Izoh
Murakkab algebraik struktura	Sxemada bir vaqtning o‘zida bir nechta algebraik guruh ishtirok etadi
Juftlashuv xossasiga bog‘liqlik	Algoritmning to‘g‘riligi ikki chiziqlilik xossasiga asoslanadi; ushbu xossaning parametrli muhitda saqlanishi alohida matematik asoslashni talab qiladi
Hisoblash mexanizmining murakkabligi	Juftlashuv maxsus algoritmlar asosida hisoblanadigan kompozit amal bo‘lib, parametrli amallarni uning ichki jarayoniga bevosita joriy etish murakkab
Umumiy moslik darajasi	Bevosita qo‘llash imkoniyati cheklangan, buning uchun qo‘shimcha algebraik model ishlab chiqilishi talab etiladi

1-jadvaldan ko‘rinadiki, parametrli algebra amallarini tatbiq etishni cheklovchi asosiy omil hisoblash murakkabligidan ko‘ra sxemaning algebraik tuzilmasi bilan bog‘liq. Juftlashuv

amalining bir nechta algebraik guruhlar o‘rtasida aniqlanishi va sxema to‘g‘riligining bilinearlik xossasiga tayanishi parametrli amallarni bevosita joriy etishni murakkablashtiradi. Shu sababli parametrli algebra asosida takomillashtirish uchun sodda algebraik tuzilishga ega, juftlashuvga asoslanmagan sxemalar istiqbolli yo‘nalish hisoblanadi.

Ikki chiziqli juftlashuvga asoslanmagan sxemalar. Bunday sxemalarda qidiruv mexanizmi Diffie–Hellman kalit kelishuvi [5] yoki El-Gamal tipidagi konstruksiyalarga tayanadi; natijada algebraik tuzilma soddalashadi va hisoblash murakkabligi kamayadi. Shu bilan birga, mazkur guruh ichida ikki xil algebraik asos uchraydi. Elliptik egri chiziqlar guruhida asosiy amal nuqtalarni qo‘shish, asosiy hisoblash jarayoni esa skalyar ko‘paytirish bo‘lgani uchun parametrli amallar bevosita qo‘llanilmaydi. Modulli siklik guruhda esa hisoblashlar modulli ko‘paytirish va darajaga oshirishdan iborat bo‘lib, klassik amallarni parametrli amallar bilan almashtirish uchun qulay sharoit mavjud. So‘nggi yillarda taklif etilgan sxemalarning shu nuqtai nazardan qiyosiy tahlili 2-jadvalda keltirilgan.

2-jadval

Juftlashuvga asoslanmagan sxemalarning parametrli algebra bilan mosligi

Sxema	Algebraik asos	Asosiy hisoblash amali	Moslik darajasi
Bai va b. [6]	Elliptik egri chiziq	Skalyar ko‘paytirish	Cheklangan: elliptik egri chiziq muhitini moslashtirish talab etiladi
Jin va b. [7]	Elliptik egri chiziq	Skalyar ko‘paytirish	O‘rtacha: integratsiyalash murakkablashadi
Chan va b. [8]	Elliptik egri chiziq, k-bardoshli konstruksiya	Skalyar ko‘paytirish, Lagranj interpolatsiyasi	O‘rtacha: qo‘shimcha algebraik moslashtirish talab etiladi
Wu va Shi [9]	Modulli siklik guruh	Modulli ko‘paytirish va darajaga oshirish	Yuqori: bevosita joriy etiladi

Juftlashuv amalidan foydalanmaslik sxemaning parametrli algebra amallariga avtomatik ravishda mos kelishini anglatmaydi. Ko‘rib chiqilgan to‘rtta sxemadan uchtasi elliptik egri chiziqlar guruhiga asoslangan bo‘lib, ularda asosiy amal skalyar ko‘paytirishdan iborat; Chan va boshqalarning sxemasidagi k-bardoshli konstruksiya va Lagranj interpolatsiyasi esa qo‘shimcha algebraik moslashtirishni talab qiladi. Wu va Shi sxemasi modulli siklik guruhga asoslangani bilan ajralib turadi.

Parametrli algebrani juftlashuvga asoslanmagan sxemalarga tatbiq etish

Modulli siklik guruhda qurilgan juftlashuvga asoslanmagan sxemalarning hisoblash oqimi to‘rt bosqichdan iborat: ishtirokchilarning kalitlarini hosil qilish; jo‘natuvchi va qabul qiluvchi o‘rtasida umumiy maxfiy qiymatni kelishish; kalit so‘z indeksi va qidiruv tuynugini shakllantirish; serverda moslikni tekshirish. Dastlabki ikki bosqich modulli darajaga oshirish amaliga tayanadi, qolgan ikkitasi esa xesh funksiyalari va modulli ko‘paytirishdan iborat. Taklif etilayotgan yondashuvda klassik darajaga oshirish amali parametrli darajaga oshirish amali bilan faqat dastlabki ikki bosqichda almashtiriladi.

Jo‘natuvchi va qabul qiluvchi mos ravishda α va β maxfiy qiymatlarini tanlab, ochiq kalitlarini quyidagi ko‘rinishda hosil qiladi:

$$pkS = g\backslash\alpha \ (mod\ q), \quad pkR = g\backslash\beta \ (mod\ q).$$

Bu yerda q - tub son, g - guruh generatori, R esa jo‘natuvchi va qabul qiluvchi o‘rtasida maxfiy saqlanadigan parametr. Umumiy maxfiy qiymat quyidagicha hisoblanadi:

$$K = (pkR)\backslash\alpha\ (mod\ q), \quad K' = (pkS)\backslash\beta\ (mod\ q).$$

Parametrli darajaga oshirish uchun $1 + R{\cdot}a^{\backslash k} \equiv (1 + R{\cdot}a)^k$ (mod q) munosabati o‘rinli. Undan foydalanib, har ikki tomon hosil qilgan qiymatlarning tengligini ko‘rsatish mumkin:

$$1 + R \cdot K \equiv (1 + R \cdot g)\alpha\beta\ (mod\ q), \quad 1 + R \cdot K' \equiv (1 + R \cdot g)\alpha\beta\ (mod\ q).$$

Demak, R parametrining modul bo‘yicha teskarisi mavjud bo‘lganda

$$K = K' = ((1 + R \cdot g)\alpha\beta - 1) \cdot R - 1\ (mod\ q).$$

Demak, parametrli darajaga oshirish tomonlarning bir xil umumiy maxfiy qiymatni hosil qilishini ta’minlaydi. Bu natija aniq sxemaga emas, umumiy maxfiy qiymatni modulli darajaga oshirish orqali hosil qiladigan barcha konstruksiyalarga taalluqlidir.

Keyingi bosqichlar o‘zgarishsiz qoldiriladi: indeks umumiy maxfiy qiymat va kalit so‘zdan, tuynuk esa tasodifiy s qiymati va serverning pkC ochiq kaliti ishtirokida shakllantiriladi:

$$CW = H1(K, W),\ T1 = H1(K, W*) \cdot H2(pkCs)(mod\ q),\ T2 = gs\ (mod\ q).$$

Server moslikni tekshirishda $MC = H2(T2\gamma)$ qiymatini hisoblaydi va $AT = T1 \cdot MC - 1(mod\ q)$ ifodasidan foydalanib, $A_T = C_W$ tengligini tekshiradi; bu yerda $pk_C = g\gamma$(mod q), γ esa serverning maxfiy kalitidir. Agar qidirilayotgan kalit so‘z indeksdagi kalit so‘zga mos kelsa, xesh funksiyasining tegishli qiymatlari teng bo‘ladi va tekshirish muvaffaqiyatli yakunlanadi. Ushbu bosqichlarda parametrli amallar qo‘llanilmaydi: ular parametrli usulda hosil qilingan umumiy maxfiy qiymatdan foydalanadigan klassik amallardir.

Natijada server parametrli darajaga oshirish amalini bajarmaydi, R parametrini bilmaydi va uning tekshirish bosqichiga qo‘shimcha hisoblash yuklamasi yuklanmaydi - bu bulutli muhitda hisoblash xarajatlarini taqsimlash nuqtayi nazaridan ahamiyatlidir. Mazkur yondashuv umumiy maxfiy qiymati modulli darajaga oshirish orqali hosil qilinadigan har qanday juftlashuvga asoslanmagan sxemaga qo‘llanilishi mumkin.

Xavfsizlik xususiyatlari. Juftlashuvga asoslanmagan sxemalarda shifrmatn va qidiruv tuynugining ajratilmasligi hamda chastota tahlili hujumiga bardoshlilik muhim hisoblanadi. Dastlabki ikki xususiyat farqlanuvchi Diffie–Hellman faraziga [5], uchinchisi esa har bir qidiruvda tuynukning randomizatsiyalanishiga asoslanadi. Taklif etilgan yondashuvda umumiy maxfiy qiymat har ikki tomonda bir xil hosil qilinadi, indeks va tuynuk klassik usulda shakllantiriladi, qidiruv tuynugining randomizatsiyasi esa saqlanadi. Shu sababli parametrli amallarni joriy etish ushbu mexanizmlarni bevosita o‘zgartirmaydi.

Biroq R parametrining serverga noma’lumligi sxemaning xavfsizligini kuchaytirishini o‘z-o‘zidan isbotlamaydi, chunki uni aniqlash masalasining murakkabligi alohida tadqiq etilmagan. Shu bois sxemaning bardoshliligi klassik diskret logarifmlash va Diffie–Hellman masalalarining murakkabligiga asoslanadi.

Xulosa qilib aytganda, parametrli algebrani tatbiq etish sxemaning algebraik tuzilishiga bog‘liq. Modulli siklik guruhda qurilgan Wu–Shi sxemasida parametrli darajaga oshirish kalitlarni hosil qilish va umumiy maxfiy qiymatni kelishish bosqichlariga joriy etiladi, indeks, qidiruv tuynugi va serverdagi tekshirish esa klassik ko‘rinishda saqlanadi. Bu yondashuv parametrli amallarni foydalanuvchi tomonida qo‘llash imkonini beradi.

Foydalanilgan adabiyotlar

1. Boneh D., Di Crescenzo G., Ostrovsky R., Persiano G. Public key encryption with keyword search // Advances in Cryptology – EUROCRYPT 2004, LNCS vol. 3027. – Berlin: Springer, 2004. – P. 506–522.

2. Zhou Y., Li N., Tian Y., An D., Wang L. Public key encryption with keyword search in cloud: a survey // Entropy. – 2020. – Vol. 22, No. 4. – Article 421.

3. Khudoykulov Z., Khudoynazarov U., Muminova M. Efficient computation of parametric exponentiation in parametric algebra // International Journal of Advanced Computer Science and Applications. – 2026. – Vol. 17, No. 4.

4. Khudoynazarov U. Public key searchable encryption algorithms // International Conference on Science, Education & Law. – 2026. – Vol. 2, Issue 9. – P. 21–25.

5. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. – 1976. – Vol. 22, No. 6. – P. 644–654.

6. Bai L., Yong L., Chen Z., Shao J. Pairing-free public-key authenticated encryption with keyword search // Computer Standards & Interfaces. – 2023.

7. Jin K., Liu K., Shi L., Wang S., Zhou J. Pairing-free public-key authenticated encryption with keyword search resistant to frequency analysis for IoT // Journal of Intelligent Computing and Networking. – 2025. – Vol. 1, No. 2. – P. 31–39.

8. Chan K.-M., Heng S.-H., Tan S.-Y., Tan S.-C. Efficient k-resilient public key authenticated encryption with keyword search // Journal of Cybersecurity and Privacy. – 2025. – Vol. 5. – Article 62.

9. Wu W., Shi H. Pairing-free searchable encryption for enhancing security against frequency analysis attacks // Electronics. – 2025. – Vol. 14, No. 3. – Article 552.

10. Xudoykulov Z.T., Xudoynazarov U.U., Jafarov M.M. Qidirish imkoniyatli shifrlash algoritmlarining tasnifi va modellari // Infocommunications: Networks – Technologies – Solutions. – 2025. – № 4 (76). – B. 37–48.

BLOKCHEYN TEXNOLOGIYASINING PAYDO BO‘LISHI VA RAQAMLI FAYLLAR YAXLITLIGINI TA’MINLASHDAGI O‘RNI

Turdibekov B.B.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada blokcheyn texnologiyasining paydo bo‘lish tarixi - Merkle xesh daraxti va hujjatlarga vaqt belgisini qo‘yish sxemalaridan Bitcoin, smart-kontraktlar va zamonaviy standartlargacha bo‘lgan bosqichlari tahlil qilinadi, uning ildizlari raqamli hujjat yaxlitligini isbotlash g‘oyasiga borib taqalishi ko‘rsatiladi. Blokcheynning raqamli fayllar yaxlitligini ta’minlashdagi o‘rni asoslab beriladi, xeshlarni bog‘lash, xesh kalendari, smart-kontraktli reyestrlar, ruxsat etilgan blokcheynlar va IPFS bilan gibrid saqlash kabi mavjud yondashuvlar qiyosiy tahlil qilinadi.

Kalit so‘zlar: blokcheyn, raqamli fayl yaxlitligi, xesh funksiya, Merkle daraxti, vaqt belgisi, konsensus, IPFS.

Аннотация. В статье анализируется история возникновения технологии блокчейн - от хеш-дерева Меркла и схем временных меток цифровых документов до Bitcoin, смарт-контрактов и современных стандартов – и показано, что её истоки восходят к идее доказательства целостности цифровых документов. Обоснована роль блокчейна в обеспечении целостности цифровых файлов, проведён сравнительный анализ существующих подходов: привязки хешей к блокчейну, хеш-календаря, реестров на смарт-контрактах, разрешённых блокчейнов и гибридного хранения с IPFS.

Ключевые слова: блокчейн, целостность цифровых файлов, хеш-функция, дерево Меркла, временная метка, консенсус, IPFS.

Kirish

Bugungi kunda davlat boshqaruvi, bank-moliya, sog‘liqni saqlash, ta’lim va sud-ekspertiza tizimlarida qarorlar asosan raqamli fayllar-elektron hujjatlar, skanerlangan nusxalar, tasvir va multimedia materiallari asosida qabul qilinmoqda. Hujjatlarda rekvizitlarni yashirin tahrirlash, tasvirlarda montaj va sun’iy intellekt yordamida soxta kontent yaratish holatlari kengaymoqda. Bunday o‘zgarishlar ko‘pincha vizual ko‘rinishda sezilmaydi, shu sababli faylning dastlabki holatini ishonchli qayd etish va keyinchalik uni isbotlanadigan tarzda tekshirish masalasi dolzarb bo‘lib qolmoqda. An’anaviy yondashuvlarda fayl xesh qiymati yoki elektron raqamli imzo bilan bog‘liq ma’lumotlar markazlashgan serverda saqlanishi mumkin. Biroq server ma’muri yoki unga ruxsatsiz kirish imkonini qo‘lga kiritgan shaxs faylni ham, nazorat uchun saqlangan xesh qiymatini ham almashtirishga urinishi mumkin. Natijada “nazoratchini kim nazorat qiladi?” degan savol tug‘iladi. Blokcheyn bitta markaziy saqlovchiga bo‘lgan ishonchni kamaytirish va yozuvlarning o‘zgartirilganini aniqlash imkonini beruvchi yondashuvlardan biridir.

Asosiy qism. *Blokcheynning paydo bo‘lishi.* Blokcheyn ko‘pincha 2008-yilda e’lon qilingan Bitcoin bilan bog‘lanadi, ammo uning ilmiy asoslari ancha oldin shakllangan. R. Merkle xesh daraxti ko‘plab yozuvlarni bitta ildiz xeshiga jamlash imkonini berdi [1], L. Lamport va hammualliflar esa ishonchsiz ishtirokchilar mavjud bo‘lgan tizimda kelishuvga erishish masalasini ta’rifladilar [2]. Fayl yaxlitligi nuqtai nazaridan eng muhim qadam 1991-yilda S. Haber va W. S. Stornetta tomonidan qo‘yilgan. Ular hujjat xeshini oldingi yozuv xeshi bilan bog‘lab, zanjir hosil qilishni taklif etishdi, natijada biror yozuvni o‘zgartirish keyingi barcha bog‘lanishlarni buzadigan

bo‘ldi [3]. Aynan shu ishlar Bitcoin hujjatidagi sakkizta manbadan uchtasini tashkil etgani blokcheynning “raqamli hujjat yaxlitligi” g‘oyasidan o‘sib chiqqanini ko‘rsatadi. Keyinchalik PBFT algoritmi amaliy Vizantiya nosozliklariga bardoshli konsensus yondashuvini ishlab chiqdi [4], S. Nakamoto esa xesh zanjiri, Merkle daraxti va ishni isbotlash (Proof of Work, PoW) mexanizmini Bitcoin tizimida birlashtirdi [5]. Keyingi yillarda smart-kontraktlar, ruxsat etilgan blokcheynlar va xeshlarni blokcheynga biriktirish xizmatlari rivojlandi. Blokcheyn atamalari va arxitekturasi NIST IR 8202 [7] hujjatida yoritilgan. 2022-yilda Ethereum PoW’dan ulushni isbotlash (Proof of Stake, PoS) mexanizmiga o‘tdi. 2024-yilda esa NIST postkvant elektron imzo standartlarini e’lon qildi [15]. Asosiy bosqichlar 1-jadvalda umumlashtirilgan.

1-jadval

Blokcheyn texnologiyasining shakllanish bosqichlari

Yil	Muallif / loyiha	Raqamli fayllar yaxlitligi uchun hissasi
1979-1987	R. Merkle [1]	Xesh daraxti, ko‘p yozuvni bitta ildiz xeshiga jamlash, bitta yozuvni tekshirish uchun odatda $O(log\ n)$ hajmli isbot
1982	L. Lamport va boshq [2].	Vizantiya generallari masalasi, nosoz va zararli ishtirokchilar mavjud bo‘lganda kelishuvga erishish nazariyasi
1991	S. Haber, W. S. Stornetta [3]	Hujjat xeshlarini zanjirga bog‘lash va vaqt belgisini qo‘yish, yozuvlar ketma-ketligini tekshirish
1999	M. Castro, B. Liskov [4]	PBFT, $n \geq 3f + 1$ sharti ostida f tagacha Vizantiya turidagi nosozlikka bardoshlilik
2008-2009	S. Nakamoto (Bitcoin) [5]	Xesh zanjiri, Merkle daraxti va ishni isbotlash konsensusining yagona ochiq reyestrda birlashtirilishi
2014-2015	V. Buterin (Ethereum) [6]	Smart-kontraktlar, yozuvlarni qayd etish va tekshirish qoidalarini dastur sifatida reyestrga kiritish
2014-2017	J. Benet (IPFS), Hyperledger Fabric [8], [9]	Kontentga asoslangan manzillash (CID), tashkilotlar uchun ruxsat etilgan blokcheynlar
2016-2017	OpenTimestamps, Chainpoint, Blockcerts [13], [14]	Fayl xeshlarini ochiq blokcheynga bog‘lash, diplomlarni blokcheynda tasdiqlash
2018	NIST IR 8202 [7]	NIST IR 8202 blokcheyn tushunchalari hamda arxitekturasini bayon qiladi
2022	Ethereum (The Merge) [5]	Postkvant raqamli imzo standartlari, ular imzo mexanizmlarini belgilaydi, ammo blokcheynni o‘z-o‘zidan kvant hujumlaridan himoya qilmaydi
2024	NIST FIPS 204 [15]	Postkvant elektron imzo standartlari, ular kelajakdagi kvant hujumlariga qarshi imzo mexanizmlarini belgilaydi

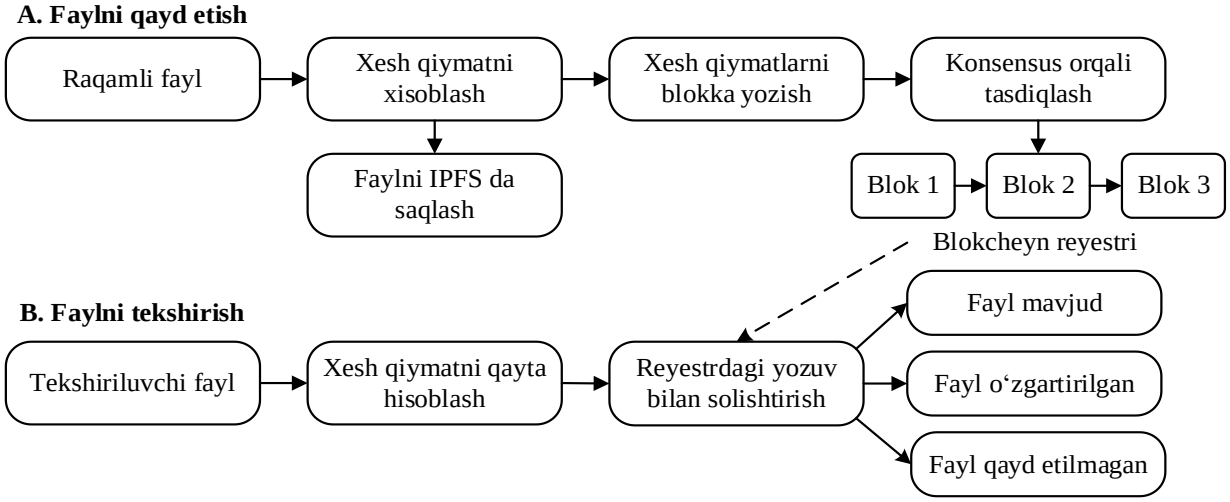
Blokcheynning fayl yaxlitligini ta’minlashdagi o‘rni. NIST IR 8202 hujjatida blokcheyn kriptografik xeshlar, elektron raqamli imzolar va konsensus mexanizmlariga tayanuvchi

taqsimlangan reyestr sifatida ta’riflanadi [7]. Fayl yaxlitligini ta’minlashda uning uch xususiyati hal qiluvchi ahamiyatga ega.

Birinchidan, xesh orqali bog‘lanish. Fayl F uchun SHA-256 kabi kriptografik xesh-funksiya [10] yordamida $h = H(F)$ qiymati hisoblanadi. Fayldagi bitta bitning o‘zgarishi odatda butunlay boshqa xesh qiymatini beradi, biroq xesh-funksiya kolliziyalarga qarshi bardoshli bo‘lishi kerak. Bloklar o‘zaro oldingi blok xeshi orqali bog‘lanadi. Umumiy ko‘rinishda i-blok xeshini $B_i = H(B_{i-1} \parallel R_i \parallel t_i)$ tarzida ifodalash mumkin, bu yerda B_{i-1} - oldingi blok xeshi, R_i - tranzaksiyalarning Merkle ildizi, t_i - vaqt belgisi. Bu formula tushuntiruvchi umumlashtirish bo‘lib, aniq blok sarlavhasi tarkibi blokcheyn protokoliga qarab farq qiladi. Shu bois oldingi yozuvni o‘zgartirishni aniqlash mumkin, ammo uni qayta hisoblashning o‘zi barcha blokcheynlarda bir xil xarajat yoki imkonsizlikni anglatmaydi.

Ikkinchidan, taqsimlanganlik va konsensus. Reyestr nusxalari bir nechta tugunda saqlanishi mumkin, biroq yozuvni qabul qilish qoidalari tanlangan protokolga bog‘liq. Klassik BFT konsensus algoritmlarining ayrimlarida $n \geq 3f + 1$ sharti bajarilganda f tagacha Vizantiya turidagi nosoz tugunga bardosh berish ko‘zda tutiladi. Bu xulosa barcha blokcheynlarga avtomatik ravishda tatbiq etilmaydi: xavfsizlik va yakuniy tasdiqlash kafolatlari konsensus mexanizmiga, tugunlar soniga hamda ishonch modeliga bog‘liq.

Uchinchidan, mavjudlikni tasdiqlash va audit. Blokcheynga fayl xeshi hamda vaqt belgisi bilan bog‘liq yozuv kiritilgani, tegishli tasdiqlar mavjud bo‘lsa, keyinchalik fayl xeshining shu yozuvga mosligini tekshirish imkonini beradi. Merkle daraxtida bitta elementga oid isbot hajmi odatda $O(log_2 n)$ ta xeshga teng bo‘ladi, aniq hajm daraxt tuzilishi va elementlar soniga bog‘liq. Xesh funksiyasini tanlash. MD5 va SHA-1 algoritmlarida kolliziyalarga qarshi amaliy hujumlar ko‘rsatilganligi sababli, yangi tizimlarda SHA-256 yoki SHA-3 kabi zamonaviy algoritmlardan foydalanish ma’qul [10]. Tanlashda xavfsizlik talablari bilan birga ishlash tezligi ham baholanadi. Samaradorlikni bayt/sikl, MB/s yoki KHash/s kabi ko‘rsatkichlarda ifodalash mumkin, biroq natijalar apparat va dasturiy muhitga bog‘liq [11]. Blokcheyn asosida fayl yaxlitligini ta’minlashning umumiy tamoyili 1-rasmda keltirilgan: *A* qismida fayl xeshi blokka jamlanib, konsensus orqali reyestrga yoziladi, *B* qismida qayta hisoblangan xesh reyestrdagi yozuv bilan solishtiriladi.



1-rasm. Blokcheyn asosida raqamli fayllarni qayd etish va yaxlitligini tekshirishning umumlashtirilgan sxemasi

Mavjud yondashuvlar. Amaliyotda blokcheyn asosida raqamli fayllar yaxlitligini ta’minlashning bir nechta yondashuvi shakllangan. Ularning barchasida reyestrga faylning o‘zi emas, xesh qiymati yoziladi.

Birinchi yondashuv - ochiq blokcheynga xeshni bog‘lash (anchoring). OpenTimestamps fayl xeshlarini Merkle daraxti orqali jamlab, yakuniy xeshni Bitcoin blokcheyniga joylashtirishga mo‘ljallangan [13]. Chainpoint ham ma’lumotlar uchun blokcheyn kvitansiyalarini yaratish va xeshlarni bog‘lash protokoli sifatida ishlab chiqilgan [14], biroq uni OpenTimestamps bilan aynan bir xil amalga oshirish deb qarash to‘g‘ri emas. Foydalanuvchi fayl xeshining blokcheyndagi yozuvga bog‘liqligini tekshirish uchun kerakli kriptografik isbotni saqlaydi. Xarajat va tasdiqlash vaqti tarmoq yuklamasi, tranzaksiya to‘lovi va protokolga bog‘liq.

Ikkinchi yondashuv - *xesh kalendari*. Guardtime kompaniyasining KSI (Keyless Signature Infrastructure) tizimida har soniyada global xesh daraxti quriladi va uning ildizlari o‘zgarmas kalendar zanjiriga bog‘lanadi [12]. Tizim yopiq kalitlarga tayanmaydi va soniyalar ichida isbot beradi. Uchinchi yondashuv - *smart-kontraktli reyestrlar*: hujjat xeshi, egasi va vaqti Ethereum smart-kontraktiga yoziladi va tekshirish qoidalari dastur sifatida belgilanadi [6]. Masalan, Blockcerts ochiq standarti diplom va sertifikatlarni blokcheynda tasdiqlash uchun ishlab chiqilgan.

To‘rtinchi yondashuv - *ruxsat etilgan (xususiy yoki konsorsium) blokcheynlar*. Hyperledger Fabric kabi platformalarda reyestr faqat ma’lum tashkilotlar tugunlarida yuritiladi, konsensus esa PBFT yoki Raft kabi algoritmlar orqali amalga oshiriladi [4], [9]. Bu tezlik va maxfiylikni ta’minlaydi, lekin ishonch ishtirokchilar soni bilan cheklanadi. Beshinchi yondashuv - *gibrid off-chain/on-chain saqlash*: faylning o‘zi kontentga asoslangan manzillashni qo‘llovchi IPFS muhitida saqlanadi [8], blokcheynda esa faqat xesh, CID va metama’lumotlar qayd etiladi. Ko‘rib chiqilgan yondashuvlarning qiyosiy tavsifi 2-jadvalda keltirilgan.

2-jadval

Blokcheyn asosida fayl yaxlitligini ta’minlash yondashuvlari

Yondashuv	Misollar	Afzalligi	Cheklovi
Ochiq blokcheynga bog‘lash	OpenTimestamps, Chainpoint	Arzon, ommaviy, markazsiz ishonch	Tarmoq va protokolga qarab tasdiqlash kechikishi
Xesh kalendari	Guardtime KSI	Tezkor isbot, an’anaviy yopiq kalitli imzo sxemasiga tayanmaydi	Operator infratuzilmasiga bog‘liqlik
Smart-kontraktli reyestr	Ethereum, Blockcerts	Tekshirish qoidalarini dasturlash	Tranzaksiya to‘lovi, ochiq reyestrda maxfiylik cheklovlari
Ruxsat etilgan blokcheyn	Hyperledger Fabric	Tezlik, kirish nazorati, maxfiylik	Raftning o‘zi Vizantiya turidagi zararli tugunlarga bardosh bermaydi
Gibrid off-chain / on-chain	IPFS + blokcheyn	Katta fayllar uchun mos, CID orqali tekshirish	Fayl mavjudligi alohida kafolatlanadi

Cheklovlar. Blokcheyn barcha muammolarni mustaqil hal qilmaydi. Birinchidan, u reyestrga kiritilgan ma’lumotni himoya qiladi, lekin kiritilgunga qadar o‘zgartirilgan faylni ham “haqiqiy” deb qayd etib qo‘yishi mumkin, shu sababli ro‘yxatga olishdan oldin faylni raqamli

kriminalistika usullari bilan tekshirish talab etiladi. Ikkinchidan, katta fayllarni zanjirda saqlash reyestr hajmi va xarajatlarni keskin oshiradi. Uchinchidan, yozuvlarning o‘zgarmasligi shaxsga doir ma’lumotlarni o‘chirish talablariga zid kelishi mumkin, shuning uchun reyestrga faqat xesh yoziladi.

Qo‘llanish sohalari. Ushbu yondashuvlar elektron hujjat aylanishi, raqamli kriminalistikada dalillarning “saqlash zanjiri”ni hujjatlashtirish, arxiv fondlari, diplom va sertifikatlarni tekshirish hamda davlat reyestrlari auditida qo‘llanilmoqda.

Xulosa. Blokcheyn texnologiyasi tasodifiy kashfiyot emas, balki raqamli hujjatlar yaxlitligini isbotlash bo‘yicha qariyb o‘ttiz yillik kriptografik tadqiqotlarning - Merkle daraxti, xesh zanjiri asosidagi vaqt belgisi va Vizantiya nosozligiga bardoshli konsensusning - mantiqiy natijasidir. Uning raqamli fayllar yaxlitligini ta’minlashdagi o‘rni faylning o‘zini saqlashda emas, balki fayl xesh qiymati, vaqt belgisi va audit dalillarini yagona ishonchli tomonga bog‘liq bo‘lmagan, o‘zgartirilishi qiyin reyestrda qayd etishdadir. Mavjud yondashuvlar tahlili shuni ko‘rsatadiki, ochiq blokcheynga bog‘lash arzon va ommaviy isbotni, xesh kalendari tezkorlikni, ruxsat etilgan blokcheynlar esa maxfiylik va boshqaruvni ta’minlaydi, amaliyotda esa gibrid arxitektura eng maqbul hisoblanadi.

Foydalanilgan adabiyotlar:

1. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function // Advances in Cryptology – CRYPTO‘87. LNCS. Vol. 293. -Springer, 1988. -P. 369-378.
2. Lamport L., Shostak R., Pease M. The Byzantine Generals Problem // ACM Transactions on Programming Languages and Systems. -1982. -Vol. 4, № 3. -P. 382-401.
3. Haber S., Stornetta W. S. How to Time-Stamp a Digital Document // Journal of Cryptology. -1991. - Vol. 3, № 2. -P. 99-111.
4. Castro M., Liskov B. Practical Byzantine Fault Tolerance // Proc. 3rd Symposium on Operating Systems Design and Implementation (OSDI). -1999. -P. 173-186.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. -2008.
6. Buterin V. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. -2014.
7. Yaga D., Mell P., Roby N., Scarfone K. Blockchain Technology Overview. NIST IR 8202. -Gaithersburg: NIST, 2018. -DOI: 10.6028/NIST.IR.8202.
8. Benet J. IPFS -Content Addressed, Versioned, P2P File System. -arXiv:1407.3561, 2014.
9. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // Proc. EuroSys’18. -ACM, 2018. -P. 30:1-30:15.
10. National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS PUB 180-4. -2015. -DOI: 10.6028/NIST.FIPS.180-4.
11. Abduraximov B., Allanov O., Turdibekov B. Blokcheyn tizimlari uchun xesh funksiyalarni tanlash mezonlari va samaradorlik ko‘rsatkichlari tahlili // Muhandislik va iqtisodiyot. -2025. -№ 12. -B. 32-38.
12. Buldas A., Kroonmaa A., Laanoja R. Keyless Signatures’ Infrastructure: How to Build Global Distributed Hash-Trees // Secure IT Systems (NordSec 2013). LNCS. Vol. 8208. -Springer, 2013. -P. 313-320.
13. Todd P. OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin. -2016. -URL: https://petertodd.org/2016/opentimestamps-announcement.
14. Vaughan W. et al. Chainpoint: A Scalable Protocol for Anchoring Data in the Blockchain and Generating Blockchain Receipts. -Tierion, 2016.
15. National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204. -2024. -DOI: https://doi.org/10.6028/NIST.FIPS.204.

KVANT KRIPTOGRAFIYASI VA UNING AXBOROT XAVFSIZLIGINI TA’MINLASHDAGI AHAMIYATI

Chunayev N.E.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda kvant kriptografiyasining nazariy asoslari, ishlash tamoyillari va zamonaviy axborot xavfsizligi tizimlaridagi ahamiyati tahlil qilinadi. Kvant mexanikasi qonunlariga asoslangan kriptografik usullarning an’anaviy shifrlash texnologiyalaridan farqli jihatlari, kvant kalitlarini taqsimlash (QKD) texnologiyasi hamda BB84 protokolining ishlash mexanizmi yoritiladi. Shuningdek, kvant kriptografiyasini amaliyotga tatbiq etishdagi muammolar va rivojlanish istiqbollari ko‘rib chiqiladi.

Kalit so‘zlar: kvant kriptografiyasi, axborot xavfsizligi, kvant kalitlarini taqsimlash, QKD, BB84 protokoli, kvant kompyuterlari, shifrlash, postkvant kriptografiya.

Аннотация. В данном тезисе анализируются теоретические основы квантовой криптографии, принципы её работы и значение в современных системах информационной безопасности. Рассматриваются отличительные особенности криптографических методов, основанных на законах квантовой механики, по сравнению с традиционными технологиями шифрования, технология квантового распределения ключей (QKD), а также механизм работы протокола BB84. Кроме того, исследуются проблемы практического внедрения квантовой криптографии и перспективы её дальнейшего развития.

Ключевые слова: квантовая криптография, информационная безопасность, квантовое распределение ключей, QKD, протокол BB84, квантовые компьютеры, шифрование, постквантовая криптография.

Kirish

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida axborotlarni himoyalash, ularning maxfiyligi va yaxlitligini ta’minlash muhim vazifalardan biriga aylandi. Internet tarmoqlari, elektron tijorat, bank tizimlari va davlat axborot resurslarida uzatilayotgan ma’lumotlarni turli kiberhujumlardan himoya qilish uchun zamonaviy kriptografik algoritmlardan foydalanilmoqda.

An’anaviy kriptografiya usullarining ayrimlari, jumladan, RSA va elliptik egri chiziqlarga asoslangan algoritmlar, katta miqyosli kvant kompyuterlari rivojlanishi natijasida xavf ostida qolishi mumkin. Shu sababli kvant texnologiyalariga asoslangan xavfsizlik usullarini tadqiq etish dolzarb ilmiy yo‘nalishlardan biri hisoblanadi.

Kvant kriptografiyasining nazariy asoslari

Kvant kriptografiyasi - kvant mexanikasining fizik qonuniyatlaridan foydalanib, kriptografik vazifalarni bajarishga mo‘ljallangan usullar majmuasidir. Ushbu texnologiyaning muhim yo‘nalishlaridan biri kvant kalitlarini taqsimlash (Quantum Key Distribution - QKD) hisoblanadi.

QKD texnologiyasida maxfiy kalitni shakllantirish uchun fotonlarning kvant holatlaridan foydalaniladi. Kvant holatlarini o‘lchash jarayonida ularning o‘zgarishi kuzatilishi mumkin. Mazkur xususiyat uzatilayotgan kalit haqidagi ma’lumotni uchinchi tomon yashirin ravishda olishga harakat qilganini aniqlash imkonini beradi [1].

Kvant kriptografiyasining nazariy asoslari quyidagi fizik tushunchalar bilan bog‘liq:

– Kvant superpozitsiyasi - kvant tizimining o‘lchashgacha bir nechta holatlarning kombinatsiyasida mavjud bo‘lishi.

– Kvant holatini o‘lchash - tizimning holati haqida ma’lumot olish jarayoni bo‘lib, ayrim holatlarda uning o‘zgarishiga olib keladi.

– Nusxalashning mumkin emasligi teoremasi - noma’lum ixtiyoriy kvant holatining mukammal nusxasini yaratish mumkin emasligini ifodalaydi.

– Mazkur tamoyillar QKD protokollarining xavfsizlik asosini tashkil etadi.

BB84 protokoli va uning ishlash tamoyili

Kvant kriptografiyasining eng mashhur protokollaridan biri 1984-yilda Charlz Bennet va Jil Brassar tomonidan taklif etilgan BB84 protokolidir [2].

BB84 protokoli ikki foydalanuvchi o‘rtasida maxfiy kalitni xavfsiz taqsimlashga xizmat qiladi. Protokolning ishlash jarayoni quyidagi bosqichlarni o‘z ichiga oladi:

1. Jo‘natuvchi tasodifiy bitlar ketma-ketligini shakllantiradi va ularni fotonlarning kvant holatlari yordamida kodlaydi.
2. Qabul qiluvchi fotonlarni tasodifiy tanlangan o‘lchash bazislari orqali qabul qiladi.
3. Tomonlar autentifikatsiyalangan ochiq aloqa kanali orqali foydalanilgan bazislarni taqqoslaydi.
4. Mos kelgan bazislar bo‘yicha olingan bitlar dastlabki kalitni hosil qiladi.
5. Xatoliklar darajasi baholanadi, zarur hollarda xatolar tuzatiladi va maxfiylikni kuchaytirish amallari bajariladi.

Agar aloqa kanaliga uchinchi tomon aralashsa, kvant holatlarining buzilishi uzatilayotgan ma’lumotlarda xatoliklar paydo bo‘lishiga sabab bo‘lishi mumkin. Natijada tomonlar kuzatilgan xatoliklar darajasiga qarab kalitni qabul qilish yoki aloqa jarayonini to‘xtatish haqida qaror qabul qiladi.

Shuni ta’kidlash kerakki, QKD ma’lumotlarning o‘zini shifrlash algoritmi emas, balki ularni shifrlash uchun zarur maxfiy kalitlarni taqsimlash texnologiyasidir.

Kvant kriptografiyasining afzalliklari va muammolari

Kvant kriptografiyasining asosiy afzalligi kvant mexanikasi qonunlariga tayangan holda maxfiy kalit almashinuvini tashkil etish imkoniyatidir. Tegishli xavfsizlik shartlari bajarilganda, bu yondashuv kalitni taqsimlash jarayonida tinglash urinishlarini aniqlashga yordam beradi.

Biroq ushbu texnologiyani amaliyotga joriy etishda bir qator muammolar mavjud. Jumladan, maxsus foton manbalari va detektorlarning qimmatligi, optik kanallardagi signal yo‘qotilishi, qurilmalardagi texnik kamchiliklar hamda aloqa kanalini autentifikatsiyalash talablari QKD tizimlarini keng miqyosda joriy etishni murakkablashtiradi [3].

Kvant kriptografiyasi bilan bir qatorda postkvant kriptografiya yo‘nalishi ham rivojlanmoqda. Postkvant kriptografiya kvant kompyuterlarining ehtimoliy hujumlariga bardosh bera oladigan matematik algoritmlarni ishlab chiqishga qaratilgan bo‘lib, odatiy kompyuter va tarmoq infratuzilmalarida qo‘llanishi mumkin.

2024-yilda AQSh Milliy standartlar va texnologiyalar instituti (NIST) ML-KEM, ML-DSA va SLH-DSA algoritmlarini o‘z ichiga olgan dastlabki uchta postkvant kriptografik standartni tasdiqladi [4]. Bu esa kelajakdagi axborot xavfsizligi tizimlarida kvantga bardoshli texnologiyalarni qo‘llash muhim ahamiyat kasb etishini ko‘rsatadi.

Xulosa

Xulosa qilib aytganda, kvant kriptografiyasi axborot xavfsizligini ta’minlashning istiqbolli yo‘nalishlaridan biri hisoblanadi. Kvant mexanikasi qonuniyatlariga asoslangan QKD

texnologiyasi maxfiy kalitlarni almashish jarayonini himoyalash uchun yangi imkoniyatlarni taqdim etadi.

Tahlillar shuni ko‘rsatadiki, kvant kriptografiyasining nazariy afzalliklari bilan bir qatorda, uning amaliy samaradorligi qurilmalar ishonchliligi, aloqa kanali sifati va autentifikatsiya mexanizmlariga ham bog‘liq. Shuning uchun QKD texnologiyasini postkvant kriptografik algoritmlar bilan birgalikda tadqiq etish va ularning o‘zaro muvofiqligini ta’minlash dolzarb vazifalardan biridir.

Kelajakda kvant kriptografiyasi telekommunikatsiya tarmoqlari, moliyaviy tizimlar va muhim axborot infratuzilmalarida maxfiy ma’lumotlarni himoyalashning qo‘shimcha mexanizmi sifatida muhim o‘rin egallashi mumkin.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. *What Is Quantum Cryptography?* https://www.nist.gov/cybersecurity-and-privacy/what-quantum-cryptography

2. Bennett C. H., Brassard G. *Quantum Cryptography: Public Key Distribution and Coin Tossing.* Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, 1984. 175–179-betlar. https://arxiv.org/abs/2003.06557

3. European Telecommunications Standards Institute (ETSI). *Quantum Key Distribution (QKD).* https://www.etsi.org/technical-groups/qkd/

4. National Institute of Standards and Technology. *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography.* 13 August 2024. https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

SHIFRLASH ALGORITMLARINING NEYRON TARMOQLAR YORDAMIDA KRIPTOTAHLILI

Imomov E.M., Salohiddinov H.F.
Kriptologiya, axborot xavfsizligi va innovatsion texnalogiyalar instituti

Annotatsiya. Maqolada tarixiy va zamonaviy simmetrik shifrlarni neyron tarmoqlar yordamida kriptotahlil qilish bo‘yicha ilmiy yondashuvlari hamda usullarning yuqori hisoblash murakkabligi fonida intellektual yondashuvlarning imkoniyatlari tahlili keltirilgan. Tahlil neyron tarmoqlar soddalashtirilgan shifrlarda yuqori samaradorligini, ammo to‘liq raundli algoritmlar uchun ularning imkoniyatlari hozircha cheklanganini hamda natijalar o‘qitish hajmi va hisoblash resurslariga bevosita bog‘liqligini ko‘rsatilgan. Neyron tarmoqlar klassik usullarni to‘liq almashtirmay, balki ularni to‘ldiruvchi vosita ekani asoslanib, istiqbolli tadqiqot yo‘nalishlar va takliflar keltiringan.

Kalit so‘zlar: kriptotahlil; neyron tarmoqlar; chuqur o‘rganish; simmetrik shifrlash; Vijener shifri; GRU/LSTM; differensial-neyron kriptotahlil; CNN; Inception_v3; shifrmatn klassifikatsiyasi; AES; GPU/TPU.

Аннотация. В статье представлен анализ научных подходов и методов криптоанализа исторических и современных симметричных шифров с использованием нейронных сетей, а также возможностей интеллектуальных методов в условиях высокой вычислительной сложности традиционных подходов. Результаты анализа показывают, что нейронные сети демонстрируют высокую эффективность при исследовании упрощённых шифров, однако их возможности в отношении алгоритмов с полным числом раундов на данном этапе остаются ограниченными. Установлено, что эффективность получаемых результатов непосредственно зависит от объёма обучающих данных и доступных вычислительных ресурсов. Обосновано, что нейронные сети не заменяют полностью классические методы криптоанализа, а выступают в качестве дополняющего инструмента. Определены перспективные направления дальнейших исследований и сформулированы соответствующие предложения.

Ключевые слова: криптоанализ; нейронные сети; глубокое обучение; симметричное шифрование; шифр Виженера; GRU/LSTM; дифференциально-нейросетевой криптоанализ; CNN; Inception_v3; классификация шифротекста; AES; GPU/TPU.

Kirish

Axborot-kommunikatsiya tizimlari, davlat boshqaruvi, moliya sohasi, elektron tijorat, bulutli texnologiyalar va IoT qurilmalarida uzatiladigan ma’lumotlarni himoyalash uchun kriptografik algoritmlar keng qo‘llanilmoqda. Hisoblash quvvatlarining ortishi hamda sun’iy intellekt va mashinaviy o‘qitish texnologiyalarining rivojlanishi mavjud kriptografik tizimlarning bardoshliligini yangi nuqtai nazardan baholashni talab etmoqda.

Respublikamizda kriptologiya va sun’iy intellekt yo‘nalishlarini rivojlantirish davlat siyosatining ustuvor vazifalaridan biri sifatida belgilangan. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi PQ-293-son qaroriga 2-ilova sifatida tasdiqlangan 2024-2028-yillarga mo‘ljallangan ilmiy-tadqiqot ishlari dasturining 15-bandi zamonaviy kriptotahlil usullarini yaratishga qaratilgan [1]; 2021-yil 17-fevraldagi PQ-4996-son qaror esa sun’iy intellekt texnologiyalarini joriy etish va ilmiy tadqiqotlarni qo‘llab-quvvatlash vazifalarini

belgilaydi [2]. Kriptografik algoritmlar bardoshliligini baholashda qo‘llaniladigan klassik usullar yuqori matematik murakkablikka ega [3]. Shu nuqtayi nazardan, shifrlash algoritmlarining kriptografik bardoshliligini baholashda neyron tarmoqlar va sun’iy intellekt texnologiyalariga asoslangan kriptotahlil usullarining nazariy asoslarini rivojlantirish hamda ularning samaradorligini oshirishga qaratilgan ilmiy yondashuvlarni ishlab chiqish mazkur tadqiqot ishining dolzarbligini belgilaydi.

Asosiy qism

Kriptotahlil atamasi XX asrning yigirmanchi yillarida amerikalik kriptograf Uilyam Fridman tomonidan kiritilgan [3]. Kriptografik algoritmlarga bog‘liq zaifliklar uch sinfga ajratiladi: shifrlash algoritmi kriptobardoshliligi bilan bog‘liq zaifliklar; algoritmdan noto‘g‘ri foydalanish bilan bog‘liq zaifliklar; kriptografik tarmoq protokollari zaifliklari. Dastlabki ikki sinf shifrlash algoritmlarini kriptotahlil qilish orqali aniqlanadi. Klassik usullar qatoriga to‘liq tanlash, chiziqli, differensial, chiziqli-differensial, slayd, integral va algebraik kriptotahlil hamda apparat xatoliklarni generatsiyalashga asoslangan usul kiritiladi [3].

Hozirgi kunga qadar jahon miqyosida hamda respublikamizda sun’iy intellekt va neyron tarmoq modellarini kriptotahlil jarayonlariga tatbiq etish bo‘yicha keng qamrovli amaliy tadqiqotlar olib borilmoqda.

Klassik shifrlash algoritmlari misolida mamlakatimizda: PyTorch muhitida rekurrent neyron tarmog‘ (GRU arxitekturasi) asosida model qurilib, ko‘p harfli almashtirishga asoslangan Vijener shifrini shifrmatn orqali ochiq matnga qaytarish (deshifrlash) tajribasi o‘tkazilgan. Natija: boshlang‘ich kichik parametrli model yuqori xatolik ko‘rsatgan bo‘lsa-da, dataset hajmi oshirilib va arxitektura optimallashtirilgach, yo‘qotish (loss) qiymati qariyb nolga tushib, shifrlangan matn tiklangan.[4]

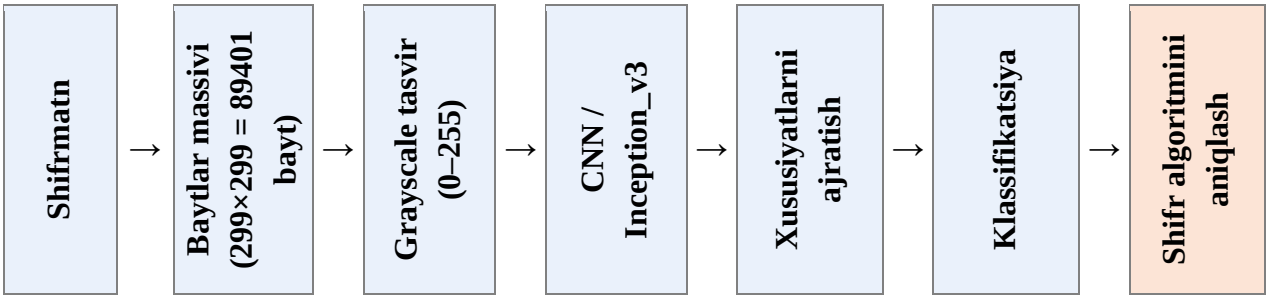
Blokli simmetrik shifrlash algoritmlari jahon va maklakatimizda amalga oshirilgan ilmiy izlanishlar:

Germaniyaning tadqiqotchisi Aron Gohr tomonidan 2019-yilda "CRYPTO 2019" xalqaro konferensiyasi (Springer-Verlag nashriyoti) doirasida e’lon qilingan ilmiy ishida raundlari qisqartirilgan Speck32/64 blokli shifriga qarshi chuqur o‘rganishga asoslangan kriptotahlil yondashuvi taklif etilgan. Muallif shifrmatn juftliklarini (4x16 matritsa ko‘rinishida) tasodifiy ma’lumotlardan farqlash uchun 1D konvolyutsion qatlamlariga ega chuqur qoldiqli neyron tarmoq (ResNet) arxitekturasidan hamda kalit qidirishda Bayes optimallashtirish algoritmidan foydalangan. Natijada, 9 raundli hujumda o‘rtacha kalit klassik usulga nisbatan 5 baravar qisqartirilgan, 11 raundli Speck32/64 shifrini buzishning hisoblash murakkabligi esa 2^{46} dan 2^{38} amalgacha tushirilgan. Ishning asosiy ilmiy yangiligi – chuqur neyron tarmoqlar va an’anaviy kriptotahlil uyg‘unligida zamonaviy simmetrik shifrlarga qarshi mavjud klassik usullardan ustunroq hujum modelining ilk bor ilmiy hamjamiyatda taqdim etgan [5].

Shu bilan birga Xitoylik olimlar Liu Zhang va Zilong Wang o‘z tadqiqotida DES, Chaskey va PRESENT kabi uchta shifrlash algoritmini tahlil qilish uchun GoogLeNet (Inception) va ResNet (qoldiqli tarmoq) arxitekturalari birlashmasiga asoslangan yangi neyron tarmoq modelini ishlab chiqqanlar. Natijada, shifrni tasodifiy sonlardan ajratish aniqligi avvalgi usullarga qaraganda keskin oshib, 6-raundli DES shifrida 55% dan 76% ga, 4-raundli Chaskey shifrida 61% dan 98.3% ga, 7-raundli PRESENT shifrida esa 54% dan 72% ga ko‘tarilgan. Oddiy qilib aytganda DES, Chaskey va PRESENT shifrlari uchun kalitni topishning o‘zini emas, balki kelgusida kalitni ancha oson va ko‘proq raundlarda topishga xizmat qiladigan kuchliroq “neyron farqlovchi” (aniqlovchi) modelni taqdim etishgan [6].

Janubiy Koreyalik olimlar Ongee Jeong, Ezat Ahmadzadeh va Inkyu Moon o‘z tadqiqotida DES, SDES, AES-128, SAES va SPECK32/64 beshta blokli shifrlash algoritmini to‘liq bog‘langan (FC), rekurrent (RNN: BiLSTM, BiGRU) hamda transformer (T5-small, BERT-base) neyron tarmoqlari yordamida kompleks tahlil qilganlar. Mualliflar shifrlarni to‘rt xil hujum – shifrlashni imitatsiya qilish (EE), ochiq matnni tiklash (PR), kalitni topish (KR) va shifrmatnni tasniflash (CC) orqali ham bitlar massivi, ham oddiy matnlar misolida sinovdan o‘tkazganlar. Yondashuvning o‘ziga xos jihati shundaki, matnlarni shifrlashda so‘zma-so‘z va gap bo‘yicha yaxlit shifrlash usullari ECB, CBC hamda CFB rejimlarida solishtirilgan. Olingan natijalarga ko‘ra, RNN (BiLSTM/BiGRU) modellari kalitni topish va shifrmatnni tasniflashda FC hamda Transformer modellaridan yuqori aniqlik ko‘rsatgan bunda: 2-raundli DES va SPECK32/64 da kalit bitlarini topish aniqligi 82.5% va 74.9% ga yetgan, kalit ochiq matn bilan bir xil bo‘lganda esa 100% topilgan.[7]

Shu bilan birga mamlakatimizda ham bu sohada ilmiy izlanishlar va tadqiqotlar amalga oshirilgan. Kriptologiya Instituti bitiruvchisi Xolmonov Sh.Sh. tomonidan olib borilgan tadqiqot ishi davomida zamonaviy blokli (AES, Magma, Kuznechik) hamda klassik (Sezar, Vijener) shifrlash algoritmlarini aniqlash uchun konvolyutsion neyron tarmoqning CNN (Inception_v3) arxitekturasini qo‘llagan. Yondashuvning o‘ziga xos va ustun jihati shundaki, odam ko‘ziga shunchaki tartibsiz shovqin bo‘lib ko‘rinadigan shifrmatn baytlari tasvir piksellariga o‘tkazilganda, har bir algoritmning o‘ziga xos yashirin statistik-strukturaviy “vizual izlari” CNN tarmog‘i orqali osonroq ajratib olinadi. O‘tkazilgan tajribalar natijasida, shifrmatnni ochmasdan (deshifrlamasdan) turib, uning aynan qaysi kriptografik algoritm yordamida shifrlanganligini 98% li yuqori aniqlikda tanib olishga erishilgan.[8]



1-rasm. Shifrmatnni tasvirga aylantirish va shifr algoritmini aniqlash sxemasi

Shu bilan birga, neyron tarmoqlar orqali kriptotahlil jarayonining samaradorligini tadqiq etishda apparat vositalarining o‘rni alohida ahamiyat kasb etadi. Bunda CPU, GPU va TPU platformalari o‘zaro bir-birini to‘ldiruvchi hisoblash zanjirini hosil qiladi. Xususan, CPU (Central Processing Unit) shifrlash algoritmlarini dasturiy bajarish, o‘quv ma’lumotlarini (ochiq matn va shifrmatn juftliklarini) shakllantirish hamda kalit qidirishning murakkab mantiqiy ketma-ket bosqichlarini boshqarish vazifasini bajaradi. GPU (Graphics Processing Unit) o‘zining minglab parallel yadrolari, yuqori o‘tkazuvchanlikka ega xotirasi hamda matritsaviy amallarni bajarishga ixtisoslashgan arxitekturasi orqali chuqur neyron tarmoqlarni millionlab shifrmatn bloklari ustida qisqa vaqtda o‘qitish, og‘irlik koeffitsiyentlarini parallel optimallashtirish va soniyasiga yuz minglab ehtimoliy kalit nomzodlarini parallel tekshirish imkonini berib, kriptotahlilning qidiruv fazosini keskin qisqartiradi. O‘z navbatida, TPU (Tensor Processing Unit) o‘zining matritsaviy hisoblash bloklari (MXU) yordamida katta hajmdagi kriptografik ma’lumotlar oqimini qayta ishlovchi, trillionlab parametrlarga ega ko‘p qatlamli chuqur neyron tarmoq modellarini o‘ta yuqori tezlikda parallel o‘qitish hamda minimal energiya sarfi bilan optimallashtirishni ta’minlaydi. [9-10] Yuqoridagilardan kelib chiqqan holda, CPUning mantiqiy boshqaruvi hamda

GPU va TPU lar ko‘p parallel-tensorli hisoblash quvvati integratsiyasi kriptotahlilning hisoblash murakkabligini keskin kamaytirib, shifrlash algoritmlarining zaifliklarini yuqori aniqlikda aniqlash imkonini beradi.

Xulosa

Neyron tarmoqlar klassik kriptotahlil usullarining o‘rnini bosuvchi vosita emas, balki ma’lumotlardan statistik va strukturaviy bog‘lanishlarni o‘rganish, shifrlarni klassifikatsiya qilish va ayrim hollarda kalit yoki ochiq matnni tiklash imkonini beruvchi qo‘shimcha yondashuv sifatida asoslandi.

Tarixiy shifrlarda neyron tarmoqlar kalit uzunligini aniqlash, shifrlash mexanizmini o‘rganish va deshifrlash masalalarida samarali ekani ko‘rsatilgan. Natija ma’lumotlar hajmi, model parametrlari va epoch soniga bog‘liq.

Kelgusidagi tadqiqot ishining yo‘nalishi sifatida sun’iy intellekt va neyron tarmoqlar orqali kam raundli shifrlar uchun kalitni aniqlash, to‘liq raundli algoritmlar uchun kalit bitlarini qisman yoki to‘liq tiklash usullarini tadqiq etish, neyron tarmoqning turli arxitekturalarni qo‘llab, blokli shifrlarning neyron tarmoqlarga bardoshliligini tahlil qilish, aniqlikni oshirish, o‘qitish vaqtini qisqartirish va katta hajmdagi ma’lumotlarda ishlovchi optimallashtirish usullarini ishlab chiqish, klassik va neyron usullarni birlashtirish istiqbolli yo‘nalish hisoblanadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi «O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida»gi PQ-293-son qarori.

2. O‘zbekiston Respublikasi Prezidentining 2021-yil 17-fevraldagi «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to‘g‘risida»gi PQ-4996-son qarori.

3. Kuryazov D.M., Axmedov B.B., Sattarov A.B. Blokli simmetrik shifrlash algoritmlarini zamonaviy kriptotahlil usullariga bardoshliligini baholash. O‘quv qo‘llanma. 2017.

4. Davlatov M.U., Allanov O.M., Turdibekov B.B. Vijener algoritmi misolida neyron tarmoqlarning kriptotahlilda qo‘llanilishi // «Al-Farg‘oniy avlodlari» elektron ilmiy jurnali, 1-tom, 3-son, 2025.

5. Gohr A. Differensial-neyron kriptotahlil // CRYPTO 2019.

6. Zhang L., Wang Z. DES, Chaskey va PRESENT shifrlari uchun differensial-neyron farqlovchi modelini takomillashtirish // «arXiv» elektron ilmiy arxivi, arXiv:2204.06341v1, 2022.

7. Jeong O., Ahmadzadeh E., Moon I. Turli shifrlash usullaridan foydalangan holda blokli shifrlarning kompleks neyron kriptotahlili // «Mathematics» (MDPI) xalqaro ilmiy jurnali, 12-tom, 13-son (1936), 2024. – B. 1–23.

8. Xolmonov Sh.Sh. «Sun’iy neyron tarmoqlarini shifrmatnni aniqlash masalalariga tadbiqi.» Magistrlik dissertatsiyasi. Nurafshon, 2025.

9. NVIDIA Blackwell Ultra B300 haqida. URL: https://www.tomshardware.com/pc-components/gpus/nvidia-announces-blackwell-ultra-b300-1-5x-faster-than-b200-with-288gb-hbm3e-and-15-pflops-dense-fp4

10. Google Cloud: TPU VM tizim arxitekturasi. URL: https://docs.cloud.google.com/tpu/docs/system-architecture-tpu-vm

TLS PROTOKOLI UCHUN SEANS KALITLARNI GENERATSIYALASH YANGI ALGORITMNI ISHLAB CHIQISH

Baxtiyorov U.B., Sattorov Sh.I.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalari instituti xodimi

Anotatsiya: Ushbu maqolada axborot xavfsizligini ta’minlashning dolzarb masalalaridan biri TLS protokoli uchun seans kalitlarini generatsiyalashning yangi milliy algoritmini ishlab chiqish va tadqiq etish masalalari yoritilgan. Tadqiqot davomida mavjud Handshake bosqichlari va PRF (Pseudo-Random Function) mexanizmlari tahlil qilinib, ularning o‘rnini bosuvchi, milliy shifrlash standartlariga asoslangan muqobil algoritm taklif etilgan. Yangi algoritm ma’lumotlar konfidensialligi va yaxlitligini ta’minlashda yuqori ishonchlilikka ega hamda TLS protokoli doirasida xavfsiz ulanishni o‘rnatish jarayonida samarali qo‘llanilishi mumkin.

Kalit so‘zlar: Kalit generatsiyalash (KDF), milliy kriptografiya, axborot xavfsizligi, PRF funksiya, BSK(Birlamchi Sirli Kalit), PMS (Pre-Master Secret), MS (Master Secret), HMAC (Hash-based Message Authentication Code), KalitDaraxt, KalitQuduq.

Аннотация: В данной статье рассматривается одна из актуальных задач обеспечения информационной безопасности по разработке и исследованию нового национального алгоритма генерации сеансовых ключей для протокола TLS. В ходе исследования были проанализированы существующие этапы рукопожатия и механизмы PRF (Pseudo-Random Function), и предложен альтернативный алгоритм на основе национальных стандартов шифрования. Новый алгоритм обладает высокой надежностью в обеспечении конфиденциальности и целостности данных и может эффективно применяться в процессе установления безопасного соединения в рамках протокола TLS.

Ключевые слова: Функция PRF, BSK(Birlamchi Sirli Kalit), BSK(Birlamchi Sirli Kalit), PMS (Pre-Master Secret), MS (Master Secret), HMAC (Hash-based Message Authentication Code), KalitDaraxt, KalitQuduq.

Kirish

Bugungi kunda global raqamlashish sharoitida ma’lumotlar almashinuvi xavfsizligini ta’minlash davlat strategik vazifalaridan biriga aylandi. Tarmoqning transport bosqich xavsizlik protokoli ochiq tarmoqlar orqali ma’lumotlarni uzatishda eng keng tarqalgan standart bo‘lsada, unda qo‘llaniluvchi xalqaro kriptografik algoritmlarga to‘liq bog‘liqlik milliy axborot xavfsizligi nuqtai-nazaridan muayyan xatarlarni keltirib chiqarishi mumkin. Xususan, xorijiy standartlardagi ehtimoliy zaifliklar va ularning milliy normativ-huquqiy hujjatlar bilan har doim ham mos kelmasligi muqobil yechimlarni talab etmoqda.

Shu maqsadda, O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora tadbirlar to‘g‘risida”gi PQ–293-son qarori bilan kriptologiya sohasida bir qator mavzularda ilmiy-tadqiqot olib borish ko‘zda tutilgan [1]. Jumladan, “Transport pog‘onasida xavfsiz aloqani o‘rnatish uchun kalitlarni generatsiya qilish algoritmini yaratish” mavzusidagi ilmiy-tadqiqot loyihasi belgilangan bo‘lib, kelgusida milliy TLS protokollarida ulardan fodalanishni maqsad qiladi.

Xavfsizlik masalalari yuzasidan yangi talablarni shakllantirish orqali transport bosqich xavfsizligi protokollarida kalit almashish jarayonlari bitta algoritmdan iborat bo‘libgina qolmay,

bir vaqtning o‘zida bir nechta algoritmlarni birgalikda qo‘llashni taqazo etmoqda. Simmetrik va asimmetrik shifrlashning kuchli tomonlaridan birgalikda foydalanish maqsadida, ko‘pincha gibrid shifrlash sxemalari qo‘llaniladi. Bu sxemalar simmetrik shifrlashning tezligi va asimmetrik shifrlashning kalitlarni boshqarishdagi afzalliklarini o‘zida mujassamlashtiradi. Odatda, asimmetrik shifrlash algoritmlari yordamida simmetrik kalit xavfsiz tarzda almashiladi, undan so‘ng esa katta hajmdagi ma’lumot aynan shu simmetrik kalit bilan shifrlanadi. Bu yondashuv xavfsizlik va samaradorlikni ta’minlashning optimal yechimi hisoblanadi [2].

Asosiy qism

TLS protokolida mijoz va server ilovalari o‘rtasida dastlabki maxfiy sirni (*Pre-master secret*) o‘zaro almashish hamda uzatish usullari bo‘yicha xorij tajribasi tahlil qilinib, milly TLS protokoli uchun yangi usullar taklif etilgan.

Bundan tashqari, TLS protokolida mijoz va server uchun ma’lum bo‘lgan *Pre-master secret* asosida seans kalitlarni generatsiya qilish bo‘yicha xorij tajribasi tahlil qilingan. Natijada, milly kriptografik algoritmlardan foydalanib seans kalitlarni generatsiya qilish yuzasidan tegishli takliflar ishlab chiqilgan [5]. Qayd etish zarurki, mazkur takliflar mijoz va server uchun ma’lum bo‘lgan *Pre-master secret* dan maxfiy sirni (*Master secret*) hamda maxfiy sirdan 6 ta seans kalitlarni generatsiya qilish masalasiga qaratilgan.

Ishlab chiqilgan takliflarni birlashtirgan holda ushbu maqolada mijoz va server o‘rtasida *Pre-master secret* sirni o‘zaro almashish algoritmlari tahlil qilinadi.

Yuqoridagi talablar va izlanishlardan kelib chiqqan holda ushbu maqolada TLS protokoli uchun milliy kriptografik standartlar asosida seans kalitlarini generatsiyalashni ta’minlovchi yangi ishlab chiqilgan algoritm xususida so‘z yuritiladi.

Bu nafaqat axborot almashinuvining konfidensialligini oshiradi, balki mamlakatimizning raqamli suverenitetini mustahkamlashda muhim qadam bo‘lib xizmat qiladi. Taklif etilayotgan 4 bosqichli Handshake va seans kalitlarni generatsiyalash mexanizmi milliy shifrlash usullarini TLS arxitekturasiga samarali integratsiya qilish imkonini beradi.

1-bosqich: BSK kalitini almashish.

Dastlab UPO‘zMSt285:2024_2 qiymati mijoz tomonidan serverga uzatiladi. Mijoz parametrni quyidagicha hosil qiladi.

$$UP\text{O‘zMSt 285:2024_2} = \text{IDSon}||\text{client_random}||\text{E}||\text{N}$$

Bu yerda IDSon 2 baytli identifikatsion son bo‘lib, avvaldan kelishilgan dastlabki uzunliklari 40 baytga teng bo‘lgan parametrlar to‘plamidagi aynan bitta uzunllikni kelishib olish uchun mo‘ljallangan. Shuningdek, clent_random mijoz tomonidan tasodifiy generatsiya qilinuvchi 48 baytli qiymat, E va N uzunligi 4096 bit bo‘lgan mijozning ochiq kalitlar juftligi hisoblanadi. Mazkur to‘plamdagi qiymatlar (1-jadval) har bir seansda BSK (Birlamchi Sirli Kalit) kalitiga bog‘liq holda $\text{KalitQuduq}_{(28+\text{BTN(BSK)}\bmod 33)}$ qonuniyati asosida o‘zgarib boradi.

Server ham 2 baytli UPO‘zMSt285:2024_2 identifikatsiya songa mos to‘plamdan qiymatni oladi va mijozga uzatadi. Ushbu parametr server uchun quyidagicha hosil qilinadi:

$$UP\text{O‘zMSt 285:2024_2} = \text{IDSon}||\text{server_random}||\text{E}||\text{N}$$

Bu yerda, IDSon avvaldan kelishilgan 40 baytli parametrlar to‘plamidagi aynan bitta uzunllikni kelishib olish uchun 2 baytli identifikatsion son. Shuningdek, server_random qiymati server tomonidan tasodifiy generatsiya qilindan 48 baytli son, E va N sonlar uzunligi 4096 bit bo‘lgan serverning ochiq kalitlar juftligi. Mazkur to‘plamdagi qiymatlar har bir seansda BSK kalitiga bog‘liq holatda $\text{KalitQuduq}_{(28+\text{BTN(BSK)}\bmod 33)}$ qonuniyati asosida o‘zgarib boradi.

BSK kaliti mijoz tomonidan tasodifiy generatsiya qilib olinadi.

1-jadval

Tanlangan IDson va tasodifiy tanlangan ID parametrlar to‘plami.

ID parametrlar to‘plami	
IDSon	ID
0x0001	cd088ac469affb17d0163514234a0075fd553ec9
0x00A1	a9f167314ea832e069414bfbcf8b8f442ddedd8d
0x0100	893e63da52c8bf52f780ea0178f419f56c6cd20b
0x1234	c27ee611bb47a054abdf937d72024f91977808f2
0xABCD	b30f7d5cb6b2cae658c19b5a26cce66d6ebaf3ad
0xDEAD	b30f7d5cb6b2cae658c19b5a26cce66d6ebaf3ad
0xBEEF	31dfa3c47e8baaa111240844c83c0c264c6e5294
0xCAFE	03dfaed8477433c1ff26979cb13f8d9deac3a242
0xFACE	9db7c369bb5dfb7312eed9793e3a6e399e219af1
0xFFFF	6e77bc9acd7828f9e203c83691ee042ef59d2f18

KalitQuduq funksiyasi psevdotasodifiy ketma-ketlini generatsiya qilish uchun mo‘ljallangan bo‘lib, uning chiqish qiymati uzunligi BSK kalitining qiymatiga bog‘liq. KalitQuduq funksiyasi ketma-ket takrorlanuvchi KalitDaraxt funktsiyasidan tashkil topgan. bo‘lib, KalitDaraxt funktsiyasi O‘zMSt 285:2024 (2-algoritm) standart hesh-funksiya yordamida kiruvchi ma’lumotlarning xesh qiymatini hisoblaydi [3].

$$KalitDaraxt = \text{H}(kiruvchi\ ma'lumotlar)$$

Bu yerda

H – Xesh funksiya algoritmi (*O‘zMSt 285:2024, 2-algoritm*);

$KalitDaraxt$ funktsiyaning kiruvchi ma’lumotlari quydagi parametrlardan iborat:

$$KalitDaraxt(\text{ID, BSK, “kalit parametri”, seed, count}) \quad (1)$$

Bu yerda

seed = client_random||server_random; count = 0x00 ÷ 0xFF

KalitQuduq funksiyasining umumiy formulasi quyidagicha:

$$\text{KalitQuduq}_{28+BTN(BSK)mod33} = KalitDarax_1||KalitDarax_2||.....||KalitDarax_P \quad (2)$$

Bu yerda $KalitDarax_1$, $KalitDarax_2$, ... $KalitDarax_P$ qiymatlar quyidagi ifoda orqali hisoblanadi:

$$KalitDarax_i = \text{H}(KalitDarax_{i-1}||\text{“kalit parametri”}||\text{seed}||\text{count})$$

P arumentning 0 < P < 255 oraliqda bo‘lishi yetarli hisoblanadi.

Shuningdek, dastlabki $KalitDarax_0$ qiymat (1) formulada keltirilgan parametrlar asosida hisoblanadi.

KalitQuduq funksiyasi chiqish qiymatining uzunligi quyidagi ifoda orqali belgilanadi

$$|\text{KalitQuduq}| = 28 + BTN(BSK)mod33$$

Bu yerda, $BTN()$ funksiyasi (Byte to number) baytlar ketma-ketligini son ko‘rinishiga o‘tkazadi. U quyidagi formula yordamida hisoblanadi:

$$BTN(BSK) = 256^{i-1}\text{x}BSK_1 + ...+256\text{x}BSK_{i-1} + BSK_i \quad (3)$$

yani,

$$\text{BSK}_{48} = (BSK_1, \dots \dots, BSK_{48})$$

Agar,

$$BTN(BSK)mod33 < 2^3$$

bo‘lsa, $BTN(BSK)mod33 = 8$ deb olinadi va KalitQuduq funksiyaning chiqish ma’lumotining umumiy uzunligi 36 bayt deb hisoblanadi, ya’ni

$$\text{KalitQuduq}_{28+8}$$

Mijoz tomonidan tasodifiy generatsiya qilingan BSK kaliti serverga quyidagi tartibda uzatiladi:

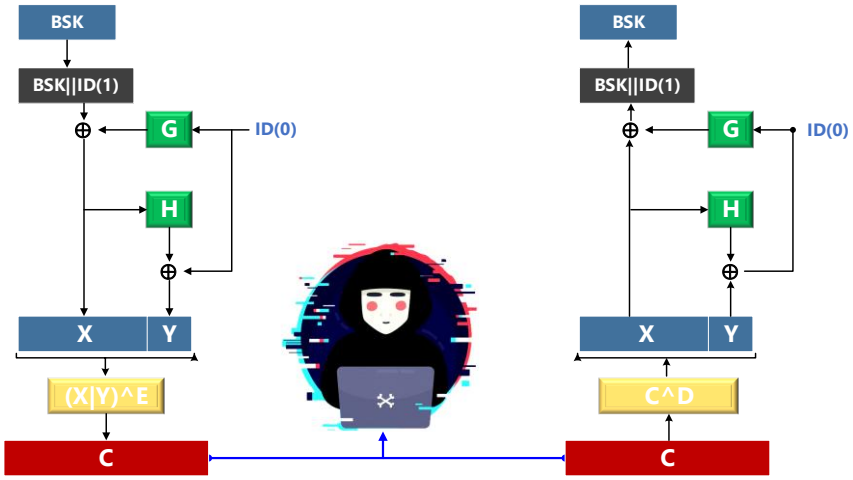
To‘plamdan (elementlar soni ixtyoriy tanlanishi mumkin) *IDSon* ga mos dastlabki uzunligi 40 baytli ID parametr ikkala tomonda ham bir xilda tanlandi. BSK kalitini shifrlash va deshifrlash jarayonlari amalga oshiriladi.

Shifrlash:

1. ID parametrni ikki qismga bo‘lib olinadi ID_0 va ID_1
2. Agar ID parametr baytlar uzunligi ikkiga bo‘linmasa, ikkiga bo‘lgandagi butun qismi ID_0 ga va qolgan qismi ID_1 ga o‘zlashtiriladi.
3. BSK va ID_1 qiymatlari o‘zaro kokatetsiya qilinib, BSK || ID_1 ko‘rinishda yoziladi.
4. G-hesh funksiya (O‘zMSt 285:2024, 2-algoritm) yordamida ID_0 qismning xesh qiymati hisoblanadi;
5. X = BSK || $ID_1 \oplus$ G(ID_0) ifodaning qiymati aniqlanib, H-hesh funksiya (O‘zMSt 285:2024, 2-algoritm) yordamida X ning xesh qiymati hisoblanadi;
6. $Y = ID_0 \oplus$ H(X) hisoblanadi;
7. Shifrlanuvchi ma’lumotni m = X || Y ifoda orqali shakllantiriladi;
8. $C = m^E(modN)$ shifrma’lumot hosil qilinadi va serverga yuboriladi.

Ochiq matnga o‘girish:

1. Qabul qilingan shifrma’lumot $m = C^D$ $(modN)$ ifoda orqali ochiq matnga o‘zgartiriladi va m = X || Y qiymatga ega bo‘linadi;
2. H-hesh funksiya (O‘zMSt 285:2024, 2-algoritm) yordamida X ning xesh qiymati hisoblanadi;
3. $ID_0 = Y \oplus$ H(X) ifoda yordamida ID_0 qism qiymati qayta tiklanadi;
4. G-hesh funksiya (O‘zMSt 285:2024, 2-algoritm) yordamida ID_0 qismning xesh qiymati hisoblanadi;
5. BSK || $ID_1 = X \oplus$ G(ID_0) ifoda yordamida boshlang‘ich xabar qayta tiklanadi;
6. Agar BSK kalitidan keyin kelgan ID_1 serverdagi ID_1 bilan mos kelsa, ma’lumot qabul qilinadi (1-rasm).



1-rasm. BSK kalitini almashish.

2-bosqich: PMS qiymatni almashish.

AES-TinyJAMBU algoritmi.

Ushbu autentifikatsiyalangan shifrlash algoritmi tarkibida asosiy primitiv sifatida O‘zMSt 270:2024 O‘zbekiston milliy standarti tarkibidagi AES (2-algoritm) blokli simmetrik shifrlash algoritmi tanlab olingan [2]. Ushbu algoritmdan foydalangan holda PMS kalitini almashish mumkun (2-rasm). Buning uchun AES-TinyJAMBU algoritimiga kiruvchi qiymatlarni shakllantirish talab etiladi [3].

Ushbu algoritmning kirish parametrlari (Key, Nonce, AD) 256 bitli shifrlash kaliti, 128 bitli noyob raqam, ixtiyoriy uzunlikdagi bog‘lovchi ma’lumotlar hisoblanadi (2-jadval). Ushbu parametrlarni BSK kaliti va KalitQuduq funksiyasidan foydalanib, quyidagi tartibda hosil qilinadi:

$KalitDarax_P$(BSK, “kalit parametri”, seed, count)

seed = client_random||server_random; count = 0x00 ÷ 0xFF

$KalitDarax_i$ = H($KalitDarax_{i-1}$||“kalit parametri”||seed||count)

$\text{KalitQuduq}_{28+BTN(BSK)mod33} = KalitDarax_1||KalitDarax_2||…..||KalitDarax_P$,

KalitQuduq funksiyasi yordamida hosil qilingan psevdotasodifiy ketma-ketlik quyidagicha taqsimlanadi:

$$\text{KalitQuduq}_{28+BTN(BSK)mod33} = \begin{cases} Key = KalitQuduq[:16] \\ Nonce = KalitQuduq[16:28] \\ AD = KalitQuduq[28:] \end{cases}$$

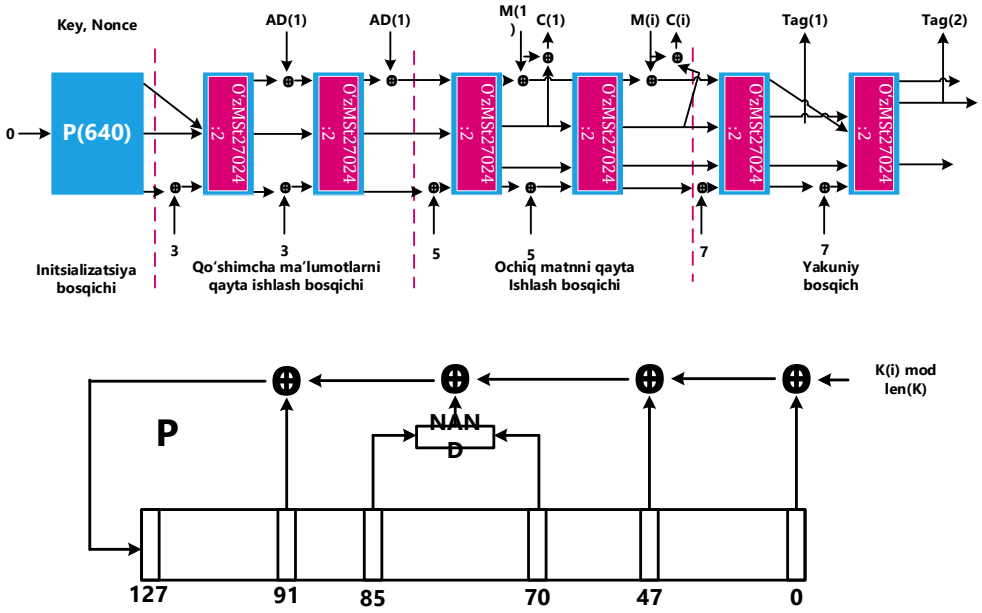
Ya’ni, hosil qilingan psevdotasodifiy ketma-ketlikning dastlabki 16 baytlari (*1-16 baytlar*) kalit (*Key*), keyingi 12 baytlari (*16-28 baytlar*) noyob initsializatsiya vektori (*Nonce*), qolgan barcha baytlari (*28-(8 dan 32 baytgacha bo‘lishi mumkin)*) bog‘lovchi ma’lumot (*AD*) sifatida olinadi.

Mijoz tomonidan tasodifiy generatsiya qilingan uzunligi 48 baytdan iborat PMS qiymati AES-TinyJAMBU autentifikatsiyalangan shifrlash algoritmi (2-rasm) hamda uning kiruvchi parametrlaridan (2-jadval) foydalanib, himoyalangan holda serverga uzatiladi.

2-jadval.

AES-TinyJAMBU algoritmi parametrlari.

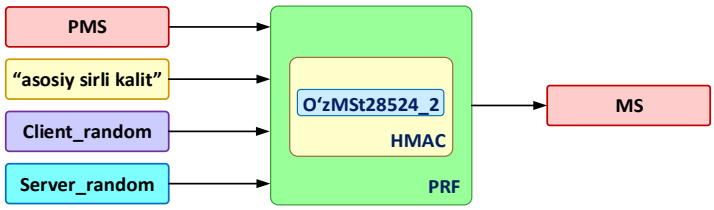
Key	Uzunligi 128 bit bo‘lgan maxfiy kalit
Nonce	uzunligi 128 bit bo‘lgan bir martalik raqam
$\oplus$	bitlar bo‘yicha eksklyuziv YOKI (XOR)
M	ixtiyoriy chekli uzunlikdagi ochiq matn
M_i	ochiq matnning i-bloki
C	shifrmatn
C_i	shifrmatnning i-bloki
AD	bog‘langan ma’lumotlar (associated data), baytlar ketma-ketligi
AD_i	bog‘langan ma’lumotning i-bloki
Tag_1, Tag_2	uzunligi 32 bitdan bo‘lgan (jami 64 bit) teg.



2-rasm. AES-TinyJAMBU algoritmining sxemasi.

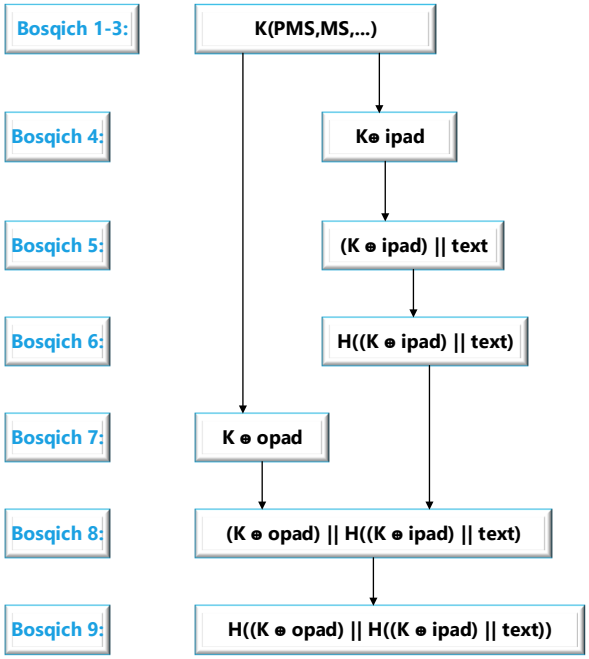
3-bosqich. PMS qiymatdan MS qiymatini hosil qilish

PRF funksiyasidan foydalangan holda PMS kalitidan foldalanib MS qiymati hosil qilinadi (3-rasm) [5].



3-rasm. PMS dan MS qiymatini hosil qilish.

PRF funksiya HMAC funktsiyasidan tashkil topgan bo'lib, uning strukturaviy sxemasi 4-rasmda keltirilgan.



4-rasm. HMAC funksiyasining blok sxemasi.

seed = "asosiy sirli kalit" || client_random || server_random

a[0] = seed

a[2], p[1], p[1] qiymatlari quyidagicha hisoblanadi:

a[1] = HMAC-O'zMSt 285_2 (PMS, a[0])

a[2] = HMAC-O'zMSt 285_2 (PMS, a[1])

p[1] = HMAC-O'zMSt 285_2 (PMS, a[1] + seed)

p[2] = HMAC-O'zMSt 285_2 (PMS, a[2] + seed)

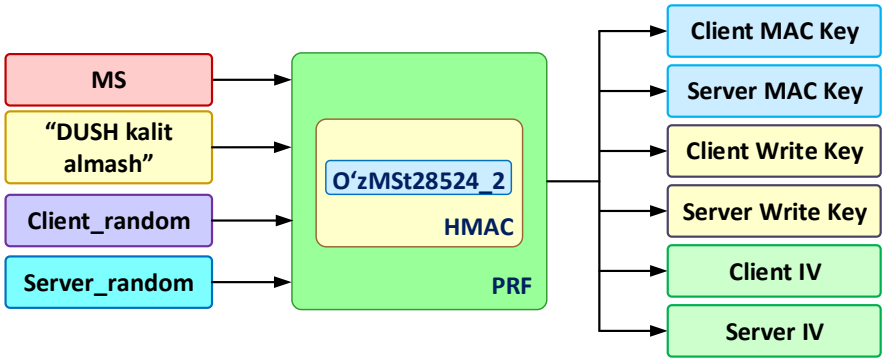
p[2] ning dastlabki 16 baytini *p[1]* ga konkatenatsiya qilish (biriktirish) orqali MS (MasterSecret) qiymati quydagicha hosil qilinadi.

MS = p1[1…32 bytes] || p2[1…16 bytes]

Shuni alohida qayd etish lozimki, HMAC funksiyasi xesh-funktsiya algoritmiga asoslangan. Taklif etilgan mexanizmda O'zMSt 285:2024 milliy kriptografik standartining 2-algoritmi bilan belgilangan xesh-funktsiya algoritmidan foydalaniladi.

4-bosqich. MS qiymatidan seans kalitlarini generatsiyalash.

PRF funksiyasidan foydalangan holda MS kalitidan seans kalitlarini hosil qilish (5-rasm) [5].



5-rasm. MS qiymatidan seans kalitlarini hosil qilish.

seed = "DUSH kalit almash" || server_random || client_random

a[0] = seed

a[1] = HMAC-O'zMSt 285_2 (MS, a[0])

a[2] = HMAC-O'zMSt 285_2 (MS, a[1])

a[3] = HMAC-O'zMSt 285_2 (MS, a[2])

….

a[n] = HMAC-O'zMSt 285_2 (MS, a[n-1])

p[1] = HMAC-O'zMSt 285_2 (MS, a[1] + seed)

p[2] = HMAC-O'zMSt 285_2 (MS, a[2] + seed)

p[3] = HMAC-O'zMSt 285_2 (MS, a[3] + seed)

….

p[n] = HMAC-O'zMSt 285_2 (MS, a[n-1] + seed)

P = p1 || p2 || p3 || … || pn

Ushbu ishda TLS protokoli uchun O'zbekiston Respublikasining milliy kriptografik standartlari (O'zMSt 285:2024 hesh-funksiyasi, O'zMSt 270:2024 asosidagi AES-TinyJAMBU simmetrik shifrlash algoritmi va HMAC-O'zMSt 285_2) asosida yangi, seans kalitlarni generatsiyalash mexanizmi ishlab chiqildi.

Xulosa

Taklif qilingan mexanizm milliy kriptografik algoritmlarni TLS protokoli arxitekturasiga samarali integratsiya qilish imkonini beradi. Tarmoqning transport bosqich xavfsizlik protokollari

tarkibiga O‘zbekiston Respublikasining milliy standartlari asosidagi kriptografik algoritmlarni joriy qilish quyidagilar ta’minlanadi:

Xorijiy algoritmlarga bog‘liqlik bartaraf etiladi;

Milliy axborot xavfsizligi va raqamli suverenitetni mustahkamlanadi;

Ma’lumotlar almashinuvining konfidensialligi, yaxlitligi ta’minlanadi va ishonchliligi ortadi.

Ushbu mexanizm O‘zbekistonning ochiq axborot infratuzilmasining xavfsizligini ta’minlashda asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining 2024 yil 15 avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora tadbirlar to‘g‘risida”gi PQ–293-son qarori.

2. O‘zMSt 270:2024 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.

3. O‘zMSt 285:2024 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi.

4. O‘zMSt 286:2024 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari.

5. Baxtiyorov U.B., Kuryazov D.M. Milliy TLS 1.2 protokoli uchun seans kalitlarni generatsiya qilish masalalari // “Axborot xavfsizligi muammolari” ilmiy jurnali 4-son. RTATM, Toshkent: 2025 yil. – B. 16-28.

6. Kuryazov D.M., Isakov M.M. “Yangi autentifikatsiyalangan shifrlash rejimini ishlab chiqish”. Magistrlik dissertatsiya ishi. Nurafshon – 2025 y.

7. Kuryazov D.M., Baxtiyorov U.B. Transport pog‘onasida xavfsiz aloqani o‘rnatish milliy protokolini yaratish bilan bog‘liq masalalar. // Axborot xavfsizligi muammolari ilmiy jurnali. 2025 yil, 3-son, 37-50 betlar.

8. FIPS PUB 186-3 Federal information processing standards publication. Digital Signature Standard (DSS).

9. СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых.

GOST 28147-89 BO‘YICHA DIFFERENSIAL NATIJALARNING PARAM-Z S-BLOKLI “MAGMA” SHIFRIGA TATBIQ ETILISH SHARTLARI

Sattarov A.B., Abdurashidov B.K.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalari instituti

Annotatsiya. GOST 28147-89 standartida S-bloklar qat’iy belgilanmagan, shu sababli amaliyotda turli S-blok to‘plamlari ishlatilgan. GOST R 34.12-2015 dagi “Magma” shifrida esa bitta to‘plam - param-Z belgilab qo‘yilgan. Maqolada GOST 28147-89 uchun ilgari olingan differensial kriptotahlil natijalarini Magmaga qanday shartlarda qo‘llash mumkinligi ko‘rib chiqildi. Buning uchun S-blok jadvallari RFC 4357 va RFC 7836 dagi to‘plamlar bilan barcha 128 ta qiymat bo‘yicha dastur yordamida solishtirildi, S-bloklarning qo‘llanish tartibi esa RFC 8891 test misollarida tekshirildi. Natijada param-Z RFC 4357 dagi yettita to‘plamning birortasi bilan ham umumiy S-blokka ega emasligi, manbalarda esa uch holatda to‘plam nomi uning qiymatlariga mos kelmasligi aniqlandi. Bitta ikki raundli xarakteristika uchun barcha holatlar to‘liq sanab chiqildi va uning ehtimolligi kalitga kuchli bog‘liq ekani aniqlandi.

Kalit so‘zlar: Magma, GOST 28147-89, differensial kriptotahlil, S-blok, param-Z, kalitga bog‘liqlik.

Аннотация. В ГОСТ 28147-89 S-блоки не зафиксированы, поэтому на практике использовались разные наборы. В шифре «Магма» из ГОСТ Р 34.12-2015 закреплён один набор - param-Z. В статье рассмотрено, при каких условиях известные результаты дифференциального криптоанализа ГОСТ 28147-89 можно применять к «Магме». Для этого таблицы S-блоков программно сравнены по всем 128 значениям с наборами из RFC 4357 и RFC 7836, а порядок применения S-блоков проверен на контрольных примерах RFC 8891. Установлено, что param-Z не имеет общих S-блоков ни с одним из семи наборов RFC 4357, а в источниках в трёх случаях название набора не соответствует его значениям. Для одной двухраундовой характеристики выполнен полный перебор, который показал сильную зависимость её вероятности от ключа.

Ключевые слова: Магма, ГОСТ 28147-89, дифференциальный криптоанализ, S-блок, param-Z, зависимость от ключа.

Kirish

O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi PQ-293-son qarorining 2-ilovasi bilan tasdiqlangan 2024–2028-yillarga mo‘ljallangan ilmiy-tadqiqot ishlari dasturida “Zamonaviy kriptotahlil usullarini yaratish” mavzusi (15-band) belgilangan [1]. 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonunda esa kiberhimoya chora-tadbirlari qatoriga ma’lumotlarni kriptografik va texnik jihatdan himoya qilish ham kiritilgan [2]. Bunday vositalar ichidagi algoritmni buzish qanchalik qiyin bo‘lsa, shunchalik ishonchli. Blokli shifrlarni tekshirishning asosiy usullaridan biri differensial kriptotahlildir [3]: unda kirishdagi farqning raundlar orqali o‘tish ehtimolligi baholanadi.

GOST R 34.12-2015 dagi “Magma” shifri [4] RFC 8891 ga ko‘ra GOST 28147-89 ning bir ko‘rinishi bo‘lib, unda S-bloklar id-tc26-gost-28147-param-Z (bundan keyin - param-Z) to‘plami bilan belgilab qo‘yilgan, kalit va ma’lumot baytlari esa big-endian tartibda (yuqori baytdan boshlab) o‘qiladi [5; 6]. GOST 28147-89 standarti esa S-bloklarni belgilamagan, amaliyotda turli to‘plamlar ishlatilgan va ularning yettitasi RFC 4357 da identifikatorlar bilan berilgan [7]. GOST 28147-89 bo‘yicha qisqartirilgan raundli [8], bog‘liq kalitli [9] va to‘liq raundli [10–12] differensial hujumlar ma’lum, biroq mualliflarning o‘zi natija S-bloklarga

bog‘liqligini va boshqa to‘plamda hujumni qayta sozlash kerakligini ta’kidlagan [11; 12]. Bundan tashqari, raund kaliti 2^{32} moduli bo‘yicha qo‘shilgani uchun xarakteristika (farqning raunddan raundga o‘tish yo‘li) ehtimolligi raund kalitining qiymatiga ham bog‘liq [9].

Param-Z uchun ehtimolliklarni qayta hisoblash qimmatga tushadi: [11] da hisoblashlar bir necha CPUda oylab davom etgan, [10] da esa 20 raundli ehtimollikni tasdiqlashga hisoblash quvvati yetmagan. Boshqa shifrlar uchun bunday hisoblarni grafik protsessorlarda (GPU) parallel bajarish usullari taklif qilingan [13]. Lekin GPU vaqtini sarflashdan oldin bir savolga javob kerak: e’lon qilingan natijalardan qaysi biri haqiqatan param-Z Magmaga tegishli va aynan nimani o‘lchash lozim?

Maqolaning maqsadi - GOST 28147-89 bo‘yicha olingan differensial natijalarni param-Z Magmaga qanday shartlarda qo‘llash mumkinligini aniqlash va bu shartlardan ikkitasini - S-blok to‘plami mosligi va kalit ta’sirini - qayta takrorlash mumkin bo‘lgan hisoblashlar bilan tekshirish.

Asosiy qism

Adabiyotdagi sonli natija param-Z Magmaga uchta shart bajarilgandagina o‘tadi: T1 - S-blok to‘plami qiymat bo‘yicha param-Z ga teng; T2 - S-bloklar 4 bitli qismlarga (tetradalarga) standartdagi tartibda qo‘llanadi; T3 - raund funksiyasi va kalit jadvali o‘zgartirilmagan. Bundan tashqari, har bir natijaning hujum modeli (bitta noma’lum yoki bog‘liq kalit), turi (kalitlar bo‘yicha o‘rtacha yoki qayd etilgan kalitdagi ehtimollik; farqlagich, nomzodlarni filtrlash yoki kalitni tiklash) va dalil turi (isbot, analitik baho yoki simulyatsiya) alohida ko‘rsatilishi kerak.

Magma raund funksiyasi quyidagicha [4; 5]:

$$t(a) = \pi'_7(a_7) \| \dots \| \pi'_0(a_0), \quad g[k](a) = t(a \boxplus k) \lll 11, \qquad (1)$$

bu yerda a_0 - eng quyi tetrada, π'_i - param-Z almashtirishlari, $\boxplus$ - 2^{32} moduli bo‘yicha qo‘shish. Aniq bir K kalit uchun xarakteristika Ω ehtimolligi $p_K(\Omega)$, kalitlar bo‘yicha o‘rtacha ehtimollik esa $\bar{p}(\Omega) = E_K[p_K(\Omega)]$ bilan belgilanadi. Ikki S-blok to‘plami A va B ni solishtirish uchun Python dasturida quyidagi ikki ko‘rsatkich hisoblandi:

$$M(A,B) = \#\{(i,x): A_i(x) = B_i(x)\}, \quad C(A,B) = \#\{i: A_i \in \{B_1, \dots, B_8\}\}, \qquad (2)$$

bu yerda $M \in [0;\ 128]$ − S-bloklar tartibi saqlanganda mos kelgan qiymatlar soni, $C \in [0;\ 8]$ - ikkala to‘plamda ham uchraydigan S-bloklar soni; M S-bloklar teskari tartibda olinganda ham hisoblandi. Namuna sifatida RFC 4357 dagi yettita to‘plam va RFC 7836 dagi param-Z olindi [6; 7]; ular mustaqil ochiq dastur gost-engine jadvallari bilan to‘liq (8 × 128/128) mos keldi [14]. Maqolalardagi jadvallar asl nusxalardan ko‘chirildi. Magma dasturimiz RFC 8891 dagi 17 ta tekshiruvdan o‘tdi. S-bloklar teskari tartibda qo‘llansa, A.1 dagi to‘rtala misol ham buziladi, ya’ni tekshiruv qo‘llanish tartibini ham sezadi [5].

Kalitning natijaga ta’sirini ko‘rish uchun param-Z dagi quyidagi ikki raundli xarakteristika ($\Delta a_1, \Delta a_0$) ko‘rinishida) olindi:

$$(0, 80000000_{16}) \to (80000000_{16}, 00000480_{16}) \to (00000480_{16}, 80638000_{16}). \qquad (3)$$

2^{31} ni 2^{32} moduli bo‘yicha qo‘shish faqat eng yuqori bitni o‘zgartiradi, shuning uchun birinchi raund ehtimolligi kalitdan qat’i nazar $q_1 = 1/4$ (π'_7 ning 8 → 9 o‘tishi). Ikkinchi raundda g ning kirishi tasodifiy (tekis taqsimlangan) va birinchi raunddagi hodisaga bog‘liq emas, shuning uchun

$$p_K(\Omega) = q_1 \cdot p_{K_2}, \quad p_{K_2} = \Pr_y[g[K_2](y) \oplus g[K_2](y \oplus 480_{16}) = 00638000_{16}]. \qquad (4)$$

Ikkinchi raundda t qatlami chiqishidagi ayirma $00638000_{16} \ggg 11 = 00000C70_{16}$, ya’ni farq faqat 1- va 2-tetradalarda bo‘lishi kerak. 480_{16} faqat 7- va 10-bitlarni o‘z ichiga olgani uchun $y \boxplus K_2$ va $(y \oplus 480_{16}) \boxplus K_2$ ning 12- va undan yuqori bitlari faqat 12-bitga o‘tadigan ko‘chirishlar teng bo‘lganda bir xil bo‘ladi; aks holda S-bloklar har xil kirishni har xil chiqishga o‘tkazgani (bijektiv bo‘lgani) uchun yuqori tetradalardan birida farq paydo bo‘ladi. Demak, p_{K_2} faqat y va K_2 ning quyi 12 bitiga bog‘liq va 2^{24} holni sanash bilan aniq topiladi. Bu qoida 2^{22} ta tasodifiy to‘liq 32 bitli holatda to‘liq g bilan tekshirildi. Hisoblashlar Python 3.13 va numpy 2.5 da uchta skript bilan bajarildi; Monte-Karlo qismlari belgilangan boshlang‘ich qiymat (seed) bilan ishlaydi, shu sababli ularni aynan takrorlash mumkin.

Olingan natijalar. Param-Z RFC 4357 dagi yettita to‘plamning har biri bilan C = 0 ga ega, ya’ni birorta ham umumiy S-blok yo‘q. Manbalar bo‘yicha natijalar 1-jadvalda keltirilgan.

1-jadval

Manbalardagi S-blok to‘plamlari va natijalarning param-Z Magmaga tatbiqi

Manba	Manbadagi nom va natija	Qiymat bo‘yicha natija	Bajarilmaydigan shartlar
[8]	“Markaziy bank to‘plami”; 13 raund: 2^{51} tanlangan ochiq matn; 21 raund, bog‘liq kalit: 2^{56}	TestParamSet: M = 128; param-Z bilan C = 0	T1
[10]	“id-GostR3411-94-CryptoProParamSet” (Markaziy bank); $\approx 2^{226}$ shifrlash, 50 %	Qiymatlar berilmagan	T1 (ikkala nomzod to‘plam ham C = 0)
[11]	“GostR3411-94-TestParamSet” (Markaziy bank); $\approx 2^{179}$ hisoblash, 95 %	Qiymatlar berilmagan	T1
[12]	id-GostR3411-94-TestParamSet; 20 raundli farqlagich	TestParamSet: M = 128	T1; farqlagich, kalit tiklanmaydi
[12]	“Gost28147-CryptoProParamSetA”	GostR3411-94-CryptoProParamSet: M = 128; CryptoPro-A bilan C = 0	T1; nom qiymatga mos emas
[15]	Magma+ ($\boxplus$ o‘rniga XOR), 8 raund; 16 ta 4 bitli nomzoddan 2–10 tasi chiqarilgan	Param-Z: C = 8; to‘g‘ri raqamlashda M = 8, teskarisida M = 128	T2, T3; kalit tiklanmaydi

Jadvaldan uchta tafovut kelib chiqadi. Birinchidan, bir xil “Markaziy bank to‘plami” tavsifi [10] da id-GostR3411-94-CryptoProParamSet ga, [11; 12] da esa TestParamSet ga nisbat berilgan; [8] dagi jadval qiymat bo‘yicha TestParamSet ga teng. Bu ikki nom aslida umumiy S-bloki yo‘q ikki xil to‘plamni bildiradi, ammo param-Z bilan ikkalasida ham C = 0. Ikkinchidan, [12] dagi “Gost28147-CryptoProParamSetA” jadvali qiymat bo‘yicha xesh-funksiya to‘plamiga teng va id-Gost28147-89-CryptoPro-A-ParamSet bilan umumiy S-blokka ega emas. Uchinchidan, [15] dagi jadval qiymatlar to‘plami bo‘yicha param-Z ga teng, lekin S8, …, S1 yorliqlari π'_0, …, π'_7 ga mos keladi va matnda S1 eng quyi qismga qo‘llanishi aytilgan; bu standartdagi (1) ga nisbatan teskari tartib. Demak, to‘plamni nomiga qarab aniqlab bo‘lmaydi, qiymatlar mosligi esa qo‘llanish tartibi bir xilligini kafolatlamaydi. Ko‘rib chiqilgan ishlarning birortasida T1–T3 birga bajarilgani tasdiqlanmadi.

(3) xarakteristika uchun barcha holatlarni sanab chiqish quyidagi natijani berdi: K_2 mod 2^{12} ning 4096 ta qiymatidan 710 tasida (17,33 %) $p_{K_2} = 0$, eng katta qiymat 1/16, o‘rtacha qiymat 5/256. Demak, kalitlar bo‘yicha o‘rtacha ehtimollik

$$\bar{p}(\Omega) = 1/4 \cdot 5/256 = 5/1024 \approx 2^{-7,68}. \quad (5)$$

Standart kalit jadvalida K_2 tekis taqsimlangan, shuning uchun bu ulushlar 256 bitli kalitlar ulushiga teng. Aniq bir kalit uchun ehtimollik qanday taqsimlangani 2-jadvalda ko‘rsatilgan.

Aniq qiymatlar tasodifiy tajribalar (Monte-Karlo usuli) bilan ham tekshirildi. To‘rtta tasodifiy kalit juftligi uchun N = 2^{25} juftlikli baholar aniq qiymatlar bilan, har bir juftlik uchun tasodifiy kalit tanlangan baho esa aniq o‘rtacha 5/1024 bilan statistik xatolik doirasida mos keldi. GOST uchun kalitga bog‘liqlik umumiy holda ma’lum edi [9], boshqa shifrlarda esa ko‘p xarakteristikalar kalitlarning kichik qismidagina bajarilishi ko‘rsatilgan [16]. Bu yerda u param-Z uchun aniq son bilan o‘lchandi.

2-jadval

(3) xarakteristikaning qayd etilgan kalitdagi ehtimolligi taqsimoti

$p_K(\Omega)$ qiymati	$p_K(\Omega) = 0$	$0 < p_K(\Omega) < \bar{p}$	$p_K(\Omega) = \bar{p} = 5/1024$	$p_K(\Omega) > \bar{p}$	shu jumladan $p_K(\Omega) \geq 2\bar{p}$	eng katta qiymat $2^{-6} = 3{,}2\bar{p}$
Kalitlar ulushi	17,3 %	33,0 %	0,6 %	49,1 %	9,4 %	1,6 %

Natijalarning amaliy ahamiyati va cheklovlari

Param-Z Magma bilan tajriba o‘tkazuvchi uchun bundan uchta amaliy talab chiqadi. Avvalo, dasturda S-bloklarning qiymatigina emas, qo‘llanish tartibi ham RFC 8891 test misollari bilan tekshirilishi kerak. Shuningdek, bitta kalitda olingan baho p_K ning bahosi bo‘lib, kalitlar bo‘yicha o‘rtacha $\bar{p}$ ni baholash uchun bir nechta kalitli tajriba va kalitlar bo‘yicha tarqoqlikni ko‘rsatish zarur. Nihoyat, ko‘rilgan misolni aniq hisoblash mumkin bo‘ldi, chunki hodisa atigi 12 ta kalit bitiga bog‘liq. Raundlar ko‘paysa, bog‘liqlik bir nechta raund kaliti va uzunroq ko‘chirish zanjirlariga yoyilishi kutiladi, demak katta hajmdagi tajriba kerak bo‘ladi. Bunday hisoblashlarda GPU foydali ekani boshqa shifrlar misolida ko‘rsatilgan [17]; param-Z Magma uchun bu alohida vazifa bo‘lib, maqolada ko‘rilmaydi. Ishning cheklovlari ham bor. Maqola to‘liq adabiyot sharhi emas: manbalar maxsus qidiruv tartibisiz tanlangan. Kalitga bog‘liqlik esa faqat bitta, tajriba asosida tanlangan ikki raundli xarakteristika uchun hisoblangan va natija raundlari kamaytirilgan variantga tegishli.

Tajriba uchun zarur hajm

Barcha holatlarni sanab bo‘lmaydigan hollarda p_K N ta juftlikda kuzatilgan hodisalar soni c bo‘yicha $\hat{p} = c/N$ ko‘rinishida baholanadi. Normal yaqinlashishda nisbiy aniqlik ε va ishonch darajasi $1 - \delta$ uchun

$$N \geq z_{1-\delta/2}^2 (1-p)/(\varepsilon^2 p) \qquad (6)$$

juftlik talab qilinadi, bu yerda $z_{1-\delta/2}$ - standart normal taqsimot kvantili. $\varepsilon = 0{,}1$ va $1 - \delta = 0{,}95$ da (3) xarakteristikaning o‘rtacha ehtimolligi $p = 5/1024$ uchun $N \approx 7{,}8 \cdot 10^4$ juftlik yetarli. Hodisa kuzatilmagan ($c = 0$) holda faqat bir tomonlama yuqori chegara $p_U = 1 - \delta^{1/N} \approx -\ln \delta / N$ beriladi [18]: $N = 2^{25}$ va $\delta = 0{,}05$ da $p_U \approx 8{,}9 \cdot 10^{-8}$. Ko‘rinib turibdiki, past ehtimollikli xarakteristikalar uchun tajriba hajmi tez o‘sadi va uni parallel, jumladan GPUda bajarishga to‘g‘ri keladi.

Xulosa

GOST 28147-89 bo‘yicha differensial natijalarni param-Z Magmaga ko‘chirish uchun uchta zaruriy shart va natija turini ajratish mezonlari taklif qilindi. Ko‘rib chiqilgan ishlarning birortasida bu shartlarning uchalasi birga bajarilgani tasdiqlanmadi, shuning uchun ulardagi sonli baholarni param-Z Magmaga to‘g‘ridan-to‘g‘ri qo‘llab bo‘lmaydi.

Param-Z RFC 4357 to‘plamlarining birortasi bilan umumiy S-blokka ega emas. Manbalarda uch holatda to‘plam nomi uning qiymatlariga mos kelmasligi aniqlandi, shuning uchun S-blok to‘plami 128 ta qiymat va RFC 8891 test misollari bo‘yicha tekshirilishi kerak.

Bitta ikki raundli xarakteristikada aniq bir kalit uchun ehtimollik 0 dan o‘rtacha qiymatning 3,2 baravarigacha o‘zgaradi. Shuning uchun param-Z Magma uchun ehtimolliklarni, jumladan GPUda, qayta baholashda natija barcha kalitlar bo‘yicha o‘rtachaga yoki bitta aniq kalitga tegishli ekanini aniq ko‘rsatish lozim.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-293-son qarori. - URL: https://lex.uz/docs/-7067656.

2. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. - URL: https://lex.uz/docs/-5960604.

3. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems // Journal of Cryptology. - 1991. - Vol. 4, No. 1. - P. 3–72. - DOI: 10.1007/BF00630563.

4. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. - Введ. 2016-01-01.

5. Dolmatov V. (Ed.), Baryshkov D. GOST R 34.12-2015: Block Cipher “Magma”. RFC 8891. - IETF, 2020. - DOI: 10.17487/RFC8891.

6. Smyshlyaev S. (Ed.) et al. Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012. RFC 7836. - IETF, 2016. - DOI: 10.17487/RFC7836.

7. Popov V., Kurepkin I., Leontiev S. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. RFC 4357. - IETF, 2006. - DOI: 10.17487/RFC4357.

8. Seki H., Kaneko T. Differential Cryptanalysis of Reduced Rounds of GOST // SAC 2000, LNCS 2012. - Springer, 2001. - P. 315–323. - DOI: 10.1007/3-540-44983-3_23.

9. Ko Y., Hong S., Lee W., Lee S., Kang J.-S. Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST // FSE 2004, LNCS 3017. - Springer, 2004. - P. 299–316. - DOI: 10.1007/978-3-540-25937-4_19.

10. Courtois N.T., Misztal M. Differential Cryptanalysis of GOST. - Cryptology ePrint Archive, Paper 2011/312. - URL: https://eprint.iacr.org/2011/312.

11. Courtois N.T. An Improved Differential Attack on Full GOST // LNCS 9100. - Springer, 2016. - P. 282–303. - DOI: 10.1007/978-3-662-49301-4_18 (kengaytirilgan versiyasi: ePrint 2012/138).

12. Courtois N.T., Mourouzis T., Misztal M. Enhanced Truncated Differential Cryptanalysis of GOST // Proc. SECRYPT 2013. - SCITEPRESS, 2013. - P. 411–418. - DOI: 10.5220/0004532504110418.

13. Chen Z., Chen J., Meng W., Teh J.S., Li P., Ren B. Analysis of Differential Distribution of Lightweight Block Cipher Based on Parallel Processing on GPU // J. Information Security and Applications. - 2020. - Vol. 55. - Art. 102565. - DOI: 10.1016/j.jisa.2020.102565.

14. gost-engine/engine. - GitHub, commit 4632029f (25.09.2026), gost89.c. - URL: https://github.com/gost-engine/engine.

15. Ищукова Е.А., Письменский М.В., Бабенко Л.К. Некоторые подходы к анализу шифра Магма+ с использованием метода невозможных дифференциалов // Современные наукоемкие технологии. - 2016. - № 12-3. - С. 481–485.

16. Peyrin T., Tan Q.Q. Mind Your Path: On (Key) Dependencies in Differential Characteristics // IACR Transactions on Symmetric Cryptology. - 2022. - No. 4. - P. 179–207. - DOI: 10.46586/tosc.v2022.i4.179-207.

17. Tezcan C., Leander G., Hadipour H. Cryptanalysis: Theory Versus Practice - Correcting Cryptanalysis Results on Ascon, ChaCha, and Serpent Using GPUs // IACR Transactions on Symmetric Cryptology. - 2025. - No. 3. - P. 729–754. - DOI: 10.46586/tosc.v2025.i3.729-754.

18. Clopper C.J., Pearson E.S. The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial // Biometrika. - 1934. - Vol. 26, No. 4. - P. 404–413. - DOI: 10.1093/biomet/26.4.404.

TARMOQNING TRANSPORT BOSQICHIDA XAVFSIZ ULANISHNI O‘RNATUVCHI XORIJIY TLS 1.3 PROTOKOLLARI TAHLILI

Baxtiyorov U.B., Tolmasov J.J.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalari instituti

Annotatsiya. Maqolada bugungi kunda dolzarb masala sifatida qaralayotgan mijoz-server o‘rtasida xavfsiz aloqani ta’minlovchi AQSH, Rossiya Federatsiyasi va Belarus Respublikasining TLS 1.3 protokollari tahlili keltirilgan.

Kalit so‘zlar: Transport sathi, TLS protokoli, RFC 8446, GOST TLS, СТБ 34.101.90, AEAD shifrlash, Elektron raqamli imzo.

Аннотация. В статье представлен анализ протоколов TLS 1.3 США, Российской Федерации и Республики Беларусь, обеспечивающих защищенное соединение между клиентом и сервером, что на сегодняшний день является актуальной задачей.

Ключевые слова: Транспортный уровень, протокол TLS, RFC 8446, ГОСТ TLS, СТБ 34.101.90, AEAD-шифрование, электронная цифровая подпись.

Kirish

Hozirgi axborot texnologiyalari jadal rivojlanib borayotgan davrda, shuningdek, raqamli ma’lumotlarning ko‘payib borishi, axborot xavfsizligiga bo‘lgan talabni yanada oshirib bormoqda.

Axborot xavfsizligini ta’minlashda har bir davlat o‘zlarining milliy kriptografik algoritmlaridan foydalangan holda milliy standartlarini yaratgan. Bundan asosiy maqsad axborot almashinuvida ma’lumotlarning oshkor bo‘lmasligi, ularning xavfsizligini ta’minlashga harakat qiladi. Belarus Respublikasida ham AQSH hamda Rossiya Federatsiyasi kabi davlatlar singari o‘zining milliy standart kriptografik algoritmlar asosida ma’lumotlarning maxfiyligi, yaxlitligi va ishtirokchilarning autentifikatsiyasini ta’minlovchi protokol ishlab chiqish bo‘yicha izlanishlar olib borilib, СТБ 34.101.90-2025 standarti qabul qilingan.

Respublikamizda Kriptologiya instituti (*avvalgi Radioelektron tizimlar va axborot texnologiyalari markazi*) bitiruvchilari Maxmudjonov K.O. tominidan “*Tarmoqning transport bosqichida xavfsiz ulanishni o‘rnatish xalqaro protokollari tadqiqi*” [11] hamda O‘ralov U.O‘. tomonidan “*Rossiya davlat kriptografik standart algorimlaridan foydalangan holda mijoz-server ilovalari o‘rtasida xavfsiz tarmoq ulanishini o‘rnatish protokollari tadqiqi*” [12], Saidov A.A. tomonidan “*Belarus Respublikasining davlat standarti asosidagi transport protokolini (TLS 1.2) o‘rganish va tadqiq qilish*” [13] va Sattorov Sh.I. tomonidan “*Transport pog‘onasida xavfsiz aloqani o‘rnatish uchun kalitlarni generatsiya qilish algoritmini yaratish*” [14] mavzularida magistrlik dissertatsiya ishlari amalga oshirilgan.

Mazkur maqolada Xalqaro RFC 8446, GOST 1323565.1.030-2020 va СТБ 34.101.90-2025 standartlarida keltirilgan TLS 1.3 protokolining AQSH, Rossiya va Belarus variantlarining qiyosiy tahlili keltirilgan.

Asosiy qism

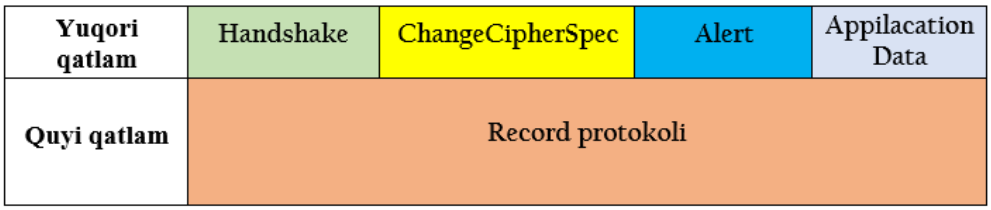
TLS (*Transport Layer Security*) – Transport qatlamida xavfsizlikni ta’minlash protokoli bo‘lib, u kompyuter tarmoqlarida mijoz va server o‘rtasida xavfsiz aloqa o‘rnatishni ta‘minlashga javob beradigan kriptografik protokol hisoblanadi. Protokol ikkita qatlamdan quyi va yuqori qatlamdan tashkil topgan (*1-rasm*). Yuqori qatlam Handshake protokoli, quyi qatlam esa Record

protokoli deb nomlanadi TLS 1.3 protokolida Handshake bosqiching 3 ta 1-RTT, PSK va 0-RTT rejimlari mavjud.

1-RTT – Mijoz va server o‘rtasida birlamchi xavfsiz ulanishni o‘rnatish jarayonida qo‘llaniladi. Mazkur rejimda mijoz boshlang‘ich *ClientHello* xabari tarkibida o‘zining efemer kalit ulushini (key_share) uzatadi, server esa *ServerHello* xabari orqali kriptografik to‘plamni tanlab, o‘z kalit parametrlarini qaytaradi. Natijada, atigi bitta tarmoq aylanishi (1-RTT – *Round Trip Time*) davomida tomonlar umumiy maxfiy kalitni hisoblab chiqadi hamda keyingi barcha autentifikatsiya va ilova ma’lumotlari to‘liq shifrlangan kanal orqali uzatiladi.

PSK – Ilgari bog‘langan mijozning serverga qayta tezkor ulanish mexanizmi. Unda qayta sertifikat tekshirish va asimmetrik hisoblashlar o‘tkazilmasdan, oldingi sessiyadan saqlab qolingan umumiy maxfiy kalit *(PSK – Pre-Shared Key)* yoki sessiya chiptasi (*Session Ticket)* orqali ulanish minimal hisoblash resurslari bilan darhol tiklanadi.

0-RTT – Qayta ulanishda mijoz serverning tasdiqlovchi javobini kutmasdan, birinchi so‘rovning o‘zidayoq ilova ma'lumotlarini (masalan, HTTP so‘rovini) shifrlab uzatadigan tezkor rejim. Ma'lumotlar oldingi sessiyadan qolgan PSK kaliti yordamida himoyalanadi. Bu ulanish kechikishini butunlay yo‘qotsa-da, paketni qayta yuborish xurujlariga (*Replay Attacks*) nisbatan zaif bo‘lganligi sababli ma’lum cheklovlar bilan qo‘llaniladi (Rossiya standartida esa qat’iyan ta’qiqlangan).



1-rasm. TLS protokolining umumiy tuzilishi

TLS protokolining ayni vaqtda to‘rtta versiyasi bor bo‘lib ular TLS 1.0, TLS 1.1, TLS 1.2 va TLS 1.3 versiyalari bilan nomlanadi.

AQSh va Yevropa

AQSh va Yevropa mamlakatlari internet tarmog‘i orqali uzatiluvchi, davlat sirini tashkil etmaydigan konfidensial ma’lumotlarni himoyalashda xalqaro RFC 8446 tavsiyasi asosidagi TLS 1.3 protokolidan foydalanadi.

Protokol umumiy 5 ta kriptoto‘plamlarni qo‘llab-quvvatlaydi va ular quyidagilar [1, 15]:

- *TLS_AES_128_GCM_SHA256*
- *TLS_AES_256_GCM_SHA384*
- *TLS_CHACHA20_POLY1305_SHA256*
- *TLS_AES_128_CCM_SHA256*
- *TLS_AES_128_CCM_8_SHA256*

TLS 1.3 versiyasi uning barcha avvalgi versiyalaridan farq qiladi. TLS 1.3 protokolining tuzilishi va ishlash prinsipi xalqaro tashkilot IETF tomonidan 2018-yilda tasdiqlangan RFC 8446 tavsiyada keltirilgan. TLS 1.3 protokolini ishlab chiqishning asosiy maqsadi TLS 1.2 protokoli bilan muvofiqlikni saqlab qolgan holda uzatiluvchi ma’lumotlar xavfsizligini ta’minlashni yanada mustahkamlash hamda tezligini oshirishdan iborat.

TLS protokollarining har bir versiyasida kalit almashish, autentifikatsiya, shifrlash va psevdotasodifiy sonlarni yaratish uchun turli xildagi standart kriptografik algoritmlardan foydalaniladi.

Rossiya Federatsiyasi

Rossiya Federatsiyasining milliy TLS 1.3 protokoli P 1323565.1.030-2020 tavsiyasi bilan tartibga solingan bo‘lib, xalqaro algoritmlar o‘rniga to‘liq standart GOST algoritmlaridan foydalanishga tayanadi. Unda simmetrik shifrlash uchun “Kuznyechik” va “Magma” algoritmlari, autentifikatsiyalangan shifrlashda esa MGM (*Multilinear Galois Mode*) rejimi qo‘llaniladi. Autentifikatsiya GOST R 34.10-2012 [5] standarti asosidagi elektron raqamli imzo algoritimi bilan ta’minlanadi. Protokolning asosiy xususiyati shundaki, yuqori xavfsizlik talablari sababli, unda zaifliklarga ega 0-RTT rejimi butunlay taqiqlangan hamda ma’lumotlar almashinuvida majburiy kalit yangilash (*rekeying*) tizimi joriy etilgan. Ushbu yondashuv amaliyotda Yandex Browser, Chromium-Gost va CryptoPro CSP vositalari orqali davlat axborot tizimlarining kriptografik suverenitetini to‘liq ta’minlaydi. Rossiya Federatsiyasida transport sathida axborot xavfsizligini ta’minlashning zamonaviy yechimi sifatida TLS 1.3 protokolining milliy kriptografik vositalarga moslashtirilgan varianti ishlab chiqilgan. Bundan asosiy maqsad xalqaro TLS 1.3 protokolidagi 1-RTT tezkor ulanish modelini saqlagan holda, barcha kriptografik operatsiyalarni to‘liq Rossiya davlat standart kriptografik (*GOST*) algortimlariga o‘tkazishdan iborat.

Rossiya Federatsiyasining TLS 1.3 protokolida xalqaro standartdagi AES, SHA va ECDSA algoritmlari butunlay inkor etilib, o‘rniga simmetrik shifrlash uchun GOST R 34.12-2015 [3] standartiga muvofiq “Kuznyechnik” va “Magma” shifrlari, AEAD sifatida MGM [4,16] rejimi, xesh-funksiya sifatida “Stribog” (*GOST R 34.11-2012*) algoritmi, Elektron raqamli imzo algoritmi sifatida GOST R 34.10-2012 [5] standartlari qo‘llanilgan. Rossiya Federatsiyasining TLS 1.3 protokolida quyidagi kriptoto‘plamlar mavjud:

- *TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L*
- *TLS_GOSTR341112_256_WITH_MAGMA_MGM_L*
- *TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S*
- *TLS_GOSTR341112_256_WITH_MAGMA_MGM_S*

Rossiya Federatsiyasining TLS 1.3 protokolidagi eng e’tiborga molik arxitekturaviy farqi shundaki, unda 0-RTT mexanizmi qat’iyan man etilgan. Standart talabiga ko‘ra, early_data kengaytmasi va EndOfEarlyData xabarlaridan foydalanishga yo‘l qo‘yilmaydi. Rossiya Federatsiyasi axborot xavfsizligi konsepsiyasida xavfsizlik ko‘rsatkichi tezlikdan ustun qo‘yilganligi sababli, qayta ulanishlar ham kamida 1-RTT kechikish bilan bajarilishi shart qilib belgilangan.

Belarus TLS 1.3

Belarus Respublikasining milliy TLS 1.3 protokoli СТБ 34.101.90-2025 davlat standarti asosida tartibga solingan. Mazkur protokol zamonaviy 1-RTT ulanish modeliga tayanib, an’anaviy blokli shifrlardan tashqari shimgich (*sponge duplex*) arxitekturasini tatbiq etgani bilan xalqaro miqyosda ajralib turadi. Standartda asosiy va majburiy shifrlash to‘plami sifatida *TLS_BASH_PRG_AE2561_BASH256*, muqobil sifatida esa *BELT-CHE* [8] algoritmi belgilangan. Asosiy AEAD primitivi hisoblangan BASH-PRG-AE2561 [9, 17] algoritmi 1536 bitli holat sig‘imiga ega bo‘lib, bitta sessiya kaliti ostida ma’lumotlarni shifrlash imkonini beradi. Autentifikatsiya bosqichida esa “Shnorr” sxemasiga asoslangan milliy “Bign” [7] elektron raqamli imzo algoritmi qo‘llaniladi. Belarus Respublikasida amaliy jihatdan mazkur protokol Chromium va Epiphany kabi ochiq kodli brauzerlarida muvaffaqiyatli tatbiq etilgan. Mazkur standart zamonaviy 1-RTT tezkor qo‘l siqish konsepsiyasini Belarus Respublikasining o‘ziga xos milliy kriptografik primitivlari bilan integratsiya qiladi.

СТБ 34.101.90-2025 standartida ikkita kriptoto‘plam belgilangan bo‘lib, ulardan biri majburiy, ikkinchisi esa ixtiyoriy hisoblanadi:

- *TLS_BELT_CHE256_BELT_HASH*
- *TLS_BASH_PRG_AE2561_BASH256*

Birinchi kriptoto‘plamda BELT simmetrik shifrlash algoritmi, uning CHE256 AEAD rejimi va BELT_HASH xesh algoritmidan foydalanilgan [8].

Belarus Respublikasining TLS 1.3 protokolida elektron raqamli imzo sifatida BIGN algoritmidan foydalangan [7].

Shuningdek, AEAD primitivi sifatida blokli shifrlardan (*AES yoki Kuznyechik*) emas, balki shimgich avtomatiga asoslangan BASH-PRG-AE algoritmidan [9] foydalanadi va bu algoritm 256 bitli imitohimoya tegini hosil qiladi, bu esa uning ma’lumotlar yaxlitligini buzishga qarshi hujumlarning AES-GCM ga nisbatan 2^{128} marotaba yuqori bo‘lishini ta’minlaydi [10].

AQSH, Rossiya Federatsiyasi va Belarus Respublikasining TLS 1.3 protokollaridagi asosiy farqlar 1-jadvalda keltirilgan.

1-jadval

Xorijiy TLS 1.3 protokollarini solishtirish jadvali

Asosiy ko‘rsatkichlar	AQSH	Rossiya	Belarus
Asosiy me’yoriy hujjat	RFC 8446	Р 1323565.1.030-2020	СТБ 34.101.90-2025
Tasdiqlangan muddati	2018-yil	2020-yil	2025-yil
Shifrlash algoritmi	AES, Chacha20	Magma, Kuznyechik	BASH-PRG-AE, BELT
Xesh-funksiya algoritmi	SHA-384	ГОСТ Р 34.11-2012	BASH-256, BELT-HASH
ERI algoritmi	ECDSA	ГОСТ Р 34.10-2012	BIGN
Autentifikatsiyalangan shifrlash	CCM, GCM, ChaCha20-Poly	MGM	BASH-PRG-AE, BELT-CHE
Psevdotasodifiy funktsiya	HKDF (Extract-Expand)	HKDF (Extract-Expand)	BASH sponge, BELT-KDF
0-RTT	+	-	+
Qo‘llab-quvvatlovchi brauzerlar	Barcha brauzerlar	Yandex, Sputnik, Chromium-Gost, Internet Explorer	Epiphany, Chromium (btls/OpenSSL patch bilan)

Xulosa

O‘tkazilgan tizimli tahlil natijalari asosida quyidagi ilmiy-amaliy xulosalar shakllantirildi:

1. Qiyosiy tahlil shuni ko‘rsatdiki, AQSH standarti global moslashuvchanlik va apparat tezlatkichlariga tayangan holda yuqori tezlikni ta’minlashga yo‘naltirilgan.

2. Rossiya Federatsiyasining TLS 1.3 protokoli esa aksincha, xavfsizlikni tezlikdan ustun qo‘yib, zaifliklarga ega 0-RTT rejimini butunlay taqiqlagan va MGM rejimini joriy etgan.

3. Belarus Respublikasi standarti ilg‘or BASH shimgich (*sponge duplex*) arxitekturasini tatbiq etgani bilan ajralib turadi.

4. Autentifikatsiya darajasida Belarus protokoli 256-bitli yirik imitohimoya kodini hosil qiladi.

5. Milliy xavfsiz protokol yaratishda Rossiya Federatsiyasining 0-RTT rejimini cheklaganligi hamda Belarus Respublikasining Bign va BASH innovatsiyalarini uyg‘unlashtirish masalasini ko‘rib chiqish maqsadga muvofiq hisoblanadi.

Foydalanilgan adabiyotlar

1. RFC 8446 “ The Transport Layer Security (*TLS*) Protocol Version 1.3”.
2. Р 1323565.1.030-2020 “Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе TLS 1.3”.
3. ГОСТ Р 34.12-2015 “Информационная технология. Криптографическая защита информации. Блочные шифры”.
4. Р 1323565.1.026-2019 “Криптографическая защита информации. Режим работы блочных шифров с одновременным обеспечением конфиденциальности и целостности (*MGM*)”.
5. ГОСТ Р 34.10-2012 “Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи”.
6. СТБ 34.101.90-2025 “Информационные технологии и безопасность. Протокол защиты транспортного уровня (*TLS 1.3*)”.
7. СТБ 34.101.45-2013 “Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых”.
8. СТБ 34.101.31-2020 “Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности”.
9. СТБ 34.101.77-2020 “Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции”.
10. S. Agievich, V.Marchuk, A. Maslau, V.Semenov “Bash-f: another LRX sponge function” Research Institute for Applied Problems of Mathematics and Informatics Belarusian State University.
11. Maxmudov K.O. Tarmoqning transport bosqichida xavfsiz ulanishni o‘rnatish xalqaro protokollarining tadqiqi. Axborot xavfsizligi mutaxasisligi bo‘yicha akademik darajasini olish uchun yozilgan dissertatsiya.
12. O‘ralov U.O‘. Rossiya davlat kriptografik algoritmlaridan foydalangan holda mijoz-server ilovalari o‘rtasida xavfsiz tarmoq ulanishini o‘rnatish protokollari tadqiq. Axborot xavfsizligi mutaxasisligi bo‘yicha akademik darajasini olish uchun yozilgan dissertatsiya.
13. Saidov A.A. Belarus Respublikasining davlat standarti asosidagi transport bosqich protokolini (*TLS 1.2*) tadqiq qilish. Axborot xavfsizligi mutaxasisligi bo‘yicha akademik darajasini olish uchun yozilgan dissertatsiya.
14. Sattorov Sh.I. Transport pog‘onasida xavfsiz aloqani o‘rnatish uchun kalitlarni generatsiya qilish algoritmini yaratish. Axborot xavfsizligi mutaxasisligi bo‘yicha akademik darajasini olish uchun yozilgan dissertatsiya.
15. https://datatracker.ietf.org
16. https://www.cryptopro.ru
17. https://www.tnpa.by

NOL-BILIM USULLARIGA ASOSLANGAN AUTENTIFIKATSIYA PROTOKOLLARINING ISHLASH MEXANIZMLARI VA XAVFSIZLIK XUSUSIYATLARINI BAHOLASH

Sattarov A.B., Normurodov T.B.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Maqolada axborot tizimlarida obyektni autentifikatsiyalash masalasi hamda nol-bilim isbotlariga (ZKP) asoslangan Fiat-Shamir, Feige-Fiat-Shamir, Guillou-Quisquater va Schnorr protokollari tahlil qilingan. Protokollarning matematik asoslari, ishlash tartibi, aldash ehtimoli bo‘yicha ko‘rsatkichlari ko‘rib chiqilgan va to‘liqlik, ishonchlilik, nol-bilimlilik mezonlari asosida xavfsizlikni baholash usullari tizimlashtirilgan. Tahlil natijasida mavjud protokollar faktorizatsiya (RSA) va diskret logarifm masalalarining murakkabligiga tayanishi, ularning amaliy xavfsizligi esa raundlar soni, tasodifiy qiymatlar sifati va parametrlar uzunligiga bog‘liqligi aniqlangan. Kriptografik parametrlar bo‘yicha minimal talablar keltirilgan.

Kalit so‘zlar: nol-bilim isboti, autentifikatsiya protokoli, kriptografik xavfsizlik, interaktiv isbot, maxfiylik, Prover, Verifier, Fiat-Shamir, Schnorr, replay, MITM.

Аннотация. В статье рассмотрена проблема аутентификации объектов в информационных системах, а также проанализированы протоколы Fiat–Shamir, Feige–Fiat–Shamir, Guillou–Quisquater и Schnorr, основанные на доказательствах с нулевым разглашением (ZKP). Рассмотрены математические основы протоколов, порядок их функционирования и показатели вероятности обмана, систематизированы методы оценки безопасности на основе критериев полноты, достоверности и нулевого разглашения. В результате анализа установлено, что существующие протоколы основываются на вычислительной сложности задач факторизации и дискретного логарифмирования, а их практическая безопасность зависит от количества раундов, качества случайных значений и длины параметров. Приведены минимальные требования к криптографическим параметрам.

Ключевые слова: доказательство с нулевым разглашением, протокол аутентификации, криптографическая безопасность, интерактивное доказательство, конфиденциальность, доказывающая сторона (Prover), проверяющая сторона (Verifier), Fiat–Shamir, Schnorr, replay, MITM.

Kirish

Zamonaviy kiberhujumlar autentifikatsiya mexanizmlariga qo‘yiladigan xavfsizlik talablarini kuchaytirmoqda. An’anaviy login-parol tizimlarida maxfiy ma’lumot tekshiruvchi tomonga uzatiladi yoki uning xeshi serverda saqlanadi, shu sababli ular fishing, replay va MITM hujumlari hamda server ma’lumotlar bazasining buzilishi xavfiga ega. Nol-bilim isbotlariga asoslangan protokollar maxfiy ma’lumotni oshkor qilmasdan uning egasi ekanligini tasdiqlash imkonini berishi bilan an’anaviy autentifikatsiya yondashuvlaridan farq qiladi. Shu sababli ZKP asosidagi autentifikatsiya protokollarini amaliy tizimlarda qo‘llashda ularning ishlash mexanizmlari, to‘liqlik, ishonchlilik, nol-bilimlilik xususiyatlari hamda replay va MITM hujumlariga bardoshliligini qiyosiy tahlil qilish hozirda dolzarb ilmiy-amaliy masalalardan biri hisoblanadi.

Asosiy qism

Nol-bilim isboti konsepsiyasi birinchi marta Goldwasser, Micali va Rackoff tomonidan 1985-yilda taklif etilgan, 1989-yilda esa «The Knowledge Complexity of Interactive Proof Systems» nomli maqolada ilmiy jihatdan asoslangan [1]. Unga ko‘ra isbotlovchi tomon *P* (Prover) tekshiruvchi *V* (Verifier) ga biror tasdiqning rostligini, ya’ni *s* sirga egaligini isbotlaydi, biroq isbotlash jarayonida sirning o‘zi yoki u haqida foydali qo‘shimcha axborot oshkor qilmaydi. Bu turdagi autentifikatsiya protokollarida *P* - da’vogar obyekt, *V* - tekshiruvchi tomon bo‘lib, *V* ochiq parametrlar va *P* ning ochiq kalitiga ega, yakunda esa faqat «qabul qilish» yoki «rad etish» qaroriga keladi. Ko‘rib chiqilayotgan protokollar uch qadamli (majburiyat - chaqiriq - javob) interaktiv sxema asosida ishlaydi.

Nol-bilim protokoli uchta xususiyatni qanoatlantirishi lozim [1]:

To‘liqlik (completeness): P haqiqatan sirga ega bo‘lib, protokol qoidalariga amal qilsa, *V* uni doimo qabul qiladi.

Ishonchlilik (soundness): sirga ega bo‘lmagan *P** ning *V* ni aldash ehtimoli juda kichik. Agar bir raundda aldash ehtimoli ε bo‘lsa, bog‘liq bo‘lmagan t ta raunddan so‘ng u ε^t gacha kamayadi, chaqiriq bitta bit bo‘lganda $\varepsilon = 1/2$, demak ehtimol 2^{-t} dan oshmaydi.

Nol-bilimlilik (zero-knowledge): V protokol davomida *s* haqida foydali qo‘shimcha axborot olmaydi. Bu xususiyat simulyator orqali asoslanadi: agar protokol transkriptiga o‘xshash ma’lumotlarni sirni bilmasdan ham hosil qilish mumkin bo‘lsa, haqiqiy transkript sir haqida qo‘shimcha axborot bermaydi.

Nol-bilim usullari asosidagi obyekt autentifikatsiyasi mexanizmlari ISO/IEC 9798-5 standartida keltirilgan bo‘lib, ushbu standart identifikatorga, butun sonlar faktorizatsiyasiga, diskret logarifmga va asimmetrik shifrlashga asoslangan mexanizmlarni qamrab oladi [2]. Mazkur mexanizmlarning kriptografik asoslari va ishlash tamoyillarini tahlil qilish maqsadida ushbu maqolada faktorizatsiya muammosiga asoslangan Fiat-Shamir va Feige-Fiat-Shamir, RSA masalasiga asoslangan Guillou-Quisquater, shuningdek, diskret logarifm muammosiga asoslangan Schnorr protokollari ko‘rib chiqiladi.

Mavjud autentifikatsiya protokollarining ishlash mexanizmi

Fiat-Shamir protokoli Fiat va Shamir tomonidan taklif etilgan [3] bo‘lib, nol-bilimga asoslangan dastlabki amaliy autentifikatsiya sxemalaridan biridir. Uning xavfsizligi $n = pq$ modulni tub ko‘paytuvchilarga ajratish masalasining hisoblash murakkabligiga tayanadi. Ishonchli markaz katta p va q tub sonlarni tanlab, n ni e’lon qiladi (p, q maxfiy qoladi). Isbotlovchi n ga o‘zaro tub s $(1 \le s \le n-1)$ maxfiy kalitni tanlaydi va ochiq kalitni hisoblaydi:

$$v = s^2 \bmod n.$$

Har bir raund quyidagicha bajariladi:

1) *P* tasodifiy *z* ni tanlab, $x = z^2 \bmod n$ ni *V* ga yuboradi;

2) *V* tasodifiy $b \in \{0,1\}$ bitni yuboradi;

3) *P* javob sifatida $y = z \cdot s^b \bmod n$ ni yuboradi, ya’ni $b = 0$ da $y = z$, $b = 1$ da $y = zs \bmod n$. *V* quyidagi shartni tekshiradi:

$$y \neq 0 \quad \text{va} \quad y^2 \equiv x \cdot v^b \pmod n.$$

To‘liqlik $b = 1$ da $y^2 = z^2 s^2 \equiv x \cdot v \pmod n$ tengligidan bevosita kelib chiqadi. Sirni bilmagan hujumchi ikkala chaqiriqqa ham javob bera olmaydi. U eng yaxshi holda bittasiga tayyorlanishi mumkin, shuning uchun bir raundda aldash ehtimoli 1/2 dan oshmaydi, t raundda

esa 2^{-t} dan oshmaydi. Amalda t ni dastlab 20 dan 40 gacha oraliqdan tanlash tavsiya etilgan; zamonaviy talablar quyida keltiriladi.

Feige-Fiat-Shamir protokoli Fiat-Shamir sxemasining umumlashmasi bo‘lib, bitta kalit o‘rniga kalitlar vektoridan foydalanadi [4]. Isbotlovchi $S = [s_1, \dots, s_m]$ maxfiy kalit vektorini tanlaydi, ochiq kalit vektori esa

$$v_i = (s_i^2)^{-1} \bmod n, \quad i = 1, \dots, m$$

munosabatidan aniqlanadi. Protokolda amalga oshiriladigan qadamlar:

1) P $(1,\ n-1)$ oraliqdan tasodifiy z sonini tanlaydi va V ga $x = z^2 \bmod n$ sonini yuboradi;

2) V tasodifiy $B = [b_1, \dots, b_m]$ bitlar vektorini tanlab, P ga yuboradi;

3) P $y = z \cdot s_1^{b_1} \cdot s_2^{b_2} \cdots s_m^{b_m} \bmod n$ sonini hisoblab, V ga yuboradi.

V quyidagi tenglikni tekshiradi:

$$y^2 \cdot \prod_{i=1}^{m} v_i^{b_i} \equiv x \ (\mathrm{mod}\ n).$$

Haqiqatan, $s_i^2 v_i \equiv 1$ bo‘lgani uchun chap tomon $z^2 \prod (s_i^2 v_i)^{b_i} \equiv z^2 \equiv x \ (\mathrm{mod}\ n)$ ga teng. Chaqiriq fazosi 2^m ta qiymatdan iborat bo‘lgani sababli t raunddan keyin aldash ehtimoli 2^{-mt} ga teng. Mualliflar $m = 5,\ t = 4$ qiymatlarini tavsiya etadi, bunda ehtimol 2^{-20} bo‘ladi. Shunday qilib, protokol aloqa raundlari sonini kamaytirishga imkon beradi, lekin maxfiy va ochiq kalit vektorlarini saqlash zarur bo‘ladi.

Guillou-Quisquater protokoli RSA kriptotizimi asosida qurilgan bo‘lib, smart-kartalar va resurslari cheklangan qurilmalar uchun mo‘ljallangan [5]. Ishonchli markaz RSA moduli $n = pq$ va $\mathrm{ekub}\big(b, \varphi(n)\big) = 1$ shartini qanoatlantiruvchi tub b ni (xavfsizlik parametri) ochiq parametr sifatida e’lon qiladi. Isbotlovchi $\mathrm{ekub}(s, n) = 1$ bo‘lgan maxfiy s kalitni tanlaydi, ochiq kalit $v = s^{-b} \bmod n$ hisoblaydi.

Protokolda:

1) P $x = r^b \bmod n$ ni V ga yuboradi (r - tasodifiy son);

2) V tasodifiy chaqiriq e $(1 \le e \le b-1)$ ni P ga yuboradi;

3) P javob sifatida $y = r \cdot s^e \bmod n$ ni V ga yuboradi.

V quyidagi shartni tekshiradi:

$$x \equiv y^b\, v^e \ (\mathrm{mod}\ n).$$

To‘liqlik: $y^b v^e \equiv r^b s^{eb} s^{-eb} \equiv r^b \equiv x \ (\mathrm{mod}\ n)$. Chaqiriq e, 1 dan b−1 gacha tanlanganligi sababli bir raundda aldash ehtimoli taxminan 1/b bo‘lib, GQ sxemasi bitta raundda ham yuqori xavfsizlikka erishishga yo‘naltirilgan, bu esa uni kam aloqa talab qiladigan qurilmalarda qulay qiladi.

Schnorr protokoli diskret logarifm masalasining murakkabligiga tayanadi [6]. Ishonchli markaz ushbu parametrlarni tanlaydi va barcha abonentlarga e’lon qiladi:

p, q - tub sonlar, q soni $p-1$ sonining tub bo‘luvchisi. Schnorr p ning uzunligi kamida 512 bit, q ning uzunligi kamida 140 bit bo‘lishini taklif qilgan;

$\alpha \in Z_p^*$ - tartibi q bo‘lgan generator: $\alpha^q \equiv 1 \ (\mathrm{mod}\ p)$;

$t \in N$ - xavfsizlik parametri: $q > 2^t$.

P ning yopiq kaliti $s \in Z_q$, ochiq kaliti $v = \alpha^{-s} \bmod p$.

Protokol:

1) $P \to V$: $x = \alpha^r \bmod p$, bu yerda $r \in Z_q$ - tasodifiy son;

2) $V \to P$: tasodifiy e, $1 \le e \le 2^t$;

3) $P \to V$: $y = (r + s \cdot e) \bmod q$.

V quyidagini tekshiradi:

$$x \equiv \alpha^y \, v^e \pmod{p}.$$

To‘liqlik: $\alpha^y v^e = \alpha^{r+se}\alpha^{-se} = \alpha^r = x \pmod{p}$. Chaqiriq sifatida *t*-bitli son o‘rniga bitta bit ($e \in \{0,1\}$) olinsa, uch qadamli sxema bir necha marta takrorlanadi. Schnorr sxemasining interaktiv bo‘lmagan varianti (Fiat-Shamir transformatsiyasi asosida) IETF RFC 8235 da bayon etilgan [7].

Xavfsizlikni baholash mezonlari va usullari

Protokol nazariy jihatdan to‘g‘ri tuzilgan bo‘lsa ham, amalda mantiqiy xatolar, zaif tasodifiy sonlar generatori, kalitlarni noto‘g‘ri boshqarish yoki kanalni tinglash natijasida zaif bo‘lishi mumkin. Shu sababli baholash formal-mantiqiy, kriptografik, statistik va amaliy tahlil usullarini qamrab olishi lozim. ZKP protokollari uchun baholash quyidagi savollarga javob izlashga keltiriladi:

1) qonuniy foydalanuvchi har doim qabul qilinadimi (to‘liqlik);

2) kalitsiz hujumchi tekshiruvchini aldash imkoniga egami (ishonchlilik);

3) uzatiladigan xabarlardan kalit yoki uning qismini tiklash mumkinmi (nol-bilimlilik);

4) eski seans transkriptlarini replay hujumida qo‘llash mumkinmi;

5) protokol MITM hujumlariga bardoshlimi.

Nol-bilimlilikni baholash. Asosiy vosita simulyator: transkriptni sirsiz, probabilistik polinomial vaqtli (PPT) algoritm bilan hosil qila olish nol-bilimlilikni asoslaydi. Qo‘shimcha ravishda javoblardan kalitni hisoblash mumkinligi, bir necha seans xabarlari yig‘ilganda sirning ochilmasligi hamda tasodifiy qiymatlarning qayta ishlatilishi tekshiriladi. Oxirgisi eng xavfli amaliy zaiflikdir. Masalan, Schnorr sxemasida bir xil *r* bilan ikki xil chaqiriq $e_1 \neq e_2$ ga javob berilsa, $y_1 - y_2 \equiv s(e_1 - e_2) \pmod{q}$ bo‘lib, maxfiy kalit

$$s \equiv (y_1 - y_2)(e_1 - e_2)^{-1} \pmod{q}$$

formulasi bilan tiklanadi. Fiat-Shamir sxemasida ham bir xil z uchun $b = 0$ va $b = 1$ javoblari ($y_0 = z$, $y_1 = zs$) sirni ochadi. Shu sababli har seans uchun yangi *r* yoki *z* ni kriptografik sifatli tasodifiy sonlar generatoridan olish majburiy talab hisoblanadi.

Ishonchlilikni baholash. Raundlar soni ortishi bilan aldash ehtimoli eksponensial kamayadi: Fiat-Shamir va Schnorr sxemalarida 2^{-t}, Feige-Fiat-Shamir da 2^{-mt}, Guillou-Quisquater da bir raundda taxminan 1/b. Biroq faqat ehtimollik yetarli emas, implementatsiya ham to‘g‘ri bo‘lishi kerak.

Replay hujumiga bardoshlilik. Replay hujumida hujumchi qonuniy foydalanuvchi va tekshiruvchi o‘rtasidagi seans transkriptini yozib olib, keyinroq tekshiruvchiga qayta yuboradi. Interaktiv protokollarda bunday hujum o‘tmaydi: tekshiruvchi har seansda yangi tasodifiy *e′* chaqiriq tanlaydi, eski *y* esa faqat eski *e* uchun yaroqli. Chaqiriq bitta bit bo‘lganda hujumchining muvaffaqiyat ehtimoli bir raundda 1/2, *t* raundda 2^{-t} ga teng. Interaktiv bo‘lmagan variantda (RFC 8235) chaqiriq xeshdan hisoblanadi, shuning uchun xesh kiritishiga nonce, vaqt belgisi va tekshiruvchi identifikatori ID_V qo‘shilmasa, yozib olingan isbotni qayta ishlatish mumkin, shunda isbot faqat bir seans va bir tekshiruvchi uchun yaroqli bo‘ladi.

MITM hujumiga bardoshlilik. Nol-bilimlilik tufayli o‘rtadagi hujumchi xabarlardan sirni tiklay olmaydi. Biroq ZKP faqat sirni bilishni isbotlaydi, kanalni himoya qilmaydi: hujumchi xabarlarni o‘zgartirmasdan uzatib (relay), joriy seansda foydalanuvchi o‘rnida qabul qilinishi mumkin. Shu sababli xabarlarni ID_P, ID_V va session_id ga bog‘lash (interaktiv

bo‘lmagan variantda ularni xeshga kiritish) hamda protokolni autentifikatsiyalangan shifrlangan kanal (masalan, TLS) ichida bajarish tavsiya etiladi.

Matematik asos va parametrlar. Dastlabki mualliflar tavsiya etgan parametrlar ($n \geq 512$ bit, $|p| \geq 512$, $|q| \geq 140$ bit) tarixiy xarakterga ega. NIST SP 800-57 [8] asosida zamonaviy minimal talablar yuqoriroq belgilanadi: $|n| \geq 2048$ bit, $|q| \geq 224$ bit, xesh-funksiya sifatida SHA-256 yoki SHA-3 qo‘llanadi. Shuningdek, seans identifikatori kamida 128 bit, raundlar soni esa $t \geq 40$ bo‘lishi tavsiya etiladi. Faktorizatsiya va diskret logarifm masalalari klassik kompyuterlar uchun qiyin deb hisoblanadi, ammo Shor algoritmi kvant kompyuterda ularni polinomial vaqtda yechish imkonini beradi [9], shu sababli kvantga bardoshlilik ochiq masala bo‘lib qoladi.

Tahlil natijalari. Protokollarning ishonchliligi chaqiriq fazosi va raundlar soniga, amaliy xavfsizligi esa tasodifiy qiymatlarning takrorlanmasligiga bog‘liq. Fiat-Shamir va Schnorr sxemalarida ularning qayta ishlatilishi maxfiy kalitni oshkor qiladi. Interaktiv protokollarda har seansdagi yangi chaqiriq replay hujumidan, xabarlarni ishtirokchilar va seans kontekstiga bog‘lash esa MITM (relay) hujumidan himoya qiladi.

Xulosa

O‘tkazilgan qiyosiy tahlil natijasida Fiat-Shamir, Feige-Fiat-Shamir, Guillou-Quisquater va Schnorr protokollarining ishlash mexanizmlari hamda xavfsizlik xususiyatlari baholandi. Natijalar ZKP asosidagi autentifikatsiyada maxfiy kalit uzatilmasligi bilan bir qatorda, protokolning amaliy xavfsizligi tasodifiy qiymatlarning sifati, raundlar soni, chaqiriqlar fazosi va kriptografik parametrlarning to‘g‘ri tanlanishiga bog‘liqligini ko‘rsatdi. Olingan natijalar keyingi bosqichda ZKP asosidagi autentifikatsiya protokolining matematik modelini ishlab chiqish, uning xavfsizligini formal tahlil qilish va samaradorligini baholash uchun asos bo‘ladi.

Foydalanilgan adabiyotlar

1. Goldwasser S., Micali S., Rackoff C. The knowledge complexity of interactive proof systems // SIAM Journal on Computing, 1989, vol. 18, no. 1, pp. 186–208.

2. ISO/IEC 9798-5:2009. Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero-knowledge techniques. ISO, 2009.

3. Fiat A., Shamir A. How to prove yourself: practical solutions to identification and signature problems // Advances in Cryptology - CRYPTO ’86, LNCS 263. Springer, 1987, pp. 186–194.

4. Feige U., Fiat A., Shamir A. Zero-knowledge proofs of identity // Journal of Cryptology, 1988, vol. 1, no. 2, pp. 77–94.

5. Guillou L.C., Quisquater J.-J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory // Advances in Cryptology - EUROCRYPT ’88, LNCS 330. Springer, 1988, pp. 123–128.

6. Schnorr C.P. Efficient signature generation by smart cards // Journal of Cryptology, 1991, vol. 4, no. 3, pp. 161–174.

7. IETF RFC 8235. Schnorr Non-interactive Zero-Knowledge Proof. IETF, 2017.

8. Barker E. Recommendation for Key Management: Part 1 - General. NIST Special Publication 800-57 Part 1 Rev. 5. NIST, 2020.

9. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing, 1997, vol. 26, no. 5, pp. 1484–1509.

KVANT TEXNOLOGIYALARI VA UNI RIVOJLANTIRISHDA XORIJ TAJRIBALARI

Allayorov Y.Sh.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar institut*i*

Annotatsiya. Ushbu maqolada kvant texnologiyalarining mazmuni, asosiy yo‘nalishlari va ularni rivojlantirish bo‘yicha xorijiy tajribalar tahlil qilingan. Kvant hisoblash, kvant kommunikatsiyasi, sensorika va metrologiya hamda kvant simulyatsiyasining maqsadlari, vazifalari, amaliy qo‘llanishi va mavjud texnologik yechimlari ko‘rib chiqilgan. Rossiya, AQSh, Xitoy, Yevropa Ittifoqi, Belarus va Qozog‘iston tajribalari qiyoslanib, ilmiy markazlar, davlat dasturlari va mutaxassislar tayyorlashning ahamiyati yoritilgan. O‘zbekistonda mazkur yo‘nalishlarni bosqichma-bosqich rivojlantirish yuzasidan xulosalar chiqarilgan.

Kalit so‘zlar: kvant texnologiyalari, kubit, kvant hisoblash, kvant kommunikatsiyasi, kvant kriptografiyasi, kvant sensorlari, metrologiya, kvant simulyatsiyasi, xorij tajribasi.

Аннотация. В статье проанализированы сущность, основные направления квантовых технологий и зарубежный опыт их развития. Рассмотрены цели, задачи, практическое применение и существующие реализации квантовых вычислений, квантовых коммуникаций, квантовой сенсорики, метрологии и квантового моделирования. Сопоставлен опыт России, США, Китая, Европейского союза, Беларуси и Казахстана, освещены роль государственных программ, научной инфраструктуры и подготовки специалистов. Сформулированы выводы о поэтапном развитии указанных направлений в Узбекистане.

Ключевые слова: квантовые технологии, кубит, квантовые вычисления, квантовая связь, квантовая криптография, квантовые сенсоры, метрология, квантовое моделирование, зарубежный опыт.

Kirish

Bugungi kunda raqamli texnologiyalarning rivojlanishi axborotni tez qayta ishlash, himoyalangan aloqa o‘rnatish va fizik jarayonlarni yuqori aniqlikda o‘lchashga bo‘lgan ehtiyojni kuchaytirmoqda. Murakkab molekulalar, yangi materiallar va katta hajmdagi hisoblash masalalarida an’anaviy kompyuterlarning imkoniyatlari ayrim cheklovlarga ega. Kvant mexanikasi qonunlariga asoslangan texnologiyalar shu turdagi masalalarning ayrimlarini yangi usullar bilan hal etish istiqbolini yaratdi. Bugun kvant kompyuterlari bilan bir qatorda kvant kalitlarini taqsimlash tizimlari, atom soatlari va kvant gravimetrlari ham ishlab chiqilmoqda.

Zamonaviy kvant texnologiyalarini rivojlantirish bo‘yicha O‘zbekiston Respublikasi Prezidentining 2025-yil 27-dekabrdagi *PQ–390-son* qarori 1-ilovasining 3-bandida “Sun’iy intellekt, Big Data va kvant texnologiyalari*”* Fanlar akademiyasi ilmiy tadqiqotlarining 2030-yilgacha bo‘lgan ustuvor yo‘nalishi sifatida belgilangan [1].

Shuningdek, 2026-yil 10-martdagi *PF–38-son* Farmoni bilan 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlangan. Farmonning 2-ilovasi (“Yo‘l xaritasi”) 4-bandida kiberxavfsizlikka oid tadqiqotlarning ustuvor mavzularini, jumladan, “Sun’iy intellekt, kvant va blokcheyn texnologiyalarini joriy etish*”* imkoniyatlarini aniqlash belgilangan [2].

Shuning uchun ham ushbu yo‘nalishda ilmiy-tadqiqot ishlarini olib borish dolzarb hisoblanadi. Mazkur ish kvant texnologiyalarini rivojlantirishda xorij taribalari tahliliga bag‘ishlanadi. Ya’ni kvant texnologiyalarining ta’rifi va to‘rtta asosiy yo‘nalishi bayon etilib,

ularning maqsadi, vazifalari, qo‘llanish sohasi va real qurilmalari qiyosiy-tavsifiy usulda o‘rganilgan. Shuningdek, olti xorijiy davlat va mintaqa tajribasi asosida ilmiy tadqiqotlarni tashkil qilishning umumiy jihatlari aniqlangan. Bu yondashuv kvant qurilmalarining bugungi imkoniyatlarini kelajakdagi istiqbollardan farqlashga va milliy ehtiyojlarga mos ustuvorliklarni belgilashga yordam beradi.

Asosiy qism

Kvant texnologiyalari – kvant mexanikasi qonunlari va hodisalaridan axborotni qayta ishlash, uzatish va himoyalash, fizik kattaliklarni yuqori aniqlikda o‘lchash hamda murakkab molekulalar va materiallarni modellashtirish uchun foydalanishga asoslangan ilmiy-texnologik yo‘nalishlar majmuasidir.

Mazkur sohada superpozitsiya, kvant entanglement va kvant interferensiyasi singari xususiyatlar muhim o‘rin tutadi. Umumiy holda kvant texnologiyalari quyidagi to‘rtta asosiy yo‘nalishni o‘z ichiga oladi.

1-jadval

Kvant texnologiyalarining asosiy yo‘nalishlari.

№	Yo‘nalish	Maqsad
1	Kvant hisoblash	Murakkab masalalarni hisoblash
2	Kvant kommunikatsiyasi	Axborotni uzatish va himoyalash
3	Kvant sensorikasi va metrologiya	Yuqori aniqlikda o‘lchash
4	Kvant simulyatsiyasi	Murakkab kvant tizimlarini modellashtirish

1. Kvant hisoblash maqsadi – kvant mexanikasining superpozitsiya va chirmashuv xususiyatlaridan foydalanib, ayrim hisoblash masalalarini klassik kompyuterlarga nisbatan samaraliroq hal etadigan tizimlarni yaratish. Kvant axborotining asosiy birligi kubit (qubit) bo‘lib, uning holati maxsus fizik usullar bilan boshqariladi. Asosiy vazifalari – kubitlarni yaratish, kvant mantiqiy amallarini bajarish, algoritmlar ishlab chiqish, hisoblashdagi shovqin va xatolarni kamaytirish hamda barqaror, kengaytiriladigan protsessorlar yaratishdan iborat. Hozirgi qurilmalarning shovqinga sezgirligi natijalarni sinchiklab tekshirishni talab qiladi. Amaliy qo‘llanishi – molekulalar va materiallar hisob-kitobi, dori vositalarini loyihalash, logistika va ta’minot zanjirlarini optimallashtirish, ilmiy modellashtirish va ayrim kriptografik masalalar. Bu qurilmalar hali barcha vazifalarda oddiy kompyuterdan tez ishlaydi degani emas. Amaldagi realizatsiyalari – IBM Quantum System Two modulli arxitekturaga ega bo‘lib, Heron kabi supero‘tkazuvchan protsessorlar bilan ishlaydi. IBM Nighthawk protsessorini ham rivojlantirmoqda. Quantinuum System Model H2 ion-tuzoq texnologiyasidan foydalanadi. Qiskit va IBM Quantum Platform kvant sxemalarini simulyatsiya qilish hamda real qurilmalarda sinash imkonini beradi [3, 4].

2. Kvant kommunikatsiyasi va kvant kriptografiyasi maqsadi – kvant holatlaridan foydalanib axborot uzatishning yangi usullarini va muhim ma’lumotlar uchun himoyalangan aloqa tizimlarini rivojlantirish. Bunda QKD (Quantum Key Distribution) – kvant kalitlarini taqsimlash usuli muhim o‘rin tutadi. Asosiy vazifalari – fotonlarda axborotni kodlash, holatlarni masofaga uzatish, maxfiy kalitlarni taqsimlash, kvant tarmoqlari yaratish hamda uzatish kanali va detektorlar ishonchliligini tekshirishdan iborat. Kvant chirmashuvi uzoq masofali kvant tarmoqlari ustidagi tadqiqotlarda o‘rganilmoqda. Amaliy qo‘llanishi – davlat tashkilotlari, banklar, ma’lumot markazlari, telekommunikatsiya tarmoqlari va muhim infratuzilmalarni himoyalash. QKD maxfiy kalit almashinuvini fizik tamoyillar asosida amalga oshiradi. Postkvant kriptografiyasi esa oddiy kompyuterlarda ishlaydigan, kvant hujumlariga bardoshli algoritmlarni nazarda tutadi. Amaldagi

realizatsiyalari – ID Quantique Clavis XG optik tolali tarmoqlarga mo‘ljallangan QKD tizimlaridan biridir. Uning turli versiyalari taxminan 60–150 km diapazondagi ulanishlarga mo‘ljallangan. Toshiba Multiplexed QKD System MU odatiy ma’lumot va kvant signallarini bir tolada uzatishga imkon beradi. ID Quantique Quantis QRNG kvant jarayonlariga asoslangan tasodifiy sonlarni hosil qiladi [5–7].

3. Kvant sensorikasi va metrologiya maqsadi – Kvant hodisalariga tayangan holda vaqt, chastota, magnit va elektr maydoni, gravitatsiya kabi fizik kattaliklarni juda yuqori aniqlik va sezgirlikda o‘lchash imkonini beruvchi qurilmalarni yaratish. Asosiy vazifalari – atomlar, fotonlar va spin holatlariga asoslangan sensorlarni loyihalash, kvant interferensiyasini o‘lchashga joriy etish, tashqi shovqinni kamaytirish, o‘lchovlarning takrorlanuvchanligi va barqarorligini oshirishdan iborat. Ayrim sensorlar sharoitga mos ravishda kalibrlanishi mumkin. Amaliy qo‘llanishi – atom va optik soatlar, aniq vaqt standartlari, navigatsiya, geologik va mineral qidiruv, gidrologiya, tibbiy diagnostika, mikroelektronikani nazorat qilish hamda fundamental tajribalar. Yuqori sezgir gravitatsion o‘lchovlar yer osti tuzilmalari va suv resurslarini o‘rganishda qo‘shimcha ma’lumot beradi. Amaldagi realizatsiyalari – Exail Absolute Quantum Gravimeter (AQG) lazer yordamida sovutilgan atomlar interferensiyasiga asoslanib gravitatsiya tezlanishini yuqori aniqlikda o‘lchaydi. Atom va optik soatlar vaqt hamda chastota etalonlarini yaratishda, kvant magnetometrlari esa kuchsiz magnit signallarni aniqlashda ishlatiladi. Sensorikadagi ayrim texnologiyalar sanoat va geofizik izlanishlarda qo‘llanmoqda [8].

4. Kvant modellashtirish va kvant simulyatsiyasi maqsadi – klassik hisoblash uchun murakkab bo‘lgan molekulalar, materiallar va ko‘p zarrachali kvant tizimlarini boshqariladigan kvant qurilmalari yordamida modellashtirish. Bunda o‘rganilayotgan tizimning asosiy fizik xususiyatlari boshqa kvant muhitida takrorlanadi. Asosiy vazifalari – atom va molekulalar xususiyatlarini baholash, ko‘p zarrachali tizimlar dinamikasini hisoblash, yangi materiallarning xossalarini oldindan o‘rganish va natijalarni tajriba yoki klassik hisoblashlar bilan solishtirishdan iborat. Amaliy qo‘llanishi – yangi materiallar va katalizatorlarni tadqiq etish, kimyoviy reaksiyalarni o‘rganish, dori vositalarini izlash, energetik materiallar, supero‘tkazuvchanlik va fundamental fizik jarayonlarni tahlil qilish. Amaldagi realizatsiyalari – QuEra Aquila neytral atomlarga asoslangan analog kvant simulyatori bo‘lib, atomlar lazer yordamida boshqariladi va Rydberg o‘zaro ta’sirlari modellashtirish uchun ishlatiladi. Amazon Braket orqali undan masofadan foydalanish mumkin. Qiskit va boshqa dasturiy muhitlarda kvant sxemalari avval klassik simulyatsiyada tekshirilib, so‘ng mavjud apparatlarda sinab ko‘riladi [9].

Shundan kelib chiqib kvant texnologiyalarini rivojlantirish bo‘yicha xorijiy davlatlar tajribalari o‘rganildi. Jumladan,

Rossiyada kvant hisoblash davlat yo‘l xaritasi, tadqiqot institutlari va sanoat korxonalari hamkorligida rivojlantirilmoqda. “Rosatom” koordinatsiyasida ion, neytral atom, supero‘tkazuvchan va fotonik platformalarda protsessorlar yaratilmoqda. Korporatsiyaning 2024-yilgi hisobotida ion va neytral atomlarga asoslangan ikkita 50 kubitli prototip ishlab chiqilgani qayd etilgan. Keyingi bosqichda dasturiy algoritmlar, bulutli hisoblash va ishlab chiqarishda foydalanishni kengaytirish vazifalari ko‘zda tutilgan. Mazkur tajriba kvant apparati, dasturiy ta’minot va kadrlar tayyorlashni birgalikda olib borishga asoslangan [10]. Kvant loyihalarining rivojlanishi faqat apparatning kubitlari soni bilan emas, yaratilgan algoritmlarning amaliy natijasi, foydalanuvchilar uchun ochiq xizmatlar va ilmiy mutaxassislar tayyorlash ko‘rsatkichlari bilan ham baholanmoqda. Shu bois sanoat buyurtmalariga mos sinov vazifalarini tanlash muhim o‘rin tutadi.

AQShda 2018-yildagi National Quantum Initiative Act ilmiy-tadqiqot ishlarini davlat idoralari, milliy laboratoriyalar, universitetlar va kompaniyalar o‘rtasida muvofiqlashtirishga asos bo‘ladi. NSF fundamental tadqiqot va ta’lim, DOE yirik ilmiy laboratoriyalar, NIST metrologiya va standartlarga e’tibor qaratadi. Asosiy ilmiy yo‘nalishlari – kvant hisoblash, sensorika va metrologiya, kvant tarmoqlari, simulyatsiya, kvant materiallari, entanglement va kvant xatolarini kamaytirishlaran iborat. 2024-yilda NIST ML-KEM, ML-DSA va SLH-DSA postkvant kriptografik standartlarini tasdiqladi. Bu davlat tajribasi fundamental ilm-fan bilan bir qatorda muhandislik, standartlashtirish, kadrlar va tijoratlashtirishga izchil e’tibor berish zarurligini ko‘rsatdi [11, 12]. Ilmiy markazlarda olib boriladigan fundamental izlanishlar xususiy korxonalarning muhandislik ishlanmalari bilan bog‘langan. Shu bilan birga, ta’lim dasturlari kvant fizikasi, dasturlash va elektronika sohasidagi mutaxassislarni birlashtirishga xizmat qilmoqda.

Xitoyda kvant kommunikatsiyasi va hisoblash uzoq muddatli milliy ilmiy-texnologik dasturlar orqali rivojlantirildi. Universitetlar, milliy laboratoriyalar va kompaniyalar kvant protsessorlari, optik aloqa tarmoqlari, sun’iy yo‘ldosh aloqasi hamda yuqori aniqlikdagi o‘lchash bo‘yicha hamkorlik qilmoqda. 2025-yilda Xitoy va Janubiy Afrika orasida taxminan 12 900 km masofaga kvant kalitini uzatishga oid mikrosun’iy yo‘ldosh tajribasi ilmiy matbuotda e’lon qilindi. Ushbu natija fundamental izlanishlarni katta infratuzilma va amaliy sinovlar bilan bog‘lash mumkinligini namoyon etdi [13]. Sun’iy yo‘ldosh orqali kvant aloqa tajribalari yuqori aniqlikdagi optik uskunalar, yerusti qabul stansiyalari va murakkab muvofiqlashtirish tizimlarini talab qiladi. Shu sababli bunday loyihalar uzoq muddatli rejalashtirish va ko‘p tarmoqli ilmiy hamkorlik misoli hisoblanadi.

Yevropada Quantum Technologies Flagship, EuroHPC va EuroQCI tashabbuslari ilmiy tadqiqotlar, yuqori unumli hisoblash va xavfsiz aloqa infratuzilmasini birlashtirmoqda. Yevropa Komissiyasi 2025-yil iyulida Quantum Europe Strategy hujjatini qabul qilib, tadqiqot va innovatsiyalar, umumiy infratuzilma, startaplar, kosmik yechimlar hamda kvant ko‘nikmalarini beshta ustuvor yo‘nalish sifatida belgiladi. Yondashuv universitetlar, biznes va davlatlarning resurslarini muvofiqlashtirishga, laboratoriya ishlanmalarini sanoat mahsulotlariga aylantirishga qaratilgan [14]. Strategiyaning alohida jihati shundaki, unda kadrlar tayyorlash, umumiy tajriba infratuzilmasi va texnologiyani bozorga olib chiqish yagona jarayon sifatida ko‘rilgan. Natijada kichik ilmiy guruhlar ham mintaqaviy hamkorlik doirasida resurslardan foydalanishi mumkin.

Belarus kvant sohasi uchun zarur texnologik salohiyatni fotonika, mikroelektronika, sensorika va optik tizimlar bilan bog‘lab rivojlantirmoqda. Prezidentning 2025-yil 1-apreldagi 135-son farmoni bilan 2026–2030-yillar uchun fan va innovatsiyaning ustuvor yo‘nalishlari belgilangan bo‘lib, ular orasida fotonika, mikroelektronika, sensorika va axborot xavfsizligi ham mavjud. Ilmiy institutlar lazerlar, optik elementlar hamda maxsus o‘lchash qurilmalari bo‘yicha ishlarni davom ettirmoqda. Bu model mavjud laboratoriyalar va komponentlar bazasidan foydalanishga tayanadi [15]. Bu yondashuv nisbatan kichik ilmiy hamjamiyat sharoitida mavjud uskunalar, muhandislik bilimlari va ta’lim bazasini yangi yo‘nalishga yo‘naltirish imkonini beradi. Kvant texnologiyalarining sensorika va fotonika bilan bog‘liq qismi uchun mazkur model muhimdir.

Qozog‘istonda kvant texnologiyalari bo‘yicha kadrlar tayyorlash, ta’lim laboratoriyalari va dasturiy tadqiqotlarga e’tibor kuchaymoqda. Al-Farobiy nomidagi Qozog‘iston Milliy universitetida tashkil etilgan Quantum AI laboratoriyasi kvant hisoblash bilan sun’iy intellekt yo‘nalishidagi o‘quv va ilmiy ishlarga xizmat qilmoqda. Xitoyning SpinQ kompaniyasi ishlab chiqargan yettita Gemini Mini Pro kvant kompyuteri (har biri 2 kubitli) o‘rnatilgan. SpinQ ishlab

chiqargan kichik kubitli qurilmalar ta’lim jarayonida real kvant amallarini ko‘rsatish imkonini beradi. Ushbu tajriba qimmat sanoat apparatlarini birdan sotib olmasdan, dastlab mutaxassislar va o‘quv-tajriba bazasini shakllantirishning amaliy yo‘lini ko‘rsatdi [16]. Dastlabki laboratoriya tajribalari kvant sxemalarini amalda tushunish, talabalarning muhandislik ko‘nikmalarini mustahkamlash va keyinchalik murakkabroq ilmiy loyihalarga o‘tish uchun tayanch vazifasini bajaradi. Bu ayniqsa yangi shakllanayotgan ilmiy guruhlar uchun foydali.

Xulosa.

1. Xorijiy tajriba kvant texnologiyalarini rivojlantirish uchun faqat laboratoriya yoki kvant kompyuterini yaratish yetarli emasligini ko‘rsatadi. Buning uchun kadrlar tayyorlash, fundamental va amaliy tadqiqotlar, umumiy foydalanishdagi infratuzilma, muhandislik ishlanmalari, standartlashtirish hamda sanoat buyurtmalarini birlashtiruvchi tizimni o‘z ichiga olgan tegishli hukumat qarori loyihasini ishlab chiqish zarur.

2. O‘zbekiston uchun eng maqbul yondashuv – mavjud kriptologiya, fizika, matematika va axborot texnologiyalari salohiyatini birlashtirib, bosqichma-bosqich milliy kvant kompetensiyasini shakllantirish hisoblanadi.

3. Dastlab postkvant kriptografiyasi, kvant dasturlash, sensorika va fotonikaning tanlangan yo‘nalishlariga e’tibor qaratish. Keyinchalik sinovdan o‘tgan ishlanmalarni mahsulot va xizmatlarga aylantirish maqsadga muvofiq.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentining PQ–390-son qarori, 27.12.2025.
2. O‘zbekiston Respublikasi Prezidentining PF–38-son Farmoni, 10.03.2026.
3. IBM Quantum. Hardware and quantum processors.
4. Quantinuum. System Model H2 – technical documentation.
5. ID Quantique. Clavis XG QKD Portfolio.
6. Toshiba. Multiplexed QKD System MU.
7. ID Quantique. Quantis QRNG PCIe.
8. Exail. Quantum gravity sensing and Absolute Quantum Gravimeter.
9. Amazon Web Services. Amazon Braket – QuEra Aquila documentation.
10. Rosatom. Annual Report 2024, “Quantum Computing” bo‘limi.
11. National Quantum Initiative. Legislation (NQI Act, 2018).
12. NIST. Post-Quantum Cryptography Standards, FIPS 203–205 (2024).
13. Gibney E. Mini-satellite paves the way for quantum messaging anywhere on Earth. Nature, 2025.
14. European Commission. Quantum Europe Strategy (2025).
15. Belarus Respublikasi Prezidentining 135-son farmoni, 01.04.2025.
16. Al-Farabi Kazakh National University. Quantum AI Laboratory, 2026.

BULUTLI HISOBLASH TIZIMLARI TAHLILI VA O‘ZBEKISTON SHAROITIDA QO‘LLASH ISTIQBOLLARI

Kuryazov D.M., Jumaboyev I.N.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Maqolada bulut texnologiyalarining arxitekturaviy asoslari, xizmat ko‘rsatish va taqsimlash modellari, Amazon Web Services, Google Cloud Platform va IBM Cloud kabi yetakchi bulut provayderlarining kriptografik arxitekturalari qiyosiy tahlil qilingan. Kvant hisoblash hujumlariga bardoshli post-kvant kriptografiyasining asosi bo‘lgan Gomomorf shifrlash algoritmlari matematik asoslari o‘rganilgan hamda «Raqamli O‘zbekiston - 2030» strategiyasi va kiberxavfsizlik qonunchiligi doirasida O‘zbekiston Respublikasida bulut tizimlarini joriy etishdagi kriptografik talablar bo‘yicha takliflar keltirilgan.

Kalit so‘zlar: bulutli hisoblash, IaaS, PaaS, SaaS, Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud, gomomorf shifrlash, bulut xavfsizligi, IBM Cloud, AWS, Google Cloud.

Аннотация. В статье проведён сравнительный анализ архитектурных основ облачных технологий, моделей обслуживания и развертывания, а также криптографических архитектур ведущих облачных провайдеров, таких как Amazon Web Services, Google Cloud Platform и IBM Cloud. Исследованы математические основы алгоритмов гомоморфного шифрования, выступающих базисом постквантовой криптографии, устойчивой к атакам квантовых вычислений, а также представлены рекомендации по криптографическим требованиям к внедрению облачных систем в Республике Узбекистан в рамках стратегии «Цифровой Узбекистан - 2030» и законодательства в сфере кибербезопасности.

Ключевые слова: облачные вычисления, IaaS, PaaS, SaaS, Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud, гомоморфное шифрование, облачная безопасность, IBM Cloud, AWS, Google Cloud.

Kirish

Bugungi kunda raqamli transformatsiya jarayonlarining jadallashuvi, «Katta ma’lumotlar» (Big Data) hajmining eksponensial o‘sishi, buyumlar interneti (IoT) hamda sun’iy intellekt (AI) texnologiyalarining amaliyotga keng joriy etilishi natijasida axborot tizimlari taraqqiyotining yangi paradigmasi - Bulutli hisoblash (Cloud Computing) texnologiyalari vujudga keldi. O‘zbekiston Respublikasida raqamli iqtisodiyotni rivojlantirish jarayonida bulutli texnologiyalardan foydalanish davlat siyosatining ustuvor yo‘nalishlaridan biriga aylandi. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-sonli Farmoni mamlakatda barcha davlat xizmatlari va korporativ boshqaruv tizimlarini bulutli platformalarga o‘tkazish uchun poydevor yaratdi[1]. «Kiberxavfsizlik to‘g‘risida»gi qonun (2022-yil, O‘RQ-764-son) esa bulutli hisoblash tizimlaridagi muhim axborot infratuzilmasi ob’ektlarini himoya qilishni tartibga soladi[2]. O‘zbekiston Respublikasi Prezidentining 2024-yil 15-avgustdagi «Kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish to‘g‘risida»gi PQ-293 sonli qarorida bulut texnologiyalari uchun shifrlash algoritmlarini yaratish va kriptologiya sohasida ilm-fanni rivojlantirish vazifasi belgilangan [3]. Ushbu qonuniy hujjat mavzuning dolzarbligini belgilaydi.

Asosiy qism

Bulutli texnologiyalarning amaliyotda keng ko‘lamda qo‘llanilishi ularning bir qator o‘ziga xos noyob xususiyatlari bilan asoslanadi. Birinchidan, elastiklik va tezkor masshtablanuvchanlik

- tizim yuklamasi keskin ortgan holatlarda bulutli arxitektura avtomatik ravishda qo‘shimcha server resurslarini ajratadi. Ikkinchidan, global mavjudlik - tarmoqqa ulangan har qanday qurilma orqali, dunyoning istalgan nuqtasidan to‘laqonli kirish imkoniyati. Uchinchidan, ma’lumotlarning zaxiraviy nusxalanishi va falokatlardan tiklanish jarayonlarining yuqori darajada avtomatlashtirilganlik holatlari mavjud. AQSh Milliy standartlar va texnologiyalar instituti (NIST) tomonidan berilgan ta’rifga ko‘ra: «Bulutli hisoblashlar – bu minimal boshqaruv harakati bilan tezkorlik taqdim etiladigan sozlangan hisoblash resurslarining umumiy hovuziga foydalanuvchining talabiga binoan, qulay va har joydan tarmoq orqali kirishini ta’minlaydigan modeldir» [14].

Bulutli hisoblashlar modeli quyidagi asosiy 5 ta xususiyatdan iborat:

1. Talabga binoan o‘z-o‘ziga xizmat ko‘rsatish: Iste’molchi provayder bilan bevosita muloqot qilmasdan, avtomatik tarzda server quvvati yoki tarmoq xotirasini boshqara oladi.

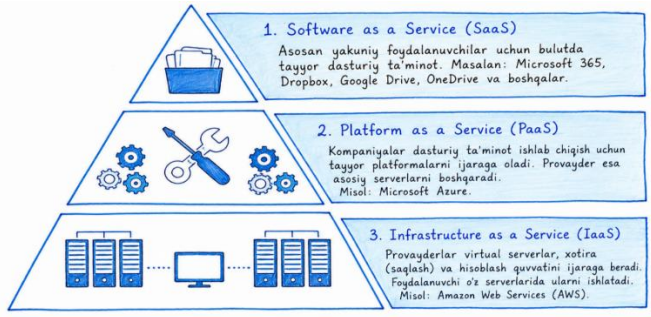
2. Keng tarmoq orqali kirish: Xizmatlar internet orqali standart platformalar (mobil qurilmalar, noutbooklar, ish stansiyalari) uchun ochiq bo‘lishi lozim.

3. Resurslarni birlashtirish: Provayder resurslari bitta umumiy hovuzga birlashtiriladi va turli foydalanuvchilarga ehtiyojga qarab dinamik ravishda taqsimlanadi.

4. Tezkor moslashuvchanlik: Resurslarni talabga qarab bir necha soniya ichida kengaytirish yoki qisqartirish imkoniyati.

5. O‘lchanuvchi xizmat: Foydalanilgan resurslar miqdori (traffik, xotira hajmi, CPU vaqti) aniq hisoblab boriladi va foydalanuvchi shunga qarab haq to‘laydi.

Xizmat ko‘rsatish modellari. Bulutli hisoblashlar xizmat ko‘rsatish turiga ko‘ra uch asosiy qatlamga bo‘linadi: SaaS, PaaS va IaaS. Bu modellar provayder va iste’molchi o‘rtasidagi mas’uliyat taqsimotini belgilab beradi [5].



1-rasm. Bulutning uch asosiy modeli: SaaS, PaaS, IaaS (NIST SP 800 -145).

SaaS (Software as a Service). Tayyor dasturiy ta’minot internet orqali ishlatiladi. Foydalanuvchi hech qanday dasturni o‘z kompyuteriga o‘rnatmaydi barcha jarayonlar provayder serverida bajariladi. SaaS ko‘p ijarachilik arxitekturasiga asoslangan. Misollar: Google Drive, Microsoft 365, Salesforce.

PaaS (Platform as a Service). Dasturchilar uchun ilovalar yaratish va ishga tushirish muhiti taqdim etiladi. Foydalanuvchi operatsion tizim va server sozlamalari haqida qayg‘urmaydi. Misollar: Google App Engine, Heroku, AWS.

IaaS (Infrastructure as a Service). Foydalanuvchiga virtual serverlar va tarmoq resurslari ijaraga beriladi. Misollar: Amazon EC2, Google Compute Engine, Microsoft Azure VM.

Xalqaro NIST (AQSh Milliy standartlar va texnologiyalar instituti) tasnifiga ko‘ra, infratuzilmaning joylashuvi, unga egalik qilish huquqi va xavfsizlik darajasiga qarab bulutli tizimlar 4 ta asosiy joylashtirish modeliga bo‘linadi:

Xususiy bulut (Private Cloud) faqat bitta tashkilot foydalanishi uchun yaratiladi. Maxfiylik darajasi juda yuqori bo‘lib, asosan banklar va davlat idoralari uchun tavsiya etiladi.

Jamoaviy bulut (Community Cloud) umumiy manfaatlarga ega bo‘lgan bir nechta tashkilot uchun mo‘ljallangan infratuzilmalar hisoblanadi.

Ommaviy bulut (Public Cloud) resurslar internet orqali barcha uchun ochiq bo‘ladi. Bu eng arzon, lekin xavfsizlik nuqtai nazaridan eng ko‘p savollar tug‘diradigan modeldir.

Gibrid bulut (Hybrid Cloud) ommaviy va xususiy bulutlarning kombinatsiyasi. Tashkilot o‘zining o‘ta maxfiy ma’lumotlarini xususiy bulutda saqlaydi, lekin yuklamani ko‘tarish uchun ommaviy bulut resurslaridan ham foydalanadi [13]. Ushbu malu’motlar asosida quyidagi Cloud texnologiyalari o‘rganilgan va tahlil qilingan.

Zamonaviy bulut texnologiyalarining tavsifi (IBM, Amazon, Google Cloud)

IBM Cloud: Korporativ Gibrid Bulutlar. IBM ning Confidential Computing texnologiyasi apparat darajasida xotirani shifrlash va Secure Enclaves yaratish orqali ma’lumotlarni nafaqat saqlashda, balki bevosita hisoblash jarayonida ham himoya qiladi. Hyper Protect Crypto Services xizmatida shifrlash kalitlari FIPS 140-2 Level 4 sertifikatiga ega HSM (Hardware Security Module) - Apparat xavfsizlik modullarida saqlanadi [16].

Amazon Web Services (AWS): AWS tizimi geografik jihatdan ajratilgan Regions va Availability Zones tizimidan iborat. AWS Nitro System arxitekturasi foydalanuvchiga jismoniy server quvvatidan deyarli 100% unumdorlik bilan foydalanish imkoniyatini beradi. S3 *(Simple Storage Service - obyektli saqlash xizmati)* ma’lumotlarning saqlanish ishonchliligini 99.999999999% (11 to‘qqizlik) darajasida kafolatlaydi [15].

Google Cloud Platform: Googlening Colossus fayl tizimida ma’lumotlar Reed-Solomon xatoliklarni to‘g‘irlash kodlari yordamida segmentlarga bo‘linib, global serverlar bo‘ylab tarqatiladi. Cloud Spanner TrueTime API texnologiyasidan foydalanadi [17].

1-jadval

Yetakchi bulut provayderlarining qiyosiy tahlili

Platforma	Asosiy Infratuzilma	Xavfsizlik Standarti	Shifrlash usuli
AWS	Nitro System, S3	FIPS 140-2 Level 2/3	Envelope Encryption
Google Cloud	Borg, Colossus FS	FIPS 140-2 Level 3	CSEK (Mijoz kalitlari)
IBM Cloud	Mainframe, OpenShift	FIPS 140-2 Level 4	KYOK (O‘z kaliting)

Bulutli tizimlarda shifrlash algoritmlari va kriptografik himoya usullari

NIST konseptual modeliga ko‘ra, bulut tizimlarida ma’lumotlar xavfsizligi apparat (Hardware), tranzit (In-Transit) va saqlash (At-Rest) qatlamlarining o‘zaro kriptografik bog‘liqligi orqali ta’minlanadi. Bulutli muhitda saqlanayotgan (At-Rest) statik ma’lumotlarni himoya qilish uchun simmetrik shifrlashning AES-256 standarti qo‘llaniladi.

2-jadval

Kriptografik standartlar 3 ta texnologiyada qiyosiy tahlili

Kriptografik element	AWS	IBM Cloud	Google Cloud
At-Rest shifrlash	AES-256-GCM	AES-256-GCM	AES-256
Tranzit shifrlash	TLS 1.2/1.3	TLS 1.3, IPSec	TLS 1.3, QUIC
Elektron imzo	RSA, ECDSA (P-256)	RSA, ECDSA, Ed25519	RSA-2048/4096, ECDSA
Xesh funksiyalari	SHA-256, SHA-384	SHA-2, SHA-3	SHA-256

Mazkur kriptografik mexanizmlarni amaliyotga tatbiq etishda yetakchi bulut infratuzilmalari turlicha yondashuvlarni qo‘llaydi. Bugungi kunda oddiy ma’lumot saqlash joyidan murakkab, ko‘p qatlamli va global taqsimlangan ekotizimga aylangan AWS, IBM Cloud va Google Cloud kabi provayderlarning tahlili shuni ko‘rsatadiki, ularning barchasi uchun birlamchi va eng muhim vazifa - ma’lumotlar xavfsizligini ta’minlashdir [15,16,17].

Gomomorf shifrlash - bulutli hisoblashlarning kelajagi

An’anaviy kriptotizimlarning asosiy kamchiligi - bulutda ma’lumotlar ustida matematik amallar bajarish uchun ularni vaqtincha shifrdan ochish majburiyatidir. Gomomorf shifrlash (Fully Homomorphic Encryption - FHE) ma’lumotlarni ochiq matnga aylantirmasdan shifrlangan holatda ularning ustida algoritmik hisob-kitoblar bajarish imkonini beradi[8]:

$$E(m_1) \otimes E(m_2) = E(m_1 \times m_2)$$

Bu yerda: E - Shifrlash funksiyasi (operatori). U ochiq ma’lumotni hech kim o‘qiy olmaydigan maxfiy kodga (shifr matnga) aylantirib beradi.

- $m1$ va $m2$ - Shifrlanishi kerak bo‘lgan dastlabki ochiq xabarlar, raqamlar yoki ma’lumotlar.

- $E(m1)$ - birinchi xabar $(m1)$ ning shifrlangan holati (shifrmatn).

- $\mathrm{E(m2)}$ - ikkinchi xabar $(m2)$ ning shifrlangan holati (shifrmatn).

- $\otimes$ - Shifrlangan matnlar (kriptogrammalar) ustida bajariladigan maxsus matematik amal. Bu amal shifrlangan ma’lumotlarni ochmasdan (deshifrlamasdan) turib ular ustida hisob-kitob qilish imkonini beradi.

- $\times$ (Multiplication) - Oddiy ma’lumotlar o‘rtasidagi an’anaviy ko‘paytirish amali.

Gomomorf shifrlashning asosiy turlari:

1. PHE - (Partially Homomorphic Encryption - *Qisman Gomomorf Shifrlash*): Faqat bitta turdagi amal (qo‘shish yoki ko‘paytirish) bajariladi.

2. SHE - (Somewhat Homomorphic Encryption - *To‘liq bo‘lmagan / Qisman chegaralangan Gomomorf Shifrlash*): Amallar soni ma’lum bir miqdor bilan chegaralangan.

3. FHE - (Fully Homomorphic Encryption - *To‘liq Gomomorf Shifrlash*): Cheksiz va ixtiyoriy amallarni bajarish imkonini beradi.

Stanford universiteti tadqiqotchisi Craig Gentry 2009-yilda FHE ning birinchi amaliy modelini taqdim etgan. FHE bulut texnologiyalari uchun mukammal xavfsizlikni ta’minlasada, uning asosiy muammosi hisoblash jarayonidagi murakkablik va shifrmatnda yig‘ilib boradigan kriptografik ‘‘shovqin’’ hisoblanadi. Bugungi kunda ushbu muammolarni yengillashtirish uchun Microsoft SEAL va IBM HElib kabi ochiq manbali FHE kutubxonalari bulutli tizimlar integratsiyasiga joriy qilinmoqda [7,12].

O‘zbekistonda bulut xavfsizligiga tavsiyalar

1. Bulutli xizmatlardan foydalanuvchi davlat tashkilotlari o‘zlarining shifrlash kalitlarini provayderga topshirmasdan, mustaqil holda boshqarish huquqini o‘zida saqlab qolishi.

2. O‘zbekiston Respublikasi uchun quyidagi kriptografik yechim tavsiya etiladi: HSM (Hardware Security Module) - Apparat xavfsizlik modul qurilmalar orqali kalit boshqaruv tizimining yaratilishi, Zero Trust (Nol Ishonch - bu kiberxavfsizlikdagi inqilobiy falsafa bo‘lib, uning asosiy qoidasi: ‘‘Hech qachon ishonma, doimo tekshir”) - arxitekturasining qabul qilinishi va 2030-yilga qadar post-kvant kriptografiya standartlariga bosqichma-bosqich o‘tish.

3. Oddiy kompyuterlar yuz yilda buzadigan RSA yoki ECC algoritmlarini *Kvant kompyuterlari* bir necha daqiqada buzib tashlashi mumkin.” Hozir o‘g‘irla, keyin ochasan‘‘ degan jumla bilan xakerlar bugungi kunda davlat sirlari va maxfiy ma’lumotlarni shifrlangan holatida o‘g‘irlab, yig‘ib qo‘ymoqda. Ular 2030-yillarda kuchli kvant kompyuterlari ixtiro qilinganda, bu ma’lumotlarni osongina ochib olishni maqsad qilgan bo‘lishlari mumkin. AQShning Milliy Xavfsizlik Agentligi va NIST tashkiloti barcha davlat va bulut tizimlarini 2030-yilgacha kvant hujumiga chidamli bo‘lgan yangi algoritmlarga [ML-KEM (CRYSTALS-Kyber) - FIPS 203, ML-DSA (CRYSTALS-Dilithium) - FIPS 204, SLH-DSA (SPHINCS+) - FIPS 205] o‘tkazishni majburiy qilib belgiladi. O‘zbekiston «Raqamli O‘zbekiston-2030» strategiyasida bulutli

tizimlarni hozirdan PQC(post-kvant kriptografiya) standartlariga moslashtirib borish hamda milliy ma’lumotlar kelajakda xakerlar oldida himoyasiz qolishini olish chora tadbirlarini ko‘rishi kerak.

4. Milliy kriptografik mahsulotlarni joriy etish: Bulut texnologiyalari uchun xavfsiz va to‘liq sertifikatlangan milliy shifrlash algoritmlarini, milliy elektron imzo, xesh hamda kalit generatsiyasi tizimlarini ishlab chiqish va integratsiya qilish.

Xulosa

Bulutli hisoblash texnologiyalari IT infratuzilmasidan tubdan farq qiluvchi yangi arxitekturaviy texnologiyasi hisoblanib IaaS, PaaS va SaaS modellarining ierarxik tuzilishi zamonaviy bulut muhitida xavfsizlikni ta’minlashning murakkabligi va ko‘p qatlamliligini ko‘rsatib kelmoqda. IBM, AWS va Google Cloud ning qiyosiy tahlili shuni ko‘rsatadiki, IBM FIPS 140-2 Level-4 sertifikati bilan eng yuqori xavfsizlik darajasini ta’minlasa, AWS Nitro System arxitekturasi eng yuqori unumdorlikni, Google Cloud esa eng tez kriptografik operatsiyalarni ta’minlaydi. Bugungi kunda gigant bulut provayderlari kelajak texnologiyasini baholash va xavfsizlikni inobatga olgan holda Gomomorf shifrlash bulutli hisoblashlar xavfsizligidagi inqilobiy texnologiyasi deb hisoblashadi. U ma’lumotlarni ochmasdan qayta ishlash imkonini berish bilan birga, kvant kompyuterlari hujumidan ham himoyalangan ekanligini keltirib chiqardi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi Prezidentining «Raqamli O‘zbekiston-2030» strategiyasini tasdiqlash to‘g‘risida: 05.10.2020y № PF-6079-sonli Farmoni.
2. O‘zbekiston Respublikasi «Kiberxavfsizlik to‘g‘risida»gi Qonuni, 15.04.2022y № O‘RQ-764-son.
3. O‘zbekiston Respublikasi Prezidentining «Kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish to‘g‘risida»gi Qarori: 15.08.2024y № PQ-293-son.
4. Mell P., Grance T. The NIST Definition of Cloud Computing // NIST SP 800-145. – Gaithersburg, 2011.
5. Hogan M., Messina J. NIST Cloud Federation Reference Architecture // NIST SP 500-322. – Gaithersburg, 2018.
6. Liu F. NIST Cloud Computing Reference Architecture. SP 500-292. – Gaithersburg, 2011.
7. Gentry C. A Fully Homomorphic Encryption Scheme. – Stanford University, 2009.
8. NIST. FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA). – NIST, 2024.
9. AWS Security Best Practices. Amazon Web Services Whitepaper. – Seattle, 2023.
10. IBM Cloud Security Architecture. IBM Corporation. – Armonk, 2023.
11. Google Cloud Security Foundations Guide. Google LLC. – Mountain View, 2024.
12. https://homomorphicencryption.org/standard
13. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf
14. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
15. https://aws.amazon.com/security
16. https://www.ibm.com/cloud/security
17. https://cloud.google.com/security

NIST POSTKVANT STANDART ALGORITMLARINI DASTUR VA QURILMALARDA QO‘LLASHDA YON-KANAL HUJUMLARI VA CONSTANT-TIME HIMOYASI

Kuryazov D.M., Mingyasharov N.B.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Maqolada NIST tasdiqlagan FIPS 203, FIPS 204 va FIPS 205 postkvant standart algoritmlarining dasturiy va apparatdagi bajarilishiga oid yon-kanal hujumlari texnik sharhi hamda qiyosiy tahlili ko‘rib chiqilgan. ML-KEM ning avvalgi shakli Kyberning ayrim dasturlaridagi KyberSlash zaifligi maxfiy qiymatga bog‘liq bo‘lish orqali ma’lumot sizdirishi, ML-DSA dagi 2025-yilgi Cortex-M4 tadqiqoti esa rad etilgan imzolashdagi quvvat yon-kanaliga taalluqli ekani ko‘rsatilgan. Constant-time yondashuvi, dudect va BINSEC/Rel vositalari hamda Arm DIT, Intel DOITM va RISC-V Zkt mexanizmlarining imkoniyatlari qiyoslangan. Qiyosiy tahlil asosida tekshirish bosqichlari va O‘zbekiston axborot tizimlarini postkvant kriptografiyasiga tayyorlash tavsiyalari berilgan.

Kalit so‘zlar. postkvant kriptografiyasi, NIST, FIPS 203, FIPS 204, FIPS 205, yon-kanal, constant-time, KyberSlash, dudect, BINSEC/Rel.

Аннотация. В статье представлены технический обзор и сравнительный анализ атак по побочным каналам на программные и аппаратные реализации постквантовых криптографических алгоритмов, стандартизованных NIST в FIPS 203, FIPS 204 и FIPS 205. Показано, что уязвимость KyberSlash в отдельных программных реализациях Kyber – предшественника ML-KEM – приводит к утечке информации вследствие выполнения операции деления с участием секретных значений. Исследование ML-DSA на платформе Cortex-M4, опубликованное в 2025 году, рассматривает утечку через энергопотребление при обработке отклонённых попыток формирования подписи. Сопоставлены возможности подхода constant-time, инструментов dudect и BINSEC/Rel, а также механизмов Arm DIT, Intel DOITM и RISC-V Zkt. На основе сравнительного анализа предложены этапы проверки реализаций и рекомендации по подготовке информационных систем Узбекистана к переходу на постквантовую криптографию.

Ключевые слова. постквантовая криптография, NIST, FIPS 203, FIPS 204, FIPS 205, побочный канал, constant-time, KyberSlash, dudect, BINSEC/Rel.

Kirish

RSA, Diffie-Hellman va elliptik egri chiziqlarga asoslangan klassik tizimlar, kriptografik masalalarni yechishga yetarli quvvatli kvant kompyuteri yaratilgan taqdirda Shor algoritmi sababli xavfsizligini yo‘qotadi. Ushbu tahdidga javoban AQSh Milliy standartlar va texnologiyalar instituti (NIST) 2024-yil avgustida dastlabki uchta postkvant Federal axborotni qayta ishlash standartini e’lon qilgan: FIPS 203 dagi ML-KEM ikki tomon uchun umumiy maxfiy kalit hosil qilish mexanizmi, FIPS 204 dagi ML-DSA raqamli imzosi hamda FIPS 205 dagi SLH-DSA xeshga (ma’lumotdan belgilangan uzunlikdagi qiymat hisoblashga) asoslangan raqamli imzo standarti [1–3]. FIPS 203 sahifasidagi kelgusi tuzatishlar haqidagi eslatma dasturlarni hujjatning amaldagi holatiga mos tekshirish zarurligini ko‘rsatgan [4].

Biroq kriptografik algoritmning matematik modeldagi mustahkamligi uning dasturiy yoki apparatdagi bajarilishi xavfsizligini kafolatlamaydi. Bajarilish vaqti, kesh (protsessorning kichik va tez xotirasi) holati, quvvat sarfi yoki elektromagnit nurlanish orqali ma’lumot sizishi mumkin.

Bunday qo‘shimcha kuzatuv yo‘llari yon-kanal deyiladi [3, 5]. Constant-time yondashuvida algoritmning bajarilish vaqti maxfiy kalit yoki boshqa maxfiy ma’lumotlarning qiymatiga bog‘liq bo‘lmasligi kerak. Bu har bir hisob mutlaqo bir xil vaqt olishini anglatmaydi. Maxfiy qiymat shartli sakrashni (shartga qarab boshqa buyruqqa o‘tish), siklning takrorlanish sonini, xotira manzilini yoki amal davomiyligini belgilamasligi lozim. Ochiq, ya’ni sir saqlanishi talab qilinmaydigan ma’lumotga bog‘liq o‘zgarish esa o‘z-o‘zidan bu talabni buzmaydi [6].

Tahlil usuli. NIST standartlari, ilmiy maqolalar va vositalarning rasmiy hujjatlari hujumchining imkoniyati, kuzatiladigan signal, tajriba qurilmasi, himoya chorasi va tekshiruv chegarasi bo‘yicha qiyoslangan.

Hujumchining imkoniyatlari va protsessor orqali ma’lumot sizishi

Yon-kanal xavfsizligini to‘g‘ri baholash uchun hujumchining kuzatish va ta’sir qilish imkoniyatlari quyidagi kuzatuv sharoitlari va faol hujum turi orqali ko‘rib chiqiladi:

1. Masofaviy vaqt kanali – hujumchi tarmoq orqali so‘rov yuborib, javob kelish vaqtidagi farqlarni statistik tahlil qiladi. Brumley va Boneh OpenSSL serveriga mahalliy tarmoq orqali vaqt hujumini amalda ko‘rsatgan [7].
2. Mahalliy protsessor kanali – bir qurilmada ishlayotgan boshqa dastur protsessordagi kichik va tez xotira (kesh) yoki shartli buyruqlar bajarilishi izlari kuzatiladi.
3. Jismoniy passiv kanal – qurilmaga yaqin masofadan quvvat sarfi va elektromagnit nurlanish o‘lchanadi.
4. Faol nosozlik kiritish hujumi (Fault injection) – kuchlanish, protsessorning vaqt signali yoki lazer yordamida hisoblash jarayoni ataylab buziladi va xatolik javoblari tahlil qilinadi.

Shartli sakrashsiz manba kodi yakuniy mashina kodining doimiy vaqtli bo‘lishini kafolatlamaydi. Dastur matnini mashina buyruqlariga aylantiruvchi vosita (Kompilyator), bit niqobini (0 va 1 bitlar yordamida qiymat tanlashni) shartli sakrashga aylantirishi yoki xotirani tozalashni olib tashlashi mumkin. Yozilgan dastur matni bilan protsessor bajaradigan kod farq qilishi mumkin [8, 9]. Shu bois yakuniy kodni ham tekshirish maqsadga muvofiq.

Postkvant standartlarini dastur va qurilmalarda qo‘llash xatarlari

FIPS 203 va KyberSlash misoli – ML-KEM ko‘phadlar, masalan, $x^2 + 2x + 1$ kabi ifodalar ustidagi qo‘shish va ko‘paytirish hisoblariga tayanadi. Bernstein va hammualliflar Kyberning ayrim dasturlaridagi maxfiy qiymatga bog‘liq bo‘lish vaqtini o‘rgangan. Dastlabki maqola 2024-yilda, jurnal nashri IACRning TCHES jurnalida 2025-yilda chiqqan [10]. KyberSlash1 shifrdan yechish, KyberSlash2 esa shifrlash va siqish hisoblariga tegishli. Ochiq kalit bilan shifrlash bosqichining vaqti ham maxfiy hisob natijasiga bog‘lanishi mumkin [1, 10]. Bu natija barcha ML-KEM dasturlari zaifligini yoki tarmoqda har qanday sharoitda hujum ishlashini bildirmaydi.

Montgomery va Barrett usullari modul bo‘yicha hisoblashlarda qo‘llanadi. Barrett usuli bo‘lish amalini ko‘paytirish va bitlarni siljitish amallari bilan almashtirib, qoldiqni hisoblash imkonini beradi. 1-kod misolida maxfiy qiymatga bog‘liq shartli o‘tishsiz ikkita qiymatdan birini tanlash hamda 3329 moduli bo‘yicha qoldiq hisoblash ko‘rsatilgan. Misoldagi a, b, secret_condition va secret_dividend – manfiy bo‘lmagan 32 bitli butun sonlar; secret_condition va secret_dividend maxfiy qiymatlarni ifodalaydi. Qoldiqni hisoblashda $1290167 = \lfloor 2^{32}/3329 \rfloor$ yordamchi doimiysidan foydalaniladi. Bu yerda $\lfloor \ldots \rfloor$ belgisi sonni pastga qarab eng yaqin butun songacha yaxlitlashni bildiradi. To‘g‘ri hisoblangan qoldiq 0 dan 3328 gacha bo‘ladi. Kod alohida amallarning ishlashini tushuntiruvchi o‘quv misolidir; uning constant-time talabiga muvofiqligi kompilyatsiyadan o‘tgan yakuniy kodda va qurilmada qayta tekshirilishi kerak [6].

Hujumning ishlashi – tadqiqotchilar tanlangan shifrmatnlarni qurilmaga berib, maxfiy kalitga bog‘liq hisoblash vaqtini ko‘p marta o‘lchagan. Vaqt farqi kalitni bevosita ko‘rsatmaydi: ko‘p o‘lchovlar orqali kalitga oid taxminlar tekshirilib, kalit tiklangan. KyberSlash1 Raspberry Pi 2 qurilmasidagi Cortex-A7 protsessorida bir necha soatda, KyberSlash2 esa Cortex-M4 mikrokontrollerida bir necha daqiqada kalitni tiklash imkonini bergan [10]. Muddatlar muayyan zaif dastur, qurilma va o‘lchov sharoitlariga tegishli.

FIPS 204 va imzolashdagi rad etilgan urinishlar. ML-DSA imzolash jarayonida hosil qilingan nomzod imzo belgilangan qabul qilish shartlariga mos kelmasa, u rad etiladi va yangi nomzod imzo yaratish uchun hisoblash takrorlanadi. Bu qabul qilingan imzolarning taqsimoti orqali kalit haqida ma’lumot chiqishini cheklaydi. Urinishlar sonining o‘zgarishi o‘z-o‘zidan kalit haqida ma’lumot sizishini isbotlamaydi. Zhou va boshqalar Cortex-M4 da rad etilgan urinishlarning quvvat sarfi vaqt davomida qanday o‘zgarganini o‘lchab, kalitni tiklash yo‘lini ko‘rsatgan [11]. Natija sinovdan o‘tgan Dilithium dasturiga tegishli. Bitta izdan oraliq ma’lumot olish butun kalitni tiklash bilan teng emas. Jismoniy kuzatuv xavfi bo‘lsa, constant-time bilan birga maskalash ham tekshiriladi: oraliq qiymatlar tasodifiy qismlarga ajratib hisoblanadi. Bu kod misolidagi oddiy bit niqobidan farq qiladi.

FIPS 205 va jismoniy himoya. SLH-DSA – xeshga asoslangan raqamli imzo usuli. U har bir imzodan keyin hisoblagichni yangilab saqlashni talab qilmaydi. Ammo bu quvvat sarfi yoki elektromagnit nurlanish orqali ma’lumot sizishidan himoyalangan degani emas. FIPS 205 da imzoni tasodifiylashtiruvchi metod(PRF) hisobiga yangi tasodifiy qiymat kiritish tavsiya etilgan [3]. Quvvat, elektromagnit kuzatuv va nosozlik xatarlari uchun qo‘shimcha himoya zarur.

1-jadval

Postkvant dasturlaridagi yon-kanal hujumlari va himoya choralari

Algoritm	Dalilga asoslangan xavf	Dalil va manba	Tavsiya etilgan chora
Kyber (ML-KEM asosi)	Maxfiy qiymatga bog‘liq bo‘lish kechikishi	KyberSlash 1 va 2 zaifliklari [10]	Bo‘lishsiz hisoblash; yakuniy kodni tekshirish
FIPS 203 (ML-KEM)	Shifrmatn taqqoslashda erta chiqish	Dasturga bog‘liq umumiy xatar [1, 6]	Barcha baytlarni tekshirish; yakuniy kodni sinash
Dilithium (ML-DSA asosi)	Rad etilgan urinishlardan quvvat sizishi	Cortex-M4 da quvvat o‘lchovi [11]	Constant-time, maskalash va jismoniy sinov
FIPS 205 (SLH-DSA)	PRF hisobida yon-kanal va nosozlik xavfi	Standartdagi dasturiy himoya talablari [3]	Tasodifiylashtirilgan imzolash, kod tekshiruvi va nosozlik himoyasi

Constant-time xususiyatini tekshirish vositalari

Dudect (dastur bajarilish vaqtining maxfiy ma’lumotlarga bog‘liqligini statistik tahlil qilish vositasi) orqali vaqt farqini tekshirish. Dasturga ikki guruhdagi kirish ma’lumotlarini berib, uni ko‘p marta ishga tushiradi va bajarilish vaqtlarini solishtiradi. Shu orqali maxfiy ma’lumot o‘zgarganda ishlash vaqtida sezilarli farq paydo bo‘lishini aniqlashga yordam beradi. Buning uchun Welch t-testining statistik usulidan foydalanadi [12]. Welch t-statistikasi quyidagicha hisoblanadi:

$$t = \frac{X_1 - X_2}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}}$$

bu yerda $\bar{X}_1$, $\bar{X}_2$ – ikki guruhdagi o‘rtacha vaqtlar, s_1^2, s_2^2 – o‘lchangan vaqtlarning tarqoqligini ifodalovchi dispersiyalar, n_1, n_2 – o‘lchovlar soni. Guruhlar teng bo‘lsa, har biri jami N ning yarmiga teng. Test uchun protsessor modeli, kompilyator versiyasi va sozlamalari, kirishlar, o‘lchovlar soni qayd etilgan. Farqni aniqlash chegarasi tanlangan testga bog‘liq. Past |t| shu sinovda farq topilmaganini bildiradi, xavfsizlikni isbotlamaydi [12].

2-jadval

Taqqoslash funksiyalarining ishlash usuli va tekshirilishi

Funksiya	Ishlash usuli	Tekshirish	Talqin
C kutubxonasidagi memcmp	Farqda erta to‘xtashi mumkin	Maxfiy kirishlar bilan vaqt sinovi	Maxfiy ma’lumot uchun xavf tug‘dirishi mumkin
To‘liq taqqoslash (ct_memcmp)	Barcha baytlar tekshiriladi	Yakuniy kod va dudect sinovi	Vaqt xususiyati yakuniy kod va qurilmada tekshirilishi kerak

BINSEC yordamida tayyor kodni tekshirish. BINSEC/Rel kompilyatsiya qilingan kodni ochiq ma’lumotlar bir xil, maxfiy qiymatlar esa turlicha bo‘lgan ikki holatda taqqoslaydi. Maxfiy qiymat dastur qaysi yo‘ldan bajarilishiga yoki xotiraning qaysi joyiga murojaat qilishiga ta’sir qiladimi – shuni tekshiradi [13]. Natija faqat vosita tekshirgan holatlarga tegishli. Eski BINSEC/Rel o‘rniga bu tekshiruv asosiy BINSEC vositasiga ko‘chirilgan [14]. Vosita zaiflikni aniqlashga yordam beradi, uni tuzatish uchun esa dastur kodini o‘zgartirish kerak.

Tavsiya etilgan ketma-ketlik: 1) Maxfiy qiymatga bog‘liq yo‘l va manzillarni tuzatish; 2) Yakuniy kodni tekshirish; 3) dudect sinovi; 4) Jismoniy kuzatuv xavfi bo‘lsa, quvvat va elektromagnit sinovlari.

5. Protsessorda bajarilish vaqtini boshqarish vositalari. Ayrim protsessorlarda hisoblash vaqti qayta ishlanayotgan ma’lumot qiymatiga bog‘liq bo‘lmasligini ta’minlashga yordam beradigan maxsus buyruq va rejimlar mavjud. Biroq ular barcha protsessorlarda qo‘llab-quvvatlanmaydi:

6. Arm DIT – Armv8.4-A arxitekturasida kiritilgan maxsus rejim yoqilganda (PSTATE.DIT=1), ayrim buyruqlarning bajarilish vaqti qayta ishlanayotgan ma’lumot qiymatiga bog‘liq bo‘lmaydi [15]. Biroq bu rejim xotiraga murojaat qilishdagi kesh farqlari yoki quvvat sarfi orqali ma’lumot sizishini bartaraf etmaydi.

RISC-V Zkt – ayrim protsessor buyruqlarining bajarilish vaqti ma’lumot qiymatiga bog‘liq bo‘lmasligini talab qiladigan kengaytma [16]. Bu talab barcha buyruqlarga tegishli emas: xotiraga murojaat qilish va dasturda boshqa buyruqqa o‘tish amallari uning doirasiga kirmaydi.

Intel DOITM – yoqilganda ayrim buyruqlarning bajarilish vaqti ma’lumot qiymatiga bog‘liq bo‘lmasligini ta’minlaydigan rejim [17]. Biroq u xotiraga murojaat qilish, quvvat sarfi yoki harorat orqali ma’lumot sizishini bartaraf etmaydi. Shu sababli dastur kodi ham constant-time talablariga mos yozilishi kerak.

Hujumchi yuborgan baytlarni maxfiy qiymat bilan taqqoslashda dastur birinchi farqda to‘xtasa, vaqt orqali dastlabki nechta bayt mos kelgani haqida ma’lumot chiqishi mumkin. Barcha baytlarni tekshirish shu erta to‘xtashni yo‘qotadi; yakuniy kod va qurilmadagi vaqt xususiyati baribir sinovdan o‘tkaziladi [6]. Bit niqobi qiymat tanlash uchun, maskalash esa maxfiy qiymatlarni tasodifiy qismlar bilan yashirib hisoblash uchun ishlatiladi.

Xulosa

NIST postkvant standartlarining matematik mustahkamligi ularning dasturiy va apparat realizatsiyalari xavfsizligini avtomatik ta’minlay olmaydi.

ML-KEM uchun KyberSlash tajribasi maxfiy bo‘linuvchili amallar masofaviy vaqt

zaifligiga aylanishini isbotlaydi.

ML-DSA da esa rad etilgan urinishlar quvvat yon-kanaliga taalluqli bo‘lib, constant-time bilan birga maskalashni taqozo etadi. dudect va BINSEC/Rel o‘z modeli doirasida tekshiruv bersa-da, barcha kanallarni mutlaq yopmaydi;

Arm DIT, Intel DOITM va RISC-V Zkt kabi apparat mexanizmlari esa dasturiy constant-time o‘rnini bosa olmaydi.

O‘zbekiston axborot tizimlarini postkvant kriptografiyasiga o‘tkazishda yon-kanallar orqali maxfiy ma’lumotlar sizib chiqishini tekshirish tavsiya etiladi.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. DOI: 10.6028/NIST.FIPS.203.

2. National Institute of Standards and Technology. (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. DOI: 10.6028/NIST.FIPS.204.

3. National Institute of Standards and Technology. (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. DOI: 10.6028/NIST.FIPS.205.

4. NIST. (2025). FIPS 203 rasmiy sahifasi, kelgusi tuzatishlar eslatmasi, 17.11.2025. Rasmiy hujjat. Murojaat: 13.10.2026.

5. Kocher, P. C. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO ’96, 104–113. DOI: 10.1007/3-540-68697-5_9.

6. Pornin, T. Constant-Time Crypto. BearSSL. Texnik izoh. Murojaat: 13.10.2026.

7. Brumley, D., va Boneh, D. (2003). Remote Timing Attacks Are Practical. 12th USENIX Security Symposium. Nashriyot sahifasi.

8. D’Silva, V., Payer, M., va Song, D. (2015). The Correctness-Security Gap in Compiler Optimization. IEEE SPW, 73–87. DOI: 10.1109/SPW.2015.33.

9. Balakrishnan, G., va Reps, T. (2010). WYSINWYX: What You See Is Not What You eXecute. ACM TOPLAS, 32(6), 23:1–23:84. DOI: 10.1145/1749608.1749612.

10. Bernstein, D. J., va boshqalar. (2025). KyberSlash: Exploiting secret-dependent division timings in Kyber implementations. TCHES, 2025(2), 209–234. DOI: 10.46586/tches.v2025.i2.209-234.

11. Zhou, Y., Wang, W., Sun, Y., va Yu, Y. (2025). Rejected Signatures’ Challenges Pose New Challenges: Key Recovery of CRYSTALS-Dilithium via Side-Channel Attacks. IACR ePrint 2025/214. Manba.

12. Reparaz, O., Balasch, J., va Verbauwhede, I. (2017). Dude, is my code constant time? DATE, 1697–1702. DOI: 10.23919/DATE.2017.7927267.

13. Daniel, L.-A., Bardin, S., va Rezk, T. (2020). BINSEC/Rel: Efficient Relational Symbolic Execution for Constant-Time at Binary-Level. IEEE S&P, 1021–1038. DOI: 10.1109/SP40000.2020.00074.

14. BINSEC loyihasi. BINSEC/Rel rasmiy kod ombori va qo‘llab-quvvatlash holati. Rasmiy hujjat. Murojaat: 13.10.2026.

15. Arm Limited. Arm Architecture Reference Manual for A-profile architecture. DDI 0487, “Data Independent Timing” va PSTATE.DIT tavsifi. Rasmiy hujjat. Murojaat: 13.10.2026.

16. RISC-V International. (2022). RISC-V Cryptography Extensions Volume I: Scalar & Entropy Source Instructions. v1.0.1, 18.02.2022, 2.13-bo‘lim (Zkt). Rasmiy hujjat. Murojaat: 13.10.2026.

17. Intel Corporation. Data Operand Independent Timing ISA Guidance. Rasmiy hujjat. Murojaat: 13.10.2026.

BULUTLI HISOBLASH TIZIMLARIDA VIRTUAL MASHINA OBRAZLARINI ZERO TRUST VA KRIPTOGRAFIK USULLAR ASOSIDA HIMOYALASH

Karimov A.A., Olimov I.S., Berdiyev H.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda bulutli hisoblash tizimlarida axborot xavfsizligini oshirish uchun virtual mashina obrazlarini Zero Trust tamoyili va kriptografik usullar asosida himoyalash masalalari ko‘rib chiqiladi. Ma’lumotlarni shifrlash, foydalanuvchilarni autentifikatsiya qilish, kriptografik kalitlarni alohida va xavfsiz saqlash hamda virtual mashina obrazlarining yaxlitligini tekshirish usullari yoritiladi. Shuningdek, har bir murojaatni tekshirish va foydalanuvchilarga faqat zarur vakolatlarni berish orqali bulutli infratuzilmadagi xavflarni kamaytirish imkoniyatlari asoslanadi.

Kalit so‘zlar: bulutli hisoblash, Zero Trust, virtual mashina obrazi, kriptografik himoya, AES-256, autentifikatsiya, yaxlitlik, kalitlarni boshqarish.

Аннотация. В тезисе рассматриваются способы повышения информационной безопасности в облачных вычислительных системах на основе принципа Zero Trust и криптографических методов защиты образов виртуальных машин. Описываются шифрование данных, аутентификация пользователей, безопасное хранение криптографических ключей и проверка целостности образов виртуальных машин. Обосновывается возможность снижения рисков за счёт проверки каждого обращения и предоставления пользователям только необходимых прав доступа.

Ключевые слова: облачные вычисления, Zero Trust, образ виртуальной машины, криптографическая защита, AES-256, аутентификация, целостность, управление ключами.

Kirish

Bulutli hisoblash tizimlarida ma’lumotlarni himoyalash va virtual resurslardan xavfsiz foydalanish muhim vazifalardan biri hisoblanadi. Bunda ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash bilan bir qatorda, virtual mashina obrazlarining ishonchliligini tekshirish ham talab etiladi. Virtual mashina obrazining ruxsatsiz o‘zgartirilishi yoki kriptografik kalitlarning himoyasiz saqlanishi bulutli infratuzilmada jiddiy xavflarni yuzaga keltirishi mumkin.

Ushbu muammolarni kamaytirish uchun Zero Trust tamoyili va zamonaviy kriptografik mexanizmlardan birgalikda foydalanish maqsadga muvofiq. Zero Trust yondashuvida hech bir foydalanuvchi yoki qurilmaga faqat uning tarmoqqa ulanganligi sababli avtomatik ishonch bildirilmaydi. Kirish huquqi foydalanuvchining shaxsi, vakolati va murojaat kontekstini tekshirish asosida belgilanadi.

Tezisning maqsadi bulutli hisoblash tizimlarida virtual mashina obrazlarini himoyalash uchun sodda, amaliy va o‘zaro bog‘langan kriptografik hamda tashkiliy mexanizmlarni taklif qilishdan iborat.

Asosiy qism

Bulutli hisoblash tizimlaridagi xavfsizlik muammolarini bartaraf etish uchun bir nechta himoya mexanizmlarini yagona yondashuv asosida qo‘llash lozim.

Birinchidan, foydalanuvchilarni ishonchli autentifikatsiya qilish va ularning vakolatlarini cheklash zarur. Bunda ko‘p faktorli autentifikatsiya (MFA) orqali foydalanuvchi shaxsini qo‘shimcha tekshirish mumkin. Shuningdek, har bir foydalanuvchiga faqat o‘z vazifasini bajarishi

uchun zarur bo‘lgan huquqlar berilishi kerak. Bu vakolatsiz kirish va ortiqcha vakolatlardan noto‘g‘ri foydalanish xavfini kamaytiradi.

Ikkinchidan, virtual mashina obrazlari kriptografik usullar yordamida himoyalanishi lozim. Masalan, AES-256-GCM algoritmidan foydalanish obraz ma’lumotlarining maxfiyligini va shifrlangan ma’lumotlarning yaxlitligini tekshirish imkonini beradi. Bunda shifrlash jarayonida autentifikatsiya tegi hosil qilinadi. Ma’lumotlar ochilishidan oldin ushbu teg tekshiriladi va tekshiruv muvaffaqiyatsiz bo‘lsa, ma’lumot ishonchli deb qabul qilinmaydi.

Uchinchidan, kriptografik kalitlarni shifrlangan ma’lumotlardan alohida boshqarish kerak. Buning uchun ma’lumotlarni shifrlash kaliti (DEK) va ushbu kalitni himoyalash uchun ishlatiladigan kalit (KEK) tushunchalaridan foydalanish mumkin. DEK ma’lumotlarni shifrlaydi, KEK esa DEKni himoyalash uchun qo‘llaniladi. Kalitlarni boshqarish xizmatlari yoki apparat xavfsizlik modullaridan foydalanish kalitlarni saqlash va ulardan foydalanishni nazorat qilishga yordam beradi.

To‘rtinchidan, virtual mashina obrazining yaxlitligi va kelib chiqishini tekshirish muhimdir. Buning uchun obrazning kriptografik xeshi hisoblanadi va uning qiymati ishonchli manbada saqlangan qiymat bilan taqqoslanadi. Bundan tashqari, obrazga tegishli manifestda uning identifikatori, versiyasi, egasi, shifrlash profili va boshqa zarur ma’lumotlar qayd etilishi mumkin. Manifestning raqamli imzo bilan tasdiqlanishi uning kelib chiqishini tekshirish imkonini beradi.

Beshinchidan, Zero Trust tamoyiliga muvofiq, virtual mashina obrazidan foydalanishdan oldin foydalanuvchi vakolati, obrazning yaxlitligi va amaldagi xavfsizlik siyosati tekshirilishi lozim. Ruxsat berish faqat zarur shartlar bajarilganda amalga oshiriladi. Masalan, obrazning raqamli imzosi noto‘g‘ri bo‘lsa yoki foydalanuvchi tegishli vakolatga ega bo‘lmasa, undan foydalanishga ruxsat berilmasligi kerak.

Taklif etilayotgan himoya yondashuvining asosiy mexanizmlari quyidagi 1-jadvalda keltirilgan

1-jadval.

Bulutli hisoblash tizimlarida xavfsizlik muammolarini bartaraf etish usullari va kutiladigan natijalar

Muammo	Taklif etilayotgan yechim	Kutiladigan natija
Ma’lumotlarning oshkor bo‘lishi	AES-256-GCM asosida shifrlash	Maxfiylikni ta’minlash
Vakolatsiz kirish	MFA va vakolatlarni cheklash	Kirishni nazorat qilish
Kriptografik kalitlarning himoyasizligi	DEK va KEKni alohida boshqarish	Kalitlar xavfsizligini oshirish
Virtual mashina obrazining o‘zgartirilishi	Xesh va raqamli imzoni tekshirish	Yaxlitlik va kelib chiqishni nazorat qilish
Foydalanuvchiga ortiqcha ishonch bildirish	Zero Trust siyosati	Har bir murojaatni tekshirish
Xavfsizlik hodisalarini kech aniqlash	Jurnallarni yuritish va monitoring	Shubhali harakatlarni aniqlash

Taklif etilayotgan yondashuvni amaliy jihatdan bulutli platformaning virtual mashinalarni boshqarish xizmatlari va kalitlarni boshqarish mexanizmlari bilan birlashtirish mumkin. Masalan, OpenStack muhitida Glance virtual mashina obrazlarini saqlash va boshqarish, Barbican esa sirlar va kriptografik kalitlarni boshqarish uchun qo‘llaniladi. Bunday muhitda obrazni yuklash, saqlash va undan foydalanish jarayonlariga xavfsizlik siyosatini tatbiq etish mumkin.

Tadqiqot usuli sifatida muammolar va himoya mexanizmlarini taqqoslash, mavjud xavflarni guruhlash hamda taklif etilayotgan yondashuvning funksional imkoniyatlarini tahlil qilishdan foydalanildi. Tahlil shuni ko‘rsatadiki, shifrlash, kalitlarni boshqarish, obraz yaxlitligini tekshirish va kirish nazoratini birgalikda qo‘llash alohida mexanizmlardan foydalanishga nisbatan kengroq himoya imkoniyatlarini yaratadi. Biroq yechimning amaliy samaradorligi alohida sinovlar va xavfsizlik ko‘rsatkichlarini o‘lchash orqali qo‘shimcha baholanishi kerak.

Xulosa

Bulutli hisoblash tizimlarida virtual mashina obrazlarini himoyalash uchun Zero Trust tamoyili va kriptografik mexanizmlarni birgalikda qo‘llash maqsadga muvofiq. Ma’lumotlarni AES-256-GCM yordamida shifrlash, kalitlarni alohida boshqarish, obrazlarning xeshi va raqamli imzosini tekshirish hamda foydalanuvchilarning vakolatlarini nazorat qilish xavfsizlikni oshirishga xizmat qiladi.

Taklif etilgan yondashuv virtual mashina obrazlarining maxfiyligi, yaxlitligi va ishonchliligini ta’minlashga qaratilgan. Kelgusida ushbu yondashuvni bulutli platformada tajriba tariqasida amalga oshirish, obrazni yuklash va tekshirish vaqti, resurs sarfi hamda xavfsizlik tekshiruvlarining samaradorligini baholash orqali takomillashtirish mumkin.

Foydalanilgan adabiyotlar

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207, 2020.

2. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.

3. Barker E. Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1.

4. OpenInfra Foundation. OpenStack Glance Documentation va OpenStack Barbican Documentation.

SHIFRLANGAN TARMOQ TRAFIGIDA ZARARLI FAOLLIKNI DESHIFRLASHSIZ ANIQLASHDA SUN'IY INTELLEKT ALGORITMLARINI QO'LLASH

Tashev K.A., Maxmudov A.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada TLS 1.3 va QUIC protokollari bilan shifrlangan tarmoq trafigida zararli faollikni trafik mazmunini deshifrlamasdan aniqlash masalasi ko'rib chiqilgan. Paket, oqim va TLS handshake darajalarida olinadigan metama'lumotlarga asoslangan uch darajali tahlil usuli taklif etilgan. Usulning mohiyati zararli dasturning boshqaruv serveriga davriy murojaati misolida tushuntirilgan. To'rtta mashinali o'qitish algoritmi eksperimental solishtirilgan. Gradiyentli kuchaytirish modeli 92,9 % F1 ko'rsatkichiga erishgan. Oqim xususiyatlariga TLS metama'lumotlarini qo'shish F1 ko'rsatkichini 1,8 foiz punktga oshirgan.

Kalit so'zlar: shifrlangan trafik, TLS 1.3, QUIC, sun'iy intellekt, mashinali o'qitish, metama'lumotlar, JA4, beaconing, gradiyentli kuchaytirish, kriptologiya.

Аннотация: В статье рассматривается задача выявления вредоносной активности в сетевом трафике, зашифрованном протоколами TLS 1.3 и QUIC, без расшифрования его содержимого. Предложен способ трёхуровневого анализа на основе метаданных, извлекаемых на уровнях пакета, потока и TLS-рукопожатия. Суть способа пояснена на примере периодических обращений вредоносной программы к управляющему серверу. Экспериментально сопоставлены четыре алгоритма машинного обучения. Модель градиентного бустинга достигла показателя F1, равного 92,9 %. Добавление метаданных TLS к признакам потока повысило F1 на 1,8 процентного пункта.

Ключевые слова: зашифрованный трафик, TLS 1.3, QUIC, искусственный интеллект, машинное обучение, метаданные, JA4, beaconing, градиентный бустинг, криптология.

Bugungi kunda internet trafigining asosiy qismi shifrlangan holda uzatiladi. TLS 1.3 va QUIC [3] protokollari foydalanuvchi ma'lumotlarining maxfiyligini ishonchli himoya qiladi, biroq xuddi shu imkoniyatdan buzg'unchilar ham foydalanmoqda. Zararli dasturlar boshqaruv serveri (C2) bilan aloqani, o'g'irlangan ma'lumotlarni tashqariga chiqarishni va yangi modullarni yuklab olishni shifrlangan kanal orqali amalga oshiradi [1]. Natijada paket mazmunini imzolar bo'yicha tekshiruvchi an'anaviy hujumlarni aniqlash tizimlari bunday faollikni ko'ra olmaydi.

Muammoni hal qilishning bir yo'li - trafikni oraliq qurilmada deshifrlab tekshirish (TLS inspection). Lekin bu yondashuv shifrlashning "uchdan-uchgacha" tamoyilini buzadi, qo'shimcha hisoblash resurslarini talab qiladi, shaxsga doir ma'lumotlarni himoya qilish nuqtai nazaridan xavf tug'diradi va sertifikat mahkamlangan (certificate pinning) ilovalarda umuman ishlamaydi [4]. "Kiberxavfsizlik to'g'risida"gi Qonun ham axborot tizimlarini himoya qilishda ma'lumotlar maxfiyligini ta'minlashni talab etadi [2]. Shu sababli trafikni deshifrlamasdan, faqat uning tashqi belgilari asosida tahlil qilish dolzarb vazifaga aylandi. Ushbu maqolaning maqsadi - shifrlangan trafik metama'lumotlariga asoslangan sun'iy intellekt usulini ishlab chiqish va uning samaradorligini eksperimental baholashdan iborat.

Shifrlangan trafikning ochiq belgilari. Shifrlash paket ichidagi ma'lumotni yashiradi, ammo trafikning "shaklini" yashirmaydi. Paketlarning o'lchami, yo'nalishi va yuborilish vaqti, ulanish davomiyligi, uzatilgan baytlar hajmi hamda TLS ulanishini o'rnatish (handshake)

bosqichida ochiq uzatiladigan parametrlar har bir ilovaning o‘ziga xos xatti-harakatini aks ettiradi [4, 5]. Mashinali o‘qitish algoritmlari aynan shu belgilar orasidagi qonuniyatlarni o‘rganib, normal va zararli trafikni farqlay oladi [6, 7]. Taklif etilayotgan usulda metama’lumotlar uch darajada olinadi (1-jadval).

1-jadval

Shifrlangan trafikdan deshifrlashsiz olinadigan xususiyatlar

Daraja	Xususiyatlar	Zararli faollikda nimani ko‘rsatadi
1. Paket darajasi	Paketning o‘rtacha o‘lchami va o‘rtacha kvadratik chetlanishi, paketlar soni	C2 buyruqlari kichik va bir xil o‘lchamli paketlar bilan uzatiladi
2. Oqim darajasi	Oqim davomiyligi, paketlar orasidagi interval, intervallarning variatsiya koeffitsiyenti, yuborilgan/qabul qilingan baytlar nisbati	Davriy murojaat (beaconing), ma’lumotlarni tashqariga chiqarish (yuklash hajmining keskin oshishi)
3. TLS handshake darajasi	JA4 mijoz izi [8], TLS kengaytmalari soni, SNI nomining entropiyasi, sertifikatning amal qilish muddati va o‘z-o‘zidan imzolanganligi	Brauzerlarga xos bo‘lmagan TLS kutubxonalari, avtomatik yaratilgan domen nomlari, soxta sertifikatlar

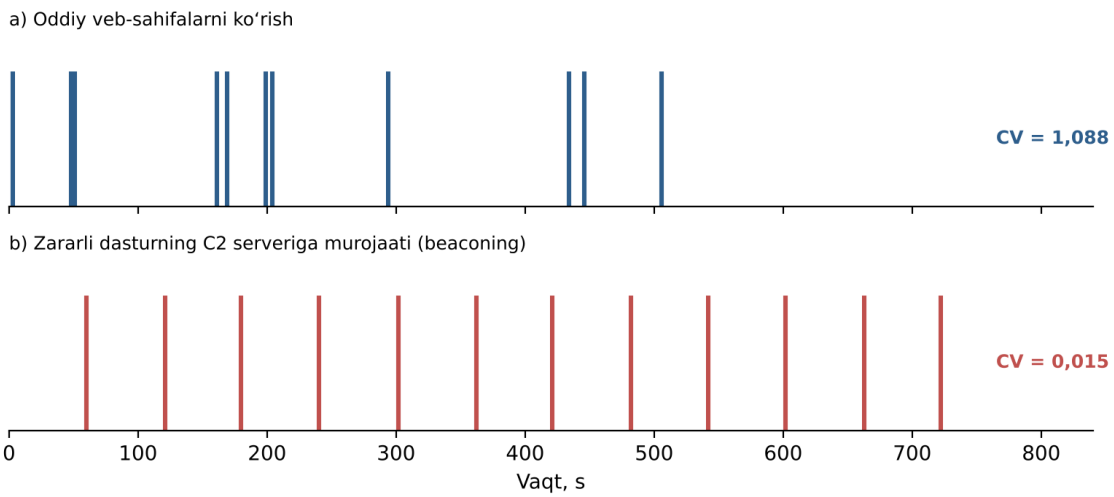
Usulni misolda tushuntirish. Usulning mohiyatini bitta misolda ko‘rib chiqamiz. Faraz qilaylik, tashkilot tarmog‘idagi kompyuter zararlangan va undagi dastur har daqiqada C2 serveriga “yangi buyruq bormi?” degan so‘rov yuboradi. Bu so‘rov HTTPS orqali shifrlangan bo‘lgani uchun uning mazmunini ko‘rib bo‘lmaydi. Ammo ulanishlar orasidagi vaqt intervallarini o‘lchash mumkin. Ketma-ket 12 ta murojaat orasidagi intervallar 60, 61, 59, 60, 62, 60, 59, 61, 60, 60, 61 va 59 sekundni tashkil etdi, deylik. Intervallarning bir xilligini variatsiya koeffitsiyenti orqali baholaymiz:

$$CV = \sigma / \mu \quad (1)$$

bu yerda μ - intervallarning o‘rtacha qiymati, σ - ularning o‘rtacha kvadratik chetlanishi. Misolimizda μ = 60,17 s, σ = 0,90 s, demak CV = 0,015. Inson veb-sahifalarni ko‘rganda esa so‘rovlar tartibsiz yuboriladi: masalan, 3, 45, 2, 1, 110, 8, 30, 5, 90, 140, 12 va 60 s intervallar uchun CV = 1,088 ga teng. Ya’ni zararli dasturning “yurak urishi” trafik shifrlangan bo‘lsa ham, vaqt bo‘yicha aniq ko‘rinib turadi (1-rasm). Xuddi shunday, ma’lumotlarni tashqariga chiqarishda yuborilgan baytlar soni qabul qilinganidan ko‘p bo‘ladi:

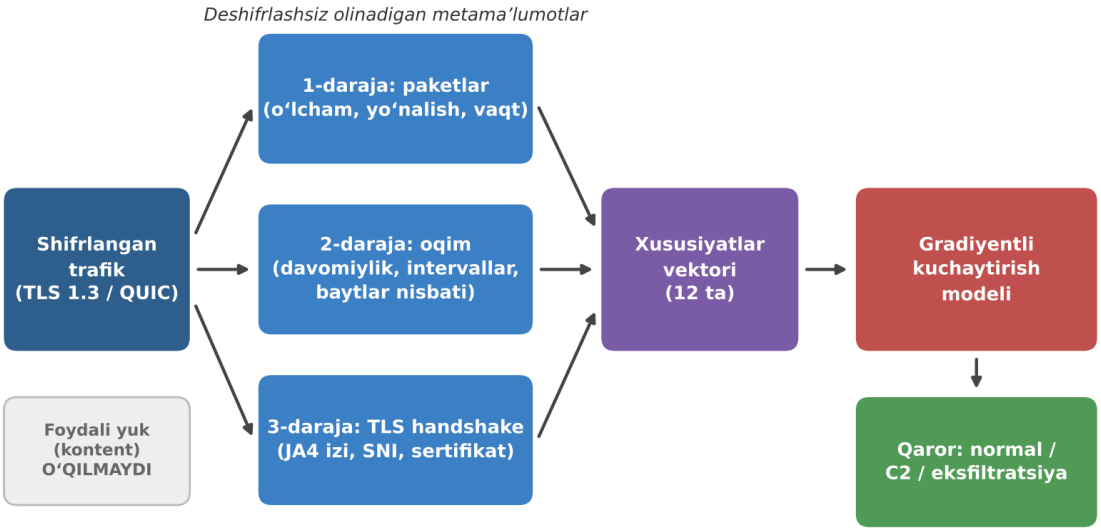
$$r = B_{out} / B_{in} \quad (2)$$

bu yerda B_{out} va B_{in} - oqim davomida yuborilgan va qabul qilingan baytlar. Oddiy veb-sahifani ko‘rishda r odatda 0,1–0,3 oralig‘ida bo‘ladi, ma’lumotlar o‘g‘irlanganda esa r birdan katta qiymatga ega bo‘ladi. Biroq bitta belgiga tayanib qaror qabul qilish ishonchsiz: zamonaviy zararli dasturlar intervallarga tasodifiy chetlanish qo‘shadi, ba’zi qonuniy xizmatlar (masalan, yangilanishlarni tekshirish) ham davriy ishlaydi. Shuning uchun barcha xususiyatlar birgalikda sun’iy intellekt modeliga beriladi.



1-rasm. Oddiy trafik va zararli dasturning davriy murojaati (shifrlangan holatda)

Taklif etilgan usul. Taklif etilgan usulning umumiy sxemasi 2-rasmda keltirilgan. Shifrlangan trafikdan uch darajada 12 ta xususiyat ajratib olinadi, ular xususiyatlar vektoriga birlashtiriladi va tasniflash modeliga uzatiladi. Model har bir oqimni to‘rt sinfdan biriga ajratadi: oddiy veb-trafik, video oqim, C2 aloqasi yoki ma’lumotlarni tashqariga chiqarish. Paket mazmuni hech bir bosqichda o‘qilmaydi.



2-rasm. Shifrlangan trafikni deshifrlashsiz tahlil qilishning uch darajali usuli

Asosiy model sifatida gradiyentli kuchaytirish (GB) algoritmi tanlandi. Bu algoritm qarorlar daraxtlarini ketma-ket qurib, har bir yangi daraxt oldingilarining xatosini kamaytiradi:

$$F_m(x) = F_{m-1}(x) + \eta \cdot h_m(x) \quad (3)$$

bu yerda $F_m(x)$ - m-qadamdagi model, $h_m(x)$ - yangi qaror daraxti, η - o‘qitish tezligi. So‘nggi yillardagi qiyosiy tahlillar jadval ko‘rinishidagi ma’lumotlarda daraxtlarga asoslangan modellar chuqur neyron tarmoqlarga nisbatan raqobatbardosh ekanini ko‘rsatgan [10]. Paketlar ketma-ketligini to‘g‘ridan-to‘g‘ri qayta ishlovchi ET-BERT kabi transformer modellar [9] yuqori natija beradi, ammo ular katta hisoblash resurslarini talab qiladi.

Eksperimental baholash. Usulni baholash uchun shifrlangan trafik oqimlarining statistik xususiyatlarini imitatsiya qiluvchi 24 000 ta oqimdan iborat sintetik ma’lumotlar to‘plami shakllantirildi. Sinflar ulushi: oddiy veb-trafik - 58 %, video oqim - 25 %, C2 aloqasi - 10 %, ma’lumotlarni chiqarish - 6 %. Vazifani murakkablashtirish uchun zararli oqimlarning xususiyatlari 35–85 % darajada oddiy trafikka “aralashtirildi”, ya’ni normal ko‘rinishga

yaqinlashtirildi, hamda shovqin qo‘shildi. Ma’lumotlar 70/30 nisbatda o‘qitish va test qismlariga ajratildi. Logistik regressiya (LR), tasodifiy o‘rmon (RF), gradiyentli kuchaytirish (GB) va ko‘p qatlamli perseptron (MLP) solishtirildi. Natijalar 2-jadvalda keltirilgan, bu yerda DR - zararli oqimlarni aniqlash darajasi, FPR - oddiy oqimlarni zararli deb noto‘g‘ri baholash ulushi.

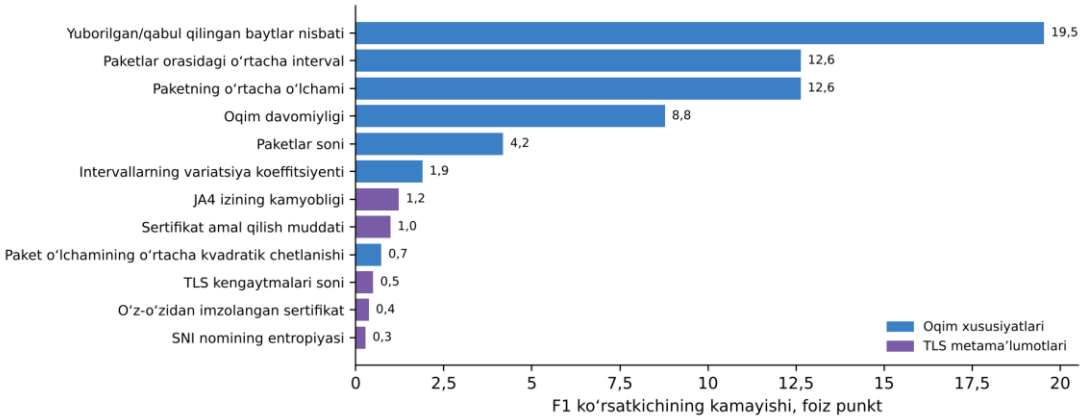
2-jadval

Algoritmlarning test to‘plamidagi natijalari

Algoritm	Precision, %	Recall, %	F1, %	DR, %	FPR, %	Vaqt, ms/oqim
Logistik regressiya (LR)	95,26	91,10	92,98	87,58	0,82	< 0,001
Tasodifiy o‘rmon (RF)	95,49	90,38	92,65	86,67	0,70	0,016
Gradiyentli kuchaytirish (GB)	94,87	91,22	92,91	88,00	0,92	0,004
Neyron tarmoq (MLP)	95,28	91,31	93,12	88,33	0,80	0,007

Natijalar tahlili. 2-jadvaldan ko‘rinadiki, to‘rtala algoritm natijalari bir-biriga juda yaqin: F1 ko‘rsatkichlari orasidagi farq 0,5 foiz punktdan oshmaydi. Bu shifrlangan trafikni tahlil qilishda algoritm tanlovidan ko‘ra xususiyatlar to‘plamining sifati muhimroq ekanini ko‘rsatadi. GB modeli eng yaxshi natijaga (MLP) deyarli teng ko‘rsatkich berdi, bitta oqimni 0,004 ms da tasniflaydi va qaysi xususiyat qarorga qanchalik ta’sir qilganini tushuntirish imkonini beradi. Xususiyatlar guruhlarining hissasini aniqlash uchun GB modeli alohida o‘qitildi: faqat oqim xususiyatlari bilan F1 = 91,08 %, faqat TLS metama’lumotlari bilan F1 = 40,47 %, ikkala guruh birgalikda F1 = 92,91 %. Demak, TLS metama’lumotlari mustaqil ravishda zaif bo‘lsa-da, oqim xususiyatlarini to‘ldiradi.

Har bir xususiyatning ahamiyati permutatsiya usuli bilan baholandi: xususiyat qiymatlari tasodifiy aralashtirilganda F1 ko‘rsatkichi qanchalik pasayishi o‘lchandi (3-rasm). Eng muhim xususiyatlar yuborilgan/qabul qilingan baytlar nisbati, paketlar orasidagi interval va paketning o‘rtacha o‘lchami bo‘ldi. Bu misolda ko‘rib chiqilgan mantiqni tasdiqlaydi.



3-rasm. Xususiyatlarning GB modeli qaroriga ta’siri (permutatsiya usuli)

Shuni ta’kidlash lozimki, natijalar sintetik ma’lumotlarda olingan. Keyingi bosqichda usulni ochiq ma’lumotlar to‘plamlarida va real tarmoq trafigida sinash rejalashtirilgan.

Xulosa

Maqolada shifrlangan tarmoq trafigida zararli faollikni deshifrlashsiz aniqlash uchun uch darajali metama’lumotlar tahliliga asoslangan sun’iy intellekt usuli taklif etildi. Misol orqali ko‘rsatildiki, shifrlash paket mazmunini yashirsa ham, zararli dasturning davriy murojaatlari (CV = 0,015) va ma’lumotlarni tashqariga chiqarish belgilari trafikning vaqt va hajm ko‘rsatkichlarida

aniq namoyon bo‘ladi. Eksperimental sinovda gradiyentli kuchaytirish modeli 92,91 % F1 va 88,0 % aniqlash darajasiga erishdi, TLS metama’lumotlarini qo‘shish esa natijani 1,8 foiz punktga yaxshiladi. Usul foydalanuvchi ma’lumotlarining maxfiyligini buzmaydi va real vaqt rejimida ishlash uchun yetarli tezlikka ega. Keyingi ishlarda QUIC protokoli uchun xususiyatlarni kengaytirish va usulni real tarmoq trafigida sinash rejalashtirilgan.

Foydalanilgan adabiyotlar

1. ENISA Threat Landscape 2024. - European Union Agency for Cybersecurity, 2024.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 2022-yil 15-aprel.
3. Iyengar J., Thomson M. QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000. - IETF, 2021.
4. Papadogiannaki E., Ioannidis S. A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures // ACM Computing Surveys. - 2021. - Vol. 54, No. 6. - Article 123.
5. Shen M., Ye K., Liu X., Zhu L., Kang J., Yu S., Li Q., Xu K. Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. - 2023. - Vol. 25, No. 1. - P. 791–824.
6. Akbari I., Salahuddin M. A., Ven L., Limam N., Boutaba R., Mathieu B., Moteau S., Tuffin S. A Look Behind the Curtain: Traffic Classification in an Increasingly Encrypted Web // Proc. of the ACM on Measurement and Analysis of Computing Systems. - 2021. - Vol. 5, No. 1. - Article 4.
7. Holland J., Schmitt P., Feamster N., Mittal P. New Directions in Automated Traffic Analysis // Proc. of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS). - 2021. - P. 3366–3383.
8. Althouse J. JA4+ Network Fingerprinting. - FoxIO, 2023.
9. Lin X., Xiong G., Gou G., Li Z., Shi J., Yu J. ET-BERT: A Contextualized Datagram Representation with Pre-training Transformers for Encrypted Traffic Classification // Proc. of the ACM Web Conference 2022 (WWW). - 2022. - P. 633-642.
10. Grinsztajn L., Oyallon E., Varoquaux G. Why do tree-based models still outperform deep learning on typical tabular data? // Advances in Neural Information Processing Systems 35 (NeurIPS 2022), Datasets and Benchmarks Track. - 2022.

IOT MUHITIDA VLC TEXNOLOGIYASINI QO‘LLASH VA EDGE COMPUTING ASOSIDA XAVFSIZLIKNI TA’MINLASH

Jurayev G.U.
Toshkent davlat iqtisodiyot universiteti
Saidmurodov M.A.
Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti

Annotatsiya. Internet of Things (IoT) texnologiyalarining jadal rivojlanishi ko‘plab qurilmalar o‘rtasida tezkor, ishonchli va energiya samaradorligi yuqori bo‘lgan aloqa texnologiyalariga bo‘lgan ehtiyojni oshirmoqda. Radiochastotali aloqa texnologiyalariga muqobil sifatida Visible Light Communication (VLC) texnologiyasi ma’lumotlarni ko‘rinadigan yorug‘lik spektri orqali uzatish imkonini beradi. VLC texnologiyasi yuqori tezlikdagi ma’lumot uzatish, elektromagnit radiochastota spektridan foydalanmaslik va mavjud LED yoritish infratuzilmasidan foydalanish imkoniyati sababli IoT tizimlari uchun istiqbolli texnologiyalardan biri hisoblanadi. Biroq VLC tizimlari ham jamming, spoofing, eavesdropping, signalni manipulyatsiya qilish va ruxsatsiz kirish kabi xavfsizlik tahdidlariga duch kelishi mumkin.

Ushbu maqolada VLC texnologiyasining IoT muhitidagi qo‘llanilishi, mavjud xavfsizlik muammolari va ularni Edge Computing yordamida bartaraf etish imkoniyatlari tahlil qilinadi. Taklif qilinayotgan yondashuvda IoT qurilmalaridan kelayotgan VLC trafik Edge node/gateway darajasida qayta ishlanadi va sun’iy intellekt asosidagi Intrusion Detection System (IDS) yordamida anomal trafik aniqlanadi. Bunday yondashuv markaziy Cloud serverga barcha ma’lumotlarni yuborish zaruratini kamaytirib, aniqlash vaqtini qisqartirish va tarmoq yuklamasini kamaytirishga xizmat qilishi mumkin.

Kalit so‘zlar: Visible Light Communication, VLC, Internet of Things, IoT, Edge Computing, Edge AI, Cybersecurity, Intrusion Detection System, Machine Learning, IoT security.

Аннотация. Стремительное развитие технологий Интернета вещей (IoT) формирует потребность в быстрых, надежных и энергоэффективных технологиях связи для взаимодействия множества устройств. В качестве альтернативы радиочастотной связи выступает технология передачи данных в диапазоне видимого света (Visible Light Communication, VLC). VLC считается перспективной технологией для систем IoT благодаря высокой скорости передачи данных, независимости от радиочастотного спектра и возможности использования существующей инфраструктуры светодиодного освещения. Однако системы VLC также подвержены угрозам безопасности, таким как создание помех (джамминг), подмена данных (спуфинг), перехват информации, манипуляция сигналами и несанкционированный доступ.

В данной статье анализируются вопросы применения технологии VLC в средах IoT, существующие проблемы безопасности и возможности их решения с помощью технологий периферийных вычислений (Edge Computing). В рамках предлагаемого подхода трафик VLC от устройств IoT обрабатывается на уровне периферийного узла или шлюза, а аномальный трафик выявляется с помощью системы обнаружения вторжений (IDS) на базе искусственного интеллекта. Такой подход позволяет сократить объем данных, передаваемых на центральный облачный сервер, тем самым уменьшая время обнаружения угроз и снижая нагрузку на сеть.

Ключевые слова: передача данных в диапазоне видимого света, VLC, Интернет вещей, IoT, периферийные вычисления, Edge AI, кибербезопасность, система обнаружения вторжений, машинное обучение, безопасность IoT.

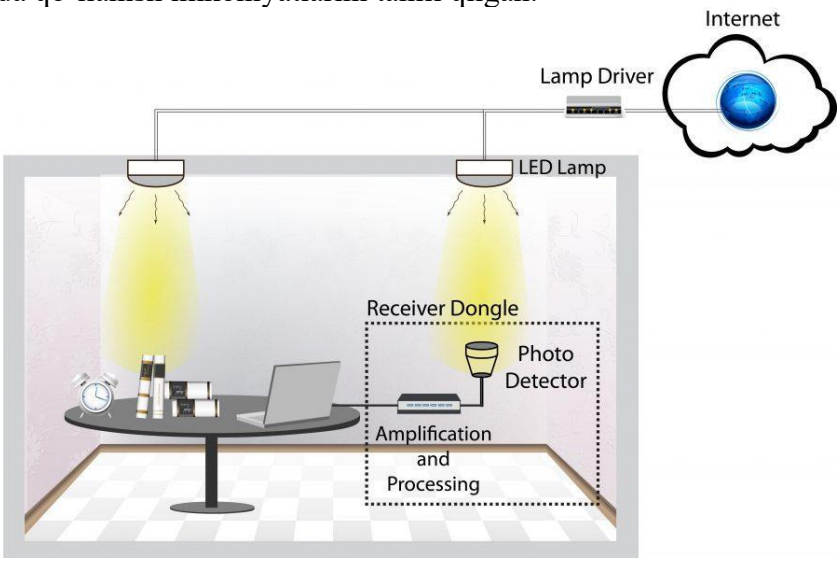
Kirish

Internet of Things konsepsiyasi fizik qurilmalarni internet va boshqa aloqa tarmoqlariga ulash orqali real vaqt rejimida ma’lumot almashish imkonini beradi. Smart home, smart city,

healthcare, industrial automation, intelligent transportation va boshqa sohalarda IoT qurilmalarining ko‘payishi tarmoq orqali uzatiladigan ma’lumotlar hajmining oshishiga olib kelmoqda.

IoT tizimlarida an’anaviy Wi-Fi, Bluetooth, Zigbee va boshqa radiochastotali texnologiyalar keng qo‘llaniladi. Shu bilan birga, radiochastota spektrining cheklanganligi va ayrim muhitlarda elektromagnit interferensiyaning mavjudligi alternativ aloqa texnologiyalarini tadqiq qilish zaruratini yuzaga keltirmoqda.

Shunday texnologiyalardan biri Visible Light Communication (VLC) hisoblanadi. VLC ma’lumotlarni LED yorug‘lik manbalarining intensivligini juda yuqori tezlikda modulyatsiya qilish orqali uzatadi. Qabul qiluvchi tomon esa photodiode yoki kamera yordamida ushbu signalni qabul qiladi. Oyewobi, Djouani va Kurien VLC texnologiyasini IoT uchun istiqbolli aloqa vositasi sifatida ko‘rsatib, uning machine-to-machine, device-to-device, vehicle-to-infrastructure kabi ko‘plab IoT ssenariylarida qo‘llanish imkoniyatlarini tahlil qilgan.



1-rasm. VLC asosidagi IoT aloqa arxitekturasi.

Asosiy qism

VLC texnologiyasining asosiy ishlash prinsipi LED transmitter va optical receiver o‘rtasida ma’lumot uzatishga asoslanadi. Umumiy VLC tizimi IoT sensor yoki qurilma, VLC transmitter, LED yorug‘lik manbai, Optik kanal, Photodiode yoki camera receiver, Edge Gateway, Cloud server kabi elementlardan tashkil topadi.

IoT qurilmasida hosil bo‘lgan ma’lumot avval VLC transmitterga uzatiladi. LED modulatsiyasi orqali ma’lumot yorug‘lik signali ko‘rinishida uzatiladi. Qabul qiluvchi qurilma signalni qayta elektr/digital signalga aylantiradi.

VLC texnologiyasining IoT uchun muhim afzalliklaridan biri mavjud LED yoritish infratuzilmasidan aloqa uchun foydalanish imkoniyatidir. Oyewobi va boshqalar VLC IoT uchun katta miqdordagi qurilmalarni ulashda, jumladan device-to-device va vehicle-to-infrastructure aloqa ssenariylarida qo‘llanishi mumkinligini ta'kidlaydi. Bundan tashqari, VLC radiochastota spektriga bog‘liq emasligi sababli RF spektri cheklangan muhitlarda qo‘shimcha aloqa kanali sifatida ishlatilishi mumkin[1].

VLC-IoT tizimlarida xavfsizlik muammolari

VLC texnologiyasi radiochastotali aloqa tizimlaridan farqli fizik xususiyatlarga ega bo‘lsada, bu uning avtomatik ravishda xavfsizligini anglatmaydi.

Blinowski tomonidan VLC xavfsizligiga bag‘ishlangan keng qamrovli surveyda VLC tizimlari uchun maxfiylik, yaxlitlik va mavjudlik bilan bog‘liq turli tahdidlar tahlil qilingan. Jumladan, jamming, ma’lumotni o‘zgartirish, fizik qatlamga qaratilgan hujumlar, xavfsiz joylashuvni aniqlash va kalit generatsiyasi kabi masalalar ko‘rib chiqilgan[2].

Jamming hujumida hujumchi VLC qabul qiluvchiga kuchli yoki maxsus shakllantirilgan optik signal yuborib, normal aloqa jarayoniga xalaqit beradi.

Natijada normal VLC signal va hujum signali Signalga xalaqit beradi va aloqa uzilishiga olib keladi. Bu ayniqsa IoT tizimlarida xavfli bo‘lishi mumkin, chunki ayrim IoT tizimlari real vaqt rejimida ishlaydi.

Spoofing hujumida hujumchi o‘zini qonuniy IoT qurilma yoki transmitter sifatida ko‘rsatishga harakat qiladi. Masalan hujumchi IoT qabul qilgichiga soxta VLC signali yuboradi. Agar autentifikatsiya mexanizmi yetarli bo‘lmasa, tizim noto‘g‘ri qurilmadan kelayotgan ma’lumotni qonuniy ma’lumot sifatida qabul qilishi mumkin.

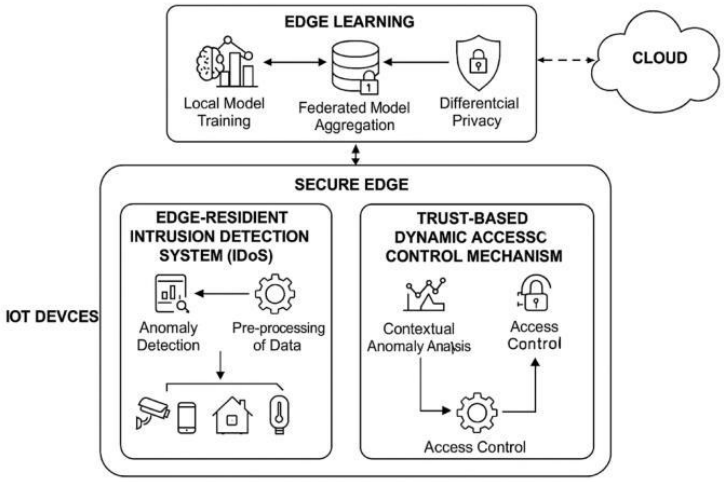
VLC signali ma’lum bir yorug‘lik hududida tarqaladi. Agar hujumchi signal tarqaladigan hududga optik qabul qiluvchi qurilmani joylashtirsa, uzatilayotgan ma’lumotni kuzatishga urinishi mumkin. Shuning uchun VLC tizimlarida fizik cheklangan aloqa zonasi mavjud bo‘lishi to‘liq maxfiylik kafolati sifatida qaralmasligi kerak.

Data modification hujum turida hujumchi uzatilayotgan ma’lumotni o‘zgartirishga harakat qilishi mumkin. Sensor ma’lumotlari VLCga uzatiladi hujumchi esa o‘zgartirilgan ma’lumotlarni chekka qurilmaga uzatadi. Natijada IoT tizimi noto‘g‘ri qaror qabul qilishi mumkin.

An’anaviy IoT arxitekturasida sensorlardan olingan ma’lumotlar Cloud serverga yuboriladi va tahlil qilinadi. Bu jarayon quyidagi sxemaga ega bo‘lishi mumkin. IoT qurilma, VLC, Gateway, Internet, Cloud, Analysis. Bunday yondashuv katta hajmdagi trafik uchun quyidagi muammolarni yuzaga keltirishi mumkin. Yuqori kechikish, tarmoq o‘tkazish qobiliyati sarfining oshishi, Cloud serverga bog‘liqlik, maxfiy ma’lumotlarning markaziy serverga yuborilishi, real vaqt hujumni aniqlash qiyinlashishi. Shuning uchun xavfsizlikni Edge Computing darajasida amalga oshirish maqsadga muvofiq.

Taklif qilinayotgan modelda ananaviy modeldan farqli o‘laroq IoT qurilmasi, VLC, Edge qurilma, SI asosidagi IDS va Cloud. Bu yerda Edge qurilma VLC trafikni qabul qiladi, trafikdan xususiyatlarni ajratadi, ma’lumotlarni qayta ishlaydi, AI/ML modelga uzatadi, anomal trafikni aniqlaydi, xavfli trafikni bloklash yoki administratorga xabar berishni amalga oshiradi.

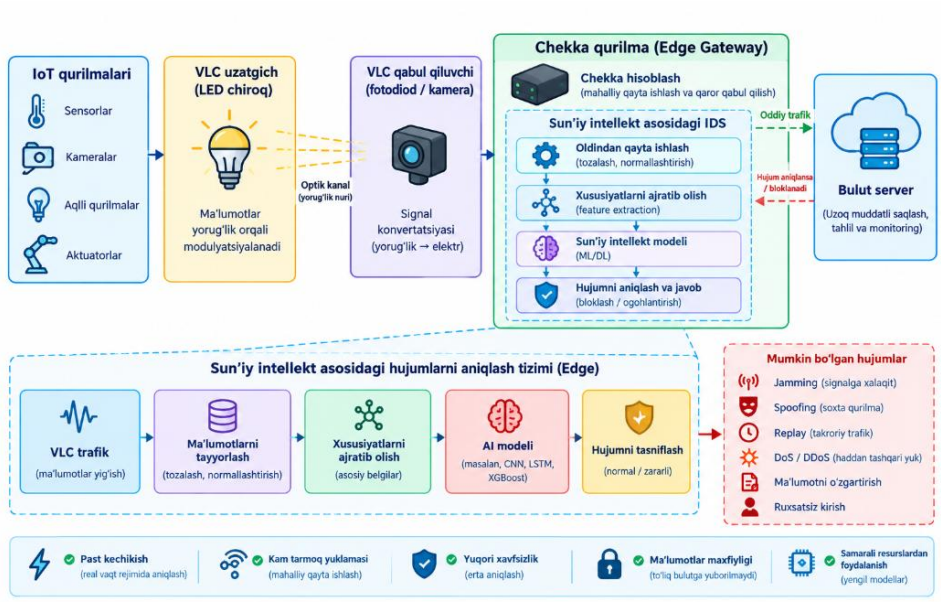
Yang va boshqalar IoT uchun cloud–edge ga asoslangan IDS modelini taklif qilgan. Ularning yondashuvida SSAE orqali yuqori o‘lchamli trafik xususiyatlari kamaytiriladi, TCN orqali trafik tahlil qilinadi va federated learning yordamida edge qurilmalar o‘rtasida modelni hamkorlikda o‘qitish ko‘rib chiqiladi. Tadqiqotda bunday yondashuv hisoblash, saqlash va xotira talablarini sezilarli kamaytirgani ko‘rsatilgan[3].



2-rasm. VLC-IoT xavfsizligini Edge Computing yordamida ta’minlash konsepsiyasi.

Taklif qilinayotgan VLC-IoT-Edge xavfsizlik modeli

Ushbu tadqiqot uchun quyidagi arxitekturani taklif qilish mumkin.



3-rasm. Taklif qilinayotgan VLC-IoT-Edge xavfsizlik arxitekturasi

Xulosa

Edge qurilmada joylashtirilgan sun’iy intellekt asosidagi hujumlarni aniqlash tizimi (IDS) VLC orqali uzatilayotgan IoT trafikni mahalliy darajada tahlil qiladi. Dastlab, VLC tarmog‘idan kelayotgan trafik yig‘iladi va qayta ishlanadi. Ushbu bosqichda keraksiz, takroriy yoki noto‘g‘ri ma’lumotlar tozalanadi hamda ma’lumotlar AI modeliga mos shaklga keltiriladi.

Keyingi bosqichda trafik tarkibidan muhim xususiyatlar (features) ajratib olinadi. Ushbu xususiyatlar tarmoqdagi normal va anomal faoliyatni farqlash uchun AI modeliga uzatiladi. Shundan so‘ng, Edge qurilmada joylashtirilgan sun’iy intellekt modeli olingan xususiyatlarni tahlil qiladi va trafikning xavfsizlik holatini baholaydi.

Modelning yakuniy bosqichida hujumlarni tasniflash amalga oshiriladi. Natijada trafik normal yoki zararli (hujum) sifatida aniqlanadi. Agar zararli faoliyat aniqlansa, Edge qurilma hujum haqida ogohlantirish yuborishi yoki tegishli trafikni bloklashi mumkin. Bunday yondashuv hujumlarni Cloud serverga yubormasdan, tarmoqning chekka qismida aniqlash imkonini beradi va shu sababli kechikishni kamaytirish, tarmoq yuklamasini pasaytirish hamda real vaqtga yaqin xavfsizlikni ta’minlash imkonini beradi.

Foydalanilgan adabiyotlar

1. Oyewobi, S. S., Djouani, K., & Kurien, A. M. (2022). Visible Light Communications for Internet of Things: Prospects and Approaches, Challenges, Solutions and Future Directions. Technologies, 10(1), 28. https://doi.org/10.3390/technologies10010028.

2. Blinowski, G. (2019). Security of Visible Light Communication systems-A survey. Physical Communication, 34, 246–260. https://doi.org/10.1016/j.phycom.2019.04.003.

3. Yang, R., He, H., Xu, Y., Xin, B., Wang, Y., Qu, Y., & Zhang, W. (2023). Efficient intrusion detection toward IoT networks using cloud–edge collaboration. Computer Networks, 228, 109724. https://doi.org/10.1016/j.comnet.2023.109724.

CAMELLIA SIMMETRIK BLOKLI SHIFRLASH ALGORITMINING SAMARADORLIGI VA ZAMONAVIY KRIPTOTIZIMLARDA QO‘LLASH ISTIQBOLLARI

Salayev A.K.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada Camellia simmetrik blokli shifrlash algoritmining tuzilishi, dasturiy samaradorligi va zamonaviy kriptotizimlarda qo‘llash imkoniyatlari o‘rganiladi. RFC hujjatlari tahlili OpenSSL muhitidagi qiyosiy mikrobenchmark bilan birlashtiriladi. Camellia va AES algoritmlari CBC rejimida, 128 va 256 bitli kalitlar hamda uch xil bufer hajmida sinovdan o‘tkazildi. Natijalar tanlangan virtual x86-64 muhitida AES realizatsiyasi tezroq ekanini ko‘rsatdi. Camellia uchun algoritmik muqobillik, mavjud tizimlar bilan moslik va kriptografik moslashuvchanlik yo‘nalishlari asoslandi. Protokol qo‘llovi, autentifikatsiya va yon kanal himoyasi tanlovning alohida mezonlari sifatida ajratildi.

Kalit so‘zlar: Camellia, simmetrik shifrlash, Feystel tarmog‘i, AES, CBC, unumdorlik, kriptografik moslashuvchanlik.

Аннотация. В статье исследуются структура, программная производительность и перспективы применения блочного шифра Camellia в современных криптосистемах. Анализ документов RFC дополнен сравнительным микротестированием в среде OpenSSL. Camellia и AES проверены в режиме CBC с ключами длиной 128 и 256 бит при трех размерах буфера. В выбранной виртуальной среде x86-64 реализация AES показала более высокую скорость. Обоснованы направления применения Camellia для алгоритмического разнообразия, совместимости с существующими системами и криптографической гибкости. Поддержка протоколов, аутентификация и защита от побочных каналов рассматриваются как самостоятельные критерии выбора.

Ключевые слова: Camellia, симметричное шифрование, сеть Фейстеля, AES, CBC, производительность, криптографическая гибкость.

Kirish

Kriptografik algoritmni tanlashda kalit uzunligi bilan bir qatorda dasturiy realizatsiya, protsessor imkoniyatlari va protokol talablari hisobga olinadi. Bir xil blok va kalit uzunligiga ega shifrlar amalda turlicha tezlik ko‘rsatishi mumkin. Shu sababli Camellia istiqbollarini baholash uning matematik tuzilishini o‘rganish va aniq hisoblash muhitida sinashni talab qiladi.

Tadqiqot maqsadi Camellia algoritmining samaradorligini takrorlanadigan sinov orqali baholash hamda undan foydalanish shartlarini aniqlashdir. Ishning amaliy hissasi bir xil rejimdagi tezlik o‘lchovlarini protokol mosligi bilan birgalikda talqin qilishdan iborat. Olingan natijalar muayyan realizatsiyaga tegishli bo‘lib, shifrning barcha platformalardagi ustunligi yoki zaifligini ifodalamaydi.

Camellia tuzilishi va baholash mezonlari

Camellia 128 bitli blok hamda 128, 192 yoki 256 bitli kalit bilan ishlaydi. 128 bitli kalitda 18, uzunroq kalitlarda 24 raundli Feystel tuzilishi qo‘llanadi. F funksiyasi kalit bilan XOR, baytli almashtirishlar va chiziqli aralashtirishni bajaradi. Raund guruhlari orasiga FL va FL^{-1} qatlamlari, kirish va chiqishga kalit bilan qo‘shimcha XOR amallari kiritiladi [1, 2].

128 bitli variantda FL va FL^{-1} qatlamlari 6- va 12-raundlardan, 192 va 256 bitli variantlarda esa 6-, 12- va 18-raundlardan keyin joylashadi. Deshifrlash tegishli qism kalitlarini teskari tartibda

ishlatish orqali tashkil etiladi [1]. Ushbu xususiyat realizatsiyada umumiy hisoblash qismlaridan foydalanish imkonini beradi, biroq shifrlash va deshifrlash tezligi aynan teng bo‘lishini kafolatlamaydi.

Raundlar sonini tezlikning yagona ko‘rsatkichi sifatida ishlatish to‘g‘ri emas. Bir raundning buyruqlar tarkibi, xotiraga murojaatlari va kutubxona optimallashtirishlari turlicha bo‘ladi. Shu bois mazkur ishda algoritm nomi emas, algoritm, kalit, rejim, kutubxona va platformadan iborat konfiguratsiya baholash obyekti sifatida olindi.

Asosiy mezon sifatida vaqt birligida qayta ishlangan ma’lumot hajmi tanlandi. Kalit jadvalini yaratish, xotira sarfi, energiya iste’moli va autentifikatsiya xarajati alohida mezonlardir. Ular mazkur mikrobenchmarkda o‘lchanmaganligi sababli tezlik natijalaridan bu ko‘rsatkichlar haqida sonli xulosa chiqarilmaydi.

Tadqiqot usuli va tajriba sharoiti

Sinov Linux x86-64 virtual muhitida bajarildi. Muhit protsessorni AMD EPYC 9V74 80-Core Processor deb ko‘rsatdi; 9 ta mantiqiy protsessor mavjud edi. OpenSSL 3.0.13 (30 Jan 2024) kutubxonasi ishlatildi. CPU imkoniyatlari ro‘yxatida AES va VAES bayroqlari mavjud bo‘lib, apparat tezlashtirishini o‘chiruvchi maxsus sozlama berilmadi. Aniq mashina kodi yo‘li alohida profil qilinmadi.

Camellia-128-CBC, Camellia-256-CBC, AES-128-CBC va AES-256-CBC uchun 64, 1024 va 16384 baytli buferlar tekshirildi. Har bir kombinatsiya alohida jarayonda bir soniyadan uch marta bajarildi. Sinovlar ketma-ket o‘tkazildi; ko‘p jarayonli tezlashtirish qo‘llanmadi. Har bir takrorda algoritmlar va buferlar bir xil tartibda tekshirildi. Natija sifatida uch o‘lchov medianasi hamda eng kichik va eng katta qiymatlar olindi.

OpenSSL speed vositasining EVP interfeysi, haqiqiy o‘tgan vaqt va aniq bufer hajmini tanlash parametrlaridan foydalanildi [3]. Buyruq namunasi: openssl speed -elapsed -seconds 1 -bytes 16384 -evp camellia-128-cbc -mr. Qolgan konfiguratsiyalar uchun faqat algoritm nomi va bufer hajmi almashtirildi. Barcha hajmlar 16 baytli blokka karrali bo‘lib, faylni o‘qish va tarmoqqa uzatish xarajatlari sinovga kiritilmadi.

Tajriba natijalari va ularning tahlili

Dastlab Camellia-128 realizatsiyasi RFC 3713 dagi nazorat vektori bilan tekshirildi: kalit va ochiq blok 0123456789abcdeffedcba9876543210 bo‘lganda 67673138549669730857065648eabe43 natijasi olindi [1]. Natija etalonga mos keldi. ECB bu yerda faqat bitta blokni tekshirish uchun ishlatildi; tezlik taqqoslanishi CBC rejimida bajarildi.

Unumdorlik V = B/t formulasi bilan ifodalanadi; bunda B qayta ishlangan baytlar soni, t esa sekunddagi vaqt. Jadvalda o‘nlik MB/s birligi qo‘llanadi: 1 MB = 1 000 000 bayt. Qavs ichidagi qiymatlar uch takrorning minimum va maksimumini bildiradi; ular statistik ishonch oralig‘i emas.

1-jadval

CBC shifrlash tezligi, MB/s

Algoritm	64 bayt	1024 bayt	16384 bayt
CAMELLIA-128	179.47 (165.41–185.49)	198.17 (174.52–207.72)	189.84 (187.17–197.71)
CAMELLIA-256	131.06 (130.69–138.04)	139.44 (137.75–146.22)	144.13 (140.46–144.90)
AES-128	1086.37 (1044.72–1211.22)	1277.65 (1211.24–1280.72)	1207.34 (1201.29–1290.04)
AES-256	888.48 (824.92–888.98)	853.27 (852.43–926.26)	888.29 (869.45–944.52)

16384 baytli buferda Camellia-128-CBC medianasi 189,84 MB/s, Camellia-256-CBC medianasi 144,13 MB/s bo‘ldi. Tegishli AES variantlari 1207,34 va 888,29 MB/s natija berdi. Shunday qilib, mazkur sharoitda AES-128-CBC taxminan 6,36 marta, AES-256-CBC esa 6,16 marta yuqori unumdorlik ko‘rsatdi. Bu nisbatlar medianalar bo‘yicha hisoblangan.

Camellia kaliti 128 bitdan 256 bitga o‘zgarganda katta buferdagi tezlik 24,08 foizga kamaydi. 24 raundli variant ko‘proq hisoblash bajarishi ushbu kuzatuvga mos keladi, ammo farqning faqat raundlar sonidan kelib chiqqani alohida isbotlanmagan. Kutubxonaning ichki realizatsiyasi ham natijaga ta’sir qiladi.

Bufer kattalashishi barcha holatda bir tekis tezlashishni bermadi. Masalan, Camellia-128 uchun 1024 baytdagi mediana 16384 baytdagidan yuqori. Qisqa sinovlar, virtual protsessorni rejalashtirish va tizimdagi boshqa yuklamalar bunday tafovutga ta’sir etishi mumkin. Uch takror mazkur omillarni ajratishga yetarli emas; shu sababli kichik farqlar universal qonuniyat sifatida talqin qilinmaydi.

Natijalar AES tezlashtirish imkoniyatlari mavjud muhitda olingan. Ularni barcha apparat yo‘riqnomalari o‘chirilgan sof dasturiy taqqoslash yoki mikrokontroller natijasi sifatida berish mumkin emas. Sinov faqat shifrlashni qamrab oldi; deshifrlash, qisqa seanslar uchun kalit tayyorlash va to‘liq himoyalangan aloqa kanalining kechikishi alohida tekshirilishi kerak.

Zamonaviy kriptotizimlarda qo‘llash shartlari

Algoritmning kutubxonada mavjudligi uning barcha protokollarda ishlashini anglatmaydi. OpenSSL 3.0 hujjatlarida Camellia uchun CBC, CTR, ECB va boshqa rejimlar ko‘rsatilgan [4]. RFC 6367 Camellia asosidagi CBC va GCM TLS shifr to‘plamlarini belgilaydi, GCM variantlarini TLS 1.2 bilan bog‘laydi [5]. RFC 8446 da belgilangan TLS 1.3 shifr to‘plamlari tarkibida esa Camellia mavjud emas [6].

Demak, Camellia kutubxonada borligini asos qilib uni TLS 1.3 ga bevosita almashtirish mumkin, degan xulosa chiqarilmaydi. Muayyan mahsulot uchun protokol versiyasi, tomonlarning kelishish mexanizmi va amaldagi kutubxona qo‘llovi birgalikda tekshirilishi zarur. Faqat Camellia ishlatish uchun aloqa protokolini eski versiyaga tushirish mazkur tadqiqot natijalaridan kelib chiqadigan tavsiya emas.

Camellia istiqbolini uchta ssenariyda ko‘rish mumkin: mavjud Camellia infratuzilmasini saqlash, boshqariladigan yopiq tizimda muqobil shifrni baholash va algoritmlarni xavfsiz almashtirish imkoniyatini tadqiq qilish. Bunda muqobillikning foydasi qo‘shimcha integratsiya, audit va texnik xizmat xarajatlari bilan solishtiriladi. Bir nechta shifrni qo‘llashning o‘zi tizimni avtomatik ravishda xavfsizroq qilmaydi.

2-jadval

Qo‘llash ssenariylari uchun baholash mezonlari

Ssenariy	Asosiy tekshiruv	Tahlildan kelib chiqadigan qaror
Mavjud tizim	Protokol va kalitlar bilan moslik	Migratsiya xarajati bilan birga baholash
Yangi tarmoq xizmati	Protokolda ruxsat etilgan shifrlar	Qo‘llab-quvvatlanadigan AEAD yechimidan boshlash
Yopiq tizim yoki arxiv	Format, autentifikatsiya, kalit aylanishi	To‘liq himoya sxemasini sinash
Cheklangan qurilma	RAM, kod hajmi va energiya sarfi	Aynan maqsadli qurilmada qayta o‘lchash

Xavfsizlik va amalga oshirish cheklovlari

CBC tezlik sinovi faqat maxfiylikni ta’minlovchi hisoblash qismini baholaydi. Amaliy tizimda xabar yaxlitligi va haqiqiyligini tekshirish ham talab etiladi. Camellia-CTR va Camellia-CCM tavsiflari RFC 5528 da berilgan [7]. Rejimni tanlashda nonce yoki boshlang‘ich vektor talablari, teg uzunligi va bir kalit bilan ishlov beriladigan hajm tekshiriladi. Blokli shifrni o‘zi bilan to‘liq himoyalangan protokolni tenglashtirish mumkin emas.

Bajarilish vaqtining yoki xotiraga murojaatlarning maxfiy qiymatlarga bog‘liqligi alohida xavf modelini talab qiladi. Ushbu ishda yon kanal hujumi bajarilmadi; yuqori tezlik bunday hujumlarga chidamlilik dalili sifatida olinmaydi. Keyingi sinovlarda doimiy vaqtli realizatsiyalar, autentifikatsiyalangan shifrlash xarajati va kalitlarni xavfsiz saqlash birgalikda baholanishi lozim.

Rivojlanish istiqbollari va xulosa

Kelgusi tadqiqotlarda ayni tajribani ajratilgan fizik x86-64 va ARM qurilmalarida takrorlash, sinovlar tartibini tasodifiylashtirish hamda o‘lchash vaqtini uzaytirish maqsadga muvofiq. CPUga biriktirish va yuklamani nazorat qilish o‘zgaruvchanlikni kamaytiradi. Kalitni har xabar uchun qayta tayyorlash va tayyor jadvaldan uzoq oqim davomida foydalanish holatlari alohida o‘lchansa, qisqa xabarli tizimlar uchun aniqroq xulosa olinadi.

Kvant hisoblash istiqbolida simmetrik shifr kaliti va ochiq kalitli almashinuv mexanizmi alohida baholanadi. Grover qidiruvi ideal modelda kalit qidirish bosqichlari sonini kvadratik kamaytiradi, biroq amaliy xarajatlar apparat va ketma-ket hisoblash cheklovlariga bog‘liq [8]. Shu sababli Camellia-256 ni tanlashning o‘zi tizimni to‘liq postkvant himoyalangan deb atashga asos bo‘lmaydi. Kalit almashinuvi, autentifikatsiya va ma’lumotni saqlash muddati ham tekshirilishi kerak.

O‘tkazilgan mikrobenchmarkda Camellia-128-CBC va Camellia-256-CBC katta bufer uchun mos ravishda 189,84 va 144,13 MB/s median tezlikka erishdi. Xuddi shu muhitda AES variantlari sezilarli tezroq bo‘ldi. Natija tanlangan OpenSSL realizatsiyasi va virtual platformaga tegishlidir; undan boshqa arxitekturalar, xotira sarfi yoki kriptografik bardoshlilik haqida umumiy hukm chiqarilmaydi.

Camellia algoritmining amaliy istiqboli algoritmik muqobillik va mavjud infratuzilma bilan moslikda namoyon bo‘lishi mumkin. Uni joriy etish qarori protokol qo‘llovi, talab etilgan unumdorlik, autentifikatsiya va audit natijalari asosida qabul qilinishi lozim. Mazkur tadqiqot Camellia tanlovini aniq platformadagi o‘lchov va tizim talablari bilan asoslash uchun takrorlanadigan boshlang‘ich baholashni taqdim etadi.

Foydalanilgan adabiyotlar

1. Matsui M., Nakajima J., Moriai S. A Description of the Camellia Encryption Algorithm. RFC 3713. 2004. DOI: 10.17487/RFC3713.
2. NTT. Handout of Camellia. Version 7.0. 2010. https://info.isl.ntt.co.jp/crypt/eng/camellia/dl/Camellia2010v7_0_eng.pdf
3. OpenSSL Project. openssl-speed. OpenSSL 3.0 Documentation. https://docs.openssl.org/3.0/man1/openssl-speed/
4. OpenSSL Project. EVP_CIPHER-CAMELLIA. OpenSSL 3.0 Documentation. https://docs.openssl.org/3.0/man7/EVP_CIPHER-CAMELLIA/
5. Kato A., Kanda M., Kanno S. Addition of the Camellia Cipher Suites to Transport Layer Security (TLS). RFC 6367. 2011. DOI: 10.17487/RFC6367.
6. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. 2018. DOI: 10.17487/RFC8446.
7. Kato A., Kanda M., Kanno S. Camellia Counter Mode and Camellia Counter with CBC-MAC Mode Algorithms. RFC 5528. 2009. DOI: 10.17487/RFC5528.
8. NIST. Post-Quantum Cryptography: FAQs. https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

KRIPTOGRAFIK XESH FUNKSIYALARNI TAKOMILLASHTIRISH YONDASHUVLARI

Allanov O.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada kriptografik xesh funksiyalarni takomillashtirishda xavfsizlik va hisoblash samaradorligini birgalikda optimallashtirish yondashuvi tahlil qilinadi. Differensial, chiziqli, algebraik, integral va strukturaviy kriptotahlilga qarshi xavfsizlik darajasini aktiv nochiziqli elementlar, chiziqli diffuziya qatlamining farqlar yoki maskalarni qanchalik kuchli tarqatishi, algebraik daraja o‘sishi va qisqartirilgan raundlarda farqlovchi kriptotahliliy xossalar orqali baholash taklif etiladi. Shuningdek, bir baytni qayta ishlash uchun nechta CPU cycle sarflanishi(cycles/byte), bitta natijani olish uchun qancha vaqt kutilishi(latency), bir vaqt birligida qancha ma’lumot qayta ishlanishi(throughput), RAM/ROM va apparat vositasida amalga oshirish uchun talab qilinadigan resurslar hajmi (hardware area) ko‘rsatkichlarini birgalikda hisobga oluvchi ko‘p mezonli loyihalash modeli shakllantiriladi.

Kalit so‘zlar: xesh funksiya, diffuziya, avalanche, kriptotahlil, xavfsizlik darajasi, yengil vaznli kriptografiya, throughput, hardware area.

Аннотация. В данной работе анализируется подход к совершенствованию криптографических хеш-функций, основанный на совместной оптимизации безопасности и вычислительной эффективности. Предлагается оценивать уровень устойчивости к дифференциальному, линейному, алгебраическому, интегральному, rebound- и структурному криптоанализу на основе числа активных нелинейных элементов, степени распространения разностей и масок линейным диффузионным слоем, роста алгебраической степени, а также различительных криптоаналитических свойств для вариантов с сокращённым числом раундов. Кроме того, формируется многокритериальная модель проектирования, совместно учитывающая количество тактов процессора, затрачиваемых на обработку одного байта (cycles/byte), время ожидания получения одного результата (latency), объём данных, обрабатываемых за единицу времени (throughput), объём RAM/ROM и объём аппаратных ресурсов, необходимых для аппаратной реализации (hardware area).

Ключевые слова: хеш-функция, диффузия, лавинный эффект, криптоанализ, запас стойкости, легковесная криптография, пропускная способность, аппаратная площадь.

Kirish

Kriptografik xesh funksiya ixtiyoriy uzunlikdagi xabarni belgilangan uzunlikdagi xesh qiymatiga akslantiradi va ma’lumot yaxlitligi, elektron raqamli imzo, kalit hosil qilish, autentifikatsiya hamda ko‘plab kriptografik protokollarning tayanch vositalaridan biri hisoblanadi. Xesh funksiyalarni loyihalashda faqat kolliziya, preimage va second-preimage hujumlariga bardoshlilikni ta’minlash yetarli emas. Xesh funksiyaning ichki almashtirishlari “reduced-round” kriptotahlilda yetarli xavfsizlik darajasiga ega bo‘lishi, shu bilan birga dasturiy va apparat platformalarda samarali bajarilishi talab etiladi [1,2].

SHA-3 standartida Keccak asosidagi permutatsiyaga asoslangan konstruktsiyaning qabul qilinishi xesh dizaynida sponge yondashuvining amaliy va nazariy ahamiyatini kuchaytirdi[1]. 2025-yilda NIST SP 800-232 orqali Ascon-Hash256 algoritmini resurslari cheklangan qurilmalar

uchun standartlashtirdi. Bu holat zamonaviy xesh funksiyalar uchun xavfsizlik, dasturiy samaradorlik va apparat xarajatlarini birgalikda ko‘rib chiqish zarurligini ko‘rsatdi [2]. Shuning uchun xesh funksiyalarni takomillashtirish masalasi “ko‘proq raund - ko‘proq xavfsizlik” ko‘rinishidagi bir o‘lchovli masala emas, balki xavfsizlik va xarajatlar orasidagi optimal nuqtani topish masalasiga aylandi.

Taklif etilayotgan “xarajatga nisbatan xavfsizlik” loyihalash metodikasi

Yangi xesh funksiyani ishlab chiqishda quyidagi ketma-ketlik taklif etiladi. Avval xavfsizlik darajasi va platformalar to‘plami belgilanadi. Keyin state size, rate/capacity yoki chaining value o‘lchami umumiy kolliziya va preimage hujumi talablaridan kelib chiqib tanlanadi. Nochiziqli qatlam uchun differensial taqsimot jadvali(Difference Distribution Table,DDT), chiziqli approksimatsiyalar jadvali (Linear Approximation Table,LAT), algebraik daraja va implementatsion xarajat bir vaqtda baholanadi. Chiziqli qatlam esa maksimal nazariy branch number emas, “aktiv S-boxlar sonining qo‘shimcha XOR/latencyga nisbati” bo‘yicha optimallashtiriladi. So‘ng minimal aktiv S-boxlar sonini aniqlash(Mixed-Integer Linear Programming, MILP), bul mantiqiy formulalarining qanoatlantiriluvchanlik masalasi (Boolean Satisfiability Problem, SAT) orqali 2, 3, 4 va undan yuqori raund chegaralar olinadi. Integral, rebound va invariant qidiruvlari bilan ushbu chegaralar mustaqil tekshiriladi. Differensial va chiziqli tahlil mezonlari hamda MILP asosidagi aktiv S-box chegaralari [3,4,6], rebound tahlili esa [5] asosida qaraladi.

Raundlar sonini tanlashda eng yaxshi ma’lum hujum qamrab olgan raundga shunchaki bir-ikki raund qo‘shish o‘rniga, xavfsizlik darajasining nisbiy koeffitsiyentidan foydalanish mumkin $\mu = (R - R_a)/R$. Bu ko‘rsatkich hujumning real vaqt/xotira murakkabligi bilan to‘ldirilishi kerak. Shu bilan birga har bir nomzod uchun cycles/byte, latency, throughput, RAM/ROM va algoirtmni qurilmada amalga oshirish xarajati(hardware area) o‘lchanib, Pareto front quriladi. Natijada faqat eng tez yoki eng katta xavfsizlik darajasiga ega variant emas, balki xavfsizlik quyi chegarasi yetarli bo‘lgan eng arzon variant tanlanadi.

Mazkur yondashuvning tahliliy yangiligi shundaki, diffuziya, avalanche effekti emas, balki statistik daraja qat’iy lavin mezoni (Strict Avalanche Criterion, SAC), bitlarning mustaqillik mezoni (Bit Independence Criterion, BIC) va Hamming masofasi, kriptotahliliy daraja aktiv S-boxlar, trail/hull chegaralari, algebraik daraja, integral/rebound margin, implementatsiya darajasi ushbu xossalarga erishish uchun sarflangan cycles, xotira va apparat maydoniga ustuvorlik beriladi. Shunday qilib, takomillashtirish natijasi bir ko‘rsatkichning o‘sishi emas, balki isbotlanadigan xavfsizlikning bir birlik hisoblash xarajatiga nisbatan oshishi bilan ifodalanadi. Avalanche/SAC mezonlarining klassik asoslari [7] da keltirilgan.

1-jadval.

Loyihalashda nazorat qilinadigan asosiy mezonlar

Yo‘nalish	Asosiy mezon	Dizayn talabi
Avalanche/ diffuziya	SAC≈0,5; BIC; raundma-raund tarqalish	50% natijani kriptotahliliy chegaralar bilan tasdiqlash
Differensial	DDT, p_max, minimal aktiv S-box	MILP/SAT bilan quyi chegara va yetarli raund darajasi
Chiziqli	LAT,maksimal korrelyatsiya, hull	Maskalar tez tarqalishi va aktiv nochiziqlilik
Algebraik	daraja, ANF, invariantlar	darajaning tez o‘sishi; past-darajali strukturani yo‘qotish

Integral/ rebound	zero-sum/balance; inbound/outbound	reduced-round distinguisherdan sezilarli to‘liq-raund darajasi
Strukturaviy	simmetriya, slide, rotational, fixed-point	konstanta, domain separation va tarmoqlararo aralashtirish
Software	cycles/byte, latency, throughput, RAM/ROM	turli xabar uzunligi va platformalarda benchmark
Hardware	GE/LUT, critical path, throughput, energy/bit	area–time va security-per-area muvozanati

Xulosa

Kriptografik xesh funksiyalarni takomillashtirishda asosiy maqsad avalanche hodisasini 50% ga yaqinlashtirish yoki raundlar sonini ko‘paytirish emas. Ilmiy asoslangan dizayn differensial, chiziqli, algebraik, integral, rebound va strukturaviy hujumlar uchun o‘lchanadigan xavfsizlik darajasini minimal implementatsiya xarajat bilan hosil qilishi kerak. Buning uchun nochiziqli qatlam, diffuziya qatlami, raund konstantalari va konstruktsiya darajasidagi mexanizmlar yagona tizim sifatida optimallashtiriladi. Taklif etilgan “xarajatga nisbatan xavfsizlik” metodikasi aktiv nochiziqli elementlar va reduced-round xavfsizlik chegaralarini cycles/byte, latency, throughput, RAM/ROM hamda hardware area bilan bog‘laydi. Natijada xesh funksiyani baholash “tez” yoki “avalanche xodisasi yetarli darajada” kabi alohida xulosalardan Pareto-optimal, qayta tekshiriladigan va platformaga mos dizayn qaroriga o‘tadi.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. NIST, 2015. DOI: 10.6028/NIST.FIPS.202. https://doi.org/10.6028/NIST.FIPS.202

2. Turan M.S., McKay K., Kang J., Kelsey J., Chang D. NIST SP 800-232: Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. NIST, 2025. DOI: 10.6028/NIST.SP.800-232. https://doi.org/10.6028/NIST.SP.800-232

3. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. Springer, 1993. DOI: 10.1007/978-1-4613-9314-6. https://doi.org/10.1007/978-1-4613-9314-6

4. Matsui M. Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology - EUROCRYPT ’93, LNCS 765, pp. 386–397, 1994. DOI: 10.1007/3-540-48285-7_33. https://doi.org/10.1007/3-540-48285-7_33

5. Mendel F., Rechberger C., Schläffer M., Thomsen S.S. The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl. Fast Software Encryption, pp. 260–276, 2009. DOI: 10.1007/978-3-642-03317-9_16. https://doi.org/10.1007/978-3-642-03317-9_16

6. Mouha N., Wang Q., Gu D., Preneel B. Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming. Inscrypt 2011, LNCS 7537, pp. 57–76, 2012. DOI: 10.1007/978-3-642-34704-7_5. https://doi.org/10.1007/978-3-642-34704-7_5

7. Webster A.F., Tavares S.E. On the Design of S-Boxes. Advances in Cryptology - CRYPTO ’85, LNCS 218, pp. 523–534, 1986. DOI: 10.1007/3-540-39799-X_41. https://doi.org/10.1007/3-540-39799-X_41

PARAMETRLI ALGEBRAGA ASOSLANGAN JAMOAVIY ELEKTRON RAQAMLI IMZO BARDOSHLIGINI OSHIRISH USULI VA ALGORITMI

Ortiqboyev A.M.
UNICON.UZ – Fan-texnika va marketing tadqiqotlari markazi

Annotatsiya. Ushbu maqolada parametrli algebraga asoslangan jamoaviy elektron raqamli imzo bardoshligini oshirish usuli bayon etildi va ushbu usul asosida takomillashtirilgan RSA jamoaviy elektron raqamli imzo algoritmi keltirildi.

Kalit so‘zlar: jamoaviy elektron raqamli imzo, elektron raqamli imzo, parametrli algebra, daraja parametri, kriptografik bardoshlilik, RSA algoritmi, jamoaviy oshkora kalit, diskret logarifmlash muammosi, faktorlash muammosi.

Аннотация. В данной статье описан метод повышения стойкости коллективной электронной цифровой подписи на основе алгебры с параметром, а также на базе этого метода приведен усовершенствованный алгоритм коллективной электронной цифровой подписи RSA.

Ключевые слова: коллективная электронная цифровая подпись, электронная цифровая подпись, параметрическая алгебра, параметр степени, криптографическая стойкость, алгоритм RSA, коллективный открытый ключ, проблема дискретного логарифмирования, проблема факторизации.

Kirish

Hozirgi kunda elektron raqamli imzo (ERI) turli sohalarda, shu jumladan, elektron hujjat aylanish tizimi, himoyalangan elektron xat aylanish tizimlari, masofaviy elektron hisobotlarni topshirish va boshqa tizimlarda autentifikatsiya masalalarida keng qo‘llanilishi sababli dolzarb ahamiyat kasb etmoqda. Shu kungacha ma’lum bo‘lgan an’anaviy ERI “karrali imzo” (direktor, buxgalter, yetakchi muhandis va sh.k.) yaratishga imkon beradi. Bunda imzolovchi jamoa a’zolari qancha ko‘p bo‘lsa, imzo o‘lchami ham shuncha ko‘p bo‘ladi va imzo qo‘yuvchilar va tekshiruvchilar ketma-ketliklarining tartiblari bir xil bo‘lishi shart.

Amaliyotda ERIdan bunday taxlitda foydalanish usuli har qachon ham yagona yechim bo‘lavermaydi. Ayniqsa, ERI biror jamoa tomonidan shakllantirilishi lozim bo‘lganda, jamoaviy oshkora kalit tushunchasidan foydalanib, ERI hosil etish qulaydir. Bunda ERI protokoli soddalashadi, ERI o‘lchami va uni shakllantirish, hamda tekshirish jarayonlariga vaqt sarfi an’anaviy ERIdan foydalanilganidan ortiq bo‘lmaydi. Ko‘rsatib o‘tilgan kamchiliklarni bartaraf etish uchun jamoaviy ERI (JERI) algoritmlari va protokollari ishlab chiqilgan [1-2].

O‘zbekiston Respublikasida raqamli hukumat shakllanayotgan hozirgi vaqtda jamoaviy loyihalarni ishlab chiqishda, elektron ovoz berishda, pasport haqiqiyligini ta’minlashda ERI algoritmlarining yangi toifasi hisoblangan JERI algoritmidan axborot xavfsizligini ta’minlashda foydalanish muhim ahamiyatga ega.

Agar hujjatga bir necha tomon imzo qo‘ysa, bunday ERI JERI deyiladi. JERI protokollari bir vaqtning o‘zida shartnomalarni va hujjatlar paketini imzolash muammosini hal etish uchun eng samarali vosita bo‘lib, imzolangan hujjatlardan amalda tezroq foydalanish imkoniyatini yaratadi.

Mavjud JERI algoritmlarining bardoshligini oshirish asosida quyidagi muammolarga tegishli shaxsiy kalitni topish murakkabligi yotadi [3-4]:

- diskret logarifm muammosining murakkabligi;

- faktorlash muammosining murakkabligi;
- elliptik egri chiziqda diskret logarifm muammosining murakkabligi;
- boshqa yangi muammolar murakkabligi [5].

Binobarin, shaxsiy kalit asosan modul uzunligi bilan aniqlanishi tufayli mavjud JERI algoritmlarining bardoshligini oshirish asosida modul binar uzunligini oshirish yotadi.

Boshqa yangi muammo sifatida daraja parametri mummosi [6] mazkur ilmiy ishda bardoshlikni oshirishning yangi muammosi sifatida qabul etilgan va uning bardoshlikni oshirish xususiyati asoslangan.

Asosiy qism

JERI bardoshligini oshirish usuli parametrli funksiyalar bilan bog‘liq yangi *muammolar murakkabligi bilan asoslanadi.* [5-6] da keltirilgan parametrli funksiya xossalari orasida asosan daraja parametri *R* ning maxfiyligi kriptografik tizim kriptobardoshligini oshirishga xizmat qiladi. Mazkur dissertatsiyada keltirilgan JERIda modul sifatida tub yoki tarkibli sondan foydalanilgan. JERI kriptobardoshligining ortishi bir tomonlama parametrli funksiya ifodasida qatnashadigan darajaga oshirish parametri (qisqacha, daraja parametri) *R* noqonuniy foydalanuvchilardan sir saqlanishiga asoslanadi.

Daraja parametri muammosi uchta murakkablik pog‘onasi bilan farqlanib, quyidagicha ta’riflanadi:

1-ta’rif. Agar parametrli algebra $(F_n; ®)$ da tashuvchi F_n ning elementlari *y* va *a* berilgan bo‘lsa, unda parametr *R* va daraja ko‘rsatkichi *e* topilsin**,** bu yerda F_n – *n* ta butun sonlardan tuzilgan chekli to‘plam, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ – *a* ni parametr *R* bilan *e*-darajasi ramzi, element *a* $a^{\backslash \omega} (mod\ n) \equiv 0$ shartini faqat $\omega = q$ bo‘lgandagina qanoatlantiradi, *q* – $\varphi(n)$ ning butun sonli bo‘luvchisi,

$\varphi(n)$ – *Eyler pi-funksiyasi* (murakkablikning ikkinchi pog‘onasiga oid muammo).

2-ta’rif. Agar parametrli algebra $(F_n; ®)$ da tashuvchi F_n ning elementlari *y, a* va daraja ko‘rsatkichi *e* berilgan bo‘lsa, unda parametr *R* topilsin**,** bu yerda F_n – *n* ta butun sonlardan tuzilgan chekli to‘plam, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ – *a* ni parametr *R* bilan *e*-darajasi ramzi, element *a* $a^{\backslash \omega} (mod\ n) \equiv 0$ shartini faqat $\omega = q$ bo‘lgandagina qanoatlantiradi, *q* – $\varphi(n)$ ning butun sonli bo‘luvchisi, $\varphi(n)$ – *Eyler pi-funksiyasi* (murakkablikning birinchi pog‘onasiga oid muammo).

Mazkur muammolarning yuzaga chiqishi bir tomonlama parametrli funksiyaning quyidagi 1-xossasi bilan bog‘liq:

$$a^{\backslash e} \equiv a * \Sigma_{i=0}^{i=e-1} F^i\ (mod\ n), \qquad (1)$$

bu yerda $F=1+R*a$, $n \in \{p, p_1 * p_2\}$.

Daraja parametri muammosiga berilgan 1-2-ta’riflarda noma’lumlar sonini e’tiborga olsak, muammoni hal etish murakkabligi o‘zaro mos tarzda ikkinchi va birinchi pog‘onaga oid deb hisoblash o‘rinlidir.

Parametr *R* berilganda qonuniy foydalanuvchilar uchun daraja parametri muammosi quyidagicha ta’riflanadi:

3-ta’rif. Agar parametrli algebra $(F_p; ®)$ da tashuvchi F_p ning elementlari *y* va *R* berilgan bo‘lsa, unda daraja ko‘rsatkichi *e* va element *a* topilsin**,** bu yerda F_p - *n* ta butun sonlardan tuzilgan chekli to‘plam, $y \equiv a^{\backslash e} (mod\ p)$, $^{\backslash e}$ - *a* ni parametr *R* bilan *e*-darajasi ramzi, element *a* $a^{\backslash \omega} (mod\ n) \equiv 0$ shartini faqat $\omega = q$ bo‘lgandagina qanoatlantiradi**,** *q* - $\varphi(n)$ ning butun sonli bo‘luvchisi, $\varphi(n)$ - *Eyler pi-funksiyasi*.

Muammolar uchun yuqorida keltirilgan ta’riflar *tashqi va ichki badniyat buzg‘unchilar uchun kriptoalgoritmlarning har xil bardoshlikka ega bo‘lishini ko‘rsatadi.*

Daraja parametri muammosining yuzaga kelishi tamoyilli yangicha yondashuvga asoslangan JERIlar yaratishga imkoniyat tug‘diradi.

Kriptobardoshligi daraja parametri muammosini hal etishning birinchi murakkablik pog‘onasiga asoslangan JERI tizimlarida modul $n \geq 2^{256}$, daraja ko‘rsatkichi tub son bo‘lib, $e \geq 2^{160}$ shartlariga javob berishi lozimligi tavsiya etiladi. Shu bilan bir qatorda, maxfiy parametr $2^{256} > R$, $R^{-1} \geq 2^{160}$ shartini qondirishi zarur.

Daraja parametri muammosining murakkabligini oshirish bardoshligi diskret logarifmlash muammosining murakkabligi bilan belgilanadigan JERI yaratilishiga olib keladi. Ma’lumki, murakkablik turlari qanchalik kam bo‘lsa, kriptotizim bardoshligi shunchalik yuqori bo‘ladi, chunki muammoning ko‘paygani bilan har doim ham bardoshlilik oshavermaydi. Shu sababdan JERIni loyihalashda optimal kriptotizim yagona muammoning murakkabligiga asoslangan kriptotizim bo‘lishiga e’tibor berish lozim.

Mazkur maqolada keltirilgan JERI tizimlarining bir qanchasida modul sifatida tub sondan foydalaniladi va ularning kriptobardoshligi daraja parametri muammosining murakkabligiga asoslangan. Shuningdek, ularning ba’zilarida maxfiy asos va/yoki maxfiy parametr ishlatiladi. Daraja parametri muammosi parametrning maxfiyligini, asosning esa maxfiy yoki oshkora bo‘lishini nazarda tutadi. Uning ta’rifida chekli maydon uchun parametrli hosil qiluvchi (generator, boshlang‘ich ildiz) elementi tushunchasidan foydalanilgan. Daraja parametri muammosining yuzaga kelishi kriptografiyada JERI tizimlarini yangicha yondashuvlar asosida yaratish imkoniyatini tug‘diradi. 2-, 1-murakkablik pog‘onasiga ega har bir daraja parametri muammosini yechish uchun avvalo parametr R ni topish kerak. Undan so‘ng bu muammoni diskret logarifm muammosiga keltirish mumkin. Ammo, parametr R ni ketma-ket tanlash usuli, ya’ni kuchli hujum usulidan o‘zgacha topish usuli hozirgacha ma’lum emas. Shuning uchun ham bu muammo yetarlicha murakkabdir.

Tadqiqotlar shuni ko‘rsatadiki, mavjud kriptografik algoritmlarni parametrli algebra asosida takomillashtirish imkoniyati mavjud. Quyida RSA algoritmiga asoslangan ERI asosida JERI shakllantirish va parametrli algebra asosida takomillashtirilgan RSA JERI algoritmi bayon etiladi.

RSA algoritmi asosida ham turlicha JERIlarni shakllantirish va haqiqqiylikka tekshirish algoritmlari keltirilgan. Ulardan biri Mihir Bellara (Mihir Bellare) va Grigoriy Neven (Gregory Neven)lar tomonidan ilgari surilgan quyidagi algoritm [7] hisoblanadi.

RSA algoritmi asosida JERI algoritmi

JERIni shakllantirish oddiy ERI kabi uch bosqichda amalga oshiriladi:

I bosqich – Tashkiliy bosqich.

1-qadam: p va q tub sonlar tanlanadi va $n=p*q$ hisoblanadi;

2-qadam: $\varphi(n)=(p-1)(q-1)$ Eyler funksiyasi hisoblanadi va e jamoaviy oshkora kalit va $d=x_1+x_2+\ldots+x_n$ n ta shaxsiy maxfiy kalitlar generatsiya qilinadi. Bu yerda $(x_1+x_2+\ldots+x_n)*e=1 \bmod \varphi(n)$.

II bosqich - JERI shakllantirish.

1-qadam: Imzolanadigan hujjatning xesh-obrazi H – xeshlash funksiyasi yordamida $h=H(M)$ hisoblanadi.

2-qadam: Jamoaning har bir a’zosi tomonidan x_i shaxsiy maxfiy kaliti yordamida JERIning o‘ziga tegishli qismini shakllantiradi (imzo qo‘yadi) $c_i = h^{x_i} \bmod n$.

3-qadam: Qabul qiluvchi tomon barcha imzolavchilardan qabul qilib olgan imzolarni jamlab $c=c_1*c_2*...*c_n$ JERIni hosil qiladi.

III bosqich - JERIni tekshirish.

1-qadam: Imzolanadigan hujjatning xesh-obrazi *H* – xeshlash funksiyasi yordamida *h=H(M)* hisoblanadi.

2-qadam: $h'=c^e \bmod n$ hisoblanadi.

3-qadam: *h'* va ma'lumotdan olingan *h* xesh-obrazi solishtiriladi: agar teng bo'lsa JERI haqiqqiy, aks holda haqiqiy emas hisoblanadi.

Quyida ushbu algoritmning parametrli algebra asosida takomillashirilgan varianti keltiriladi.

Parametrli algebra asosida takomillashtirilgan RSA JERI algoritmi

Taklif etilayotgan algoritmda *R* parametr qo'shish orqali hisoblash murakkabligi oshishi ta'minlangan:

I bosqich – Tashkiliy bosqich.

1-qadam: *p* va *q* tub sonlar tanlanadi va *n=p*q* hisoblanadi;

2-qadam: $\varphi(n)=(p-1)(q-1)$ Eyler funksiyasi hisoblanadi va *e* jamoaviy oshkora kalit va $d=x_1+x_2+...+x_n$ *n* ta shaxsiy maxfiy kalitlar generatsiya qilinadi.

Bu yerda $(x_1+x_2+...+x_n)*e=1 \bmod \varphi(n)$.

II bosqich - JERI shakllantirish.

1-qadam: Imzolanadigan hujjatning xesh-obrazi *H* – xeshlash funksiyasi yordamida *h=H(M)* hisoblanadi.

2-qadam: Jamoaning har bir a'zosi tomonidan x_i shaxsiy maxfiy kaliti yordamida JERIning o'ziga tegishli qismini shakllantiradi (imzo qo'yadi) $c_i = h^{\backslash x_i} \bmod n$. Bu yerda *R* parametr bilan parametrli darajaga oshirish amalidan foydalaniladi.

3-qadam: Qabul qiluvchi tomon barcha imzolavchilardan qabul qilib olgan imzolarni jamlab $c=c_1®c_2®...®c_n$ (® - parametrli ko'paytirish amali belgisi) JERIni hosil qiladi.

III bosqich - JERIni tekshirish.

1-qadam: Imzolanadigan hujjatning xesh-obrazi *H* – xeshlash funksiyasi yordamida *h=H(M)* hisoblanadi.

2-qadam: $h'=c^{\backslash e} \bmod n$ hisoblanadi.

3-qadam: *h'* va ma'lumotdan olingan *h* xesh-obrazi solishtiriladi: agar teng bo'lsa JERI haqiqqiy, aks holda haqiqqiy emas hisoblanadi.

Misol:

Tashkiliy bosqich:

$p=13, q=17, \quad n=p*q=221, \ \varphi(n)=192;$

$d=35, x_1=23, x_2=12, e=11;$

$R=2;$

JERIni shakllantirish:

$h=H(M)=18;$

$c_1=h^{\backslash 23}=18^{\backslash 23} \bmod 221=78;$

$c_2= h^{\backslash 12}=18^{\backslash 12} \bmod 221=22;$

$c=c_1*^{\backslash}c_2=78*^{\backslash}22=217;$

JERIni tekshirish (verifikatsiya):

$h=H(M)=18;$

$h'=c^{\backslash 11}=217^{\backslash 11} \bmod 221=18;$

$h=h'$.

JERI haqiqiy.

Xulosa

JERI bardoshligini oshirish usullarining tadqiqi shuni ko‘rsatdiki, mavjud JERI bardoshligi asosan diskret logarifmlash usuliga tegishli modul uzunligini oshirish, faktorlash usuliga tegishli modul uzunligini oshirish va EECh bazaviy nuqtalari tartibini oshirishga asoslangan. Ushbu maqolada JERI bardoshligini oshirish usuli parametrli funksiyalar bilan bog‘liq yangi muammolar murakkabligi bilan asoslanadi. JERIda modul sifatida tub yoki tarkibli sondan foydalanilgan. JERI kriptobardoshligining ortishi bir tomonlama parametrli funksiya ifodasida qatnashadigan darajaga oshirish parametri R ni noqonuniy foydalanuvchilardan sir saqlanishi hisobiga erishiladi. Bardoshligi faktorlash, diskret logarifmlash va EECh gruppasida diskret logarifmlash muammolarining murakkabligiga asoslangan JERI algoritmlari asosan maxsus apparatli kriptomodullarda amalga oshirilsa, bardoshlik eng yuqori chegarada bo‘ladi. Agar JERIni ishlab chiqishda dasturiy kriptomodullardan foydalanilsa ham unda vakolatli sub’ekt xizmatlaridan foydalangan holda mazkur maxfiy kattaliklarni dasturiy kriptomodulga o‘rnatish va yuqori bardoshlikka erishish mumkin.

Foydalanilgan adabiyotlar

1 Коллективная ЭЦП - специальный криптографический протокол на основе новой трудной задачи / Молдовян А.А., Молдовян Н.А. // Вопросы защиты информации. 2008. № 1.

2 Мирин А. Ю., Заболотный А. П., Молдовян У. А. Протокол коллективной подписи на основе сложности задачи факторизации // Материалы VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009.

3 Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005.

4 Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. Издательство: Диалектика, 2022.

5 Axmedova O.P. Parametrlar algebrasi asosida nosimmetrik kriptotizimlar yaratish usuli va algoritmlari // Nomzodlik dissertatsiya ishi, Toshkent-2007.

6 Хасанов Х.П. Криптографические системы на основе односторонних функций диапреобразования // Шестая ежегодная международная научно-практическая конференция PKI-Forum-2008: Программа конференции и тезисы выступлений – Санкт-Петербург, 2008.

PINN YORDAMIDA KIBERFIZIK TIZIMLARDA SENSOR MA'LUMOTLARI YAXLITLIGINI NAZORAT QILISH

Salayev A.K.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada kiberfizik tizimlarda sensor ma'lumotlarining fizik jihatdan izchilligini nazorat qilish uchun fizik qonuniyatlarga asoslangan neyron tarmoq (PINN) yondashuvi taklif etiladi. Nazorat sxemasi ishonchli ma'lumotlarda o'qitilgan model, mustaqil kalibrlash va kuzatuv bosqichlaridan tashkil topadi. Yupqa plastinkaning egilish tenglamasi asosida matematik qo'yilish, normallashtirilgan xatolik va ogohlantirish qoidasi shakllantiriladi. Analitik misol yordamida mezonning ishlashi va kuzatiluvchanlik cheklovi ko'rsatiladi. Fizik nomuvofiqlik kiberhujumning bevosita isboti emasligi asoslanadi. Ish uslubiy xarakterga ega; neyron tarmoqning tajribaviy aniqlash ko'rsatkichlari da'vo qilinmaydi.

Kalit so'zlar: kiberfizik tizim, PINN, sensor ma'lumotlari, yaxlitlik nazorati, anomaliya, yupqa plastinka, R-funksiyalar.

Аннотация. Предлагается подход к контролю физической согласованности сенсорных данных в киберфизических системах на основе физически информированной нейронной сети (PINN). Схема включает обучение на доверенных данных, независимую калибровку и мониторинг. Для модели изгиба тонкой пластины формулируются математическая постановка, нормированная ошибка и правило сигнализации. Аналитический пример иллюстрирует работу критерия и ограничение наблюдаемости. Показано, что физическое несоответствие само по себе не доказывает наличие кибератаки. Работа носит методический характер; экспериментальная точность обнаружения нейронной сетью не заявляется.

Ключевые слова: киберфизическая система, PINN, сенсорные данные, контроль целостности, аномалия, тонкая пластина, R-функции.

Kirish

Kiberfizik tizimda sensor o'lchovi boshqaruv qaroriga ta'sir qiladi. Harorat, siljish yoki bosimning noto'g'ri qiymati jarayon haqidagi tasavvurni buzishi mumkin. NIST qo'llanmasida operatsion texnologiyalar xavfsizligini ularning ishonchliligi, ishlash talablari va fizik xavfsizligi bilan birga ko'rish zarurligi ta'kidlanadi [1]. Shuning uchun uzatilgan paketning autentikligini tekshirishni o'lchovning fizik mazmunini baholash bilan to'ldirish foydali.

Tadqiqot maqsadi sensor qiymatlarini boshqaruvchi fizik modelga solishtirish uchun PINN asosidagi nazorat usulini ishlab chiqishdir. Amaliy obyekt sifatida yupqa plastinka tanlanadi. Bu qo'yilish termo-magnit-elektroelastik plastinkalarni modellashtirishga tayanch bo'la oladi, biroq mazkur ishda elektromagnit va termik bog'lanishlar hisobga olinmaydi. Asosiy natija nazorat mezoni, uni kalibrlash tartibi va ishlash chegaralarining matematik ifodasidir.

Muammo qo'yilishi va tahdid modeli

O'lchov qiymati fizik holat, odatiy shovqin, sensor nosozligi va tashqi o'zgartirishning yig'indisi sifatida tasvirlanadi. i-sensor va k-kuzatuv uchun quyidagi model olinadi:

$$y_{i,k} = H_i[u_k] + \varepsilon_{i,k} + d_{i,k} + a_{i,k}. \quad (1)$$

Bu yerda u fizik holat maydoni, H_i sensor operatori, ε o'lchash shovqini, d nosozlik yoki kalibrlash siljishi, a esa hujum tufayli kiritilgan o'zgarishdir. Siljish sensori uchun $H_i[u]$ nuqtadagi

egilish qiymatini beradi. Deformatsiya sensori ishlatilsa, operator tegishli hosilalar va sensorning fazoviy yo‘nalishini ham o‘z ichiga olishi kerak.

Tahdid modelida hujumchi ayrim sensor kanallarini o‘zgartira oladi, ammo ishonchli yuklama yozuvi, model parametrlari va nazorat dasturini to‘liq boshqara olmaydi, deb faraz qilinadi. Ushbu tayanchlardan birortasi qolmasa, fizik modelga mos soxta holatni haqiqiy holatdan ajratish mumkin bo‘lmasligi ehtimoli mavjud. Shuning uchun qaysi axborot ishonchli deb olinishi tizim loyihasida aniq belgilanadi.

Paketga autentifikatsiya kodi yoki raqamli imzo qo‘yilishi uning manbasi va uzatishdagi o‘zgarmaganligini tekshirishga xizmat qiladi. Ammo buzilgan sensorning o‘zi yolg‘on qiymatni qonuniy kalit bilan yuborishi mumkin. PINN nazorati bunday vaziyatda fizik izchillikni tekshiruvchi qo‘shimcha qatlam sifatida qaraladi. U kriptografik himoya, kirishni boshqarish yoki hodisalarni qayd etish mexanizmlarini almashtirmaydi.

Mavjud yondashuvlar va tadqiqotning o‘rni

Raissi, Perdikaris va Karniadakis PINN yondashuvida ma’lumotga moslashish bilan differensial tenglama talablarini birgalikda o‘qitish maqsadiga kiritgan [2]. Fizik qonunlar kam kuzatilgan nuqtalar orasidagi yechimni cheklashga yordam beradi. Biroq bu cheklovning mavjudligi zararli ma’lumotlar ta’siriga avtomatik bardoshlilikni anglatmaydi.

Falas, Konstantinou va Michael suv taqsimlash tizimi misolida PINNdan kiberfizik himoya maqsadida foydalanishni ko‘rsatgan [3]. Wong va hammualliflar esa sensor shovqinining PINN yechimiga ta’sirini o‘rgangan [4]. Bu ishlar fizik model bilan o‘lchovni birgalikda tahlil qilish imkoniyatini asoslaydi, lekin ularning natijalarini plastinka monitoringiga tajribasiz ko‘chirish mumkin emas.

Mazkur ish umumiy yondashuvni yupqa plastinka uchun aniqlashtiradi: modelga kiritiladigan ishonchli kattaliklar, tekshiriladigan sensorlar va ogohlantirish mezoni ajratiladi. Usulni yangi PINN arxitekturasi sifatida emas, fizik holatni baholashni xavfsizlik monitoringiga bog‘lovchi uslubiy sxema sifatida talqin qilish lozim.

Yupqa plastinka uchun fizik va neyron tarmoq modeli

Bir jinsli izotrop, kichik egilishli plastinka uchun kvazistatik Kirchhoff–Love modeli olinadi. Yuklama sekin o‘zgaradi va inertsiya ta’siri e’tiborga olinmaydi. Har bir k-kuzatuvdagi muvozanat quyidagicha yoziladi:

$$D\nabla^4 w_k(x,y) = q_k(x,y), \quad D = Eh^3/[12(1-\nu^2)]. \quad (2)$$

Bu yerda w egilish, q sirtga taqsimlangan ko‘ndalang yuklama, E Yung moduli, h qalinlik, ν Puasson koeffitsiyenti; $\nabla^4 w = w_{xxxx} + 2w_{xx\gamma\gamma} + w_{\gamma\gamma\gamma\gamma}$. Qattiq mahkamlangan chegarada w = 0 va $\partial w/\partial n = 0$ shartlari olinadi. Tez o‘zgaruvchi jarayonda ushbu model yetarli emas: inertsiya, zarur bo‘lsa so‘nish, boshlang‘ich shartlar va vaqt bo‘yicha kuzatuvlar qo‘shilishi kerak.

Neyron tarmoq $w\theta(x,y;s)$ egilish maydonini yaqinlashtiradi; s yuklamaning ishonchli parametrlari, θ o‘qitiladigan og‘irliklardir. Birgina yuklama uchun o‘qitilgan modelni barcha ish rejimlariga qo‘llash mumkin emas. Bir necha rejimda ishlash uchun parametrik o‘qitish sohasi oldindan belgilanadi va kuzatuv shu soha ichida bajariladi.

Tenglama, chegara va ma’lumot qoldiqlari alohida fizik birliklarga ega. Shu sababli koordinatalar L, egilish W_0, yuklama esa DW_0/L^4 masshtabida o‘lchamsizlashtiriladi. Yo‘qotish funksiyasida aynan shu o‘lchamsiz kattaliklar ishlatiladi:

$$L(\theta) = \lambda_f L_f + \lambda_b L_b + \lambda_d L_d. \quad (3)$$

$$L_f = \text{mean}[(\nabla^4 w_\theta - q)^2], \quad L_d = \text{mean}[(H_i[w_\theta] - y_i)^2]. \quad (4)$$

$\mathscr{D}$b chegaradagi egilish va normal hosila kvadratlarining o‘rtachasidan tuziladi. Musbat λ koeffitsiyentlar ishonchli validatsiya ma’lumotlari asosida tanlanadi. Avtomatik differensiallash hosilalarni hisoblashga xizmat qiladi. To‘rtinchi tartibli tenglama uchun yetarlicha silliq aktivatsiya, masalan tanh, tanlash zarur; bo‘lakli chiziqli aktivatsiya bu kuchli shakldagi qoldiq uchun mos emas.

Murakkab geometriyada R-funksiyalar yordamida chegarani ifodalash va uni sinov funksiyasiga kiritish mumkin. Geometriyani hisobga oluvchi funksiyalar bilan chegaraviy shartlarni aniq qo‘yish yondashuvi [5] da yoritilgan. Agar φ chegarada nol va yetarlicha silliq bo‘lsa, $w\theta = \varphi^2 N\theta$ ifoda qattiq mahkamlanishning ikkala shartini bajaradi. Ammo to‘rtinchi hosilalarni hisoblashda φ ning silliqligi alohida tekshiriladi; burchak yoki tutashish nuqtalaridagi muammo yo‘qolgan deb olinmaydi.

Model faqat ishonchli o‘qitish to‘plamida tayyorlanadi. Shubhali joriy o‘lchovni shu zahoti o‘qitishga qo‘shish taqiqlanadi: aks holda tarmoq zararli qiymatga moslashib, xatolikni yashirishi mumkin. Monitoring bosqichida parametrlar o‘zgartirilmaydi; yangilash faqat tekshirilgan ma’lumot va qayta validatsiyadan keyin amalga oshiriladi.

Yaxlitlikni nazorat qilish va ogohlantirish mezoni

Nazorat uchta mustaqil bosqichdan iborat: ishonchli o‘qitish, toza kalibrlash va keyingi kuzatuv. Vaqt qatorida ketma-ket davrlar shu tartibda ajratiladi. Bir xil davrga tegishli yaqin kuzatuvlarni tasodifiy bo‘lib yuborish ma’lumot sizishiga olib kelishi mumkin. Hujumli sinov namunalaridan chegara qiymatini tanlashda foydalanilmaydi.

Ishonchli yuklama s_k bo‘yicha model bashorati olinadi va sensor xatosi hisoblanadi. Har bir kanal uchun kalibrlash xatolari medianasi b_i hamda robust masshtabi σ_i aniqlanadi:

$$e_{i,k} = y_{i,k} - H_i[w_\theta(s_k)], \quad z_{i,k} = |e_{i,k} - b_i|/\sigma_i. \quad (5)$$

$$b_i = \mathrm{median}(e_i), \quad \sigma_i = \max[1{,}4826 \cdot \mathrm{MAD}(e_i), \sigma_{\min}]. \quad (6)$$

MAD medianadan mutlaq chetlanishlar medianasidir; σmin nolga yaqin maxrajni cheklovchi, sensor aniqligiga mos musbat qiymatdir. 1,4826 koeffitsiyenti normal taqsimot bilan masshtab mosligini beradi, ammo xatoliklar normal taqsimlanganini isbotlamaydi. σ_i amalda shovqin bilan birga model nomuvofiqligini ham aks ettiradi.

Tizim statistikasi $S_k = \max_i z_{i,k}$ ko‘rinishida olinadi. τ chegarasi kalibrlash davridagi S qiymatlarining tanlangan yuqori kvantili orqali belgilanadi. Maksimumni tizim bo‘yicha kalibrlash ko‘p sensor tekshirilganda yolg‘on ogohlantirishlarning yig‘ilib borishini hisobga olishga yordam beradi. Chegara yangi sensor qo‘shilganda yoki ish rejimi o‘zgarganda qayta tekshiriladi.

Bir martalik shovqin sakrashini ajratish uchun oxirgi L kuzatuvdan kamida m tasida $S_k > \tau$ bo‘lsa ogohlantirish berish taklif etiladi. L va m aniqlash kechikishi bilan yolg‘on signal orasidagi muvozanatni belgilaydi. Vaqt bo‘yicha bog‘liq ma’lumotlarda kvantilning o‘zi qat’iy ehtimollik kafolati bermaydi; yakuniy qoida mustaqil toza vaqt oralig‘ida tekshirilishi kerak.

1-jadval

Nazorat qatlamlarining vazifalari

Qatlam	Tekshiriladigan holat	Natijaning talqini
Paket nazorati	Autentiklik, vaqt belgisi va takrorlanish	Aloqa yoki hisob yozuvi bilan bog‘liq signal
PINN solishtiruvi	Sensor va fizik bashorat farqi	Fizik nomuvofiqlik haqida ogohlantirish

Qatlam	Tekshiriladigan holat	Natijaning talqini
Kontekst tahlili	Yuklama, sensor holati va tizim jurnallari	Hujum, nosozlik yoki rejim o‘zgarishini tekshirish

O‘zgarmas PINNning tenglama qoldig‘i sensor qiymati buzilganda avtomatik oshmaydi, chunki sensor o‘lchovi tarmoq chiqishiga qayta kiritilmayapti. Shuning uchun hujum indikatori sifatida (5) dagi o‘lchov farqi olinadi; fizik qoldiq esa model sifatini kuzatish uchun ishlatiladi. Bu ikki ko‘rsatkichning vazifalarini aralashtirish noto‘g‘ri xulosaga olib keladi.

Analitik misol va aniqlash chegaralari

Mezonni tekshirish uchun o‘lchamsiz $\Omega = (-1,1)^2$ kvadrat sohada $P(\xi) = (1 - \xi^2)^2$ va $w^*(x,y) = P(x)P(y)$ etalon maydon tanlanadi. Bu funksiya chegarada egilish va normal hosilaning nol bo‘lishini ta’minlaydi. $D = 1$ deb olingan o‘lchamsiz tenglama uchun unga mos yuklama differensiallash orqali hosil qilinadi:

$$q^* = 24P(y) + 2(-4 + 12x^2)(-4 + 12y^2) + 24P(x). \quad (7)$$

Bu tayyorlangan analitik yechim tekshiruv uchun xizmat qiladi; u faqat plastinkaning o‘z og‘irligidan hosil bo‘ladigan doimiy yuklama yechimi emas. Nuqtalardagi qiymatlar (7) ga mos egilish maydonidan hisoblanadi. Quyidagi misolda bashorat aynan w^*, $b_i = 0$, $\sigma_i = 0{,}02$ va $\tau = 3$ deb berilgan. Bu sonlar ko‘rsatma parametrlar bo‘lib, o‘qitilgan PINN yoki real sensor tajribasi natijasi emas.

2-jadval

Bir kuzatuv uchun mezonning analitik tekshiruvi

Sensor nuqtasi	Etalon w^*	O‘zgarish a	Kuzatuv y	$z = \lvert a \rvert / 0{,}02$
(0; 0)	1,0000	0,00	1,0000	0,0
(0,5; 0)	0,5625	0,10	0,6625	5,0
(0; 0,5)	0,5625	0,04	0,6025	2,0
(0,5; 0,5)	0,3164	−0,08	0,2364	4,0

Ikkinchi va to‘rtinchi sensor mezondan oshadi; uchinchi sensorning o‘zgarishi chegaradan past qoladi. $S = 5$ bo‘lgani uchun ushbu kuzatuv chegaradan oshgan deb belgilanadi. Biroq m ta takror talab qilinsa, bitta kuzatuv yakuniy ogohlantirish uchun yetmasligi mumkin. Jadvaldagi nol shovqin farazi faqat hisobni ochiq ko‘rsatish uchun ishlatilgan.

Misol ikki cheklovni ko‘rsatadi. Birinchidan, kichik zararli o‘zgarish kalibrlangan noaniqlik ichida qolishi mumkin. Ikkinchidan, +0,10 siljishni sensor nosozligi yoki hujum keltirib chiqargan bo‘lsa, (5) aynan bir xil natija beradi. Demak, fizik qoldiqning kattaligi zararli niyatni aniqlamaydi; sababni ajratish uchun mustaqil ma’lumot zarur.

Kuzatiluvchanlikning yanada jiddiy cheklovi chiziqli modelda ko‘rinadi. Agar w^* va q^* mos yechim bo‘lsa, $c \cdot w^*$ va $c \cdot q^*$ ham muvozanat tenglamasini bajaradi. Hujumchi barcha o‘lchovlarni va yuklama haqidagi ma’lumotni bir xil c koeffitsiyent bilan almashtira olsa, fizik izchillik saqlanadi. Ishonchli yuklama yoki himoyalangan tayanch sensor bo‘lmasa, bunday muvofiqlashtirilgan almashtirishni faqat shu model bilan aniqlab bo‘lmaydi.

O‘rta qismidan teshik ochilgan plastinkada geometriya va ichki chegara shartlari yangidan kiritiladi. Kvadrat uchun yuqoridagi polinom etalonni bunday sohaga ko‘chirish mumkin emas. Shuningdek, faqat chegaraga joylashtirilgan siljish sensorlari qattiq mahkamlangan holatda doim nol ko‘rsatadi; ichki deformatsiyani kuzatish uchun soha ichidagi informativ nuqtalar talab etiladi.

Tekshirish dasturi va xulosa

Keyingi hisoblash tajribasida etalon yechimdan hosil qilingan ma’lumotlar bilan o‘qitish, kalibrlash va sinov to‘plamlari ajratilishi kerak. Oddiy shovqin, doimiy siljish, sekin drift, qayta uzatish va muvofiqlashtirilgan almashtirish alohida ssenariylarda tekshiriladi. Qayta uzatishning qiymatga asoslangan aniqlanishi jarayonning o‘zgarishiga bog‘liq: statsionar rejimda eski va yangi o‘lchov bir xil bo‘lishi mumkin.

PINN detektori oddiy chegaraviy nazorat va ayni fizik modelning klassik sonli yechimiga asoslangan detektor bilan solishtiriladi. Aniqlash ulushi TP/(TP+FN), yolg‘on signal ulushi FP/(FP+TN), kechikish va hisoblash xarajati hisobotga kiritiladi. Hisob birligi sensor kuzatuvimi yoki butun hodisami, oldindan belgilanadi. O‘qitish va onlayn bashorat vaqti alohida beriladi; tez bashorat qimmat o‘qitish bosqichini bekor qilmaydi.

Taklif etilgan sxema PINNni sensor ma’lumotlarining fizik izchilligini tekshiruvchi qo‘shimcha vosita sifatida qo‘llaydi. Ishonchli tayanchlar, o‘lchamsiz fizik model va mustaqil kalibrlash usulning asosiy shartlaridir. Analitik misol chegara mezonining ishlashini ko‘rsatdi, ammo neyron tarmoqning aniqlash samaradorligini tasdiqlamaydi. Buni baholash uchun o‘qitish va mustaqil sinovlar bajarilishi zarur.

Yupqa plastinka modeli dissertatsiya doirasidagi RFM va PINN hisoblashlarini xavfsizlik monitoringi bilan bog‘lash imkonini beradi. To‘liq termo-magnit-elektroelastik holatga o‘tishda qo‘shimcha maydonlar, o‘zaro bog‘lanishlar va mustaqil o‘lchovlar kiritiladi. Fizik izchillik ogohlantirishni asoslaydi, lekin ma’lumotning autentikligini yoki hujum mavjudligini yakka o‘zi kafolatlamaydi.

Foydalanilgan adabiyotlar

1. Stouffer K. va boshq. Guide to Operational Technology (OT) Security. NIST SP 800-82 Rev. 3. 2023. DOI: 10.6028/NIST.SP.800-82r3.

2. Raissi M., Perdikaris P., Karniadakis G. E. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations. Journal of Computational Physics. 2019. Vol. 378. P. 686–707. DOI: 10.1016/j.jcp.2018.10.045.

3. Falas S., Konstantinou C., Michael M. K. Physics-Informed Neural Networks for Securing Water Distribution Systems. 2020. arXiv:2009.08842. https://arxiv.org/abs/2009.08842

4. Wong J. C., Chiu P.-H., Ooi C. C., My Ha Da. Robustness of Physics-Informed Neural Networks to Noise in Sensor Data. 2022. arXiv:2211.12042. https://arxiv.org/abs/2211.12042

5. Sukumar N., Srivastava A. Exact imposition of boundary conditions with distance functions in physics-informed deep neural networks. Computer Methods in Applied Mechanics and Engineering. 2022. Vol. 389. Article 114333. DOI: 10.1016/j.cma.2021.114333.

RSA VA ML-KEM ALGORITMLARINING KVANT TAHDIDLARIGA CHIDAMLILIGI HAMDA AMALIY CHEKLOVLARINING QIYOSIY TAHLILI

Mahmanazarova Z.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda klassik ochiq kalitli RSA algoritmi va NIST tomonidan 2024-yilda FIPS 203 standarti sifatida qabul qilingan ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) mexanizmining kvant hisoblash tahdidlariga chidamliligi qiyosiy tahlil qilingan. RSA xavfsizligining asosi bo‘lgan butun sonlarni faktorlash masalasi Shor algoritmi yordamida polinomial vaqtda yechilishi hamda so‘nggi baholarga ko‘ra RSA-2048 ni buzish uchun talab etiladigan kubitlar soni keskin kamaygani ko‘rsatilgan. ML-KEM xavfsizligining modulli panjaralarda xatolar bilan o‘rganish (Module-LWE) masalasiga tayanishi va unga qarshi samarali kvant algoritmi ma’lum emasligi asoslab berilgan. Algoritmlar kalit va shifrmatn o‘lchamlari, hisoblash samaradorligi, tarmoq protokollariga integratsiyalash, yon kanal hujumlariga moyillik va amaliy joriy etish nuqtai nazaridan solishtirilgan. ML-KEM ni klassik algoritmlar bilan gibrid rejimda bosqichma-bosqich joriy etish bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: RSA, ML-KEM, FIPS 203, postkvant kriptografiya, Shor algoritmi, Module-LWE, kalit inkapsulyatsiyasi, gibrid kalit almashinuvi.

Abstract. This thesis presents a comparative analysis of the resistance to quantum-computing threats of the classical public-key algorithm RSA and of ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), standardized by NIST as FIPS 203 in 2024. It is shown that the integer factorization problem underlying RSA is solvable in polynomial time by Shor’s algorithm, and that recent resource estimates have sharply reduced the number of qubits required to break RSA-2048. The security of ML-KEM is substantiated by its reliance on the Module Learning With Errors (Module-LWE) problem, for which no efficient quantum algorithm is known. The algorithms are compared in terms of key and ciphertext sizes, computational efficiency, integration into network protocols, susceptibility to side-channel attacks and practical deployment. Recommendations are given for the phased deployment of ML-KEM in hybrid mode together with classical algorithms.

Keywords: RSA, ML-KEM, FIPS 203, post-quantum cryptography, Shor’s algorithm, Module-LWE, key encapsulation, hybrid key exchange.

Kirish

Zamonaviy axborot-kommunikatsiya tizimlarida ma’lumotlar maxfiyligi asosan ochiq kalitli kriptografiyaga tayanadi: TLS, SSH, VPN protokollarida, elektron raqamli imzo va ochiq kalitlar infratuzilmasida (PKI) kalit almashinuvi uchun RSA va elliptik egri chiziqlarga asoslangan algoritmlar keng qo‘llaniladi. Biroq P. Shor tomonidan taklif etilgan kvant algoritmi [1] faktorlash va diskret logarifmlash masalalarini polinomial vaqtda yechish imkonini beradi. Shu sababli yetarli quvvatga ega kriptografik ahamiyatli kvant kompyuteri (CRQC) yaratilishi bilan ushbu algoritmlar xavfsizligini butunlay yo‘qotadi.

Muammoning dolzarbligi «hozir yig‘ib ol, keyin deshifrla» (Harvest Now, Decrypt Later – HNDL) tahdidi bilan yanada kuchayadi: buzg‘unchi bugun shifrlangan trafikni yozib olib, kelajakda uni kvant kompyuter yordamida ochishi mumkin. M. Moska tengsizligiga ko‘ra, agar ma’lumotning maxfiylik muddati (x) va yangi kriptotizimga o‘tish muddati (y) yig‘indisi CRQC

paydo bo‘lishigacha qolgan vaqtdan (z) katta bo‘lsa, ya’ni $x + y > z$ bo‘lsa, tizim allaqachon xavf ostida hisoblanadi [2]. Shu munosabat bilan AQSh Standartlar va texnologiyalar milliy instituti (NIST) 2024-yil avgustida dastlabki postkvant standartlarini, jumladan kalit inkapsulyatsiyasi uchun FIPS 203 (ML-KEM) standartini e’lon qildi [3]. NIST IR 8547 hujjati loyihasida esa RSA va ECC algoritmlarini 2030-yildan keyin eskirgan, 2035-yildan keyin esa taqiqlangan deb belgilash rejalashtirilgan [4].

Ushbu tezisning maqsadi RSA va ML-KEM algoritmlarini kvant tahdidlariga chidamlilik hamda amaliy cheklovlar nuqtai nazaridan qiyosiy tahlil qilish va ularni joriy etish bo‘yicha tavsiyalar ishlab chiqishdan iborat.

RSA algoritmining kvant tahdidlari oldidagi zaifligi

RSA xavfsizligi $n = p \cdot q$ ko‘rinishidagi katta modulni tub ko‘paytuvchilarga ajratish murakkabligiga asoslanadi. Klassik hisoblashda eng samarali usul – umumiy son maydoni g‘alviri (GNFS) subeksponensial murakkablikka ega bo‘lib, unga ko‘ra RSA-2048 taxminan 112 bitli, RSA-3072 esa 128 bitli klassik xavfsizlik darajasini ta’minlaydi [15]. Shor algoritmi esa faktorlashni modul bo‘yicha darajaga ko‘tarish funksiyasining davrini kvant Furye almashtirishi yordamida topish masalasiga keltiradi va uni $O((\log n)^3)$ tartibidagi kvant amallar bilan yechadi [1]. Demak, kalit uzunligini oshirish kvant tahdidga qarshi samarali chora emas: modul uzunligi ikki baravar oshirilganda hujum narxi faqat polinomial ravishda o‘sadi.

Hujum uchun zarur resurslar baholari so‘nggi yillarda sezilarli darajada kamaydi. C. Gidney va M. Ekerå RSA-2048 ni taxminan 20 million shovqinli fizik kubit yordamida 8 soat ichida faktorlash mumkinligini ko‘rsatgan bo‘lsa [5], 2025-yilda C. Gidney bu talabni bir milliondan kam shovqinli kubit va bir haftadan kam vaqtgacha pasaytirdi [6]. Hozirgi kvant protsessorlari bu darajadan hali ancha uzoq bo‘lsa-da, resurs talablarining tez kamayishi tahdidni nazariy emas, balki oldindan rejalashtirilishi lozim bo‘lgan amaliy xavf sifatida ko‘rishni taqozo etadi.

Bundan tashqari RSA ning klassik muhitdagi amaliy cheklovlari ham mavjud: PKCS#1 v1.5 to‘ldirish sxemasiga qarshi Bleichenbacher hujumi va uning ROBOT kabi zamonaviy ko‘rinishlari [7]; RSA kalit transportida oldinga maxfiylik (forward secrecy) yo‘qligi, shu sababli bu rejim TLS 1.3 dan olib tashlangan; kalit generatsiyasining sekinligi hamda yuqori xavfsizlik darajalari uchun kalit uzunligining keskin o‘sishi (256 bitli xavfsizlik uchun 15360 bitli modul talab etiladi) [15].

ML-KEM mexanizmining tuzilishi va kvantga chidamliligi

ML-KEM CRYSTALS-Kyber algoritmi asosida ishlab chiqilgan bo‘lib, uning xavfsizligi modulli panjaralarda xatolar bilan o‘rganish (Module Learning With Errors, M-LWE) masalasining murakkabligiga tayanadi [3, 8]. Algoritm $R_{//q//} = \mathbb{Z}_{//q//}[X]/(X^{256} + 1)$, $q = 3329$ halqasi ustida ishlaydi, ko‘phadlarni ko‘paytirish esa sonli-nazariy almashtirish (NTT) yordamida tezlashtiriladi. Asosiy shifrlash sxemasi K-PKE faqat tanlangan ochiq matnli hujumlarga (IND-CPA) chidamli bo‘lib, Fujisaki–Okamoto almashtirishi va yashirin rad etish (implicit rejection) mexanizmi orqali tanlangan shifrmatnli hujumlarga (IND-CCA2) chidamli KEM ga aylantiriladi. Standartda uchta parametr to‘plami belgilangan: ML-KEM-512, ML-KEM-768 va ML-KEM-1024; ular mos ravishda NIST ning 1, 3 va 5-xavfsizlik kategoriyalariga (AES-128, AES-192 va AES-256 ga ekvivalent) mos keladi. Barcha to‘plamlarda umumiy sir uzunligi 32 baytni tashkil etadi.

M-LWE masalasi uchun Shor algoritmiga o‘xshash polinomial vaqtli kvant algoritmi ma’lum emas. Eng samarali ma’lum hujumlar panjara bazisini reduksiyalash (BKZ) va eng qisqa

vektorni izlash (SVP) algoritmlariga asoslanadi; kvant usullar, masalan, elak (sieving) algoritmlarida Grover tipidagi qidiruvdan foydalanish, hujum murakkabligi ko‘rsatkichini faqat nisbatan kichik koeffitsiyentga kamaytiradi [8, 9]. Parametrlar ushbu kamayishni hisobga olgan holda xavfsizlik zaxirasi bilan tanlanganligi sababli ML-KEM kvant hujumchi modelida ham o‘z xavfsizligini saqlaydi.

RSA va ML-KEM ning qiyosiy tahlili

1-jadvalda RSA va ML-KEM parametr to‘plamlarining xavfsizlik darajalari hamda kalit va shifrmatn o‘lchamlari keltirilgan [3, 15].

1-jadval

Xavfsizlik darajalari va ma’lumotlar o‘lchamlari (baytlarda)

Algoritm	Klassik xavfsizlik	Kvant hujumga chidamlilik	Ochiq kalit	Shifrmatn	Maxfiy kalit
RSA-2048	112 bit	Yo‘q (Shor)	256*	256	≈1 190**
RSA-3072	128 bit	Yo‘q (Shor)	384*	384	≈1 770**
ML-KEM-512	1-kat. (≈AES-128)	Ha	800	768	1 632
ML-KEM-768	3-kat. (≈AES-192)	Ha	1 184	1 088	2 400
ML-KEM-1024	5-kat. (≈AES-256)	Ha	1 568	1 568	3 168

** modul uzunligi; ** PKCS#1 DER formatidagi CRT parametrlari bilan taxminiy qiymat.*

Jadvaldan ko‘rinadiki, ML-KEM-768 ning ochiq kaliti RSA-3072 nikidan taxminan 3 baravar, shifrmatni esa 2,8 baravar katta. Hisoblash samaradorligi bo‘yicha esa vaziyat teskari: ML-KEM amallari NTT asosida bajarilib, AVX2 bilan optimallashtirilgan realizatsiyalarda kalit generatsiyasi, inkapsulyatsiya va dekapsulyatsiyaning har biri bir necha o‘n ming protsessor takti tartibida bajariladi [10]. RSA-2048 da ochiq kalit bilan shifrlash ($e = 65537$) tez bo‘lsa-da, maxfiy kalit bilan deshifrlash millionlab taktni, kalit generatsiyasi esa tub sonlarni izlash tufayli o‘nlab–yuzlab millisekundni talab qiladi. Resursi cheklangan qurilmalarda ham ML-KEM ning optimallashtirilgan realizatsiyalari (masalan, ARM Cortex-M4 uchun pqm4 loyihasi) bir necha kilobayt stek xotirasi bilan ishlay oladi [11]. Boshqacha aytganda, ML-KEM hisoblash yukini kamaytiradi, ammo tarmoq orqali uzatiladigan ma’lumot hajmini oshiradi. Algoritmlarning sifat ko‘rsatkichlari bo‘yicha qiyosiy tavsifi 2-jadvalda keltirilgan.

2-jadval

RSA va ML-KEM ning sifat ko‘rsatkichlari bo‘yicha taqqoslanishi

Mezon	RSA	ML-KEM
Matematik asos	Butun sonlarni faktorlash	Module-LWE masalasi
Eng samarali kvant hujumi	Shor algoritmi – polinomial vaqt	Ma’lum emas (faqat kichik koeffitsiyentli tezlashuv)
Funksionallik	Shifrlash, imzo, kalit transporti	Faqat kalit inkapsulyatsiyasi
Kalit va shifrmatn o‘lchami	Kichik	RSA ga nisbatan 3–6 baravar katta
Hisoblash tezligi	Deshifrlash va kalit generatsiyasi sekin	Barcha amallar tez

Mezon	RSA	ML-KEM
Deshifrlash xatoligi	Mavjud emas	Juda kichik (ML-KEM-768 uchun $\approx 2^{-164}$)
Kriptotahlil tarixi	45 yildan ortiq	LWE – 2005-yildan, Kyber – 2017-yildan
Yon kanal xavflari	Vaqt va quvvat tahlili, to‘ldirish orakuli	Vaqt hujumlari (KyberSlash), quvvat tahlili, xatolik kiritish
Standart holati	NIST: 2030-yildan eskirgan, 2035-yildan taqiqlangan (reja)	FIPS 203 (2024)

Amaliy cheklovlar va joriy etish masalalari

RSA ning asosiy cheklovi – kvant hujumlariga chidamsizlik – parametrlarni o‘zgartirish orqali bartaraf etilmaydi, shuning uchun uni almashtirish muqarrar. ML-KEM ni joriy etishda esa quyidagi amaliy cheklovlar inobatga olinishi lozim.

Birinchidan, ma’lumotlar hajmining ortishi. ML-KEM-768 kaliti qo‘shilganda TLS 1.3 ning ClientHello xabari bir necha kilobaytgacha kattalashib, bir nechta TCP segmentiga bo‘linadi; ayrim eskirgan oraliq tarmoq qurilmalari bunday xabarlarni noto‘g‘ri qayta ishlashi kuzatilgan. UDP asosidagi protokollarda (DTLS, QUIC, IKEv2) esa paket fragmentatsiyasi qo‘shimcha kechikish va yo‘qotishlarga olib kelishi mumkin.

Ikkinchidan, yon kanal hujumlari. 2023–2024-yillarda aniqlangan KyberSlash zaifligi bir qator realizatsiyalarda maxfiy qiymatga bog‘liq bo‘lish amali bajarilish vaqti orqali maxfiy kalitni tiklash mumkinligini ko‘rsatdi [12]. Shu sababli doimiy vaqtli dasturlash, maskalash va xatolik kiritishga qarshi himoya choralari majburiy hisoblanadi.

Uchinchidan, kriptotahlil tarixining nisbatan qisqaligi. NIST tanlovining yakuniy bosqichiga chiqqan SIKE algoritmining 2022-yilda oddiy kompyuterda buzilishi [13] postkvant algoritmlarga ehtiyotkorlik bilan yondashish zarurligini ko‘rsatdi, garchi panjara asosidagi kriptografiya ancha puxta o‘rganilgan bo‘lsa-da.

To‘rtinchidan, funksional cheklov: ML-KEM faqat kalit inkapsulyatsiyasini ta’minlaydi. Raqamli imzo uchun alohida ML-DSA (FIPS 204) yoki SLH-DSA (FIPS 205) algoritmlari zarur bo‘lib, bu sertifikatlar va PKI infratuzilmasi hajmining oshishiga olib keladi.

Ushbu xavflarni kamaytirishning amaliy yechimi – gibrid kalit almashinuvidir. Masalan, X25519MLKEM768 sxemasida klassik X25519 va ML-KEM-768 dan olingan umumiy sirlar kalit hosil qilish funksiyasi orqali birlashtiriladi; natijada ulardan biri buzilgan taqdirda ham seans kaliti xavfsizligi saqlanib qoladi [14]. Bu sxema 2024-yildan boshlab yetakchi brauzerlar va kontent yetkazib berish tarmoqlarida keng qo‘llanilmoqda.

Xulosa

O‘tkazilgan tahlil natijasida quyidagi xulosalarga kelindi. RSA kvant tahdidlariga nisbatan tubdan zaif bo‘lib, bu zaiflikni kalit uzunligini oshirish bilan bartaraf etib bo‘lmaydi; RSA-2048 ni buzish uchun zarur kvant resurslar baholarining tez kamayishi va HNDL tahdidi uzoq muddatli maxfiylik talab etiladigan ma’lumotlar uchun o‘tishni hozirdanoq boshlashni taqozo etadi. ML-KEM kvant hujumlariga chidamli bo‘lib, hisoblash tezligi bo‘yicha RSA dan ustun, biroq kattaroq kalit va shifrmatn o‘lchamlari, yon kanal hujumlariga sezgir realizatsiyalar va kriptotahlil tarixining nisbatan qisqaligi bilan bog‘liq amaliy cheklovlarga ega.

Amaliyot uchun quyidagilar tavsiya etiladi: tashkilotlarda qo‘llanilayotgan kriptografik algoritmlarni inventarizatsiya qilish; uzoq muddat saqlanadigan ma’lumotlar bilan ishlovchi

tizimlarda birinchi navbatda ML-KEM-768 ni X25519 bilan gibrid rejimda joriy etish; faqat doimiy vaqtli va sertifikatlangan realizatsiyalardan foydalanish; tizimlarni kripto-moslashuvchanlik (crypto-agility) tamoyili asosida loyihalash. Resursi cheklangan IoT va videokuzatuv qurilmalari uchun esa ML-KEM ning xotira va energiya sarfini hisobga olgan holda optimallashtirilgan realizatsiyalarini tanlash muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Journal on Computing. – 1997. – Vol. 26, No. 5. – P. 1484–1509.
2. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? // IEEE Security & Privacy. – 2018. – Vol. 16, No. 5. – P. 38–41.
3. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. – Gaithersburg: NIST, 2024. – DOI: 10.6028/NIST.FIPS.203.
4. Moody D. et al. Transition to Post-Quantum Cryptography Standards: NIST IR 8547 (Initial Public Draft). – Gaithersburg: NIST, 2024.
5. Gidney C., Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits // Quantum. – 2021. – Vol. 5. – P. 433.
6. Gidney C. How to factor 2048 bit RSA integers with less than a million noisy qubits // arXiv preprint arXiv:2505.15917. – 2025.
7. Böck H., Somorovsky J., Young C. Return of Bleichenbacher's Oracle Threat (ROBOT) // Proc. 27th USENIX Security Symposium. – 2018. – P. 817–849.
8. Bos J., Ducas L., Kiltz E. et al. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM // Proc. IEEE European Symposium on Security and Privacy (EuroS&P). – 2018. – P. 353–367.
9. Albrecht M.R., Player R., Scott S. On the concrete hardness of Learning with Errors // Journal of Mathematical Cryptology. – 2015. – Vol. 9, No. 3. – P. 169–203.
10. Avanzi R., Bos J., Ducas L. et al. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation (version 3.02). – 2021.
11. Kannwischer M.J., Rijneveld J., Schwabe P., Stoffelen K. pqm4: Testing and benchmarking NIST PQC on ARM Cortex-M4 // IACR Cryptology ePrint Archive. – 2019. – Report 2019/844.
12. Bernstein D.J., Bhargavan K., Bhasin S. et al. KyberSlash: Exploiting secret-dependent division timings in Kyber implementations // IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2025. – Vol. 2025, No. 2.
13. Castryck W., Decru T. An efficient key recovery attack on SIDH // Advances in Cryptology – EUROCRYPT 2023. LNCS 14008. – Springer, 2023. – P. 423–447.
14. Kwiatkowski K., Kampanakis P., Westerbaan B., Stebila D. Post-quantum hybrid ECDHE-MLKEM key agreement for TLS 1.3 // IETF Internet-Draft draft-ietf-tls-ecdhe-mlkem. – 2025.
15. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Part 1 Rev. 5. – Gaithersburg: NIST, 2020.

SHA-256 VA SHA-512 HESH FUNKSIYALARINING IKKINCHI PROOBRAZGA BARDOSHLILIGIGA XABAR UZUNLIGINING TA'SIRI

Xaydarov T.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Merkle–Damgård konstruksiyasiga asoslangan SHA-256 va SHA-512 funksiyalarida xabar uzunligining ikkinchi proobraz hujumi xarajatiga ta'siri tahlil qilindi. Kelsey–Schneier bahosi bir xil bayt hajmidagi xabarlar uchun hisoblanib, NIST xavfsizlik mezoni bilan solishtirildi. Bir mebibaytdan bir eksbibaytgacha bo'lgan diapazonda hujumning yetakchi daraja ko'rsatkichlari SHA-256 uchun 243 dan 203 gacha, SHA-512 uchun 500 dan 460 gacha kamayadi. Natijalar klassik hisoblash modeli va hujumning resurs farazlari doirasida talqin qilinadi.

Kalit so'zlar: Merkle–Damgård, SHA-256, SHA-512, ikkinchi proobraz, xabar uzunligi, Kelsey–Schneier, kompressiya funksiyasi.

Аннотация. Проанализировано влияние длины сообщения на стоимость поиска второго прообраза для SHA-256 и SHA-512 на основе конструкции Меркла–Дамгора. Оценка Келси–Шнайера рассчитана для сообщений одинакового размера в байтах и сопоставлена с критерием безопасности NIST. В диапазоне от одного мебибайта до одного эксбибайта показатели ведущей степени стоимости атаки уменьшаются с 243 до 203 для SHA-256 и с 500 до 460 для SHA-512. Результаты интерпретируются в классической модели вычислений с учётом ресурсных предпосылок атаки.

Ключевые слова: Меркл–Дамгор, SHA-256, SHA-512, второй прообраз, длина сообщения, Келси–Шнайер, функция сжатия.

Kirish

Hesh funksiyasining ikkinchi proobrazga bardoshliligi berilgan M xabar uchun undan farqli, lekin bir xil heshga ega M′ xabarni topish qiyinligini ifodalaydi. Bunda boshlang'ich xabar oldindan belgilangan; kolliziya qidiruvida esa ikkala xabarni ham tanlash mumkin. Shu sababli kolliziya, proobraz va ikkinchi proobraz hujumlarining xarajatlarini bitta xavfsizlik ko'rsatkichi sifatida ishlatish to'g'ri emas.

SHA-256 va SHA-512 parametrlarining standart ta'rifi FIPS 180-4 da berilgan [1]. Ularning iterativ tuzilishida uzun xabar ko'plab oraliq holatlarni hosil qiladi. Kelsey va Schneier bu xususiyatdan foydalanib, n-bit ichki holatli Merkle–Damgård funksiyalarida uzun xabar uchun ikkinchi proobraz topishning umumiy usulini ko'rsatgan [2]. Mazkur tezisning maqsadi ushbu bahoda xabar hajmi va blok uzunligi ta'sirini ajratib, ikki algoritmni teng bayt hajmida solishtirishdir.

Tahlil modeli va algoritm parametrlari

Tahlilda klassik hisoblash modeli, to'liq SHA-256 va SHA-512 hamda bitta oldindan berilgan nishon xabar ko'rib chiqildi. Qisqartirilgan qadamli kriptoanaliz va kvant hujumlari ushbu hisobga kiritilmadi. n ichki holat va chiqish uzunligini, B esa xabar blokining bit uzunligini bildiradi. Jadvaldagi barcha hajmlar padding, ya'ni to'ldirish qo'shilishidan oldingi xabarga tegishli.

1-jadval

Tahlil uchun zarur SHA-2 parametrlari [1]

Parametr	SHA-256	SHA-512
Ichki holat va chiqish, n (bit)	256	512
Xabar bloki, B (bit / bayt)	512 / 64	1024 / 128

Ruxsat etilgan xabar uzunligi (bit)	< 264	< 2128

Xabar hajmi V = 2^q bayt bo‘lsa, to‘liq ma’lumot bloklari soni SHA-256 uchun 2^{q-6}, SHA-512 uchun 2^{q-7} ga teng. Demak, bir xil xabar SHA-256 da ikki baravar ko‘p blokdan iborat. Hisoblarda MiB, GiB, TiB, PiB va EiB birliklari mos ravishda 2^{20}, 2^{30}, 2^{40}, 2^{50} va 2^{60} bayt sifatida olindi. EiB satri kundalik fayl hajmi emas, nazariy chegaralarni tekshirish ssenariysidir.

Hujum xarajatini hisoblash usuli

Kelsey–Schneier usulida turli uzunlikdagi, bir xil oraliq holatga olib keladigan kengaytiriluvchi xabar quriladi. Keyin bog‘lovchi blok yordamida nishon xabarning oraliq holatlaridan biriga o‘tiladi va uning qolgan qismi ulanadi. Kengaytiriluvchi qism uzunligi moslashtirilgani sababli yakuniy uzunlik maydoni ham nishon xabarnikiga teng bo‘ladi [2]. Bu mexanizm padding mavjudligini hisobga oladi.

Taxminan 2^k blokli nishon uchun manbada quyidagi klassik xarajat bahosi keltirilgan. C kompressiya funksiyasini hisoblashlar soni bilan o‘lchanadi; u bajarilish vaqti yoki energiya sarfi emas [2]:

$$C(n,k) \approx k \cdot 2^{n/2+1} + 2^{n-k+1} \quad (1)$$

Birinchi had kengaytiriluvchi xabarni qurish, ikkinchisi bog‘lovchi blokni qidirish xarajatini ifodalaydi. Nishon xabarni ko‘rib chiqish hamda oraliq holatlarni saqlash uchun ham resurs kerak. Jadval (1) formuladagi yetakchi hadlar bahosini beradi; to‘ldirish bloklari va konstruksiyaning kichik qo‘shimcha uzunliklari bu asimptotik hisobda e’tiborga olinmaydi. Jadvalning eng kichik ssenariysida ham bloklar soni minglab birlikni tashkil qiladi.

Hisoblashda katta sonlarni bevosita yaratish o‘rniga ularning ikkilik logarifmi olindi. a = n/2 + 1 + $\log_2 k$ va b = n − k + 1 deb belgilansa, quyidagi barqaror ifoda qo‘llanadi:

$$E(n,k) = \log_2 C(n,k) = \max(a,b) + \log_2(1 + 2^{-|a-b|}) \quad (2)$$

(2) ifoda Python yordamida hisoblandi. Bu amaliy hujumni bajarish tajribasi emas, mavjud nazariy formulani sonli baholashdir. O‘rganilgan diapazonda b hadi ustun keladi; natijalar butun daraja ko‘rsatkichi aniqligida yaxlitlandi. Hujum modeli kompressiya natijalarini tasodifiyga yaqin deb qarash va yetarli xotiradan foydalanish farazlariga tayanadi [2].

Hisoblash natijalari va qiyosiy tahlil

2-jadval

Teng bayt hajmidagi xabarlar uchun (1) formula bo‘yicha muallif hisoblari

Xabar hajmi	k SHA-256	k SHA-512	E ≈ $\log_2$C SHA-256	E ≈ $\log_2$C SHA-512
1 MiB (220 bayt)	14	13	243	500
1 GiB (230 bayt)	24	23	233	490
1 TiB (240 bayt)	34	33	223	480
1 PiB (250 bayt)	44	43	213	470
1 EiB (260 bayt)	54	53	203	460

Jadvalda bir TiB xabar uchun baho SHA-256 da taxminan 2^{223}, SHA-512 da 2^{480} kompressiya hisobiga teng. Xabar hajmi 2^{10} marta oshirilganda k o‘n birlikka ortadi va bog‘lovchi qidiruvning yetakchi darajasi o‘n birlikka kamayadi. Shunday qilib, bir MiB dan bir EiB gacha hajmning o‘sishi ikkala algoritmda ham E ni 40 birlikka pasaytiradi. Bu pasayish biror amaliy hujum muvaffaqiyati kuzatilganini anglatmaydi.

Teng bayt hajmida k qiymatlari bir birlikka farq qiladi. Ikkinchi had ustun bo‘lgan diapazonda (1) formuladan quyidagi bog‘lanish kelib chiqadi:

$$E_{256} \approx 263 - q, \quad E_{512} \approx 520 - q \quad (3)$$

Shu sababli jadvaldagi daraja ko‘rsatkichlari farqi 257 ga teng. Buning 256 birligi ichki holat uzunliklari farqidan, yana bir birligi esa SHA-512 blokining ikki baravar kattaligidan kelib chiqadi. Mazkur farq faqat tanlangan kompressiya-so‘rov modelidagi hujum bahosiga tegishli. Kompressiya amallarining protsessor vaqti bir xil emasligi uchun uni real bajarilish tezligi nisbati deb talqin qilib bo‘lmaydi.

NISTning joriy Hash Functions sahifasida SHA-256 va SHA-512 uchun ikkinchi proobraz xavfsizlik baholari mos ravishda 256 − L(M) va 512 − L(M) ko‘rinishida berilgan; L(M) xabar bloklari sonining ikkilik logarifmiga bog‘liq [3]. Masalan, bir TiB xabar uchun bu mezonlar 222 va 479 bit bo‘ladi. Ular 2-jadvaldagi 223 va 480 bilan zid emas: (1) formuladagi ikkinchi had 2^{n-k+1} koeffitsiyentini saqlaydi, NISTning soddalashtirilgan daraja bahosi esa n − k ni ishlatadi.

Natijalarni qo‘llash chegaralari

Hisoblar hujum xarajatining ma’lum usul bo‘yicha bahosidir; ular har qanday hujum uchun qat’iy pastki chegarani isbotlamaydi. Ayniqsa, kompressiya-so‘rovlar soni xotira narxini to‘liq ifodalamaydi. Nishonning oraliq holatlari va kengaytiriluvchi xabarni qurishdagi qidiruv tuzilmalari katta hajmdagi xotirani talab qilishi mumkin. Shu bois faqat E sonidan apparat xarajati yoki hujumni bajarish muddati chiqarilmaydi.

Bir EiB xabar SHA-256 standartining ruxsat etilgan uzunlik chegarasidan oshmaydi: uning bit hajmi 2^{63} bo‘lib, 2^{64} dan kichik [1]. Biroq bunday xabarni bitta yaxlit nishon sifatida qayta ishlashning o‘zi amaliy cheklovdir. SHA-512 ning kattaroq maksimal xabar uzunligini SHA-256 bilan teng bayt hajmidagi taqqoslashga aralashtirish noto‘g‘ri xulosaga olib keladi. Juda katta va turlicha nishonlar uchun olingan darajalar alohida shartlari bilan berilishi kerak.

Uzun xabar muammosining protokol darajasidagi ahamiyati FIPS 205 da ham aks etgan. Standartning A-ilovasida SHA2 parametrlaridagi H_msg hisoblashda MGF1 kirishiga R va PK.seed qo‘shilishi ko‘p nishonli, uzun xabarga qaratilgan ikkinchi proobraz hujumlarini yumshatish bilan izohlanadi [4]. Bu holat xabar uzunligi va protokol tuzilishini birga baholash zarurligini ko‘rsatadi. Biroq SLH-DSA ning umumiy xavfsizligini ushbu tezisdagi bitta nishonli formula bilan aniqlab bo‘lmaydi.

Xulosa

Teng bayt hajmidagi xabarlar uchun Kelsey–Schneier bahosi hisoblanganda xabar hajmining har ikki baravar ortishi, ikkinchi had ustun bo‘lgan diapazonda, hujumning yetakchi darajasini taxminan bir birlikka kamaytiradi. Bir MiB–bir EiB oralig‘ida SHA-256 uchun E ≈ 243–203, SHA-512 uchun E ≈ 500–460 olindi. Bir xil hajmda 257 birlik farq ichki holat uzunligi va blok o‘lchamining qo‘shma ta’sirini ifodalaydi. Hesh tanlashda chiqish uzunligi bilan birga nishon xabar hajmi, hujum modeli va xotira farazlarini ko‘rsatish zarur. Natijalar SHA-2 ga qarshi bajarilgan amaliy hujum emas, Merkle–Damgård konstruksiyasining nazariy xavfsizlik tahlilidir.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. Secure Hash Standard (SHS): FIPS PUB 180-4. - Gaithersburg: NIST, 2015. - DOI: 10.6028/NIST.FIPS.180-4.

2. Kelsey J., Schneier B. Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work // Advances in Cryptology - EUROCRYPT 2005. - LNCS. Vol. 3494. - Springer, 2005. - P. 474–490. - DOI: 10.1007/11426639_28.

3. National Institute of Standards and Technology. Hash Functions [Elektron resurs]. - URL: https://csrc.nist.gov/projects/hash-functions (murojaat sanasi: 11.10.2026).

4. National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard: FIPS 205. - Gaithersburg: NIST, 2024. - DOI: 10.6028/NIST.FIPS.205.

O‘zMSt 285:2024 STANDARTIDAGI XESHLASH ALGORITMLARI: ARXITEKTURASI, MATEMATIK ASOSLARI VA DASTURIY AMALGA OSHIRISH SAMARADORLIGI

Xudoykulov Z.T., Qutlimurotov A.H.
Muhammad al-Xorazmiy nomidagi TATU

Annotatsiya. Maqolada O‘z DSt 1106:2009 o‘rniga 2024-yilda qabul qilingan O‘zMSt 285:2024 milliy standartidagi ikki xeshlash algoritmi tahlil qilinadi. 1-algoritm modul arifmetikasidagi parametrli algebra amallariga asoslangan va 128 hamda 256 bitli rejimlarga ega; 2-algoritm 64 bitli blokli shifrga asoslangan bosqich funksiyasidan foydalanadi va tuzilishi jihatidan Rossiya Federatsiyasining GOST R 34.11-94 davlat standarti bilan mos keladi. Algoritmlarning arxitekturasi, parametrlari va matematik asosi bayon qilingan, parametrli teskarilashning kvadratik tartibni saqlash xossasi va kalitning *R* parametriga qo‘yiladigan juftlik sharti asoslangan. Mustaqil C va Python implementatsiyalari standart ilovalaridagi nazorat misollari bilan tasdiqlangan, standart matnidagi noaniqliklar va bosma xatolar ko‘rsatilgan. Tezkorlik o‘lchovlari 1-algoritmning 2-algoritmga nisbatan taxminan 16–18 marta sekinligini ko‘rsatdi; bu farqni belgilovchi hisoblash sarfi baholangan.

Kalit so‘zlar: xesh-funksiya, O‘zMSt 285:2024, parametrli algebra, parametrli teskarilash, GOST R 34.11-94, nazorat misoli, dasturiy amalga oshirish, tezkorlik.

Аннотация. В статье анализируются два алгоритма хэширования национального стандарта O‘zMSt 285:2024, принятого в 2024 году взамен O‘z DSt 1106:2009. Алгоритм 1 основан на операциях параметрической алгебры в модулярной арифметике и имеет 128- и 256-битный режимы; алгоритм 2 использует шаговую функцию на основе 64-битного блочного шифра и по структуре совпадает с ГОСТ Р 34.11-94. Описаны архитектура, параметры и математическая основа алгоритмов, обоснованы свойство сохранения 2-адического порядка при параметрическом обращении и требование чётности параметра *R* ключа. Независимые реализации на C и Python подтверждены контрольными примерами приложений стандарта; указаны неоднозначности и опечатки в тексте стандарта. Измерения показали, что алгоритм 1 примерно в 16–18 раз медленнее алгоритма 2; оценены вычислительные затраты, определяющие это различие.

Ключевые слова: хэш-функция, O‘zMSt 285:2024, параметрическая алгебра, параметрическое обращение, ГОСТ Р 34.11-94, контрольный пример, программная реализация, производительность.

Kirish

Xesh-funksiya (hash function) ixtiyoriy uzunlikdagi xabarni qayd etilgan uzunlikdagi qiymatga akslantiradi va elektron raqamli imzo, ma’lumotlar yaxlitligini nazorat qilish hamda kalitlarni hosil qilish mexanizmlarining tarkibiy qismi hisoblanadi. Kriptografik xesh-funksiyadan asl obrazni topishga bardoshlilik (preimage resistance), ikkinchi asl obrazni topishga bardoshlilik (second preimage resistance) va kolliziyaga bardoshlilik (collision resistance) talab qilinadi; *n* bitli ideal funksiya uchun tegishli umumiy hujumlar murakkabligi 2^n, 2^n va $2^{n/2}$ ga teng [1].

O‘zbekistonda xeshlash funksiyasini belgilovchi O‘zMSt 285:2024 standarti O‘zbekiston standartlar institutining 2024-yil 23-sentabrdagi 38/MSt-sonli buyrug‘i bilan tasdiqlangan, 2024-yil 23-oktabrdan amalga kiritilgan va O‘z DSt 1106:2009 o‘rniga ishlab chiqilgan [2]. Standart matematik asosi bo‘yicha farq qiluvchi ikki algoritmni belgilaydi. Maqolaning maqsadi - ularning arxitekturasi, parametrlari va matematik asosini qiyosiy tahlil qilish, standart matnini nazorat

misollari asosida tekshirish natijalarini bayon etish hamda dasturiy amalga oshirishda tezkorlikni belgilovchi omillarni baholash.

Algoritmlarning arxitekturasi va parametrlari

Ikkala algoritm iterativ tuzilishga ega: xabar qayd etilgan uzunlikdagi bloklarga bo‘linadi, bloklar siqish funksiyasi (compression function) orqali ketma-ket qayta ishlanadi, so‘ngra xabar uzunligi va NY (Checksum – nazorat summasi) qo‘shimcha bloklar sifatida beriladi. Bu Merkle–Damgård sxemasining (Merkle–Damgård construction) [3, 4] uzunlik va nazorat summasi bilan kengaytirilgan varianti hisoblanadi. Asosiy parametrlar 1-jadvalda keltirilgan.

1-jadval

O‘zMSt 285:2024 algoritmlarining asosiy parametrlari [2]

Parametr	1-algoritm, $p = 256$	1-algoritm, $p = 16$	2-algoritm
Matematik asos	parametrli algebra, mod 256	parametrli algebra, mod 16	64 bitli blokli shifr
Blok / kalit / xesh, bit	256 / 256 / 256	128 / 128 / 128	256 / – / 256
Ishlov birligi	bayt, 4×8 massiv	yarim bayt, 4×8 massiv	64 va 16 bitli so‘zlar
Bir blokka raundlar	10	10	4 shifrlash × 32 raund
Nochiziqli element	parametrli teskarilash, B-ilova jadvali	parametrli teskarilash	O‘rniga qo‘yish jadvali $\pi_1 \ldots \pi_8$
Yakunlovchi bloklar	uzunlik, NY	uzunlik, NY	L, Σ
Nazorat misoli	A-ilova	yo‘q	C-ilova (2 ta)

1-algoritmda holat (state) va bosqich kaliti (round key) 4×8 o‘lchamli massiv sifatida ifodalanadi. Xabarning b ta asosiy blokiga uzunlik bloki va NY bloki, ya’ni asosiy bloklarning 2^{256} modul bo‘yicha yig‘indisi qo‘shiladi. Birinchi blok boshlang‘ich holat bo‘lib xizmat qiladi; qolgan $b + 1$ blokning har biri uchun Qo‘sh va BaytZichlash o‘zgartirishlari juftligidan so‘ng 10 ta raund bajariladi. Raund Aralash, Qo‘sh, SurHolat, SurKalit va TuzilmaKalit o‘zgartirishlaridan iborat, 8- va 9-raundlarda kirish bloki qayta kiritiladi [2]. BaytZichlash $p = 16$ da XOR (Exclusive OR – istisno qiluvchi YOKI) amalidan, $p = 256$ da esa B-ilovadagi 256 elementli zichlash jadvalidan foydalanadi. Standartga ko‘ra $p = 16$ rejimi kalitli, $p = 256$ rejimi kalitsiz xeshlash funksiyasi sifatida qo‘llanadi, biroq psevdokodda har ikki holatda k kalit ishlatiladi va 256 bitli nazorat misoli ham aniq kalit bilan berilgan [2].

1-algoritmning matematik asosi va xossalari

1-algoritmning nochiziqli yadrosi - modul $p = 2^n$ ($n \in \{4, 8\}$) bo‘yicha (A, B, R) parametrli algebra (parametric algebra) teskarilash amali va uning uch karra qo‘llanishidan hosil bo‘ladigan -3 darajaga ko‘tarish [2]:

$$a^{\backslash -1} \equiv -A \cdot a \cdot (B + R \cdot a)^{-1} \pmod{p}, \quad (1)$$

$$a^{\backslash -3} \equiv ((a^{\backslash -1})^{\backslash -1})^{\backslash -1} \pmod{p}. \quad (2)$$

Qo‘sh(holat, holatn) o‘zgartirishi ikkala massivning har bir elementiga (2) amalini qo‘llaydi; A va B koeffitsiyentlari sherik massiv elementlari yig‘indisi J, toqlashtirilgan elementlar ko‘paytmasi K va Δ tuzatmalar orqali hisoblanadi. Aralash o‘zgartirishi holat va kalitning 4×4 yarimlarini diamatritsa (diamatrix) ko‘paytmasi bilan aralashtiradi; standartda bu amal oddiy matritsa ko‘paytmasiga nisbatan bitta kirish elementi o‘zgarganda o‘zgaradigan chiqish elementlari sonini 1,5–1,75 marta oshirishi qayd etilgan. Standartda parametrlar noma’lum bo‘lganda (2) ni teskarilash diskret logarifm masalasidan ko‘proq hisoblash sarfini talab qilishi ta’kidlanadi, biroq bu tasdiqning formal isboti standart matnida keltirilmagan [2].

Formulalar tahlilidan dasturiy tajribada ham tasdiqlangan quyidagi xossalar kelib chiqadi.

Birinchidan, K koeffitsiyenti toq sonlar ko‘paytmasiga 0 yoki 10 qo‘shib hosil qilinadi, shuning uchun u doim toq, $B = K - 2a$ ham doim toq bo‘ladi. Agar R toq bo‘lsa, toq a uchun $B +$

Ra juft bo‘ladi va uning 2^n modul bo‘yicha teskarisi mavjud emas. Demak, algoritm aniqlangan bo‘lishi uchun $R = k[1]$ juft bo‘lishi zarur. Standartning 5.1.2-bandi faqat kalitning ikkinchi yarim bayti (bayti) juft va 4…10 (10…120) oralig‘ida bo‘lishini talab qiladi, *R* ga oid shart esa aniq ko‘rsatilmagan [2].

Ikkinchidan, Δ tuzatmasi *A* koeffitsiyentini doim toq qiladi. *A* va $B + Ra\ 2^n$ modul bo‘yicha teskarilanuvchi bo‘lgani uchun (1) dan $a^{\backslash -1} = u \cdot a$ kelib chiqadi, bu yerda *u* - toq son. Bundan nolga teng bo‘lmagan har bir element uchun parametrli teskarilash uning kvadratik tartibini (2-adic valuation), ya’ni oxiridagi nol bitlar sonini, xususan juft-toqligini saqlashi kelib chiqadi. Natijada ikkinchi daraja uchun *A* ham doim toq bo‘lib, standartdagi «$A_{2h} \equiv 0$ bo‘lsa, $A_{2h} = 1$» qoidasi hech qachon bajarilmaydi, Δ sharti ikki xil o‘qilganda esa ($J_{1h} + J_{2h}$ yoki $J_{1hn} + J_{2hn}$) natija o‘zgarmaydi. Tasodifiy kirishlarda o‘tkazilgan $3{,}7 \cdot 10^5$ ta tekshiruvda bu xossa buzilmadi. Shunday qilib, Qo‘sh o‘zgartirishi elementlarning quyi bitlarini aralashtirmaydi, bu vazifa BaytZichlash jadvali va Aralash o‘zgartirishi zimmasiga tushadi; kriptotahlil (cryptanalysis) uchun bu tuzilmaviy xossa alohida e’tiborga loyiq.

Uchinchidan, standart matnining A-ilovadagi nazorat misoli (test vector) bilan solishtirilishi quyidagilarni ko‘rsatdi. B-ilovadagi zichlash jadvalining 7 ta elementi (15, 32, 47, 111, 127, 207, 255-o‘rinlar) o‘n oltilik emas, o‘nlik sanoq tizimida yozilgan (masalan, «14» = 0x0E); shunday o‘qilganda jadvalning har bir 16 elementli satri 0…15 sonlarining o‘rin almashtirishiga aylanadi. *R* ning kalitning birinchi bayti ekanligi va holat massivining satr bo‘yicha to‘ldirilishi faqat nazorat misoli orqali bir qiymatli aniqlanadi. A-ilovada bitta bosma xato («sc» o‘rniga «cc») mavjud. Ushbu aniqlashtirishlar bilan A-ilovadagi yakuniy xesh va barcha 118 ta oraliq massiv bayt aniqligida takrorlandi.

2-algoritmning tuzilishi va xavfsizligi

2-algoritmning $\chi(M, H)$ qadam funksiyasi (step function) uch qismdan iborat [2]. Kalitlarni generatsiya qilishda *H* va *M* so‘zlaridan chiziqli *A*, *P* o‘zgartirishlar va C_3 konstanta yordamida to‘rtta 256 bitli $K_1 \ldots K_4$ kalit hosil qilinadi. Shifrlovchi o‘zgartirishda *H* ning to‘rtta 64 bitli qismi O‘zMSt 270:2024 [5] algoritmi bo‘yicha oddiy almashtirish rejimida (electronic codebook mode) K_i kalitlarda shifrlanadi. C-ilovada shifrlash GOST (Государственный стандарт – davlat standarti) 28147 bo‘yicha bajarilgani ko‘rsatilgan; bu algoritm 64 bitli blok, 256 bitli kalit va 32 raundga ega [6]. Aralashtiruvchi ψ akslantirishi 16 bitli so‘zlar ustidagi siljitish registri (shift register) bo‘lib, qadam funksiyasi quyidagicha aniqlanadi:

$$\chi(M, H) = \psi^{61}(H \oplus \psi(M \oplus \psi^{12}(S))), \qquad (3)$$

bu yerda, *S* - to‘rtta shifrmatn konkatenatsiyasi. Barcha bloklardan so‘ng $\chi(L, H)$ va $\chi(\Sigma, H)$ hisoblanadi; *L* - xabar uzunligi, Σ - bloklarning 2^{256} modul bo‘yicha yig‘indisi.

Kalitlar generatsiyasi, ψ akslantirishi va yakunlovchi protsedura GOST R 34.11-94 ning RFC (Request for Comments – sharhlar uchun so‘rov) 5831 hujjatidagi tavsifi [7] bilan mos keladi. C-ilovadagi $\pi_1 \ldots \pi_8$ almashtirish uzellari RFC 5831 da faqat test misollari uchun berilgan o‘rniga qo‘yish bloklari (S-box) bilan bir xil. Mustaqil implementatsiya C.3.1 va C.3.2 nazorat misollarining yakuniy qiymatlarini hamda 42 ta oraliq qiymatdan ($K_1 \ldots K_4$, *S*, *YE*) 38 tasini aynan takrorladi; qolgan 4 tasining bosma xato ekanligi qo‘shni qiymatlar orqali isbotlandi. Masalan, C.3.1 dagi K_4 ning chop etilgan qiymati bilan shifrlash keyingi chop etilgan s_4 ni bermaydi, hisoblangan qiymat esa aynan beradi. C-ilovadagi ikkala nazorat misoli (xabarlar, nol boshlang‘ich vektor va yakuniy xesh qiymatlari) RFC 5831 ning 7.3-bandidagi misollar bilan bir xil [7].

Demak, 2-algoritmga GOST R 34.11-94 bo‘yicha ma’lum kriptotahlil natijalari bevosita taalluqli: taxminan 2^{105} murakkablikdagi kolliziya hujumi va 2^{192} murakkablikdagi asl obrazni topish hujumi [8] umumiy chegaralar (2^{128} va 2^{256}) dan past, biroq amalda bajarib bo‘lmaydigan darajada qoladi. Chiziqli va additiv nazorat summalari Merkle–Damgård sxemasini umumiy hujumlardan sezilarli himoya qilmasligi ko‘rsatilgan [9]; bu xulosa 1-algoritmdagi NY bloki uchun ham tegishli. Rossiya Federatsiyasida GOST R 34.11-94 2013-yil 1-yanvardan GOST R 34.11-2012 bilan almashtirilgan [10]. Bundan tashqari, O‘zMSt 285:2024 C.1 almashtirish uzellari

va H boshlang‘ich vektorini faqat tekshirish misollari uchun tavsiya etadi [2]; o‘zaro moslashuvchanlik (interoperability) uchun amaliy qiymatlar alohida qayd etilishi lozim.

Dasturiy amalga oshirish va tezkorlik

Tahlil uchun ikkala algoritmning C99 tilidagi kutubxonasi va Python tilidagi mustaqil namunaviy implementatsiyasi (reference implementation) ishlab chiqildi; ular 0…4096 bayt uzunlikdagi 430 ta xabarda bir xil natija berdi. 128 bitli rejim uchun standartda nazorat misoli bo‘lmagani sababli uning to‘g‘riligi faqat shu o‘zaro moslik bilan tasdiqlangan.

1-algoritmda bir blokni qayta ishlash 22 ta Qo‘sh chaqiruvini o‘z ichiga oladi; har bir chaqiruv 64 element ustida uchtadan parametrli teskarilash bajaradi, ya’ni bir blokka 4224 ta modul teskarilash to‘g‘ri keladi. J va K kattaliklar butun massiv bo‘yicha hisoblangani sababli teskarilash darajalari ketma-ket bajariladi. 2-algoritmda bir blokka 4 ta shifrlash (128 raund) va 74 ta ψ siljitish to‘g‘ri keladi.

Implementatsiyada elementlar 8 bitli ishorasiz turda saqlanadi va mod p amali ($p-1$) niqob bilan bajariladi. Toq x ning 2^8 modul bo‘yicha teskarisi kengaytirilgan Yevklid algoritmi o‘rniga Nyuton iteratsiyasi (Newton iteration) $y \leftarrow y(2 - xy)$ ning ikki qadami bilan topiladi: $x^2 \equiv 1 \pmod 8$ bo‘lgani uchun $y_0 = x$ dan boshlab aniq bitlar soni $3 \to 6 \to 12$ ga oshadi. 2-algoritmda almashtirish uzellari va 11 bitga siklik surish to‘rtta 256 elementli jadvalga birlashtirildi. O‘lchovlar Intel Xeon 2,8 GHz protsessorli virtual mashinada (bitta oqim), Linux va gcc 13.3 muhitida o‘tkazildi; har bir qiymat -O2 uchun 7 ta, -O3 uchun 5 ta o‘lchovning medianasi (2-jadval).

2-jadval

C implementatsiyaning tezkorlik ko‘rsatkichlari

Algoritm	32 baytli xabar xeshi, µs	1 MB, MB/s (gcc -O2)	1 MB, MB/s (-O3 -march=native)	Bir blokdagi asosiy amallar
1-algoritm, $p = 256$	38,7	1,72	3,88	22 Qo‘sh, 4224 teskarilash
1-algoritm, $p = 16$	54,9	0,84	2,00	22 Qo‘sh, 4224 teskarilash
2-algoritm	4,6	27,3	31,1	4 shifrlash, 74 ψ

Uzun xabarlarda 1-algoritm ($p = 256$) 2-algoritmdan taxminan 16–18 marta sekin. $p = 16$ rejimi yana ikki marta sekinroq, chunki blok 16 baytdan iborat, bir blokdagi amallar soni esa o‘zgarmaydi. Qisqa xabarlarda yakunlovchi bloklar hal qiluvchi: 32 baytli xabar uchun 1-algoritm 2 ta, 2-algoritm 3 ta siqish chaqiruvini bajaradi. Optimallashtirishning -O3 -march=native rejimida kompilyator element bo‘yicha mustaqil hisoblashlarni SIMD (Single Instruction, Multiple Data – bitta buyruq bilan ko‘p ma’lumotni qayta ishlash) buyruqlariga o‘tkazishi hisobiga 1-algoritm tezligi 2,2–2,4 marta oshadi; 2-algoritmda o‘sish 15 % dan oshmaydi, chunki shifrlash raundlari ketma-ket bog‘liqlikka ega. Elementlarni 64 bitli turda saqlovchi va teskarini Yevklid algoritmi bilan hisoblovchi dastlabki implementatsiya 1-algoritm uchun 0,18 MB/s ko‘rsatgan; yuqoridagi usullar natijani o‘zgartirmagan holda tezlikni taxminan 10 marta oshirdi. 1-algoritmda bir daraja doirasidagi 32 ta teskarilash o‘zaro bog‘liq emas, 2-algoritmda esa to‘rtta shifrlash mustaqil bajariladi; bu ikkala algoritmni parallel hisoblash orqali yanada tezlashtirish imkonini beradi.

Xulosa

O‘zMSt 285:2024 matematik asosi turlicha bo‘lgan ikki algoritmni birlashtiradi: 1-algoritm parametrli algebraga, 2-algoritm esa tuzilishi va nazorat misollari bo‘yicha GOST R 34.11-94 bilan mos keluvchi blokli shifr asosidagi sxemaga tayanadi.

1-algoritm uchun R parametrining juftligi zarur shart ekanligi va parametrli teskarilash nolmas elementlarning kvadratik tartibini saqlashi ko‘rsatildi; shu sababli standartdagi ayrim tarmoqlanish shartlari hech qachon bajarilmaydi. Standartning keyingi tahririda R ga qo‘yiladigan shartni, B-ilova qiymatlarining sanoq tizimini va massivni to‘ldirish tartibini aniq belgilash, A- va

C-ilovalardagi bosma xatolarni tuzatish hamda 128 bitli rejim uchun nazorat misoli kiritish maqsadga muvofiq.

2-algoritmga GOST R 34.11-94 bo‘yicha ma’lum kriptotahlil natijalari taalluqli; amaliy qo‘llashda almashtirish uzellari va boshlang‘ich vektor qiymatlarini qayd etish talab etiladi.

Dasturiy tezkorlik jihatidan 1-algoritm 2-algoritmdan bir tartibga sekin; uning samaradorligini oshirishning asosiy yo‘nalishlari - modul teskarilashni tezlashtirish va massiv elementlari bo‘yicha parallel hisoblash.

Foydalanilgan adabiyotlar

1. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. - Boca Raton: CRC Press, 1996.
2. O‘zMSt 285:2024. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi. - Rasmiy nashr. - Toshkent: O‘zbekiston standartlar instituti, 2024.
3. Merkle R. C. One Way Hash Functions and DES // Advances in Cryptology - CRYPTO ’89. LNCS. Vol. 435. - Springer, 1990. - P. 428–446.
4. Damgård I. B. A Design Principle for Hash Functions // Advances in Cryptology - CRYPTO ’89. LNCS. Vol. 435. - Springer, 1990. - P. 416–427.
5. O‘zMSt 270:2024. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi. - Toshkent: O‘zbekiston standartlar instituti, 2024.
6. Dolmatov V. (Ed.). GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms. RFC 5830. - IETF, March 2010. - https://www.rfc-editor.org/rfc/rfc5830
7. Dolmatov V. (Ed.). GOST R 34.11-94: Hash Function Algorithm. RFC 5831. - IETF, March 2010. - https://www.rfc-editor.org/rfc/rfc5831
8. Mendel F., Pramstaller N., Rechberger C., Kontak M., Szmidt J. Cryptanalysis of the GOST Hash Function // Advances in Cryptology - CRYPTO 2008. LNCS. Vol. 5157. - Springer, 2008. - P. 162–178. - DOI: 10.1007/978-3-540-85174-5_10
9. Gauravaram P., Kelsey J. Linear-XOR and Additive Checksums Don’t Protect Damgård-Merkle Hashes from Generic Attacks // Topics in Cryptology - CT-RSA 2008. LNCS. Vol. 4964. - Springer, 2008. - P. 36–51. - DOI: 10.1007/978-3-540-79263-5_3
10. Dolmatov V. (Ed.), Degtyarev A. GOST R 34.11-2012: Hash Function. RFC 6986. - IETF, August 2013. - https://www.rfc-editor.org/rfc/rfc6986

ML-DSA VA SLH-DSA RAQAMLI IMZO ALGORITMLARINING AMALIY SAMARADORLIGINI QIYOSIY TADQIQ QILISH

Axmedova O.P.
UNICON.UZ Fan-texnika va marketing tadqiqotlari markazi
Akbarova S.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda kvant hisoblash texnologiyalari rivojlanishi sharoitida ML-DSA va SLH-DSA postkvant raqamli imzo algoritmlarining amaliy samaradorligi tahlil qilinadi. Klassik imzolarga kvant tahdidi, postkvant standartlarini tanlash jarayoni, algoritmlarning matematik asoslari, kalit va imzo hajmlari hamda hisoblash resurslariga talablari o‘rganiladi. Tahlil natijalari algoritmlarni tanlashda xavfsizlik darajasi, tezkorlik va apparat imkoniyatlarini birgalikda hisobga olish zarurligini ko‘rsatadi.

Kalit so‘zlar: postkvant kriptografiya, raqamli imzo, ML-DSA, SLH-DSA, kvant kompyuterlari, Shor algoritmi, modulli panjaralar, xesh-funksiyalar, kriptografik xavfsizlik, NIST standartlari.

Аннотация. В данной тезисной работе проводится сравнительный анализ практической эффективности постквантовых алгоритмов цифровой подписи ML-DSA и SLH-DSA в условиях развития квантовых вычислительных технологий. Рассматриваются квантовые угрозы классическим алгоритмам цифровой подписи, процесс выбора стандартов постквантовой криптографии, математические основы и механизмы работы исследуемых алгоритмов. На основе стандартов NIST FIPS 204 и FIPS 205, а также результатов экспериментальных исследований анализируются размеры ключей и подписей, вычислительные затраты, требования к памяти и возможности практического применения. Результаты показывают, что при выборе алгоритма необходимо учитывать уровень безопасности, быстродействие и аппаратные ограничения системы.

Ключевые слова: постквантовая криптография, цифровая подпись, ML-DSA, SLH-DSA, квантовые компьютеры, алгоритм Шора, модульные решётки, хеш-функции, криптографическая безопасность, стандарты NIST.

Kirish

RSA, DSA va ECDSA kabi klassik raqamli imzo algoritmlarining xavfsizligi katta sonlarni faktorlash yoki diskret logarifm masalalarining murakkabligiga asoslanadi. Shor algoritmi yetarli quvvatli, xatolarga bardoshli kvant kompyuterida ushbu masalalarni polinomial vaqt ichida yechish imkonini beradi. Natijada mazkur algoritmlarning asosiy xavfsizlik taxminlari zaiflashadi. Hozirgi kvant kompyuterlari ularni keng miqyosda amaliy buzgan emas, biroq uzoq muddatli axborot xavfsizligi uchun postkvant algoritmlariga o‘tish zarur.

NIST postkvant algoritmlarini ochiq tanlov, mustaqil kriptotahlil, xavfsizlik va samaradorlik baholashlari asosida tanladi. 2024-yil avgustida CRYSTALS-Dilithium asosidagi ML-DSA FIPS 204, SPHINCS+ asosidagi SLH-DSA esa FIPS 205 standarti sifatida tasdiqlandi. Ular panjaraga va xesh funksiyalariga asoslangan ikki xil yondashuvni ifodalaydi.

Asosiy qism

Klassik imzolar Shor algoritmi orqali yechilishi mumkin bo‘lgan matematik masalalarga tayansa, postkvant imzolar kvant hujumlariga nisbatan ham murakkab bo‘lib qolishi kutiladigan

masalalardan foydalanadi. Ularni joriy etish dasturiy ta’minot, sertifikatlar va kalitlarni boshqarish tizimlarini ham moslashtirishni talab qiladi.

Postkvant imzolarning asosiy matematik sinflari

– *Panjaraga asoslangan imzolar***:** yuqori o‘lchamli panjara masalalariga tayanadi. ML-DSA ushbu sinfga kiradi.

– *Xeshga asoslangan imzolar:* kriptografik xesh funksiyalaridan foydalanadi. SLH-DSA shu sinf vakilidir.

– *Kodga asoslangan imzolar:* kodlash nazariyasiga oid matematik masalalarga tayanadi; bu sinfdagi barcha algoritmlar imzo yaratish uchun mo‘ljallanmagan.

– *Multivariat imzolar:* chekli maydonlardagi ko‘p o‘zgaruvchili algebraik tenglamalarga asoslanadi va algebraik hujumlarga nisbatan alohida tekshiruvni talab qiladi.

ML-DSA modulli panjaralar nazariyasiga asoslanadi. Uning xavfsizligi Learning With Errors (LWE) va Short Integer Solution (SIS) kabi murakkablik masalalari bilan bog‘liq. Algoritm avval CRYSTALS-Dilithium nomi bilan ishlab chiqilgan.

ML-DSA uchta asosiy bosqichdan iborat:

1. *Kalit generatsiyasi:* ochiq va yopiq kalitlar yaratiladi.
2. *Imzo yaratish:* xabar va yopiq kalit asosida elektron imzo hosil qilinadi.
3. *Imzoni tekshirish:* qabul qiluvchi ochiq kalit yordamida imzoning haqiqiyligini tekshiradi.

ML-DSA nisbatan ixcham imzolar, samarali hisoblash va keng qo‘llanish imkoniyatlari bilan ajralib turadi. Biroq xavfsizlik parametrlari oshganda resurs sarfi ham ortadi. Panjaralarga oid yangi kriptotahlil natijalari, yon kanal va xatolik kiritish hujumlariga qarshi himoyani muntazam baholash lozim.

SLH-DSA kriptografik xesh funksiyalari va daraxtga asoslangan imzo mexanizmlariga tayanadi. U avval SPHINCS+ nomi bilan tanilgan. Algoritm WOTS+, FORS va xesh daraxtlari kabi mexanizmlarni birlashtiradi.

SLH-DSA holatsiz algoritm bo‘lib, imzo yaratishda oldingi imzolar sonini alohida holat sifatida saqlab borishni talab qilmaydi. Bu holatni yo‘qotish yoki noto‘g‘ri yangilash bilan bog‘liq xavflarni kamaytiradi. Biroq maxfiy kalitlarni himoyalash va standart talablariga rioya qilish baribir zarur.

SLH-DSA panjaralarga bog‘liq bo‘lmagan, xesh funksiyalariga asoslangan xavfsizlik yondashuvini taqdim etadi. Shu sababli u kriptografik xilma-xillik talab qilinadigan tizimlarda foydali. Asosiy cheklovlari - imzo hajmining kattaligi va ayrim variantlarda hisoblash vaqtining yuqoriligidir.

1-jadval

Kalit va imzo hajmlari

Algoritm	NIST xavfsizlik kategoriyasi	Ochiq kalit	Yopiq kalit	Imzo
ML-DSA-44	2	1 312 B	2 560 B	2 420 B
ML-DSA-65	3	1 952 B	4 032 B	3 309 B
SLH-DSA-192s	3	48 B	96 B	16 224 B
ML-DSA-87	5	2 592 B	4 896 B	4 627 B

SLH-DSA-256s	5	64 B	128 B	29 792 B

Jadvaldan ko‘rinadiki, SLH-DSA kalitlari kichik, biroq imzolari ancha katta. ML-DSA esa imzo hajmi va hisoblash samaradorligi jihatidan ko‘plab amaliy vazifalar uchun qulay. SLH-DSA uchun 2-kategoriyaga mos parametr mavjud emas; shu sababli ushbu darajada to‘g‘ridan-to‘g‘ri taqqoslash mumkin emas.

Protsessor va xotira sarfi qurilma, dasturiy kutubxona hamda algoritm parametrlariga bog‘liq. ESP32-C6 mikrokontrollerida o‘tkazilgan tadqiqotda ikkala algoritmni tashqi operativ xotirasiz bajarish mumkinligi ko‘rsatilgan. Biroq ayrim SLH-DSA variantlarida hisoblash vaqti yuqori bo‘lgan. Raspberry Pi 4 qurilmasida o‘rganilgan Dilithium variantlarida esa xavfsizlik parametrlari ortishi bilan hisoblash xarajatlari ham oshgan. Ushbu natijalar turli platformalarda olingani sababli, ularni bevosita bir-biriga tenglashtirish mumkin emas.

ML-DSA elektron hujjatlar, raqamli sertifikatlar, dasturiy ta’minot yangilanishlari va kundalik tarmoq protokollari uchun maqbul tanlov bo‘lishi mumkin. SLH-DSA esa xeshga asoslangan muqobil xavfsizlik yondashuvi zarur bo‘lgan uzoq muddatli tizimlar, arxivlar va proshivkalarni imzolashda ko‘rib chiqilishi mumkin. Yakuniy tanlov xavfsizlik kategoriyasi, imzo hajmi va qurilma resurslariga bog‘liq.

Xulosa

ML-DSA va SLH-DSA postkvant raqamli imzolar uchun ikki xil matematik yondashuvni taqdim etadi. ML-DSA ixchamroq imzolari va samarali ishlashi bilan, SLH-DSA esa xesh funksiyalariga asoslangan muqobil xavfsizlik modeli bilan ajralib turadi. Biroq SLH-DSA ning katta imzo hajmi va ayrim variantlaridagi hisoblash xarajatlari amaliy qo‘llanishda hisobga olinishi lozim.

Postkvant migratsiyasi algoritmlarni almashtirish bilan birga sertifikatlar, kalitlarni boshqarish va mavjud qurilmalar mosligini yangilashni ham talab qiladi. Kelgusida ikkala algoritmni bir xil apparat va dasturiy muhitda sinash, bajarilish vaqti, xotira va energiya sarfini o‘lchash hamda yon kanal hujumlariga chidamliligini baholash muhim tadqiqot yo‘nalishlari hisoblanadi.

Foydalanilgan adabiyotlar

1. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

2. NIST. *FIPS 204: Module-Lattice-Based Digital Signature Standard*. 2024. https://doi.org/10.6028/NIST.FIPS.204.

3. NIST. *FIPS 205: Stateless Hash-Based Digital Signature Standard*. 2024. https://doi.org/10.6028/NIST.FIPS.205.

4. Karcz, D. P., Niemiec, M., Kourtis, M. A., & Köppl, T. Exploring hardware implementation feasibility of post-quantum cryptography in embedded systems: Evaluation of NIST-standardized ML-KEM, ML-DSA and SLH-DSA on ESP32-C6. *PLOS ONE*, 2026. https://doi.org/10.1371/journal.pone.0355179.

5. Al-Shareeda, M. A. et al. Efficient implementation of post-quantum digital signatures on Raspberry Pi. *Discover Applied Sciences*, 2025, 7, 597. https://doi.org/10.1007/s42452-025-07201-z.

6. Prokopovych-Tkachenko, Khrushkov, Derkach. Постквантові загрози для інформаційної безпеки: виклики глобального та національного рівня. *Системи та технології*, 2025, № 1 (69), 119–123.

TLS 1.2 VA TLS 1.3 PROTOKOLLARIDA PRF/KDF MEXANIZMLARINING KRIPTOGRAFIK XAVFSIZLIGINING QIYOSIY TAHLIL QILISH

Allanov O.M.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu tezisda TLS protokolida sessiya kalitlarini hosil qilish mexanizmlarining evolyutsiyasi, xususan TLS 1.2 protokoli (TLS 1.2) dagi HMAC asosidagi PRF hamda TLS 1.3 protokoli (TLS 1.3) dagi HKDF mexanizmlari qiyosiy tahlil qilingan. Kalitlarni ajratish, domenlar bo‘yicha ajratish, iyerarxik c kalitlarni hosil qilish sxemasi (key schedule), oldingi sessiyalar maxfiyligini saqlash(Perfect Forward Secrecy, PFS) bilan uyg‘unlik va kompromatga chidamlilik mezonlari ko‘rib chiqiladi. TLS 1.3 da HKDF-Extract, HKDF-Expand va HKDF-Expand-Label asosida Early Secret, Handshake Secret va Master Secret bosqichlarining ajratilishi turli maqsadli kalitlar o‘rtasidagi mantiqiy bog‘liqlikni kamaytirishi ko‘rsatiladi.

Kalit so‘zlar: TLS 1.2, TLS 1.3, PRF, KDF, HKDF, HMAC, key separation, domain separation, Perfect Forward Secrecy.

Аннотация. В тезисе проведён сравнительный анализ механизмов формирования сеансовых ключей в протоколе TLS: PRF на основе HMAC в TLS 1.2 и HKDF в TLS 1.3. Рассмотрены псевдослучайность, разделение ключей и доменов, иерархическое расписание ключей, совместимость с Perfect Forward Secrecy и устойчивость к компрометации. Показано, что применение HKDF-Extract, HKDF-Expand и HKDF-Expand-Label с разделением Early Secret, Handshake Secret и Master Secret формирует более структурированную систему производных ключей.

Ключевые слова: TLS 1.2, TLS 1.3, PRF, KDF, HKDF, HMAC, разделение ключей, разделение доменов, Perfect Forward Secrecy.

Kirish

Transport Layer Security (TLS) protokoli Internet va korporativ tarmoqlarda ma’lumotlarning maxfiyligi, yaxlitligi hamda tomonlarning autentifikatsiyasini ta’minlashning asosiy kriptografik mexanizmlaridan biridir. TLS xavfsizligi faqat simmetrik shifrlash yoki elektron imzo algoritmlariga emas, balki kalitni qanday hosil qilish va foydalanish maqsadlari bo‘yicha ajratishga ham bevosita bog‘liq. Sessiya davomida ishlatiladigan shifrlash kalitlari, autentifikatsiya qiymatlari va boshlang‘ich vektor (Initialization Vector, IV) kabi parametrlar tarmoq orqali tayyor ko‘rinishda uzatilmaydi, ular umumiy maxfiy qiymat va protokol kontekstidan PRF yoki KDF yordamida hosil qilinadi [1–4].

TLS 1.2 protokolida PRF asosida kalit hosil qilish

TLS 1.2 da psevdotasodifiy funksiya secret, label va seed qiymatlarini kirish sifatida qabul qilib, kerakli uzunlikdagi kalitni hosil qiladi. RFC 5246 hujjatiga ko‘ra, standart kriptografik algoritmlar to‘plami uchun PRF HMAC va SHA-256 asosida quriladi [1]. PRF ning umumiy ko‘rinishi $PRF(secret, label, seed) = P_hash(secret, label||seed)$ tarzida ifodalanadi. P_hash esa HMAC ning iterativ qo‘llanishi orqali ixtiyoriy uzunlikdagi psevdotasodifiy ketma-ketlik yaratadi.

TLS 1.2 da kalitlar zanjiri $Pre-Master \rightarrow Secret \rightarrow Master\,Secret \rightarrow key_block$ tamoyiliga asoslangan. Bunday yondashuv amaliy jihatdan ishonchli bo‘lsada, ko‘plab hosil qilingan kalitlarning yagona Master Secret qiymatiga bog‘liqligi sababli TLS 1.2 dagi kalitlar

iyerarxiyasi TLS 1.3 dagiga nisbatan kamroq darajada funksional ajratilgan. Label mexanizmi maqsadlarni ajratishga yordam beradi, biroq key schedulening bosqichlari va kontekst bilan bog‘lash imkoniyatlari TLS 1.3 dagi HKDF-Expand-Label darajasidagi kabi tizimlashtirilmagan [1, 2].

TLS 1.3 da HKDF asosidagi kalitlar iyerarxiyasi

TLS 1.3 da oldingi PRF o‘rniga RFC 5869 hujjatida tavsiflangan HMAC-based Extract-and-Expand Key Derivation Function (HKDF) asosiy primitiv sifatida tanlangan [2, 3]. HKDF ikki konseptual bosqichdan iborat. HKDF-Extract boshlang‘ich kalitdan psevdotasodifiy kalitni (PRK) hosil qiladi, $PRK = HMAC - Hash(salt, IKM)$. HKDF-Expand esa PRK va info kontekstidan kerakli uzunlikdagi kalitni hosil qiladi. Extract-then-Expand yondashuvi turli entropiya xususiyatiga ega kirish materialini qayta ishlash va undan kontekstga bog‘langan mustaqil kalitlarni olish uchun qulay kriptografik konstruksiya hisoblanadi [3, 4].

RFC 8446 hujjatidagi TLS 1.3 key schedule PSK va (EC)DHE umumiy maxfiylikni bosqichma-bosqich qo‘shadi. Natijada Early Secret, Handshake Secret va Master Secret kabi alohida bosqichlar shakllanadi. Derive-Secret va HKDF-Expand-Label funksiyalari esa hosil qilingan qiymatlarni handshake transcript xeshi, maxsus label va kontekst bilan bog‘laydi [2]. Masalan, klient va server handshake traffic secretlari hamda application traffic secretlari alohida yorliqlar bilan hosil qilinadi. Bu yondashuv bir xil ildiz materialidan olingan kalitlarning vazifalari aralashib ketishini cheklovchi domain ajratish mexanizmini protokol darajasiga olib chiqadi.

PRF va HKDF xavfsizligini qiyosiy taqqoslash

Psevdotasodifiylik. TLS 1.2 dagi PRF ham, TLS dagi 1.3 HKDF ham HMAC ga tayanadi. Shuning uchun ushbu mexanizmlarning kriptografik bardoshliligi qo‘llaniladigan xesh funksiyasining xavfsizlik xossalari, HMAC mexanizmining mustahkamligi hamda boshlang‘ich maxfiy qiymatning yetarli darajadagi tasodifiyligi va entropiyasiga bog‘liq. TLS 1.2 da SHA-256 asosidagi P_hash secret va seedni kengaytirsa, TLS 1.3 da Extract va Expand vazifalarining ajratilishi kirish kalitini normallashtirish hamda keyingi hosil qilingan kalitlarni maqsadga bog‘lab kengaytirish imkonini beradi [1–3].

Key separation va domain separation. TLS 1.3 ning muhim konstruktiv afzalligi har bir kriptografik maqsad uchun alohida kalit hosil qilinishi va HKDF-Expand-Label tarkibiga “tls13 ” prefiksi, Label hamda Context kiritilishidir [2]. Buning natijasida handshake trafik kalitlari, application trafik kalitlari va boshqa hosil qilingan kalitlar bir-biridan mantiqiy ajratiladi. Bu xususiyat kalitlardan noto‘g‘ri kontekstda foydalanish xavfini kamaytiradi va protokolning formal tahlilini soddalashtiradi.

Kalit kompromatining ta’sirini cheklash. Biror trafik kalitining oshkor bo‘lishi butun key scheduleni avtomatik ravishda tiklash imkonini bermasligi kerak. TLS 1.3 dagi iyerarxik kalit hosil qilish mexanizmi hamda HMAC/HKDFning bir yo‘nalishli kriptografik xossalari hosila kalit ma’lum bo‘lgan taqdirda undan oldingi bosqichdagi maxfiy kalit materialini qayta tiklashni hisoblash nuqtai nazaridan murakkablashtiradi. Biroq bu xususiyatni mutloq “bitta kalit kompromati boshqa hech narsaga ta’sir qilmaydi” degan da’vo sifatida talqin qilish to‘g‘ri emas. Xavfsizlik aynan qaysi kalit yoki aloqa tomoni(endpoint) holati kompromat qilinganiga bog‘liq. Shu sababli kalitlarni o‘z vaqtida yo‘q qilish va endpoint himoyasi protokol kriptografiyasi bilan bir xil darajada muhim hisoblanadi.

PFS bilan uyg‘unlik. PFS bevosita KDF ning emas, vaqtinchalik (EC)DHE kabi kalit kelishuvi mexanizmining xususiyatidir. Biroq TLS 1.3 key schedule (EC)DHE umumiy kalitni HKDF orqali Handshake Secret va keyingi kalitlar bilan bog‘lagani sababli vaqtinchalik kalit

almashinuvi bilan izchil ishlaydi. Sessiya tugagach vaqtinchalik kalitlar to‘g‘ri yo‘q qilinsa, uzoq muddatli autentifikatsiya kalitining keyingi kompromati oldingi odatiy (EC)DHE sessiyalarining trafik kalitlarini bevosita tiklashga yetarli bo‘lmaydi [2].

1-jadval

Qiyosiy tahlil

Mezon	TLS 1.2 PRF	TLS 1.3 HKDF
Asosiy mexanizm	HMAC asosidagi PRF	HKDF-Extract + HKDF-Expand
Kalitlar iyerarxiyasi	Master Secret markazli	Early → Handshake → Master Secret
Kontekst bilan bog‘lash	Label va seed	HKDF-Expand-Label + transcript context
Key separation	Mavjud, kamroq granular	Tizimli va maqsadga yo‘naltirilgan
PFS bilan integratsiya	Cipher suite/kalit almashinuviga bog‘liq	(EC)DHE key schedule bilan tizimli

Xulosa

Tadqiqotlar TLS kalit hosil qilish arxitekturasida TLS 1.2 dan TLS 1.3 ga o‘tish oddiy algoritm almashtirish emas, balki key schedule ni qayta loyihalash ekanini ko‘rsatadi. TLS 1.2 dagi HMAC asosidagi PRF kriptografik jihatdan mustahkam mexanizm bo‘lib qolsada, TLS 1.3 HKDF yordamida Extract va Expand vazifalarini ajratadi, kalitlarni bosqichlarga bo‘ladi va HKDF-Expand-Label orqali kuchliroq kontekstual ajratishni ta’minlaydi. Shu sababli TLS 1.3 arxitekturasi kalitlar hayot sikli va vazifalarini aniqroq chegaralashga imkon beradi [1–4].

Amaliy xavfsizlik nuqtai nazaridan zamonaviy TLS tizimini baholashda faqat AES yoki SHA oilasining kriptobardoshliligini tekshirish yetarli emas. Kalit almashinuvi, KDF, transcript bog‘lanishi, domain separation, secretlarni o‘z vaqtida yo‘q qilish va implementatsiyaning xavfsizligi yagona tizim sifatida ko‘rilishi zarur. TLS 1.3 ning HKDF asosidagi iyerarxiyasi aynan shu tizimli yondashuvni kriptografik protokol darajasida kuchaytiradi.

Foydalanilgan adabiyotlar

1. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. IETF, 2008. https://www.rfc-editor.org/rfc/rfc5246

2. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018. https://www.rfc-editor.org/rfc/rfc8446

3. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869. IETF, 2010. https://www.rfc-editor.org/rfc/rfc5869

4. Barker E., Chen L., Davis R. Recommendation for Key-Derivation Methods in Key-Establishment Schemes. NIST SP 800-56C Rev. 2. NIST, 2020. https://doi.org/10.6028/NIST.SP.800-56Cr2

5. McKay K., Cooper D. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. NIST SP 800-52 Rev. 2. NIST, 2019. https://doi.org/10.6028/NIST.SP.800-52r2

6. McGrew D. An Interface and Algorithms for Authenticated Encryption. RFC 5116. IETF, 2008. https://www.rfc-editor.org/rfc/rfc5116

РОЛЬ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ОБЕСПЕЧЕНИИ ЦЕЛОСТНОСТИ И НЕОТРЕКАЕМОСТИ ДАННЫХ В ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ

Урозова С.Г.
Национальный университет Узбекистана имени Мирзо Улугбека

Annotatsiya: Ushbu ishda electron raqamli imzo algoritmlari(RSA, El-Gamal, DSA, ECDSA) hamda ularning ochiq kalitlar infraluzilmasida(PKI) ma’mumotlar yaxlitligi, autentifikatsiyasi va rad etilmasligini ta’minlashdagi o‘rni bo‘yicha kompleks matematik tadqiqot o‘tkazilgan. Kriptotizimlarning matematik tuzilmalari, jumladan modul arifmetika, taqqoslamalar nazariyasi va elliptik egri chiziqlar tahlil qilingan. Hisoblash murakkabligining asimptotik ko‘rsatkichlari hamda kalit uzunligini qiyosiy tahlil qilish asosida raqamli ekotizimlarning xavfsiz elektron hujjat aylanishida qo‘llash uchun elliptik kriptografiyaning afzalliklari isbotlangan.

Kalit so‘zlar: Ochiq kalitlar infratuzilmasi, elektron raqamli imzo, RSA, El-Gamal, DSA, ECDSA, elliptik egri chiziqlar, ma’lumotlar yaxlitligi, rad etilmaslik, hisoblash murakkabligi

Аннотация: В данной работе проведено комплексное математическое исследование алгоритмов электронной цифровой подписи(RSA, El-Gamal, DSA, ECDSA) и их роли в обеспечении целостности, аутентификации и неотрекаемости данных в инфраструктуре открытых ключей (PKI). Проанализированы математические структуры криптосистем, включая модульную арифметику, теорию сравнений и эллиптические кривые. На основе сравнительного анализа показателей вычислительной асимптотической сложности и длины ключа доказано преимущество эллиптической криптографии для применения в защищенном электронном документообороте цифровых экосистем.

Ключевые слова: инфраструктура открытых ключей, электронная цифровая подпись, RSA, El- Gamal, DSA, ECDSA, эллиптические кривые, целостность данных, неотрекаемость

Введение

В современном информационном обществе цифровые технологии стали неотъемлемой основой функционирования государственного управления, финансово-банковского сектора, электронной коммерции, здравоохранения и образования. Массовый переход к электронному документообороту (ЭДО) и межведомственному обмену данными ставит на первый план задачи обеспечения комплексной информационной безопасности. При этом традиционные механизмы защиты информации, такие как парольная аутентификация или симметричное шифрование, оказываются недостаточными для решения фундаментальных проблем доверия в распределенных открытых сетях.

Базовыми сервисами информационной безопасности в условиях цифровой трансформации являются: 1) конфиденциальность (защита от несанкционированного чтения); 2) целостность (гарантия неизменности данных с момента создания); 3) аутентификация (достоверное установление авторства и подлинности источника); 4) неотрекаемость (non-repudiation - невозможность для отправителя оспорить факт формирования и отправки документа). Ключевым технологическим фундаментом для реализации сервисов целостности, аутентификации и неотрекаемости выступает

инфраструктура открытых ключей (Public Key Infrastructure, PKI) и механизмы электронной цифровой подписи (ЭЦП)[1].

Электронная цифровая подпись представляет собой последовательность байт, полученную в результате криптографического преобразования исходного электронного документа с использованием закрытого ключа отправителя. Безопасность и криптографическая стойкость систем ЭЦП напрямую зависят от сложности трудноразрешимых математических задач, лежащих в основе асимметричных алгоритмов. Рост вычислительных мощностей, развитие методов параллельных вычислений и квантового криптоанализа требуют регулярной оценки стойкости используемых алгоритмов и поиска более эффективных криптографических схем.

Целью данной работы является глубокое математическое исследование алгоритмов электронной цифровой подписи (RSA, El-Gamal, DSA, ECDSA), теоретический анализ их вычислительной сложности и криптографической устойчивости, а также обоснование выбора наиболее эффективных алгоритмов для применения в системах защищенного электронного документооборота.

Математический аппарат и теоретико-числовые основы ЭЦП

Построение асимметричных криптосистем базируется на однонаправленных функциях с секретом (trapdoor one-way functions). Такие функции легко вычисляются в одну сторону, однако нахождение обратного значения без владения секретным параметром (закрытым ключом) является вычислительно нереализуемой задачей за приемлемое время[2]. В основе рассматриваемых алгоритмов ЭЦП лежат три основных класса математических проблем:

1. Задача факторизации целых чисел (Integer Factorization Problem, IFP) - разложение составного числа $n = p \cdot q$ на два неизвестных больших простых множителя p и q. Данная проблема составляет основу стойкости алгоритма RSA[3].
2. Задача дискретного логарифмирования в конечном поле (Discrete Logarithm Problem, DLP) - нахождение неизвестного показателя степени x из равенства y = $g^x \ mod \ p$ при известных y, g и p. На DLP базируются алгоритмы El-Gamal и DSA[2].
3. Задача дискретного логарифмирования в группе точек эллиптической кривой (Elliptic Curve Discrete Logarithm Problem, ECDLP) - нахождение целого числа d из равенства $Q = d \cdot G$, где Q и G - точки эллиптической кривой над конечным полем[4]. На этой задаче построен алгоритм ECDSA.

Для построения корректных алгоритмов ЭЦП используется развитый математический аппарат теории чисел и модульной арифметики. Рассмотрим ключевые понятия и алгоритмы, применяемые при формировании ключей и выполнении подписи:

Модульная арифметика и сравнения. Двум целым числам a и b соответствует отношение сравнения по модулю n, если их разность делится на n без остатка[5]:

$$a \equiv b(mod\ n) \qquad (1)$$

При выполнении криптографических операций фундаментальное значение имеют полная и приведенная системы вычетов по модулю n, а также свойства мультипликативной группы кольца Z_n. В частности, для существования мультипликативного обратного элемента $a^{-1}\ (mod\ n)$ необходимо и достаточно, чтобы наибольший общий делитель (НОД) чисел a и n был равен единице: gcd(a, n) = 1[5].

Расширенный алгоритм Евклида. Алгоритм Евклида позволяет эффективно находить gcd(a, b) за время O(log(min(a, b))). Расширенный алгоритм Евклида находит линейное представление Безу, то есть целые числа x и y, такие что[2, 5]:

$$a \cdot x + b \cdot y = \gcd(a, b) \quad (2)$$

Если gcd(a, n) = 1, то значение x (mod n) является обратным элементом a^{-1} $(mod\ n)$. Данная операция регулярно используется при генерации секретных экспонент в RSA и DSA[2].

Функция Эйлера. Функция Эйлера φ(n) определяет количество натуральных чисел, не превосходящих n и взаимно простых с ним. Если n является произведением двух простых чисел n = p · q, то значение функции Эйлера рассчитывается по формуле[2, 3]:

$$\varphi(n) = (p-1) \cdot (q-1) \quad (3)$$

Согласно теореме Эйлера, для любого целого a, взаимно простого с n, выполняется соотношение $a^{\varphi(n)} \equiv 1\ (mod\ n)$. Именно это равенство обеспечивает обратимость операций шифрования и расшифрования в алгоритме RSA[3].

Исследование алгоритмов электронной цифровой подписи

Приведем детальный разбор математических моделей и процедур функционирования основных алгоритмов ЭЦП.

Алгоритм RSA

Генерация ключей: выбираются два больших случайных простых числа p и q. Вычисляется модуль $n = p \cdot q$ и значение $\varphi(n) = (p-1) \cdot (q-1)$. Выбирается открытая экспонента e, такая что 1< e<φ(n) и gcd(e, φ(n))=1. Находится секретная экспонента d из условия $e \cdot d \equiv 1\big(mod\ \varphi(n)\big)$. Открытый ключ – пара(e, n), закрытый ключ – d. Формирование подписи: для документа M вычисляется его хеш-значение $h = H(M) \epsilon [1, n-1]$[3]. Подпись S формируется по формуле:

$$S = h^d (mod\ n) \quad (4)$$

Проверка подписи: получатель проверяет соотношение $S^e \equiv h'(mod n)$, где $h' = H(M)$[3]. Если $h' = h$, подпись признается действительной. Математическое доказательство корректности вытекает из теоремы Эйлера: $S^e \equiv (h^d)^e \equiv h^{e \cdot d} \equiv h^{1+k \cdot \varphi(n)} \equiv h \cdot \left(h^{\varphi(n)}\right)^k \equiv h(mod\ n)$.

Алгоритм El-Gamal

Генерация ключей: выбирается большое простое число p и первообразный корень g по модулю p. Выбирается секретный ключ $x \epsilon (1, p-1)$. Вычисляется открытый ключ $y = g^x\ (mod\ p)$.

Формирование подписи: для документа M с хеш-значением h=H(M) генерируется случайное разовое число k, такое что gcd(k, p-1) = 1. Вычисляется первый компонент подписи $a = g^k (mod\ p)$ Второй компонент b находится из сравнения h ≡ x · a + k · b (mod p-1)[2]:

$$b = k^{-1} \cdot (h - x \cdot a) (mod\ p-1) \quad (5)$$

Пара (a, b) образует цифровую подпись. Проверка подписи заключается в проверке равенства $y^a \cdot a^b \equiv g^h (mod\ p)$[2].

Алгоритм DSA

Алгоритм DSA является стандартом США (FIPS 186) и представляет собой модификацию схемы Эль-Гамаля, снижающую размер подписи. Используются параметры:

простое число p, простое число q(делитель p-1), и число $g = h^{\frac{p-1}{q}}(mod\ p) > 1$. Закрытый ключ $x\epsilon(0, q)$, открытый ключ $y = g^x(mod\ p)$.

Подпись (r, s) формируется с использованием случайного $k\epsilon(0, q)$:

$$r = \left(g^k(mod\ p)\right)(mod\ q), s = k^{-1} \cdot (H(M) + x \cdot r)(mod\ q) \quad (6)$$

Проверка осуществляется вычислением $v = s^{-1}(mod\ q), u_1 = H(M) \cdot v(modq), u_2 = r \cdot v(mod\ q)$ и построением $u = \left(g^{u_1} \cdot y^{u_2}\ (mod\ p)\right)(mod\ q)$. Подпись верна, если $u = r$[2].

Алгоритм ECDSA

Алгоритм ECDSA переносит идеи DSA на эллиптические кривые над конечными полями. Неособая эллиптическая кривая E над полем GF(p) задается уравнением Вейерштрасса $y^2 = x^3 + a \cdot x + b\ (mod\ p)$ при условии $4a^3 + 27b^2 \not\equiv 0(mod\ p)$[4, 6]. Точки кривой вместе с бесконечно удаленной точкой O образуют абелеву группу относительно операции сложения.

Для точек P(x_1, y_1) и Q(x_2, y_2) координата суммы R=P+Q=(x_3, y_3) вычисляется через угловой коэффициент λ:

– Если P≠Q, то $\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mod\ p)$

– Если P=Q (удвоение точки), то $\lambda = \frac{3x_1^2 + a}{2y_1}(mod\ p)$.

Тогда $x_3 = \lambda^2 - x_1 - x_2\ (mod\ p), y_3 = \lambda \cdot (x_1 - x_3) - y_1(mod\ p)$.

Параметры ECDSA включают базовую точку G порядка n. Закрытый ключ $k\epsilon[1, n-1]$, открытый ключ $Q = d \cdot G$[4, 6]. При подписи сообщения M вычисляется $e = H(M)$, выбирается случайное $k\epsilon[1, n-1]$, находится точка $(x_1, y_1) = k \cdot G$. Параметры подписи рассчитываются как:

$$r = x_1\ (mod\ n), s = k^{-1} \cdot (e + d \cdot r)(mod\ n) \quad (7)$$

Строгое математическое доказательство корректности ECDSA: при проверке вычисляются $w = s^{-1}(mod\ n), u_1 = r \cdot w(mod\ n)$ и точка $(x_2, y_2) = u_1 \cdot G + u_2 \cdot Q$. Поскольку $u_1 \cdot G + u_2 \cdot Q = w \cdot e \cdot G + w \cdot r \cdot (d \cdot G) = w \cdot (e + d \cdot r) \cdot G = s^{-1} \cdot (e + d \cdot r) \cdot G = k \cdot G = (x_1, y_1)$ то $x_2\ (mod\ n) \equiv x_1\ (mod\ n) \equiv r$, что доказательно гарантирует подлинность[4, 6].

Сравнительный анализ и оценка вычислительной сложности

Проведем теоретико-криптографическое сопоставление алгоритмов ЭЦП с точки зрения длины ключей, размера подписи, асимптотической сложности и ресурсоемкости. Сводные данные приведены в табл. 1.

Таблица 1

Сравнение параметров и асимптотической сложности алгоритмов ЭЦП

Алгоритм	Математическая проблема	Длина ключей	Размер подписи	Вычислительная сложность
RSA	Факторизация(IFP)	3072 бит	3072 бит	$O(k^3)$
El-Gamal	Дискретный логарифм(DLP)	3072 бит	6144 бит	$O(k^3)$
DSA	Дискретный логарифм(DLP)	3072 бит(p), 256 бит(q)	512 бит	$O(k^3)$

ECDSA	Дискретный логарифм эллиптические кривые (ECDLP)	256 бит	512 бит	$O(k^2)$

Анализ данных табл. 1 показывает, что криптосистемы на эллиптических кривых (ECDSA) обеспечивают эквивалентный уровень криптостойкости (128 бит в симметричном эквиваленте) при длине ключа всего 256 бит, в то время как алгоритмам RSA и El-Gamal требуется длина ключа 3072 бит[2, 4]. Это обеспечивает уменьшение размера ключа более чем в 12 раз и размера подписи в 6 раз по сравнению с RSA. С точки зрения вычислительной сложности, генерация ключей и выполнение операций в ECDSA требуют вычислений над меньшими разрядами чисел, что существенно снижает нагрузку на процессор и оперативную память[4, 6]. Это делает эллиптическую криптографию наиболее эффективным выбором для построения высоконагруженных систем электронного документооборота и узлов инфраструктуры PKI[1, 2].

Заключение

В процессе выполнения работы проведен комплексный математический анализ ключевых алгоритмов электронной цифровой подписи (RSA, El-Gamal, DSA, ECDSA) и их фундаментальной роли в обеспечении целостности, аутентификации и неотрекаемости данных в инфраструктуре открытых ключей (PKI). Строго доказана математическая корректность процедур формирования и проверки цифровых подписей. Теоретический анализ показателей алгоритмической сложности доказал преимущество эллиптической криптографии (ECDSA), обеспечивающей высочайший уровень криптографической устойчивости при минимальных требованиях к размеру ключа и вычислительным ресурсам[2, 4, 6].

Список литературы

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017. -800 с.

2. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. – 784 с.

3. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978, vol. 21, no. 2, с. 120-126.

4. Johnson D., Menezes A., Vanstone S. The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, 2001, vol. 1, no. 1, с. 36-63.

5. Хацкевич М.В. Теория сравнений. М., 2019. - 140 с.

6. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer, 2004. -312 с.

SMART KONTRAKTLARDAGI REENTRANCY ZAIFLIGINI ANIQLASH VA BARTARAF ETISH USULLARINI TAHLIL QILISH

Mamatqulova H.S., Abduganiyev B.
Sambhram universiteti

Annotatsiya. Smart kontrakt blokcheynga joylashtirilgach, uning kodini o‘zgartirib bo‘lmaydi, shu sababli mantiqiy xato, jumladan reentrancy, to‘g‘ridan-to‘g‘ri mablag‘ yo‘qotilishiga olib kelishi mumkin. Tezisda reentrancy hujumining mexanizmi UML va BPMN 2.0 yordamida modellashtiriladi, uni aniqlash usullari (statik, simvolik va ishga tushirish vaqtidagi tahlil) hamda bartaraf etish usullari (Checks-Effects-Interactions tartibi, mutex-qulf, ishga tushirish vaqtidagi himoya) tahlil qilinadi. Statik aniqlash uchun boshqaruv oqimi grafiga tayanadigan algoritm bayon etiladi, usullarni aniqlik, to‘liqlik va gaz xarajati bo‘yicha solishtirish mezonlari taklif qilinadi. Mezonlar shartli sonli misolda ko‘rsatilgan.

Kalit so‘zlar: reentrancy, smart kontrakt, Solidity, Ethereum, statik tahlil, Checks-Effects-Interactions, ReentrancyGuard

Аннотация. Поскольку код смарт-контракта после размещения в блокчейне изменить нельзя, логическая ошибка, в том числе reentrancy, может напрямую привести к потере средств. В тезисах механизм атаки reentrancy моделируется средствами UML и BPMN 2.0, анализируются методы её обнаружения (статический, символьный анализ и контроль во время выполнения) и устранения (порядок Checks-Effects-Interactions, мьютекс-блокировка, защита во время выполнения). Для статического обнаружения описан алгоритм на основе графа потока управления, предложены критерии сравнения методов по точности, полноте и затратам газа. Критерии показаны на условном числовом примере.

Ключевые слова: reentrancy, смарт-контракт, Solidity, Ethereum, статический анализ, Checks-Effects-Interactions, ReentrancyGuard

Kirish

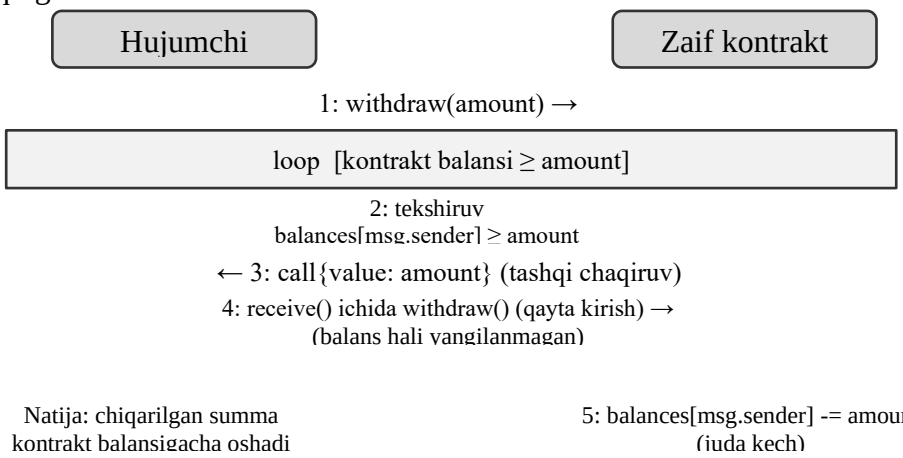
Smart kontrakt blokcheynga joylashtirilgach, uning kodini o‘zgartirib bo‘lmaydi, shuning uchun mantiqdagi xato ham doimiy qoladi va u bevosita mablag‘ yo‘qotilishiga aylanishi mumkin [1]. Ethereum kontraktlariga qilingan hujumlar tasnifida reentrancy alohida o‘rin tutadi: 2016-yilda The DAO kontraktining buzilishi shu zaiflik bilan bog‘liq edi [1]. Zaiflikning mohiyati sodda: kontrakt tashqi manzilga mablag‘ yuborganda boshqaruv qabul qiluvchiga o‘tadi, qabul qiluvchi esa chaqiruv tugamasdan turib asl kontraktga qaytib kirishi mumkin [2].

Amalda muammo faqat bitta funksiyadagi xatoda emas. Qaytib kirish bir funksiya ichida, bir nechta funksiya orasida yoki bir necha kontrakt o‘rtasida sodir bo‘lishi mumkin, tashqi chaqiruv esa faqat ether yuborish bilan cheklanmaydi: boshqa kontraktning istalgan funksiyasini chaqirish ham xuddi shunday xavf tug‘diradi [2]. Tezisning maqsadi reentrancy zaifligini aniqlash va bartaraf etish usullarini yagona mezonlar asosida tahlil qilishdir.

Zaiflik mexanizmi va hujum modeli

Zaif kontraktning tipik holati 1-rasmda berilgan. Foydalanuvchi withdraw() funksiyasini chaqiradi, kontrakt balans yetarliligini tekshiradi va mablag‘ni tashqi chaqiruv (call{value: amount}) orqali yuboradi, balansni esa faqat shundan so‘ng kamaytiradi. Qabul qiluvchi hujumchi kontrakt bo‘lsa, uning receive() funksiyasi boshqaruvni olib, withdraw() ni yana chaqiradi. Balans

hali yangilanmagani uchun tekshiruv qayta o‘tadi va sikl kontrakt balansi tugaguncha yoki gaz yetmay qolguncha davom etadi.



1-rasm. Zaif kontraktda reentrancy hujumining UML ketma-ketlik diagrammasi

Hujum natijasini miqdoriy baholash mumkin. Har bir qayta kirish g birlik gaz sarflasin, hujumchiga ajratilgan gaz G bo‘lsin. U holda qayta kirishlar soni $n_{max} = \min(G / g, D_{max})$ bilan chegaralanadi, bunda D_{max} chaqiruv chuqurligi chegarasidan kelib chiqadigan yuqori baho (barcha nisbatlarda butun qism olinadi). Kontrakt balansi B, bir chaqiruvda yechiladigan summa a bo‘lsa, hujum natijasida chiqarib olinadigan jami summa quyidagicha topiladi:

$$W = a \cdot \min(B / a, n_{max}) \quad (1)$$

bu yerda W - chiqarilgan jami summa, a - bir chaqiruvdagi summa, B - kontrakt balansi.

Aniqlash usullari tahlili

Reentrancy aniqlash usullari kontrakt kodi qachon va qanday tahlil qilinishiga qarab uch guruhga bo‘linadi. Statik tahlil kodni ishga tushirmasdan o‘rganadi: Slither Solidity kodini SSA shaklidagi oraliq tasvirga (SlithIR) o‘tkazadi va ma’lumotlar oqimi hamda taint tahlilini qo‘llaydi, ammo xavfli ko‘ringan tartibni belgilagani uchun yolg‘on ijobiy natijalar mumkin [3]. Simvolik bajarish kontrakt yo‘llarini simvolik kirishlar bilan yuradi va shartlarni qanoatlantiruvchi qiymatlarni qidiradi, lekin yo‘llar soni tez o‘sgani sababli katta kontraktlarda sekinlashadi. Ishga tushirish vaqtidagi (runtime) usullar esa bajarilayotgan tranzaksiyani kuzatadi: Sereum joylashtirilgan kontraktlarni o‘zgartirmasdan, ularning haqiqiy bajarilish oqimini kuzatib reentrancy ni to‘xtatadi [4]. Turli vositalarni bir xil kontraktlarda solishtirish uchun SmartBugs kabi umumiy muhitdan foydalaniladi: shunday tadqiqotda to‘qqizta vosita 69 ta qo‘lda belgilangan zaif kontraktda baholangan [5].

Statik aniqlash reentrancy ning xarakterli belgisiga tayanadi: funksiyada tashqi chaqiruv bajariladi, chaqiruvdan oldin tekshirilgan xotira o‘zgaruvchisi esa chaqiruvdan keyin yoziladi. Funksiyaning boshqaruv oqimi grafi $G_f(V, E)$ tuziladi, har bir tashqi chaqiruv tuguni c uchun undan oldingi shartlarda o‘qiladigan o‘zgaruvchilar to‘plami aniqlanadi, so‘ng c dan erishiladigan tugunlarda shu o‘zgaruvchilarning yozilishi qidiriladi (1-algoritm). Funksiyadagi tashqi chaqiruvlar soni X bo‘lsa, hisoblash murakkabligi quyidagicha:

$$O(X \cdot (V + E)) \quad (2)$$

Bu yerda O(·) - asimptotik murakkablik, V va E - grafning tugunlari va qirralari soni.

1-algoritm. Reentrancy zaifligini statik aniqlash

Kirish: kontrakt funksiyalari to‘plami F; har bir f ∈ F uchun boshqaruv oqimi grafi Gf(V, E), tashqi chaqiruv tugunlari Xf, tugunlarda o‘qiladigan R(v) va yoziladigan W(v) xotira o‘zgaruvchilari to‘plami

Chiqish: shubhali (f, c, w, x) to‘rtliklar to‘plami Z

1: $Z \leftarrow \emptyset$

2: for har bir $f \in F$ do

3: if f nonReentrant qulf bilan himoyalangan then continue

4: for har bir $c \in Xf$ do

5: S ← c dan oldingi shartlarda o‘qiladigan o‘zgaruvchilar (balans, ruxsat) to‘plami

6: for c dan erishiladigan har bir w tugun do

7: if $W(w) \cap S \neq \emptyset$ then

8: $x \in W(w) \cap S$; $Z \leftarrow Z \cup \{(f, c, w, x)\}$

9: end if

10: end for

11: end for

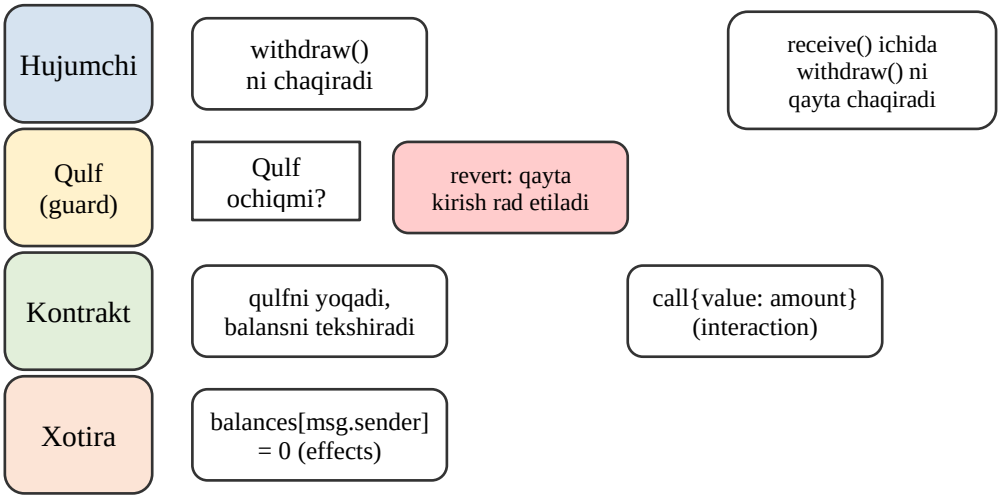
12: end for

13: har bir $(f, c, w, x) \in Z$ uchun x ni o‘qiydigan yoki yozadigan boshqa ochiq $g \neq f$ funksiyani kross-funksiya reentrancy sifatida Z ga qo‘shish

14: Z ni qaytarish

Bartaraf etish usullari

Eng sodda usul Checks-Effects-Interactions tartibidir: avval shartlar tekshiriladi, so‘ng barcha holat o‘zgarishlari xotiraga yoziladi va tashqi kontraktlar bilan o‘zaro ta’sir funksiyaning eng oxirida bajariladi [2]. Zaif misolda bu balansni chaqiruvdan oldin nolga tenglashtirishni bildiradi: qayta kirishda tekshiruv o‘tmaydi va hujum bir marta olingan summa bilan tugaydi. Ikkinchi usul mutex-qulf: OpenZeppelin ReentrancyGuard kutubxonasidagi nonReentrant modifikatori kontraktning o‘ziga bevosita yoki bilvosita qayta chaqiruvni taqiqlaydi [6]. 2-rasmda ikkala usul birlashtirilgan himoyalangan jarayon ko‘rsatilgan: qulf tekshiriladi, balans chaqiruvdan oldin yangilanadi va qayta kirish revert bilan to‘xtatiladi.



2-rasm. Himoyalangan chaqiruv jarayonining BPMN 2.0 diagrammasi

Qulf ikki holatda bo‘ladi: funksiya chaqirilganda yoqiladi, tashqi chaqiruv paytida qayta kirishga urinish rad etiladi, funksiya tugagach esa qulf ochiladi. Usulning cheklovlari ham bor: umumiy qulf tufayli nonReentrant funksiyalar bir-birini chaqira olmaydi, ularni ichki (private) funksiya orqali ishlashga o‘tkazish tavsiya etiladi [6]. Kutubxonaning o‘tish xotirasidan (EIP-1153) foydalanadigan varianti ham mavjud, u faqat shu imkoniyatni qo‘llaydigan tarmoqlarda ishlaydi [6].

Kodini o‘zgartirib bo‘lmaydigan, allaqachon joylashtirilgan kontraktlar uchun ishga tushirish vaqtidagi himoya mumkin bo‘lgan yo‘llardan biridir: Sereum kontraktlarni

o‘zgartirmasdan, ularning bajarilish oqimini kuzatib, reentrancy ga urinishni tranzaksiya paytida to‘xtatadi. Mualliflar yolg‘on ijobiy natijalar ulushi juda past va qo‘shimcha xarajat ahamiyatsiz ekanini xabar qiladi [4].

Baholash usullari

Usullar besh mezon bo‘yicha solishtiriladi: aniqlash sifati (P, R, F_1), himoya samaradorligi (Δ_W), gaz xarajati (Δ_G), tahlil ko‘lami (vaqt va murakkablik (2)) hamda qo‘llash sharti (bosqich va kodni o‘zgartirish zarurati). Aniqlash vositalari markirovkalangan zaif kontraktlar to‘plamida, masalan SmartBugs muhitida [5], bir xil kirishlarda ishga tushirilib, chiqishi tayyor markirovka bilan solishtiriladi. Bartaraf etish usullari esa zaif va himoyalangan kontrakt versiyalarida bir xil hujum stsenariysini bajarish orqali baholanadi (masalan, Foundry yoki Hardhat test muhitida), (3)–(6) formulalar esa natijani solishtirishga xizmat qiladi.

Aniqlash sifati xatolar matritsasi orqali baholanadi: TP - to‘g‘ri topilgan zaif kontraktlar, FP - yolg‘on signal, FN - o‘tkazib yuborilgan zaiflik. Aniqlik va to‘liqlik hamda ularning uyg‘unlashuvi (F_1):

$$P = TP / (TP + FP), \quad R = TP / (TP + FN) \tag{3}$$

$$F_1 = 2PR / (P + R) \tag{4}$$

Gaz xarajati va himoya samaradorligi nisbiy o‘zgarish bilan baholanadi:

$$\Delta_G = (G_h - G_a) / G_a \cdot 100\ \% \tag{5}$$

$$\Delta_W = (W_{old} - W_{new}) / W_{old} \cdot 100\ \% \tag{6}$$

Bu yerda TP, FP va FN - mos ravishda to‘g‘ri ijobiy, yolg‘on ijobiy va yolg‘on salbiy natijalar soni, G_a va G_h - asosiy va himoyalangan funksiyaning gaz sarfi, W_{old} va W_{new} - himoyagacha va undan keyin chiqarilgan summa ((1) formula).

Namunaviy hisob. Usul qanday ishlashini ko‘rsatish uchun shartli (sintetik) qiymatlar olindi, ular real kontraktlarni tahlil qilish natijasi emas. Aniqlash vositasi 100 ta kontraktdan iborat to‘plamda ishga tushirilsin, ularning 24 tasida reentrancy bor. Vosita 22 ta kontraktga signal bersin, shundan 18 tasi haqiqatan zaif: TP = 18, FP = 4, FN = 6. U holda (3) va (4) formulalar bo‘yicha $P = 18 / 22 \approx 0{,}818$; $R = 18 / 24 = 0{,}75$; $F_1 \approx 0{,}783$.

Hujum modeli uchun B = 100 ETH, a = 1 ETH, ajratilgan gaz G = 3 000 000 va bitta qayta kirishning gaz sarfi g = 30 000 bo‘lsin, D_{max} esa 100 dan kichik emas. U holda $n_{max} = 3\,000\,000 / 30\,000 = 100$ va (1) formulaga ko‘ra $W_{old} = 1 \cdot \min(100, 100) = 100$ ETH, ya’ni kontraktdagi barcha mablag‘ chiqib ketadi. Checks-Effects-Interactions tartibi yoki qulf joriy etilganda hujumchi faqat o‘z depozitini (1 ETH) olishi mumkin: $W_{new} = 1$ ETH. (6) formula bo‘yicha $\Delta_W = (100 - 1) / 100 \cdot 100\ \% = 99\ \%$. Mutex-qulf funksiya gaz sarfini 48 000 dan 50 500 gacha oshirsin deb olsak, (5) formula bo‘yicha $\Delta_G = (50\,500 - 48\,000) / 48\,000 \cdot 100\ \% \approx 5{,}2\ \%$. Bu natijalar tanlangan shartli qiymatlarning oqibati, real samarani faqat o‘lchangan ma’lumotlar asosida baholash mumkin; real qiymatlarda hisob shu formulalar bo‘yicha qaytadan bajariladi.

Xulosa

Tahlil reentrancy sababi tashqi chaqiruvdan keyin holat yangilanishi ekanini ko‘rsatdi: shu tartib tufayli qayta kirishda tekshiruv yana o‘tadi. Hujum mexanizmi UML, himoyalangan jarayon esa BPMN 2.0 bilan ifodalandi. Aniqlash va bartaraf etish usullari qo‘llanish bosqichi va cheklovlari bo‘yicha solishtirildi, statik aniqlash uchun boshqaruv oqimi grafiga tayanadigan algoritm bayon etildi, aniqlik, to‘liqlik, himoya samaradorligi va gaz xarajati mezonlari shartli sonli misolda ko‘rsatildi. Keyingi bosqichda mezonlarni markirovkalangan kontraktlar to‘plamida (masalan, SmartBugs) real o‘lchash lozim.

Foydalanilgan adabiyotlar

1. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on Ethereum smart contracts (SoK) // Principles of Security and Trust (POST 2017), Lecture Notes in Computer Science. - Vol. 10204. - Berlin: Springer, 2017. - P. 164–186. - DOI: 10.1007/978-3-662-54455-6_8.

2. Solidity Documentation. Security Considerations. - URL: https://docs.soliditylang.org/en/latest/security-considerations.html (murojaat sanasi: 20.10.2026).

3. Feist J., Grieco G., Groce A. Slither: a static analysis framework for smart contracts // 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). - 2019. - P. 8–15. - DOI: 10.1109/WETSEB.2019.00008.

4. Rodler M., Li W., Karame G.O., Davi L. Sereum: protecting existing smart contracts against re-entrancy attacks // Proceedings of the Network and Distributed System Security Symposium (NDSS). - 2019. - DOI: 10.14722/ndss.2019.23413.

5. Durieux T., Ferreira J.F., Abreu R., Cruz P. Empirical review of automated analysis tools on 47,587 Ethereum smart contracts // Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering (ICSE). - 2020. - P. 530–541. - DOI: 10.1145/3377811.3380364.

6. OpenZeppelin Contracts 5.x. Utilities: ReentrancyGuard. - URL: https://docs.openzeppelin.com/contracts/5.x/api/utils.

KRIPTOGRAFIK TIZIMLARDA PSEVDOTASODIFIY FUNKSIYALAR VA KALIT HOSIL QILISH FUNKSIYALARINING O‘RNI

Haydarov E.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda psevdotasodifiy funksiyalar (PRF) va kalit hosil qilish funksiyalari (KDF) tushunchalari, ularning rasmiy ta’riflari, zamonaviy kriptografik tizimlardagi o‘rni va o‘zaro bog‘liqligi tahlil qilinadi. HMAC, CMAC va KMAC konstruksiyalari, NIST SP 800-108 bo‘yicha KDF rejimlari, HKDF ning extract-then-expand paradigmasi hamda parolga asoslangan KDFlar ko‘rib chiqiladi. Entropiya, PRF va KDF o‘rtasidagi bog‘liqlik asoslanib, TLS 1.3 protokolidagi kalit jadvali misolida ularning amaliy ahamiyati ko‘rsatiladi va xavfsiz loyihalash bo‘yicha tavsiyalar beriladi.

Kalit so‘zlar: psevdotasodifiy funksiya, kalit hosil qilish funksiyasi, HMAC, HKDF, NIST SP 800-108, entropiya, min-entropiya, TLS 1.3.

Аннотация. В тезисе анализируются понятия псевдослучайных функций (PRF) и функций выработки ключей (KDF), их формальные определения, роль в современных криптографических системах и взаимосвязь. Рассматриваются конструкции HMAC, CMAC и KMAC, режимы KDF согласно NIST SP 800-108, парадигма extract-then-expand схемы HKDF, а также KDF на основе паролей. Обосновывается связь между энтропией, PRF и KDF, на примере ключевого расписания протокола TLS 1.3 показывается их практическое значение и даются рекомендации по безопасному проектированию.

Ключевые слова: псевдослучайная функция, функция выработки ключа, HMAC, HKDF, NIST SP 800-108, энтропия, мин-энтропия, TLS 1.3.

Kirish. Zamonaviy axborot xavfsizligi tizimlarining aksariyati – TLS protokoli, VPN tunnellari, diskni to‘liq shifrlash vositalari, parolga asoslangan autentifikatsiya va apparat xavfsizlik modullari (HSM) – ikkita fundamental kriptografik primitivga tayanadi: psevdotasodifiy funksiyalar (Pseudorandom Function, PRF) va kalit hosil qilish funksiyalari (Key Derivation Function, KDF). Shifrlash algoritmi qanchalik bardoshli bo‘lmasin, kalitlar noto‘g‘ri hosil qilinsa yoki bir kalit turli maqsadlarda qayta ishlatilsa, butun tizim xavfsizligi buziladi. Shu sababli PRF va KDF ning nazariy asoslari hamda ularni amaliyotda to‘g‘ri qo‘llash masalalari kriptologiyaning dolzarb yo‘nalishlaridan biri hisoblanadi. Ushbu tezisda mazkur tushunchalar NIST standartlari, IETF RFC hujjatlari va ilmiy adabiyotlar asosida tahlil qilinadi.

Asosiy qism.

1. Psevdotasodifiy funksiyalar. PRF tushunchasi 1986-yilda O. Goldreich, S. Goldwasser va S. Micali tomonidan rasmiy ta’riflangan (GGM konstruksiyasi). PRF – kalit K bilan boshqariladigan $F: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$ funksiyalar oilasi bo‘lib, kalit tasodifiy va maxfiy tanlanganda polinomial resursga ega har qanday tahlilchi D uchun uning chiqishi haqiqiy tasodifiy funksiya f chiqishidan amalda ajratib bo‘lmaydigan bo‘ladi:

$$Pr[\{D^{F_K}\}(\cdot) = 1] - Pr[D^{\{f\}}(\cdot) = 1] \leq negl(k).$$

PRF ning asosiy xossalari – kalitga bog‘liqlik, determinizm, hisoblash jihatidan ajratib bo‘lmaslik va polinomial vaqtda hisoblanishidir. PRF ni psevdotasodifiy generator (PRG) va psevdotasodifiy o‘rin almashtirishdan (PRP) farqlash lozim: PRG qisqa urug‘dan uzun ketma-

ketlik hosil qiladi, PRP (masalan, AES) qaytariladigan funksiya bo‘lsa, PRF teskarilanishi shart bo‘lmagan kalitli funksiyadir.

NIST standartlarida PRF sifatida uchta konstruksiya rasman tan olingan: xesh funksiya asosidagi HMAC (FIPS 198-1, RFC 2104), blokli shifr asosidagi CMAC (SP 800-38B) va SHA-3 oilasining sponge funksiyasiga asoslangan KMAC (SP 800-185). HMAC quyidagicha hisoblanadi:

$$HMAC(K, m) = H((K' \oplus opad) \| H((K' \oplus ipad) \| m)).$$

Ichki tuzilishi turlicha bo‘lishiga qaramay, uchala konstruksiya bir xil xavfsizlik xossasini ta’minlaydi, shu sababli ular yagona KDF freymvorkida o‘zaro almashtiriladigan qurilish bloki sifatida ishlatiladi.

2. Kalit hosil qilish funksiyalari. KDF ning vazifasi dastlabki kalit materialidan (IKM) bir yoki bir nechta kriptografik mustahkam kalitlarni hosil qilishdir. Kirish sifatida Diffie–Hellman almashinuvining umumiy siri, asosiy (master) kalit yoki foydalanuvchi paroli xizmat qilishi mumkin. NIST SP 800-108 Rev.1 standarti PRF asosida kalit hosil qilishning uchta rejimini belgilaydi: hisoblagich (counter), teskari aloqa (feedback) va ikkilangan quvur (double-pipeline) rejimlari. Masalan, hisoblagich rejimida:

$$K(i) = PRF(K_IN, [i]_2 \| Label \| 0x00 \| Context \| [L]_2), \quad i = 1, \ldots, \lceil L/h \rceil.$$

Label (kalit maqsadi) va Context (tomonlar identifikatorlari, nonce) parametrlarining aniq kodlanishi turli maqsadlar uchun bir-biridan mustaqil kalitlar hosil bo‘lishini kafolatlaydi – bu “soha ajratish” (domain separation) tamoyili deyiladi. Aynan shu tamoyil HSM ichidagi bitta root kalitdan har bir sessiya, dastur yoki ma’lumotlar bazasi uchun alohida kalit hosil qiluvchi kalitlar ierarxiyasini qurish imkonini beradi.

RFC 5869 da ta’riflangan HKDF ikki bosqichli extract-then-expand paradigmasiga asoslanadi. Extract bosqichi bir tekis taqsimlanmagan IKM entropiyasini qisqa psevdotasodifiy kalitga jamlaydi, expand bosqichi esa uni kerakli uzunlikdagi chiqish kalit materialiga (OKM) kengaytiradi:

$$PRK = HMAC(salt, IKM); \quad T(i) = HMAC(PRK, T(i-1) \| info \| i).$$

Past entropiyali parollar uchun HKDF yoki SP 800-108 yetarli emas, chunki ular lug‘at va to‘liq saralash hujumlariga zaif. Bunday holatlarda hisoblashni ataylab sekinlashtiruvchi PBKDF2 (RFC 2898), katta xotira talab qiluvchi scrypt va Argon2 (RFC 9106) funksiyalari qo‘llaniladi.

3. PRF va KDF o‘rtasidagi bog‘liqlik. PRF va KDF orasidagi munosabatni quyidagicha ifodalash mumkin: KDF - bu PRFning ko‘p martalik (iterativ) qo‘llanilishi orqali quriladigan yuqori darajadagi (higher-level) protokol. Bog‘liqlik ikki jihatda namoyon bo‘ladi. Har qanday amaliy KDF konstruksiyasi (HKDF, SP 800-108 KDFlari) o‘zining ichki mexanizmi sifatida PRFdan foydalanadi. Masalan, HKDFning extract bosqichi HMAC-PRFni bir marta chaqiradi, expand bosqichi esa uni bir necha marta ketma-ket (zanjirsimon) chaqiradi. Xuddi shunday, SP 800-108dagi hisoblagich rejimi PRFni [L/h] marta chaqiradi, bu yerda h - PRF chiqishining bit uzunligi, L - talab qilinadigan chiqish uzunligi. Xavfsizlik isboti jihatidan KDF ning xavfsizligi ishlatilgan PRF xavfsizligiga qisqartiriladi: agar PRF (masalan, HMAC-SHA256) xavfsiz bo‘lsa, yetarli entropiya va mustaqil kirishlar sharti bajarilganda KDF ham xavfsiz bo‘ladi. Ikkala primitivning asosiy farqlari 1-jadvalda keltirilgan.

1-jadval

PRF va KDF ning qiyosiy tavsifi

Mezon	PRF	KDF

Maqsadi	Kalit bilan boshqariladigan psevdotasodifiylikni ta’minlash	Bitta manbadan bir nechta mustaqil kalit hosil qilish
Kirish	Kalit K va ixtiyoriy kirish x	Dastlabki kalit materiali (IKM), Label, Context, uzunlik L
Chiqish uzunligi	Belgilangan (fixed-length)	Ixtiyoriy (variable-length)
Amaliy misollar	HMAC, CMAC, KMAC	HKDF, SP 800-108 KDF, PBKDF2, Argon2
Standartlar	FIPS 198-1, RFC 2104, SP 800-185	NIST SP 800-108r1, SP 800-56C, RFC 5869
Nazariy asos	GGM konstruksiyasi (1986)	PRF xavfsizligiga qisqartirish (reduction)

4. Entropiyaning roli. PRF va KDF ning xavfsizlik kafolatlari shartli xarakterga ega – ular kirish materiali tahlilchi uchun yetarlicha bashorat qilib bo‘lmaydigan bo‘lgandagina amal qiladi. Kriptografiyada o‘rtacha holatni tavsiflovchi Shannon entropiyasi o‘rniga eng yomon holat ko‘rsatkichi – min-entropiya ishlatiladi:

$$H_{\infty(X)} = -\log_2 (\max_x p(x)).$$

NIST SP 800-90 seriyasi tasodifiy bit generatorlarining to‘liq zanjirini belgilaydi: SP 800-90B entropiya manbalari va ularni testlashni, SP 800-90A esa urug‘ asosida ishlovchi Hash_DRBG, HMAC_DRBG va CTR_DRBG mexanizmlarini tavsiflaydi. Xom entropiya kondensatsiya funksiyasi (odatda HMAC) orqali bir tekis taqsimlangan bitlarga aylantiriladi. Muhim cheklov shundaki, HKDF ning extract bosqichi entropiyani kuchaytira olmaydi, faqat mavjud entropiyani qayta taqsimlaydi. Shunday qilib, entropiya – xom resurs, PRF – uni qayta ishlovchi mexanizm, KDF esa amaliy tizimda kalitlarni tashkil etuvchi yuqori qatlamdir.

5. Amaliy misol va xavfsizlik tavsiyalari. TLS 1.3 protokoli (RFC 8446) butun kalitlar ierarxiyasini HKDF asosida quradi: Diffie–Hellman umumiy siri HKDF-Extract orqali Early, Handshake va Master Secret larga aylantiriladi, HKDF-Expand-Label funksiyasi esa “tls13 c hs traffic” kabi aniq belgilar yordamida har bir yo‘nalish va bosqich uchun mustaqil trafik kalitlari va IV larni hosil qiladi. Shunday qilib, butun TLS 1.3 kalitlar daraxti bitta PRF (HMAC-SHA256 yoki HMAC-SHA384) ning kontekstga bog‘langan ko‘p martalik chaqiruvidan iborat.

2025-yilda IACR ePrint arxivida (2025/815) e’lon qilingan tadqiqotda SP 800-108 KDFlarida CMAC PRF sifatida ishlatilganda “kalitni nazorat qilish” (key control) xossasi buzilishi mumkinligi ko‘rsatilgan, HMAC va KMAC asosidagi rejimlar esa bunday hujumga chidamli ekani qayd etilgan. Shu asosda quyidagi tavsiyalarni berish mumkin: PRF sifatida imkon qadar HMAC yoki KMAC dan foydalanish; Label va Context maydonlarini har doim aniq va mustaqil shakllantirish; bir tekis taqsimlanmagan kirishlar uchun extract bosqichini tashlab ketmaslik; parollardan kalit hosil qilishda Argon2 yoki PBKDF2 kabi sekinlashtiruvchi funksiyalarni qo‘llash.

Xulosa

PRF va KDF zamonaviy kriptografik tizimlarning o‘zaro chambarchas bog‘liq, ammo funksional jihatdan farqli tarkibiy qismlaridir. PRF – hisoblash jihatidan ajratib bo‘lmaslik xossasiga ega fundamental primitiv bo‘lsa, KDF uni o‘zgaruvchan uzunlikdagi, kontekstga bog‘langan va bir nechta maqsadli kalitlarni hosil qilish ehtiyojlariga moslashtiruvchi protokol darajasidagi mexanizmdir. Ularning xavfsizligi kirish materialining yetarli min-entropiyasiga bog‘liq. Milliy kriptografik vositalar va kalitlarni boshqarish tizimlarini ishlab chiqishda NIST SP 800-108, RFC 5869 va SP 800-90 standartlarida ishlab chiqilgan tamoyillarni – soha ajratish,

extract-then-expand va entropiyani baholashni – hisobga olish xavfsiz kalit infratuzilmasini yaratishning muhim sharti hisoblanadi.

Foydalanilgan adabiyotlar:

1. Goldreich O., Goldwasser S., Micali S. How to Construct Random Functions // Journal of the ACM. – 1986. – Vol. 33, No. 4. – P. 792–807.

2. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. – Boca Raton: CRC Press, 2020.

3. NIST SP 800-108 Rev.1. Recommendation for Key Derivation Using Pseudorandom Functions. – Gaithersburg: NIST, 2022 (upd. 2024).

4. NIST SP 800-90A Rev.1. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. – NIST, 2015.

5. NIST SP 800-90B. Recommendation for the Entropy Sources Used for Random Bit Generation. – NIST, 2018.

6. FIPS 198-1. The Keyed-Hash Message Authentication Code (HMAC). – NIST, 2008.

7. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869. – IETF, 2010.

8. Krawczyk H. Cryptographic Extraction and Key Derivation: The HKDF Scheme // CRYPTO 2010, LNCS. – Springer, 2010.

9. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. – IETF, 2018.

10. Security Analysis of NIST Key Derivation Using Pseudorandom Functions. IACR ePrint Archive, Report 2025/815.

ZAMONAVIY PSEVDOTASODIFIY FUNKSIYALAR VA KALIT HOSIL QILISH SXEMALARINING QIYOSIY TAHLILI

Abdurazzoqov J.R.
Toshkent xalqaro universiteti

Annotatsiya. Maqolada zamonaviy psevdotasodifiy funksiyalar (PRF) va kalit hosil qilish funksiyalarining (KDF) kriptografik qurilish tamoyillari hamda ularni tanlash mezonlari qiyosiy tahlil qilinadi. HMAC, AES-CMAC va KMACning asosiy farqlari, HKDFning ajratib olish va kengaytirish bosqichlari, NIST SP 800-108 oilasidagi rejimlar hamda PBKDF2, scrypt va Argon2idning parolga asoslangan kalit hosil qilishdagi o‘rni yoritiladi. Kirish sirining entropiyasi, kontekst bo‘yicha ajratish, hisoblash va xotira xarajatlari asosida amaliy tanlov mezonlari umumlashtiriladi. Qiyosiy xulosalar standartlar va ochiq ilmiy manbalarning tahliliga asoslangan.

Kalit so‘zlar: psevdotasodifiy funksiya, kalit hosil qilish funksiyasi, HMAC, CMAC, KMAC, HKDF, NIST SP 800-108, PBKDF2, scrypt, Argon2id.

Аннотация. В статье проводится сравнительный анализ принципов построения современных псевдослучайных функций (PRF) и функций выработки ключей (KDF), а также критериев их выбора. Рассматриваются различия между HMAC, AES-CMAC и KMAC, этапы извлечения и расширения HKDF, режимы семейства NIST SP 800-108 и назначение PBKDF2, scrypt и Argon2id при получении ключей из паролей. Обобщены практические критерии, учитывающие энтропию входного секрета, разделение по контексту, вычислительные затраты и потребление памяти. Выводы основаны на сравнении нормативных и научных источников.

Ключевые слова: псевдослучайная функция, функция выработки ключей, HMAC, CMAC, KMAC, HKDF, PBKDF2, scrypt, Argon2id.

Kirish

Zamonaviy simmetrik kriptografik protokollarda yagona maxfiy qiymatdan bir nechta vazifaga mo‘ljallangan kalitlarni xavfsiz hosil qilish talab etiladi. Masalan, aloqa seansi uchun shifrlash va autentifikatsiyalash kalitlari, ikki yo‘nalishdagi trafik kalitlari hamda kalitlarni yangilash uchun alohida hosila qiymatlar kerak bo‘ladi. Bu vazifalarda asosiy kriptografik primitivning mustahkamligi bilan bir qatorda kalit materialining qayerdan kelgani, qanday qayta ishlangani va qaysi kontekstga bog‘langani ham muhim.

PRF maxfiy kalit bilan parametrlangan, chiqishini tasodifiy funksiyadan hisoblash jihatidan farqlash qiyin bo‘lgan akslantirishdir. KDF esa kirishdagi sir va yordamchi ma’lumotlar asosida belgilangan uzunlikdagi kalit materialini hosil qiluvchi mexanizmdir. Har qanday PRF avtomatik tarzda barcha turdagi sirlar uchun xavfsiz KDF bo‘lavermaydi: boshlang‘ich kalit past entropiyali parol bo‘lsa, tezkor PRF qo‘shimcha ravishda taxmin qilish hujumini qimmatlashtirishi zarur [1, 4, 8]. Mazkur maqolaning maqsadi ushbu konstruksiyalarni yagona xavfsizlik mezonlari asosida qiyoslash va ular qo‘llanadigan sharoitlarni aniqlashtirishdir.

Tahlil HMACning nazariy asoslari va RFC 2104, HKDFning RFC 5869 tavsifi, AES-CMACga oid NIST SP 800-38B, KMACga oid SP 800-185 hamda kalitni kengaytirish bo‘yicha NIST SP 800-108 Rev. 1 (2024-yilgi yangilanish) hujjatlari asosida olib borildi [1–6]. Parolga asoslangan KDFlar uchun PBKDF2, scrypt va Argon2idning tegishli standart tavsiflari solishtirildi [8–10]. Mezonlar sifatida kirish siriga qo‘yiladigan talab, PRFga tayanish, kalitlarni ajratish

mexanizmi, parametrlar, resurs sarfi va qo‘llanish sohasi olindi. Ushbu ish nazariy-qiyosiy tadqiqot bo‘lib, mustaqil tezlik sinovlari yoki tajriba natijalari sifatida ko‘rsatiladigan o‘lchovlar keltirilmaydi.

HMAC AES-CMAC va KMACning PRF sifatidagi o‘rni

HMAC kalitlangan xeshlashga asoslanadi. Uning ichki va tashqi qatlamlari bir-biridan ipad va opad konstantalari bilan ajratilgan bo‘lib, maxfiy kalit va xabar ikki bosqichli qayta ishlanadi [1, 2]. HMAC umumiy holda quyidagicha ifodalanadi:

$$\mathrm{HMAC}(\mathrm{K}, \mathrm{M}) = \mathrm{H}((\mathrm{K}' \oplus \mathrm{opad}) \parallel \mathrm{H}((\mathrm{K}' \oplus \mathrm{ipad}) \parallel \mathrm{M})).$$

Bu yerda H – xesh-funksiya, K′ – blok uzunligiga keltirilgan kalit, M – xabar, $\oplus$ – XOR, $\parallel$ – konkatenatsiya amali. HMAC-SHA-256da ichki blok o‘lchami 512 bit va natija uzunligi 256 bit. HMAC tayyor dasturiy xesh kutubxonalari asosida ishlaydi va o‘zgaruvchan uzunlikdagi xabarlar uchun qulay. Biroq PRF sifatidagi ishonchlilik kalitni boshqarish, tanlangan xeshning xavfsizlik farazlari hamda teg uzunligini o‘rinli tanlashga bog‘liq.

AES-CMAC AES blokli shifriga tayangan holda o‘zgaruvchan uzunlikdagi ma’lumotdan autentifikatsiya kodini hosil qiladi. U CBC-MACdan farqli ravishda oxirgi blokning to‘liqligini ajratuvchi K_1 va K_2 yordamchi kalitlardan foydalanadi. AES apparat tezlatgichi mavjud bo‘lsa, CMAC ayniqsa qulay; dasturiy muhitda unumdorlik platformaga bog‘liq [3]. PRP va PRF tushunchalari turli: AES kalitlangan o‘rin almashtirish bo‘lsa, CMAC butun xabarga qo‘llanadigan alohida konstruksiyadir.

KMAC Keccak/SHA-3 oilasiga tayangan kalitlangan mexanizm bo‘lib, o‘zgaruvchan uzunlikdagi chiqish va qo‘llanish sohasini ajratuvchi sozlash satri bilan ishlaydi [6]. NIST SP 800-108 Rev. 1 HMAC, CMAC va KMACdan foydalanuvchi KDF sxemalarini qamrab oladi [4]. Universal eng tez algoritm yo‘q: tanlov kutubxonalar, apparat tezlatkichlari va protokolning muvofiqlik talablariga bog‘liq.

1-jadval

PRF konstruksiyalarining qiyosiy tavsifi

Mezon	HMAC	AES-CMAC	KMAC
Asos	Xesh-funksiya	AES blokli shifri	Keccak/SHA-3
Kirish	O‘zgaruvchan	Bloklarga ajratiladi	O‘zgaruvchan
Chiqish	Xesh natijasiga bog‘liq	Blok uzunligigacha	Sozlanadigan
Afzallik	Keng dasturiy moslik	AES apparat tezlatgichi	Moslashuvchan chiqish
KDFdagi o‘rni	HKDF; SP 800-108	SP 800-108	SP 800-108

HKDFning ajratib olish va kengaytirish bosqichlari

HKDFning asosiy g‘oyasi kirish kalit materialidan (IKM) psevdotasodifiy tayanch kalit (PRK) olishni, keyinchalik undan kerakli miqdorda hosila kalit ishlab chiqarishdan ajratishdir [5, 7]. Ajratib olish bosqichi quyidagicha yoziladi:

$$\mathrm{PRK} = \mathrm{HMAC}(\mathrm{salt}, \mathrm{IKM}).$$

salt qiymati odatda oshkor bo‘lishi mumkin, biroq u mustaqil va tasodifiy tanlansa, ayrim xavfsizlik asoslarini kuchaytiradi. salt berilmasa, RFC 5869 bo‘yicha xesh natijasi uzunligidagi nol baytlar ishlatiladi. Bu sukut bo‘yicha ruxsat etilgan holat bo‘lib, protokol dizaynida sifatli salt qo‘llashning foydasini inkor etmaydi. Kengaytirishda esa quyidagi zanjir hisoblanadi:

$$T(0) = \varepsilon;\ \ T(i) = HMAC(PRK, T(i-1) \parallel info \parallel octet(i)).$$

Natija OKM = T(1) ‖ T(2) ‖ … qiymatining dastlabki L baytidir; bunda i = 1, …, ⌈L/HashLen⌉ va L ≤ 255·HashLen. HMAC-SHA-256 uchun bitta HKDF-Expand chaqiruvining yuqori chegarasi 8160 bayt bo‘ladi [5]. info maydoniga protokol versiyasi, seans identifikatori, tomonlar roli va kalit vazifasi kabi oldindan belgilangan kodlangan ma’lumotlarni kiritish mumkin. Masalan, “enc/client” va “enc/server” kabi turli yorliqlar bitta PRKdan ikki yo‘nalish uchun alohida kalitlar olishga yordam beradi.

HKDFdagi xavfsizlik kirish materialining yetarli shartli entropiyaga egaligi va HMACga oid kriptografik farazlarga tayanadi. U past entropiyali parolni kuchli maxfiy kalitga o‘z-o‘zidan aylantirmaydi. Shu sababli parollar uchun HKDFni mustaqil himoya mexanizmi deb ko‘rsatish noto‘g‘ri. Bundan tashqari, turli kontekstlarni ajratishda info maydonlari uzunligi va chegaralari bir qiymatli kodlanishi lozim; aks holda turlicha semantik maydonlar bir xil bitlar satriga birlashib qolishi mumkin.

NIST SP 800-108 asosidagi kalitni kengaytirish rejimlari.

NIST SP 800-108 Rev. 1 mavjud kuchli K_i tayanch kalitdan hosila material olishni standartlashtiradi [4]. Hisoblagichli rejimning HMAC yoki CMAC asosidagi asosiy ko‘rinishi quyidagicha ifodalanadi:

$$K(i) = PRF(K_i, [i]_r \parallel Label \parallel 0x00 \parallel Context \parallel [L]_2)$$

Bu yerda $[i]_r$ – r bitli hisoblagich, Label – kalit vazifasi, Context – sessiya yoki qurilma kabi bog‘lovchi axborot, $[L]_2$ – chiqish uzunligining qat’iy kodlangan ifodasi. Har bir blokning oldingisidan mustaqilligi hisoblagichli rejimni parallel hisoblash uchun qulay qiladi. Teskari bog‘lanishli rejimda oldingi chiqish bloki navbatdagi PRF kirishiga qo‘shiladi; ikki konveyerli rejimda esa oraliq A(i) va yakuniy K(i) zanjirlari yuritiladi. Bu ikki rejimning bosqichlari o‘zaro bog‘langanligi sababli to‘liq parallel emas [4].

Standartdagi KMAC asosidagi yechim o‘zgaruvchan uzunlikdagi chiqishni bir funksiya chaqiruvida hosil qilish imkonini beradi. Barcha rejimlarda Label va Contextni to‘g‘ri kodlash, chiqish uzunligini chegaralash hamda hosila kalitni unga mo‘ljallangan vazifadan tashqarida ishlatmaslik prinsipial talablardir. Muhim chegara shuki, SP 800-108 tayanch kalitning yetarli entropiyasini faraz qiladi: uni foydalanuvchi parolini qayta ishlashning o‘rniga qo‘yish mumkin emas.

Parolga asoslangan KDFlar.

Foydalanuvchi tanlagan parol ko‘pincha tasodifiy kalitga qaraganda ancha past entropiyaga ega. Shuning uchun unga tezkor PRFni bir marta qo‘llash oflayn lug‘at hujumlari uchun yetarli to‘siq yaratmaydi. PBKDF2 ushbu muammoni HMAC kabi PRFni c marta takrorlash va har bir blokda natijalarni XOR orqali birlashtirish bilan kamaytiradi [8]. PBKDF2 uchun salt va takrorlashlar sonini to‘g‘ri tanlash muhim, lekin uning xotira talabi kichikligi hisoblashni ko‘plab grafik protsessorlarda parallellashtirishga imkon beradi.

scrypt katta xotira bilan bog‘liq hisoblash xarajatlarini joriy etadi; uning N, r va p parametrlari vaqt va xotira sarfini boshqaradi [9]. Argon2 oilasida esa m – xotira, t – o‘tishlar soni, p – parallel ishlash darajasi orqali hujumchiga nisbatan qo‘shimcha resurs talabi shakllantiriladi. Argon2id ma’lumotga mustaqil va ma’lumotga bog‘liq murojaat usullarini uyg‘unlashtirib, yon-kanal kuzatuvlari hamda vaqt–xotira almashinuvi hujumlari nuqtayi nazaridan muvozanatli profilni taklif etadi [10]. Belgilangan resurslar miqdori platforma, tahdid modeli va foydalanuvchi uchun maqbul kechikishga qarab sinov orqali tanlanishi kerak.

Parol xeshini ma’lumotlar bazasida saqlash bilan paroldan shifrlash kalitini hosil qilish turli vazifalardir. Ikkalasida ham qayta ishlashning hisoblash narxi muhim bo‘lsa-da, saqlash formatida algoritm versiyasi va parametrlar, foydalanuvchiga xos salt ham qayd etilishi kerak. Parolni baholashda algoritmning nomi emas, balki xavfsiz parametrlar, serverning xotira budjeti va hujumchining taxminiy hisoblash imkoniyatlari asosiy mezon hisoblanadi.

2-jadval

Kirish sirining turiga ko‘ra KDF tanlash

Kirish materiali	Maqsadga muvofiq sxema	Asosiy tekshiruv
Strukturali umumiy sir, masalan, DH qiymati	HKDF-Extract + HKDF-Expand	Entropiya farazi, salt, info, L
Mavjud yuqori entropiyali simmetrik kalit	SP 800-108 asosidagi PRF-KDF	Label, Context, hisoblagich, K_i himoyasi
Inson tanlagan parol	Argon2id yoki scrypt; muvofiqlik talabida PBKDF2	Noyob salt, resurs parametrlari, kechikish

Tahlil natijalari va amaliy tavsiyalar.

Qiyosiy tahlil PRF va KDF sxemalarini uch qatlamda baholash maqsadga muvofiqligini ko‘rsatadi. Birinchisi – kriptografik qatlam: asosiy PRFning farazlari, kalit kuchi, hosila chiqish uzunligi va domenlarni ajratish talablarini tekshirish. Ikkinchisi – protokol qatlami: salt, Label, Context va info maydonlarini versiyalangan, bir qiymatli formatda kodlash, har bir kalitning rolini hamda amal qilish muddatini belgilash. Uchinchisi – amalga oshirish qatlami: mavjud protsessor, apparat tezlatgichi, xotira limiti va yon-kanal xavflarini hisobga olish. Bitta qatlamdagi afzallik qolgan ikkitasidagi nuqsonlarni qoplamaydi.

Amaliy loyihada (1) kirish sirining manbai va entropiyasi tavsiflanadi; (2) oflayn parol tanlash va fizik kirish kabi tahdidlar ajratiladi; (3) mos KDF oilasi tanlanadi; (4) hosila kalitlarga bir qiymatli kontekst yorliqlari biriktiriladi; (5) standart test vektorlari va noto‘g‘ri parametrlarni rad etish holatlari tekshiriladi; (6) unumdorlik va xotira sarfi maqsadli platformada o‘lchanadi. Ushbu ketma-ketlik standart konstruksiyalardan noto‘g‘ri foydalanish xavfini kamaytiradi.

Xulosa

HMAC, AES-CMAC va KMAC zamonaviy PRF-KDF tizimlarining muhim qurilish bloklari hisoblanadi, lekin ularning samaradorligi va mosligi foydalanilayotgan platforma hamda protokolga bog‘liq. HKDF statistik jihatdan notekis bo‘lishi mumkin bo‘lgan yetarli entropiyali sirdan tayanch kalit ajratish va uni kontekstga bog‘liq ravishda kengaytirish uchun qulay. NIST SP 800-108 Rev. 1 esa mavjud kuchli kalitni hisoblagichli, teskari bog‘lanishli, ikki konveyerli hamda KMACga oid usullar bilan kengaytirishni tartibga soladi. Parol uchun esa PBKDF2, scrypt va Argon2id kabi maxsus, resurs xarajatini boshqaruvchi mexanizmlar zarur. Demak, xavfsiz tanlovning hal qiluvchi mezoni algoritmning umumiy ommabopligi emas, balki kirish materialining tabiati, domenlarni ajratish sifati va amalga oshirishning tahdid modeliga mosligidir.

Foydalanilgan adabiyotlar

1. Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997. DOI: 10.17487/RFC2104.

2. NIST. The Keyed-Hash Message Authentication Code (HMAC). FIPS 198-1, 2008. DOI: 10.6028/NIST.FIPS.198-1.

3. NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. SP 800-38B, 2016 update. DOI: 10.6028/NIST.SP.800-38B.

4. Chen L. Recommendation for Key Derivation Using Pseudorandom Functions. NIST SP 800-108 Rev. 1, Update 1, 2024. DOI: 10.6028/NIST.SP.800-108r1-upd1.

5. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, 2010. DOI: 10.17487/RFC5869.

6. Kelsey J., Chang S., Perlner R. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. NIST SP 800-185, 2016. DOI: 10.6028/NIST.SP.800-185.

7. Krawczyk H. Cryptographic Extraction and Key Derivation: The HKDF Scheme. CRYPTO 2010, LNCS 6223, pp. 631–648. DOI: 10.1007/978-3-642-14623-7_34.

8. Moriarty K. et al. PKCS #5: Password-Based Cryptography Specification Version 2.1. RFC 8018, 2017. DOI: 10.17487/RFC8018.

9. Percival C., Josefsson S. The scrypt Password-Based Key Derivation Function. RFC 7914, 2016. DOI: 10.17487/RFC7914.

10. Biryukov A., Dinu D., Khovratovich D., Josefsson S. Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications. RFC 9106, 2021. DOI: 10.17487/RFC9106.

XFA-256 XESH FUNKSIYA ALGORITMINI ISHLAB CHIQISH VA KRIPTOBARDOSHLILIGINI ASOSLASH

Ortikov J.K.
O‘zbekiston Respublikasi Mudofaa vazirligi Markaziy apparati

Annotatsiya. Mazkur maqolada yangi XFA-256 xesh funksiya algoritmini ishlab chiqish va kriptobardoshliligini asoslash bilan bog‘liq masalalar bayoni keltirilgan. Kriptoalgoritmlarni yaratish bo‘yicha umum e’tirof etilgan talablar hamda xesh-funksiya algoritmini qurish sxemalarining qiyosiy tahlili asosida XFA-256 kalitsiz xesh funksiya algoritmi ishlab chiqilib, barcha variantlarni saralash qilish, tug‘ilgan kun haqidagi porodoks hamda 11 raunddan keyin differensial kriptotahlil usuliga bardoshli ekanligi nazariy asoslangan. Shuningdek, XFA-256 xesh funksiya algoritmidan olingan qiymatlarning Lavin effekt samaradorligi NIST testlariga tekshirish orqali baholangan va 16 ta NIST testining 11 tasidan muvaffaqiyatli o‘tkazilgan.

Kalit so‘zlar: xesh funksiya, “Gubka” sxemasi, siqish funksiyasi, xesh qiymat, ma’lumotlarning butunligi, chiziqsiz akslantirish, differensial kriptotahlil, NIST testlari.

Аннотация. В статье рассматриваются вопросы разработки нового криптографического алгоритма хеш-функции XFA-256 и теоретического обоснования его криптографической стойкости. На основе сравнительного анализа общепринятых требований к разработке криптографических алгоритмов и схем построения хеш-функций разработан новый алгоритм бесключевой хеш-функции XFA-256. Теоретически обоснована его устойчивость к атакам методом полного перебора и атакам, основанным на парадоксе дней рождения, а также к дифференциальному криптоанализу после 11 раундов. Кроме того, эффективность лавинного эффекта хеш-функции XFA-256 оценена с использованием набора статистических тестов NIST. Алгоритм успешно прошёл 11 из 16 статистических тестов NIST.

Ключевые слова: хеш-функция, конструкция «Губка», функция сжатия, хеш-значение, целостность данных, нелинейное преобразование, дифференциальный криптоанализ, статистические тесты NIST.

Kirish

Zamonaviy telekommunikatsiya texnologiyalarining jadal sur’atlarda rivojlanishi natijasida bugungi kunda dunyoning istalgan joyidan turib axborotni elektron ko‘rinishda tezkor almashish imkoniyati yaratildi. Shu bilan birga, ushbu axborotning butunligini buzish (o‘zgartirish, boshqa axborotga almashtirish) kabi xavflar ham ortib bormoqda. Elektron axborotning butunligini ta’minlashda kriptografik usul eng samaralisi bo‘lib, bu asosan kriptografik xesh funksiya algoritmlari yordamida amalga oshiriladi. Shu bois, kriptoalgoritmlarni yaratish bo‘yicha umum e’tirof etilgan talablar va xesh-funksiya algoritmini qurish sxemalari tahlili asosida xavfsizlik va tezlik ko‘rsatkichlari bo‘yicha yuqori samaradorlikka ega bo‘lgan yangi xesh funksiya algoritmlarini ishlab chiqish hamda uning kriptobardoshliligini baholash dolzarb hisoblanadi.

Asosiy qism

XFA-256 kalitsiz xesh funksiya algoritmini ishlab chiqish

Xesh funksiya algoritmlarini yaratish bo‘yicha umum e’tirof etilgan zaruriy talab va tamoyillaridan kelib chiqib, shuningdek xesh funksiya algoritmlarini loyihalash bosqichlari [1] asosida XFA-256 kalitsiz xesh funksiya algoritmi yaratildi. XFA-256 xesh funksiya algoritmini

yaratish uchun “Gubka” sxemasi va siqish funksiyasi sifatida “psevdotasodifiy o‘rin almashtirish” usuli tanlandi [2].

XFA-256 kalitsiz xesh funksiya algoritmi akslantirishlari har bir elementi 32 bitdan iborat bo‘lgan A[8x8] massiv yoki b bit uzunlikdagi vektor ustida amalga oshiriladi, ya’ni “Gubka”ning ichki holati $S = b = 64 * 32 = 2048$ bit. S ikki qismdan iborat bo‘lib, $S = S_1||S_2$, S_1 qismi $r = 768$ bit, S_2 qismi $c = 1280$ bit. S ning dastlabki holati 0^{2048} (2048 ta 0) ga teng.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

1-bosqich. To‘ldirish bitlarini qo‘shish. Xeshlanadigan ma’lumot uzunligi ixtiyoriy bo‘lib, ushbu ma’lumot uzunligi 768 bit bo‘lgan teng bloklarga ajratiladi. Agar oxirgi blok uzunligi 768 bitdan kichik bo‘lsa, $0x80_{16}$ va 768 bitgacha nol bilan to‘ldiriladi:

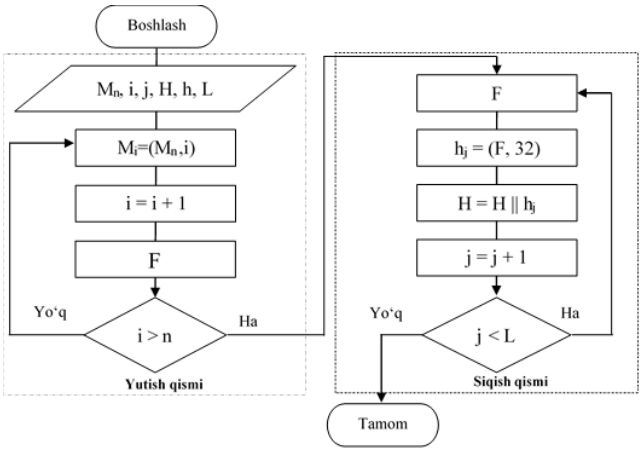
$$M = M_n||80_{16}, 0_{16} \dots . 0_{16}. \quad (1)$$

2-bosqich. Ma’lumotning uzunligini qo‘shish. 1- bosqichning natijasiga berilgan ma’lumot uzunligining 768 bit registrda tasvirlanadigan qiymati biriktiriladi. Ya’ni, xeshlanadigan ma’lumotning uzunligining ikkilik sanoq tizimidagi ko‘rinishi mod 2^{768} bo‘yicha hisoblanib, bitlar soni bilan aniqlanadigan ma’lumot uzunligini bildiruvchi blok hosil qilinadi.

3-bosqich. Nazorat yig‘indisini qo‘shish. 2- bosqichning natijasiga berilgan ma’lumotning nazorat yig‘indisini bildiruvchi 768 bitli blok biriktiriladi. Nazorat yig‘indisini bildiruvchi blok oxirgi to‘liqmas blok nol bilan to‘ldirilgandan keyin har bir 768 bitli blokning mos 32 bit qismlari mod 2^{32} amali bo‘yicha qo‘shiladi. Hosil bo‘lgan natijalar konketenatsiya qilinib, 768 bitli blok ma’lumot oxiriga qo‘yiladi.

4-bosqich. Ma’lumotni 768 bitli bloklarga ajratib qayta ishlash. Yuqoridagi 3 ta bosqich bajarilgandan keyin kengaytirilgan ma’lumotni 768 bitli bloklarga ajratib Gubka sxemasi asosida qayta ishlash amalga oshiriladi.

Quyida XFA-256 xesh funksiya algoritmining blok-sxemasi keltirilgan (1- rasm):



1- rasm. XFA-256 xesh funksiya algoritmining blok-sxemasi.

Bu yerda M_n – n ta blokdan iborat ma’lumot, i va j o‘zgaruvchilar, H – xesh qiymat, h – F funksiyadan olinadigan 32 bitli qiymat, L – xesh qiymat uzunligining 32 ga karrali son miqdori (XFA-256 uchun L = 8 ga teng).

F-siqish funksiyasining qadamlar ketma-ketligi:

1. 768 bitli M_x blok 24 ta 32 bitli elementlarga $M_x = m_0||m_1|| \dots ||m_{23}$ bo‘linadi va hosil bo‘lgan m_k bloklarning XOR amali bo‘yicha yig‘indisi hisoblanadi:

$$P = \sum_{k=0}^{23} m_k,$$

yoki,

$$P = m_0 \oplus m_1 \oplus \dots \oplus m_{23}. \quad (2)$$

2. A[8x8] massivning dastlabki 24 ta elementiga m_k blok qiymati va P ning qiymati 11 bitga siklik surilib, XOR amali bo‘yicha qo‘shiladi:

$$A_{i,j} = A_{i,j} \oplus m_{(8i+j)}, \quad (3)$$

bu yerda $i = \overline{0,2};\ j = \overline{0,7};$

$$A_{i,j} = A_{i,j} \oplus P \ll 11, \quad (4)$$

bu yerda $i = \overline{0,7};\ j = \overline{0,7};$

3. Ma’lumotning bir bitining o‘zgarishi boshqa bitlarga o‘z ta’sirini yanada samarali o‘tkazishi uchun A massivning har bir elementi shu element turgan satr va ustun elementlarining XOR yig‘indisi (SUXY) 11 bit chapga surilib, XOR amali bo‘yicha $A_{i,j}$ elementga qo‘shiladi:

$$A_{i,j} = A_{i,j} \oplus SUXY \ll 11, \quad (5)$$

bu yerda SUXY =SUXY $\oplus \begin{cases} A_{k,j}, & k \neq i \text{ bo‘lsa;} \\ A_{i,k}, & k \neq j \text{ bo‘lsa;} \end{cases}$ $i = \overline{0,7};\ k = \overline{0,7};$

A massivning bitta elementining o‘zgarishi (5) formula orqali ushbu massivning kamida 50 ta elementning o‘zgartirishiga sabab bo‘ladi.

4. Aralashtirish almashtirishi sifatida 64 elementdan iborat buffer massivdan foydalanilgan. Buffer massivining har bir elementi 32 bitga va uning umumiy uzunligi 2048 bitga teng. Buffer massivining indeksi sifatida OY massividan olingan elementlar ketma-ketligi qaraladi:

$$\mathrm{Buf}_{\mathrm{OY[8i+j]}} = \mathrm{A_{i,j}}. \quad (6)$$

OY – shaxmat doskasidagi ot yurishi ketma-ketligini o‘zida mujassamlashtirgan 64 elementdan iborat bir o‘lchovli massivdir.

Bugungi kunda oddiy, jadvalli, gamilton marshruti asosidagi o‘rin almashtirish sxemalari mavjud bo‘lib, gamilton marshruti asosidagi o‘rin almashtirish sxemalari qolgan o‘rin almashtirish sxemalariga qaraganda bardoshli hisoblanadi [3]. Shunga ko‘ra, 8x8 shaxmat doskasida (x,y) pozitsiyada turgan otning barcha kataklarga bir martadan yurib bosib o‘tish ketma-ketligi asosida to‘ldirilgan jadval o‘rin almashtirish sxemasi sifatida tanlangan.

5. A massivning elementlari (7) formula orqali chiziqsiz akslantirishdan o‘tkaziladi.

Yagona chiziqsiz akslantirish quyidagi formulada keltirilgan bo‘lib, ushbu akslantirish buffer massiviga olingan elementlarni o‘zaro mantiqiy AND, NOT, XOR, siklik surish amallaridan foydalanib A massivga qayta yozishdan iborat.

$$\mathrm{A}_{i,j} = \mathrm{A}_{i,j} \oplus \Big(\sim \mathrm{Buf}_{(8i+j)} \oplus \mathrm{Buf}_{((8i+j)+1)mod64} \oplus (\mathrm{Buf}_{((8i+j)+2)mod64} \wedge$$
$$\wedge\, \mathrm{Buf}_{((8i+j)+3)mod64}) \ll 11\Big), \quad (7)$$

bu yerda $i = \overline{0,7};\ j = \overline{0,7};$ ~ -“inkor” NOT, ∧- “mantiqiy ko‘paytirish” amallari.

6. A massivning birinchi elementiga raund konstantasi qo‘shiladi:

$$\mathrm{A}_{0,0} = \mathrm{A}_{0,0} \oplus L_r\ , \quad (8)$$

bu yerda L_r raund konstantasi.

7. A massivning $\mathrm{A}_{0,0}$ elementi H o‘zgaruvchiga quyidagicha konketenatsiya qilib yig‘ilib boriladi:

$$H = H||A_{0,0}. \quad (9)$$

XFA-256 xesh funksiya algoritmining kriptobardoshliligini baholash

XFA-256 xesh funksiya algoritmi mavjud barcha variantlarni tahlil qilish (to‘liq saralash), tug‘ilgan kun haqidagi paradoks va differensial kriptotahlil usullariga bardoshliligi baholandi.

XFA-256 xesh funksiya algoritmining chiquvchi xesh qiymati 256 bit uzunlikka ega bo‘lganligi sababli to‘liq tanlash usuli bilan kolliziya topish uchun H (256) ni beradigan 2^{256} ta ochiq matnni tahlil qilish talab etiladi. Bu o‘z navbatida bugungi kundagi hisoblash texnikasi imkoniyat darajasidan chiqib ketadi.

Umumiy holda tug‘ilgan kun haqidagi paradoks usuli yordamida kolliziya topish quyidagi ifoda orqali topiladi [4].

$$k = \sqrt{n \cdot \ln\left(\frac{1}{1-P_z}\right)} \quad (10)$$

bu yerda P_z- ixtiyoriy ikkita qiymatning bir xil bo‘lish ehtimolligi, P_z=0.5 bo‘lganda:

$$k = \sqrt{n * \ln\left(\frac{1}{1-0.5}\right)} = \sqrt{n * ln2} = 0.83\sqrt{n} \quad (11)$$

XFA-256 kalitsiz xesh funksiya algoritmi uchun ushbu usul yordamida kolliziya topish uchun,

$\text{Matnlar soni} \approx \sqrt{2 * 2^{\mathrm{H}} * \ln \mathrm{p}^{-1}} = \sqrt{2 * 2^{256} * \ln 2^{1}} \approx 2^{128}$ ta ochiq matnni tahlil qilish kerak bo‘ladi. Bugungi kundagi hisoblash texnikasi imkoniyat orqali 2^{128} ta ochiq matnni tahlil qilish imkonsiz.

Xesh funksiya algoritmlarida differensial kriptotahlil usuli chiquvchi ayirma 0 ga teng bo‘ladigan kiruvchi orttirmani topishga asoslangan. Ya’ni, kirishda bir-biridan farqli ikkita ma’lumotdan chiqishda bir xil xesh qiymatga ega bo‘lish holati kolliziya deb ataladi [5, 6].

“XFA-256” xesh funksiya algoritmi uchun differensial kriptotahlil usuliga bardoshliligini baholash deganda unda qatnashgan chiziqsiz akslantirishga kiruvchi orttirmani har bir raunddan o‘tgandan keyin qanday ehtimollik bilan chiquvchi orttirmaga tengligini hisoblab chiqish va umumiy ehtimollik bugungi kundagi hisoblash texnikasi imkoniyat darajasidan qanchalik farq qilishi bilan baholanadi. “XFA-256” xesh funksiya algoritmining chiziqsiz akslantirishi 8x8 matritsa ko‘rinishida bo‘lib, uni har bir elementi 32 bitdan iborat. Chiziqsiz akslantirishga 2048 bit kirib 2048 bit chiqadi.

“XFA-256” xesh funksiya algoritmining differensial kriptotahlil usuliga bardoshliligini baholashda 2048 bitli orttirmani kuzatishning imkoni bo‘lmaganligi sababli o‘quv algoritmiga nisbatan kriptotahlil o‘tkaziladi va “XFA-256” xesh funksiya algoritmiga nisbatan fikrlar aytiladi. Shuning uchun algoritm xususiyatini saqlab qolgan holda uning kichik bitlar ustida ishlovchi “XFA-3” o‘quv algoritmi ishlab chiqildi va quyida bayoni keltiriladi.

“XFA-3” xesh funksiya o‘quv algoritmi akslantirishlari har bir elementi L = 3 bitdan iborat bo‘lgan A[5x5] massiv yoki b = 75 bitli vektor ustida amalga oshiriladi, ya’ni Gubka sxemasi ichki holati S = b = 25*3 = 75 bit. L = 3 bit bo‘lgan holatda S = 75 bit bo‘ladi va S ikki qismdan iborat bo‘lib, $S = S_1||S_2$, S_1 qismi r = 15 bit, S_2 qismi s = 60 bit. S ning dastlabki holati 0^{75} (75 ta 0) ga teng.

Ma’lumotni 15 bitli bloklarga ajratib qayta ishlash.

1. M_x blok 5 ta 3 bitli so‘zlarga bo‘linib, $M_x = m_0|| m_1||\dots ||m_4$, $P_x=\sum_{k=0}^{23} m_k = m_0 \oplus m_1 \oplus \dots \oplus m_4$ formula yordamida m_k bloklarning XOR amali bo‘yicha yig‘indisi hisoblanadi.

2. A[5x5] massivning dastlabki 5 ta elementiga m_k blok qiymati XOR amali bo‘yicha $A_{0,j} = A_{0,j} \oplus m_k$ formula yordamida qo‘shiladi, bu yerda k, j = 0.. 4.

3. A[5x5] massivning har bir elementiga va P_x ning qiymati 1 bitga siklik surib, $A_{i,j} = A_{i,j} \oplus P_x << 1$ formula yordamida qo‘shiladi, bu yerda i = 0..2, j=0..7.

4. Raund akslantirishlari. A massivning har bir elementi uchun shu element ($A_{i,j}$) turgan satr va ustun elementlarining XOR yig‘indisi hisoblanib, natija 1 bitga siklik suriladi va $A_{i,j}$ elementga qo‘shiladi.

5. Elementlarni o‘rnini almashtirish uchun bir o‘lchovli 25 ta elementdan iborat bufer massivdan foydalaniladi. Buf[0..24], $|buf_s|$ = 3 bit, s = 0..24. Buffer massivi 5x5 shaxmat doskasidagi ot yurishi ketma-ketligini o‘zida mujassamlashtirgan 25 elementli bir o‘lchovli massiv.

6. A massiv elementlari (2.18) formula orqali chiziqsiz akslantirishdan o‘tkaziladi. Bunda, siklik surish 11 bit o‘rniga 1 bit va indeksda turgan ifodalar qiymati mod64 o‘rniga mod25 bo‘yicha olinadi.

7. A massivning birinchi elementiga raund konstantasi qo‘shiladi.

8. A massivning $A_{0,0}$ elementi H o‘zgaruvchiga konketenatsiya qilib yig‘ilib boriladi, agar qayta ishlanadigan blok bo‘lsa, 1- qadamga, aks holda 9- qadamga o‘tiladi.

9. Agar H ning uzunligi 3 bitdan kichik bo‘lsa, 6- qadamga o‘tiladi, H = 3 bit bo‘lsa ushbu qiymat natija sifatida olinadi.

O‘quv algoritmiga 15 bit ma’lumot kiradi va 3 bit uzunlikdagi xesh qiymat chiqadi. Algoritm akslantirishlarining differensial xususiyati o‘rganib chiqildi va unga ko‘ra 1- akslantirish kiruvchi orttirmani P = 1 ehtimollik bilan keyingi akslantirishga o‘tkazadi.

Algoritmda $A_{i,j} = A_{i,j} \oplus {\sim}Buf_{5i+j} \oplus Buf_{5i+j+1} \oplus (Buf_{5i+j+2} \wedge Buf_{5i+j+3}) << 1$ yagona chiziqsiz akslantirish bo‘lib, ayirmani P = 1 ehtimollik bilan kuzatish imkoni mavjud emas. Qolgan barcha akslantirishlarda orttirmani P = 1 ehtimollikda kuzatish mumkin.

Aynan ushbu akslantirishga ayirma matritsa jadvalini qurish talab etiladi. Ushbu akslantirish mohiyatini saqlab qolgan (bu yerda 1 bitga siklik chapga surish amal o‘z ta’sirini o‘tkazmaydi) holda quyidagicha tasvirlab olindi:

$$y = x_1 \oplus {\sim}x_2 \oplus x_3 \oplus x_4 \wedge x_5 \quad (12)$$

va chinlik jadvali 1 bitga nisbatan qurildi va unda balanslashganlik ta’minlanganligi aniqlandi. Agar chinlik jadvalida 1 bitga nisbatan balanslashganlik ta’minlansa, 3 bit va 32 bitga nisbatan ham balanslashganlik ta’minlanadi.

Differensial kriptotahlil o‘tkazishda chiziqsiz akslantirishga nisbatan ayirma matritsa tuzish zarur hisoblanadi.

Ta’rif. Elementlari quyidagi ifoda bilan aniqlanadigan matritsaga ayirmalar matritsasi deyiladi [5]:

$$\delta = \Delta_{a\to b}^{(F)} |F(x) \oplus F(x \oplus a) = b| \quad x, a \in Z_2^n, b \in Z_2^m \quad (13)$$

bu yerda F kriptografik algoritmlaridagi chiziqsiz akslantirishlardir.

(13) formula bilan aniqlanuvchi eng katta element akslantirishga nisbatan ayirmalar matritsasining maksimumi deyiladi va δ_F kabi belgilanadi [5].

Quyida ayirma matritsani qurish a = 45 (000 000 000 101 101_2) orttirma misolida ko‘rib chiqilgan (ayirma matritsaning bir qismi 1- jadvalda keltirilgan).

1- jadval.

a=45(000 000 000 101 101_2) orttirma uchun ayirma matritsa jadvali

$x = 2^{15}$	y(x)	$x \oplus a$	$y(x \oplus a)$	$b_2=y(x) \oplus y(x+a)$	b_{10}
000000000000001	111	000000000101100	011	100	4
000000000000010	111	000000000101111	010	101	5
.....	.....	.....	.....	.....	.....

.....	.....	.....	.....	.....	.....
111111111111110	011	111111111010011	010	001	1
111111111111111	100	111111111010010	010	110	6

Yuqoridagi jadval hisoblash natijalaridan *a* = 45 kirishga nisbatan quyidagi taqsimot jadvalga ega bo‘linadi (2- jadvalga qarang):

2- jadval.

a = 45 kirishga nisbatan taqsimot jadvali.

$\Delta_{a\to b}^{(F)}$		B							
		0	1	2	3	4	5	6	7
A	45	1558	4694	1542	3590	2562	5762	2049	11010

Xuddi shu amallarni *a* ning barcha 0 dan 2^{15}-1 gacha qiymatlari uchun bajarib, quyidagi umumiy kirish va chiqishga nisbatan taqsimot jadvali hosil qilinadi (ayirma matritsaning bir qismi 3- jadvalda keltirilgan):

3- jadval.

Kirish va chiqishga nisbatan taqsimot jadvali

15 bit kirib 3 bit chiquvchi akslantirish uchun ayirma matritsa jadvali								
a/b	000	001	010	011	100	101	110	111
000000000000001	1558	4694	1542	3590	2562	5762	2049	11010
000000000000010	518	4614	2582	3670	1025	9986	3586	6786
000000000000011	3670	2582	2566	2566	6786	1538	7938	5121
000000000000100	4738	2562	7938	5121	5718	1558	2566	2566
000000000000101	1558	4694	1542	3590	2562	5762	2049	11010
000000000000110	1	**9986**	3586	6786	1542	4614	2582	3670
000000000000111	3670	2582	2566	2566	6786	1538	7938	5121
000000000011000	2566	2566	2582	3670	5121	4938	1538	**6786**
.....	...	...	...	...	...	...	**...**	...
111111111111110	4095	4096	4096	4096	4096	4096	4096	4096
111111111111111	1558	4694	1542	3590	2562	5762	2049	11010

Yuqorida keltirilgan tahlil natijalaridan kelib chiqib, quyida bitta optimal orttirma uchun “XFA-3” xesh funksiya o‘quv algoritmiga differensial kriptotahlil o‘tkazish jarayoni ko‘rib chiqiladi.

Kiruvchi orttirma $\Delta X = 000\ 000\ 000\ 101\ 101_2$ bo‘lsin. Ushbu orttirma 5 ta 3 bitli so‘zlarga ajratiladi ($m_0 = 000$, $m_1 = 000$, $m_2 = 000$, $m_3 = 101$, $m_4 = 101$) va akslantirishlardan o‘tishini kuzatiladi.

$A_{0,0}$ ni hisoblashda akslantirishga kiruvchi orttirma $\Delta X = 000\ 000\ 000\ 110\ 000_2$ bo‘lganda 000_2 chiqishi $P = 7938/2^{15} = 1/4$ ehtimollik bilan bajariladi. Shu tariqa qolgan elementlar ham hisoblab chiqilsa quyidagi jadvalga ega bo‘linadi (4-jadvalga qarang).

4- jadval.

1- raund chiziqsiz akslantirish natijasining ehtimolli qiymatlari jadvali.

Element	Kiruvchi orttirma, ΔX	Chiquvchi qiymat, ΔY	Ehtimollik, P
$A_{0,0}$	000 000 000 110 000	000	1/4
$A_{0,1}$	000 000 110 000 000	000	1/4
$A_{0,2}$	000 110 000 000 000	000	4/25

$A_{0,3}$	110 000 000 000 000	001,011,101,111	1/5
$A_{0,4}$	000 000 000 000 110	001	3/10
$A_{1,0}$	000 000 101 101 110	001	3/10
$A_{1,1}$	000 101 101 110 000	001	1/7
$A_{1,2}$	101 101 110 000 000	101	4/25
$A_{1,3}$	101 110 000 000 101	110	1/4
$A_{1,4}$	110 000 000 101 101	110	1/4
$A_{2,0}$	000 000 000 000 000	000	1
$A_{2,1}$	000 000 000 000 000	000	1
$A_{2,2}$	000 000 000 000 000	000	1
$A_{2,3}$	000 000 000 000 000	000	1
$A_{2,4}$	000 000 000 000 000	000	1
$A_{3,0}$	000 000 000 000 000	000	1
$A_{3,1}$	000 000 000 000 000	000	1
$A_{3,2}$	000 000 000 000 000	000	1
$A_{3,3}$	000 000 000 000 000	000	1
$A_{3,4}$	000 000 000 000 000	000	1
$A_{4,0}$	000 000 000 000 011	110	1/4
$A_{4,1}$	000 000 000 011 000	111	1/5
$A_{4,2}$	000 000 011 000 000	111	1/5
$A_{4,3}$	000 011 000 000 000	100	4/25
$A_{4,4}$	011 000 000 000000	101,110,111	4/25

$A_{0,0} = A_{0,0} \oplus L_1 = 000_2 \oplus 001_2 = 001_2$

$H = H \parallel A_{0,0} = 001_2$, demak, birinchi raundda o‘quv algoritmining 3 bit xesh qiymati va asosiy algoritmdagi 32 bit xesh qiymatga kolliziya topish uchun kerak bo‘ladigan matnlar soni (N) quyida keltirilgan:

$$N_{3\text{ bit uchun}} \approx \sqrt{2 * 2^N * \ln p^{-1}} = \sqrt{2 * 2^3 * \ln 2^2} \approx 2^2$$

$$N_{32\text{ bit uchun}} \approx \sqrt{2 * 2^N * \ln p^{-1}} = \sqrt{2 * 2^{32} * \ln 2^2} \approx 2^{17}$$

Agar algoritm 1 raunddan iborat bo‘lsa “XFA-256” xesh funksiya algoritmiga bugungi kundgi hisoblash texnikasi yordamida kolliziya topish mumkin.

$A_{0,0}$ ni hisoblashda akslantirishga kiruvchi orttirma $\Delta X=000\ 101\ 000\ 100\ 110_2$ bo‘lganda 2.5- jadvalga ko‘ra 000_2 chiqishi $P=4172/2^{15}=1/8$ ehtimollik bilan bajariladi. $A_{0,0}$ ni hisoblash jarayonida oldingi raunddan ma’lum bir ehtimollik bilan chiqqan $A_{0,0}$, $A_{0,1}$, $A_{0,2}$, $A_{0,3}$, $A_{0,4}$ elementlar ishtirok etadi. Umumiy ehtimollik

$P_{3umum}=P*P(A_{0,0})*P(A_{0,1})*P(A_{0,2})*P(A_{0,3})*P(A_{0,4})= 1/8*1/2^{13}*1/2^{13}*1/2^{12}*1/2^{12}*1/2^{13} \approx 1/2^{66}$. Shu tariqa qolgan raundlar ham hisoblab chiqiladi.

$P_{4umum}=P*P(A_{0,0})*P(A_{0,1})*P(A_{0,2})*P(A_{0,3})*P(A_{0,4})= 1/8*1/2^{66}*1/2^{66}*1/2^{66}*1/2^{66}*1/2^{66} \approx 1/2^{333}$.

$P_{5umum}=P*P(A_{0,0})*P(A_{0,1})*P(A_{0,2})*P(A_{0,3})*P(A_{0,4})= 1/4*1/2^{333}*1/2^{333}*1/2^{333}*1/2^{333}*1/2^{333} \approx 1/2^{1667}$

Tug‘ilgan kun paradoksi usuli yordamida algoritmi raundlarida kolliziya topishda zaruriy ochiq matnlar soni quyidagi 5-jadvalda keltirilgan.

5- jadval.

“XFA-256” xesh funksiya algoritmi raundlarida kolliziya topish uchun kerak bo‘ladigan ochiq matnlar soni jadvali

“XFA-256” raundlari	Kolliziya topish uchun zaruriy matnlar soni

1-raund	2^{17}
2-raund	2^{18}
3-raund	2^{19}
4-raund	2^{22}
5-raund	2^{23}
6-raund	2^{24}
7-raund	2^{25}
8-raund	2^{26}
9-raund	2^{28}
10-raund	2^{30}
11-raund	2^{32}

XFA-256 xesh funksiya algoritmidan chiquvchi qiymat bitlarining tasodifiyligini tekshirish uchun grafik va baholash testlarini o‘zida mujassamlashtirgan NIST STS testlariga tekshirildi va 20 raund natijasiga ko‘ra testlarning 11 tasidan muvaffaqiyatli o‘tkazildi [40; 27 – 33- b]. Shuningdek, XFA-256 xesh funksiya algoritmida raund xesh qiymatlari bir-biriga bog‘liqligini tekshirish maqsadida korelyatsiya koeffitsienti va Xemming masofasini hisoblovchi dasturiy ta’minot yaratildi. Texnik imkoniyatlardan kelib chiqib, ketma- ket raunddan olingan 128 bit xesh qiymatlar tahlil qilindi. Ularning korelyatsiya koeffisienti hamda Xemming masofalari belgilangan oraliqda yotishi va bundan raund xesh qiymatlari orasida bog‘liqlik yo‘q ekanligi dasturiy ta’minot yordamida aniqlandi.

Xulosa

Tadqiqot ishi doirasida kriptografik akslantirishlarni matematik asoslagan holda tanlash orqali ma’lumotlarning yaxlitligini ta’minlash hamda psevdotasodifiy qiymatlarni generatsiya qilish imkonini beruvchi XFA-256 xesh funksiya algoritmi ishlab chiqilgan hamda barcha variantlarni tahlil qilish, tug‘ilgan kun haqidagi paradoks va 11 raunddan keyin differensial kriptotahlil usuliga bardoshli ekanligi nazariy asoslangan. Shuningdek, NIST STS testlarining 11 tasidan muvaffaqiyatli o‘tkazilgan. Taklif etilgan XFA-256 kalitsiz xesh funksiya algoritmini milliy kriptografik standartlar bilan uyg‘unlashtirgan holda axborotni kriptografik muhofaza qilish vositalarida konfidensial ma’lumotlarning butunligini ta’minlashda, Elektron raqamli imzo vositalarida hamda maxfiy parametrlarni generatsiya qilishda, shuningdek o‘quv jarayonlarida qo‘llash tavsiya etiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. Ortikov, J.K. Yangi kriptobardoshli xesh-funksiya algoritmlarini qurish bosqichlari / J.K. Ortikov // Axborot texnologiyalari va kommunikatsiyalari sohasida axborot xavfsizligi muammolari respublika ilmiy-texnik seminari materiallari to‘plami. –2020. –B. 3-13.

2. Ortikov, J.K. Gubka sxemasi asosidagi yangi kalitsiz xesh funksiya algoritmi / J.K. Ortikov // Professional armiyaning rivojlanishida raqamli iqtisodiyot va intellektual tizimlarning o‘rni mavzusidagi respublika ilmiy-uslubiy konferensiyasi maqolalar to‘plami. –T.: AKT va AHI, 2020. – B.71-76.

3. Гик Е.Я. “Шахматы и математика”.Библотека математического колледжа НМУ. Москва 1983.(22-28 бет.)

4. Нилс, Ф. Практическая криптография / Ф. Нилс, Б. Шнаер. –М., 2005. 419 с.

5. Бабенко, Л.К. Дифференциальный криптоанализ упрощенной функции хеширования SHA / Л.К. Бабенко, Е.А. Ищукова // Известия ЮФУ. Технические науки. – Таганрог., 2010. № 11, 203-219 с.

6. Тевяшев, А.Д. Оценка опасности криптоаналитических атак методом создания коллизий / А.Д. Тевяшев, Ю.И. Горбенко. // Известия Харьковский национальный университет радиоэлектроники. –Харьков., 2013. №4(4). –С 18-25.

IOT ALOQA PROTOKOLLARINI HIMOYA QILISH UCHUN ELLIPTIK KRIPTOGRAFIYA ASOSIDA SAMARALI KALIT YARATISH USULLARI

Fozilov Sh.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu ishda Internet of Things (IoT) qurilmalarida aloqa protokollarini himoya qilish uchun elliptik kriptografiya (ECC) asosidagi kalit yaratish usullarining samaradorligi tadqiq etiladi. Resurslari cheklangan IoT qurilmalarida an'anaviy RSA va DH algoritmlari samarali ishlamaydi. MQTT va CoAP protokollarida qo'llaniladigan ECDH va ECDSA algoritmlari xavfsizlik darajasi, kalit va uzatiladigan ma'lumotlar hajmi, 8-bitli mikrokontrollerlarda bajarilish vaqti va energiya sarfi bo'yicha ilmiy manbalar va standartlar asosida qiyosiy tahlil qilindi. Natijalar Curve25519 egri chizig'i asosidagi ECDH (X25519) algoritmi IoT uchun eng maqbul yechim ekanini ko'rsatadi.

Kalit so'zlar: elliptik kriptografiya, ECC, IoT, kalit yaratish, ECDH, ECDSA, Curve25519, MQTT, CoAP, resurs cheklangan qurilmalar.

Аннотация: В работе исследуется эффективность методов генерации ключей на основе эллиптической криптографии (ECC) для защиты протоколов связи устройств Интернета вещей (IoT). На устройствах с ограниченными ресурсами традиционные алгоритмы RSA и DH работают неэффективно. На основе научных источников и стандартов проведён сравнительный анализ алгоритмов ECDH и ECDSA, применяемых в протоколах MQTT и CoAP, по уровню стойкости, размеру ключей и передаваемых данных, времени выполнения и энергопотреблению на 8-битных микроконтроллерах. Результаты показывают, что алгоритм ECDH на кривой Curve25519 (X25519) является наиболее оптимальным решением для IoT.

Ключевые слова: эллиптическая криптография, ECC, IoT, генерация ключей, ECDH, ECDSA, Curve25519, MQTT, CoAP, устройства с ограниченными ресурсами.

Kirish

Bugungi kunda Internet of Things (IoT) texnologiyasi sanoat avtomatikasi, aqlli shaharlar, tibbiyot va qishloq xo'jaligida keng qo'llanilmoqda. Qurilmalar soni ortishi bilan ularning axborot xavfsizligini ta'minlash muammosi ham dolzarblashib bormoqda.

IoT qurilmalari odatda cheklangan hisoblash quvvati, kichik xotira va past energiya sarfiga ega. Shu sababli RSA va Diffie-Hellman (DH) kabi an'anaviy algoritmlarni ularda qo'llash qiyin. Elliptik kriptografiya (ECC) esa ancha qisqa kalit bilan teng xavfsizlikni ta'minlaydi: 256-bitli ECC kaliti 3072-bitli RSA kalitiga ekvivalent xavfsizlikni ta'minlaydi [1].

Shu sababli ECC ning IoT qurilmalarida qo'llanilishi ilmiy va amaliy jihatdan muhim ahamiyat kasb etadi. Ishning maqsadi - MQTT va CoAP protokollarida qo'llaniladigan ECDH va ECDSA algoritmlarini xavfsizlik darajasi, ma'lumotlar hajmi va resurs sarfi bo'yicha qiyosiy tahlil qilib, IoT qurilmalari uchun maqbul kalit yaratish sxemasini aniqlash. Ishning ilmiy yangiligi shundaki, kalit va imzo hajmlari IEEE 802.15.4 kadri chegarasi bilan bog'lab baholandi. Shuningdek, 8-bitli mikrokontrollerlar bo'yicha turli manbalardagi natijalar umumlashtirilib, sensor qurilmalari uchun algoritm tanlash mezonlari ishlab chiqildi.

Asosiy qism

ECC asoslari N. Koblitz [2] va V. Miller [3] tomonidan bir-biridan mustaqil ravishda taklif etilgan. Keyinchalik D. Hankerson, A. Menezes va S. Vanstone [4] elliptik egri chiziqlar ustidagi arifmetik amallar, kalit almashinuvi va raqamli imzo algoritmlarining nazariy va algoritmik asoslarini batafsil yoritdi. Resurs cheklangan qurilmalarda ECC ning afzalligi bir qator eksperimental ishlarda tasdiqlangan. N. Gura va boshqalar [5] 8 MGs chastotali 8-bitli ATmega128 mikrokontrollerida 160-bitli ECC nuqtani ko‘paytirish amali 0,81 s, RSA-1024 yopiq kalit amali esa 10,99 s davom etishini aniqlagan. A. Wander va boshqalar [6] esa ECC-160 asosidagi autentifikatsiya RSA-1024 ga nisbatan 12 baravar kam energiya sarflashini ko‘rsatgan. IETF ning RFC 7925 tavsiyasi [7] ham IoT qurilmalari uchun TLS/DTLS profilida elliptik egri chiziqlarga asoslangan ECDHE va ECDSA algoritmlaridan foydalanishni belgilaydi. Biroq bu natijalar turli platformalarda olingan bo‘lib, ularni MQTT va CoAP protokollari talablari bilan bog‘lab umumlashtiruvchi ishlar hali yetarli emas.

ECC ning matematik asosini chekli maydon F_p ustida berilgan $y^2 = x^3 + ax + b$ ko‘rinishidagi elliptik egri chiziq nuqtalari to‘plami tashkil etadi. Yopiq kalit d tasodifiy butun son sifatida tanlanadi, ochiq kalit esa $Q = d \cdot G$ formula bo‘yicha hisoblanadi, bu yerda G - egri chiziqning bazaviy nuqtasi. Q va G ma’lum bo‘lganda d ni topish masalasi (ECDLP) uchun umumiy egri chiziqlarda subeksponensial algoritm ma’lum emas. Shu sababli ECC qisqa kalit bilan yuqori bardoshlilikni ta’minlaydi [4].

ECDH protokolida ikki tomon o‘z yopiq kalitlari d_A va d_B hamda ochiq kalitlari Q_A va Q_B ni almashib, umumiy maxfiy qiymatni $S = d_A \cdot Q_B = d_B \cdot Q_A$ ko‘rinishida hisoblaydi. ECDSA algoritmi esa xabarlarning yaxlitligi va manbasini tasdiqlash uchun qo‘llaniladi. D. Bernstein tomonidan taklif etilgan Curve25519 egri chizig‘i aynan ECDH uchun tezkor va xavfsiz amalga oshirishga mo‘ljallangan [8]. IoT protokollarida ushbu ikki algoritm birgalikda ishlatiladi: ECDH sessiya kalitini yaratadi, ECDSA esa tomonlarni autentifikatsiya qiladi. MQTT 5.0 [9] TCP ustida TLS orqali, CoAP [10] esa UDP ustida DTLS orqali himoyalanadi. Ikkala holatda ham kalit almashinuvi aynan shu algoritmlar yordamida bajariladi.

Tadqiqotda adabiyotlar tahlili, standartlarni qiyosiy o‘rganish va analitik baholash usullaridan foydalanildi. Algoritmlar to‘rt mezon bo‘yicha taqqoslandi: xavfsizlik darajasi, kalit va imzo hajmi, 8-bitli mikrokontrollerlarda bajarilish vaqti va energiya sarfi. Kam quvvatli simsiz sensor tarmoqlarida keng qo‘llaniladigan IEEE 802.15.4 standartida fizik kadrning umumiy hajmi 127 bayt bilan cheklangan [12]. Shu sababli ochiq kalitni uzatish uchun zarur kadrlar soni ⌈ochiq kalit hajmi / 127⌉ ko‘rinishida quyi chegara sifatida baholandi. Sarlavhalar hisobga olinsa, haqiqiy kadrlar soni bundan ham ko‘p bo‘ladi. Natijalar 1-jadvalda keltirilgan.

1-jadval

Algoritmlarning xavfsizlik darajasi va uzatiladigan ma’lumotlar hajmi

№	Algoritm	Xavfsizlik darajasi (bit) [1]	Ochiq kalit hajmi (bayt)	Imzo hajmi (bayt)	IEEE 802.15.4 kadrlari (kamida)
1	RSA-2048	112	256	256	3
2	DH-2048	112	256	–	3
3	RSA-3072	128	384	384	4
4	ECDH / ECDSA P-256	128	65	64	1
5	ECDH Curve25519 (X25519)	128	32	–	1

Jadvaldan ko‘rinib turibdiki, 128-bitli xavfsizlik darajasida X25519 ochiq kaliti RSA-3072 nikidan 12 marta, P-256 nikidan esa 2 martadan ko‘proq qisqa. ECC ochiq kaliti bitta IEEE 802.15.4 kadriga sig‘adi. RSA va DH esa xavfsizlik darajasi pastroq bo‘lsa ham kamida 3–4 ta kadrni talab qiladi. Har bir qo‘shimcha kadr radiomodulning qo‘shimcha ishlashini, ya’ni batareya sarfini va paket yo‘qolish ehtimolini oshiradi. Bu ayniqsa UDP ustida ishlaydigan CoAP/DTLS uchun muhim. ECDSA P-256 imzosi (64 bayt) ham RSA-3072 imzosidan (384 bayt) 6 marta qisqa.

Hisoblash yuki bo‘yicha 8-bitli AVR mikrokontrollerlarida olingan natijalar 2-jadvalda umumlashtirilgan.

2-jadval

8-bitli AVR mikrokontrollerlarida algoritmlarning bajarilish ko‘rsatkichlari

№	Amal	Platforma	Natija
1	ECC-160 nuqtani ko‘paytirish	ATmega128, 8 MGs	0,81 s [5]
2	ECC-224 nuqtani ko‘paytirish	ATmega128, 8 MGs	2,19 s [5]
3	RSA-1024 yopiq kalit amali	ATmega128, 8 MGs	10,99 s [5]
4	RSA-2048 yopiq kalit amali	ATmega128, 8 MGs	83,26 s [5]
5	X25519 (Curve25519 ECDH)	ATmega2560, 16 MGs	13 900 397 takt ≈ 0,87 s [13]
6	ECC-160 va RSA-1024 autentifikatsiyasi energiyasi	ATmega128L (Mica2dot)	25,5 mJ va 311,8 mJ, ECC 12 baravar kam [6]

2-jadvaldan ko‘rinadiki, bir xil mikrokontrollerda ECC-160 amali RSA-1024 ga nisbatan 13,6 marta tezroq bajariladi (10,99 / 0,81). ECC-224 amali esa 128-bitli darajaga yaqin xavfsizlikni ta’minlagan holda ham RSA-1024 dan 5 marta tez. RSA-2048 yopiq kalit amali esa shu platformada 83,26 s davom etadi, ya’ni RSA-1024 dan 7,6 marta sekin. Bu kalit uzunligi ikki baravar oshganda modulli darajaga ko‘tarish murakkabligining kubik o‘sishiga mos keladi va sensor qurilmalari uchun amalda yaroqsiz qiymatdir. ATmega2560 ning Arduino Mega platasida ishlatiladigan X25519 128-bitli xavfsizlikda bir soniyadan kam, ≈ 0,87 s da bajariladi [13]. Kalit almashinuvi qurilmani ulashda yoki sessiyani yangilashda bir marta bajarilishini hisobga olsak, bu ko‘rsatkich amaliy foydalanish uchun yetarli.

Kuchliroq hisoblash resurslariga ega IoT shlyuzlarida (masalan, ARM Cortex-A protsessorli Raspberry Pi 4) ECC amallari kalit almashinuvi vaqtiga sezilarli hissa qo‘shmaydi. Shu sababli tizimdagi asosiy cheklov oxirgi sensor qurilmalari hisoblanadi.

Xavfsizlik nuqtayi nazaridan, NIST tomonidan tavsiya etilgan P-256 egri chizig‘i 128-bitli xavfsizlik darajasini ta’minlaydi [11]. Curve25519 ham 128-bitli xavfsizlikni ta’minlaydi va doimiy vaqtda bajariladigan Montgomery zinapoyasi hisobiga yon kanal (side-channel) hujumlariga bardoshliroq [8]. RFC 7748 [14] ga ko‘ra, X25519 da istalgan 32 baytli qiymat to‘g‘ri ochiq kalit hisoblanadi, shu sababli nuqtani egri chiziqqa tegishliligini alohida tekshirish talab etilmaydi. Bu esa mikrokontrollerdagi dastur kodini soddalashtiradi va xatolik ehtimolini kamaytiradi.

Xulosa

Tadqiqot natijalari asosida quyidagi xulosalarga kelindi:

1. ECC algoritmlari IoT qurilmalari uchun RSA va DH ga nisbatan ancha samaraliroq. 8-bitli mikrokontrollerda ECC amali RSA ga nisbatan 13,6 marta tezroq bajariladi va 12 baravar kam energiya sarflaydi. 128-bitli xavfsizlikda ECC kaliti RSA kalitidan 12 marta qisqa.

2. Curve25519 asosidagi ECDH (X25519) algoritmi IoT qurilmalari uchun eng maqbul tanlov hisoblanadi. Uning ochiq kaliti 32 bayt bo‘lib, bitta IEEE 802.15.4 kadriga sig‘adi. U ATmega2560 da ≈ 0,87 s da bajariladi va doimiy vaqtli amallar hisobiga yon kanal hujumlariga bardoshli.

3. MQTT (TLS) va CoAP (DTLS) protokollarida kalit almashinuvi uchun ECDHE, autentifikatsiya uchun ECDSA P-256 dan foydalanish RFC 7925 profiliga mos keladi. Bu sxema sensor qurilmalarida RSA ga asoslangan yechimlarga nisbatan uzatiladigan ma’lumotlar hajmini 4–6 baravar kamaytiradi.

O‘zbekistonda aqlli shahar va sanoat avtomatikasi tizimlarini joriy etishda ECC asosidagi kalit boshqarish tizimlarini standart sifatida qabul qilish tavsiya etiladi. Kelgusida mikrokontrollerlarda yopiq kalit uchun ishonchli entropiya manbalarini ta’minlash hamda post-kvant kriptografiya va ECC ni birlashtirgan gibrid sxemalarni tadqiq qilish maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. Barker E. Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1, Revision 5. – Gaithersburg: National Institute of Standards and Technology, 2020. – 158 p. – DOI: 10.6028/NIST.SP.800-57pt1r5.

2. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. – 1987. – Vol. 48, № 177. – P. 203–209.

3. Miller V. S. Use of elliptic curves in cryptography // Advances in Cryptology – CRYPTO ’85. Lecture Notes in Computer Science, vol. 218. – Berlin: Springer, 1986. – P. 417–426.

4. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. – New York: Springer, 2004. – 311 p.

5. Gura N., Patel A., Wander A., Eberle H., Shantz S. C. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs // Cryptographic Hardware and Embedded Systems – CHES 2004. Lecture Notes in Computer Science, vol. 3156. – Berlin: Springer, 2004. – P. 119–132. – DOI: 10.1007/978-3-540-28632-5_9.

6. Wander A., Gura N., Eberle H., Gupta V., Shantz S. C. Energy analysis of public-key cryptography for wireless sensor networks // Proc. 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom 2005). – IEEE, 2005. – P. 324–328.

7. Tschofenig H., Fossati T. Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things. RFC 7925. – IETF, 2016. – DOI: 10.17487/RFC7925.

8. Bernstein D. J. Curve25519: New Diffie-Hellman Speed Records // Public Key Cryptography – PKC 2006. Lecture Notes in Computer Science, vol. 3958. – Berlin: Springer, 2006. – P. 207–228. – DOI: 10.1007/11745853_14.

9. MQTT Version 5.0. OASIS Standard / Eds. A. Banks, E. Briggs, K. Borgendale, R. Gupta. – OASIS, 2019.

10. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP). RFC 7252. – IETF, 2014. – DOI: 10.17487/RFC7252.

11. Chen L., Moody D., Regenscheid A., Robinson A., Randall K. Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. NIST Special Publication 800-186. – Gaithersburg: NIST, 2023. – DOI: 10.6028/NIST.SP.800-186.

12. IEEE Standard for Low-Rate Wireless Networks. IEEE Std 802.15.4-2020. – New York: IEEE, 2020..

13. Düll M., Haase B., Hinterwälder G., Hutter M., Paar C., Sánchez A. H., Schwabe P. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers // Designs, Codes and Cryptography. – 2015. – Vol. 77, № 2–3. – P. 493–514. – DOI: 10.1007/s10623-015-0087-1.

14. Langley A., Hamburg M., Turner S. Elliptic Curves for Security. RFC 7748. – IETF, 2016. – DOI: 10.17487/RFC7748.

RESURSLARI CHEKLANGAN IOT QURILMALARIDA KRIPTOGRAFIK KALITLAR UCHUN ENTROPIYA MANBALARIGA ASOSLANGAN TASODIFIY SONLAR GENERATSIYALASH ALGORITMI

Fozilov Sh.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu ishda apparat tasodifiy sonlar generatoriga (TRNG) ega bo‘lmagan, resurslari cheklangan IoT qurilmalarida kriptografik kalitlar uchun yetarli entropiyani ta’minlash muammosi tadqiq etiladi. Arduino muhitida keng tarqalgan randomSeed(analogRead()) usuli yopiq kalit entropiyasini 10 bitdan oshirmasligi ko‘rsatildi. Muammoni hal etish uchun SRAM ishga tushish holati va soat generatorlari jitteridan entropiya yig‘uvchi, NIST SP 800-90B sog‘lomlik testlari, Hash_df konditsionlash funksiyasi va HMAC_DRBG mexanizmini birlashtirgan kalit generatsiyalash algoritmi taklif etildi. ATmega2560 mikrokontrolleri uchun tuzilgan entropiya balansi algoritm sovuq ishga tushishda kamida 472 bit, issiq qayta ishga tushishda esa 384 bit min-entropiya yig‘ishini ko‘rsatadi.

Kalit so‘zlar: entropiya, tasodifiy sonlar generatori, TRNG, DRBG, HMAC_DRBG, SRAM PUF, NIST SP 800-90B, IoT, X25519, kalit generatsiyasi.

Аннотация: В работе исследуется проблема обеспечения достаточной энтропии для криптографических ключей на IoT-устройствах с ограниченными ресурсами, не имеющих аппаратного генератора случайных чисел (TRNG). Показано, что распространённый в среде Arduino способ randomSeed(analogRead()) ограничивает энтропию закрытого ключа 10 битами. Для решения проблемы предложен алгоритм генерации ключей, который собирает энтропию из начального состояния SRAM и джиттера тактовых генераторов и объединяет тесты работоспособности NIST SP 800-90B, функцию кондиционирования Hash_df и механизм HMAC_DRBG. Составленный для микроконтроллера ATmega2560 энтропийный баланс показывает, что алгоритм собирает не менее 472 бит мин-энтропии при холодном старте и 384 бит при тёплом перезапуске.

Ключевые слова: энтропия, генератор случайных чисел, TRNG, DRBG, HMAC_DRBG, SRAM PUF, NIST SP 800-90B, IoT, X25519, генерация ключей.

Kirish

Kriptografik protokollarning xavfsizligi nafaqat algoritmning matematik bardoshliligiga, balki yopiq kalitning oldindan aytib bo‘lmasligiga ham tayanadi. Elliptik egri chiziqlarga asoslangan ECDH protokolida yopiq kalit d tasodifiy son sifatida tanlanadi. Agar d ni yaratishda ishlatilgan generator yetarli entropiyaga ega bo‘lmasa, hujumchi ECDLP masalasini yechmasdan, mumkin bo‘lgan kalitlarni oddiy saralash orqali topishi mumkin.

Bu xavf nazariy emas. 2008-yilda Debian OpenSSL paketidagi xato tufayli generator urug‘i amalda faqat jarayon identifikatoriga bog‘liq bo‘lib qolgan va har bir kalit turi hamda uzunligi uchun atigi 32 768 ta kalit yaratilishi mumkin bo‘lgan [1]. N. Heninger va boshqalar [2] internet miqyosidagi skanerlash natijasida TLS xostlarining 0,50 % va SSH xostlarining 0,03 % RSA yopiq kalitlarini, shuningdek SSH xostlarining 1,03 % DSA yopiq kalitlarini tiklashgan. Buning asosiy sababi - o‘rnatilgan tarmoq qurilmalarida kalit ishga tushish paytida, entropiya hali yetarli to‘planmagan holatda yaratilishidir.

IoT qurilmalarida muammo yanada keskin. P. Kietzmann va boshqalarning [3] tahliliga ko‘ra, keng qo‘llaniladigan SAMD21 va ATmega2560 mikrokontrollerlarida apparat tasodifiy sonlar manbai umuman mavjud emas. Muallifning avvalgi tadqiqotida Curve25519 asosidagi ECDH algoritmi IoT qurilmalari, jumladan ATmega2560 asosidagi Arduino Mega uchun maqbul ekani ko‘rsatilgan edi. Biroq bu natija *d* kaliti haqiqatan tasodifiy bo‘lgandagina o‘z kuchini saqlaydi.

Ishning maqsadi - apparat TRNG ga ega bo‘lmagan 8-bitli mikrokontrollerlarda qo‘shimcha apparat qurilmalarisiz 128-bitli xavfsizlik darajasiga mos yopiq kalit yaratuvchi algoritmni ishlab chiqish. Ishning ilmiy yangiligi shundaki, bir-biriga bog‘liq bo‘lmagan ikki entropiya manbai, uzluksiz sog‘lomlik testlari va energiyaga bog‘liq bo‘lmagan xotirada saqlanadigan urug‘ yagona sxemaga birlashtirildi. Shu bilan birga, manbalardan istalgan biri ishdan chiqqanda ham talab etilgan xavfsizlik darajasi saqlanishini kafolatlovchi entropiya balansi modeli taklif etildi.

Asosiy qism

Tasodifiy manbaning kriptografik sifati Shennon entropiyasi bilan emas, balki min-entropiya bilan baholanadi [4]:

$$H_\infty(X) = -\log_2 \max_i p_i, \qquad (1)$$

bu yerda p_i - X tasodifiy miqdorning i-qiymatni qabul qilish ehtimoli. Min-entropiya hujumchining kalitni bitta urinishda topish ehtimolini $2^{-H\infty}$ bilan cheklaydi. RFC 7748 [5] ga ko‘ra X25519 128-bitli xavfsizlik darajasini ta’minlaydi, shu sababli yopiq kalit uchun $H_\infty(d) \geq 128$ bit talab qilinadi.

Arduino muhitida tasodifiy son olishning eng keng tarqalgan usuli - randomSeed(analogRead(0)) chaqiruvi, ya’ni avr-libc kutubxonasidagi random() psevdotasodifiy generatorini ulanmagan analog kirishdan o‘qilgan qiymat bilan urug‘lantirish. Bu usulning ikki jiddiy kamchiligi bor. Birinchidan, analogRead() 10-bitli ADC natijasini (0…1023) qaytaradi. Generator deterministik bo‘lgani uchun undan olingan kalit to‘liq urug‘ bilan aniqlanadi: $H_\infty(d) \leq$ 10 bit, ya’ni qurilma ko‘pi bilan 1024 xil kalit yarata oladi. Ikkinchidan, B. Kristinsson [6] ulanmagan analog kirish qiymatlari kuchli tuzilmaga ega ekanini va harorat hamda ulangan kompyuterga bog‘liqligini ko‘rsatgan. Bu qiymatlar ko‘pchilik konfiguratsiyalarda FIPS 140-1 testlaridan o‘tmagan, muallif esa shu usulda urug‘lantirilgan generatorning urug‘ini tiklovchi vositani yaratgan. Demak, haqiqiy urug‘ fazosi 1024 dan ham ancha kichik.

Qo‘shimcha apparat talab qilmaydigan muqobil entropiya manbalari bo‘yicha adabiyotlardagi ma’lumotlar 1-jadvalda umumlashtirilgan.

1-jadval

Resurslari cheklangan mikrokontrollerlarda entropiya manbalari

№	Manba	Platforma	Min-entropiya bahosi	Qo‘llanish imkoniyati
1	Apparat TRNG	ATmega2560, SAMD21	Mavjud emas [3]	Qo‘llab bo‘lmaydi
2	Ulanmagan analog kirish (analogRead)	ATmega328	Barqaror emas, FIPS 140-1 testlaridan ko‘pincha o‘tmaydi [6]	Yaroqsiz
3	SRAM ishga tushish holati (1 KB)	SAMD21	Bitning 4,2–5,5 % [3]	Faqat sovuq ishga tushishda

№	Manba	Platforma	Min-entropiya bahosi	Qo‘llanish imkoniyati
4	SRAM ishga tushish holati (10 KB)	MSP430	0,458 bit/bayt [7]	Faqat sovuq ishga tushishda
5	Ichki past chastotali generator jitteri	MSP430	1,47 bit / 8-bitli namuna [7]	Uzluksiz manba

Jadvaldan ko‘rinadiki, ikki mustaqil manbadan birgalikda foydalanish maqsadga muvofiq. SRAM ishga tushish holati bir martalik, lekin katta hajmdagi entropiya beradi [8]. Soat generatorlari jitteri esa sekin, ammo uzluksiz manbadir. SRAM uchun ikki xil arxitekturada olingan baholar o‘zaro yaqin: 0,458 bit/bayt bitning taxminan 5,7 % iga to‘g‘ri keladi. Biroq qisqa muddatli o‘chirish yoki qayta yuklashda SRAM avvalgi holatini saqlab qoladi. Shu sababli uning entropiyasi faqat sovuq ishga tushishda hisobga olinadi.

Taklif etilgan algoritm quyidagi bosqichlardan iborat:

1) Ishga tushish turini aniqlash. MCUSR registridagi PORF bayrog‘i tekshiriladi. Sovuq ishga tushishda (elektr ta’minoti ulanganda) SRAM entropiyasi hisobga olinadi. Issiq qayta ishga tushishda (watchdog yoki tashqi reset) esa uning hissasi nolga teng deb olinadi.

2) SRAM namunasini olish. Ishga tushirish kodi xotirani nollashidan oldin .noinit bo‘limidagi $N_S = 1024$ baytlik S sohasi o‘qiladi.

3) Jitter namunalarini yig‘ish. ATmega2560 ning 128 kGs chastotali mustaqil watchdog generatori har $T = 16$ ms da uzilish hosil qiladi [9]. Har bir uzilishda kvarts rezonatori bilan taktlanuvchi 16-bitli Timer1 hisoblagichining eng kichik biti olinadi va J ketma-ketligiga qo‘shiladi. Sovuq ishga tushishda $N_J = 256$, issiq ishga tushishda $N_J = 768$ ta namuna yig‘iladi.

4) Sog‘lomlik testlari. Har bir jitter namunasi NIST SP 800-90B [4] ning takrorlanishlar soni testi (RCT) va moslashuvchan ulush testi (APT) orqali tekshiriladi. $h_J = 0{,}5$ bit/namuna va soxta signal ehtimoli $\alpha = 2^{-20}$ uchun RCT chegarasi $C = 1 + \lceil 20 / h_J \rceil = 41$ ga, $W = 1024$ oynali APT chegarasi esa $C = 793$ ga teng. Test muvaffaqiyatsiz tugasa, kalit yaratilmaydi va manba qayta ishga tushiriladi.

5) Konditsionlash va DRBG ni ishga tushirish. SHA-256 asosidagi Hash_df funksiyasi yordamida 512-bitli $E = \text{Hash_df}(S \parallel J)$ qiymati hisoblanadi. HMAC_DRBG [10] quyidagi kirishlar bilan ishga tushiriladi: entropy_input = E, nonce = EEPROM dagi 32 baytli urug‘ R_{prev} va 32-bitli ishga tushish hisoblagichi, personalization_string = qurilmaning noyob identifikatori.

6) Kalitni hosil qilish. DRBG dan 32 bayt olinib, RFC 7748 [5] bo‘yicha qayta ishlanadi: birinchi baytning uchta kichik biti va oxirgi baytning eng katta biti nolga, 254-bit esa birga o‘rnatiladi. Natijada d yopiq kaliti va $Q = \text{X25519}(d, 9)$ ochiq kaliti hosil bo‘ladi.

7) Holatni yangilash. DRBG dan yana 32 bayt olinib, EEPROM ga yangi urug‘ R_{new} sifatida yoziladi va ishga tushish hisoblagichi oshiriladi. S, J, E buferlari nollanadi.

EEPROM dagi urug‘ entropiya balansida hisobga olinmaydi. U qurilma entropiyasi past holatda qayta ishga tushganda ham DRBG holatining takrorlanmasligini ta’minlaydi va [2] da qayd etilgan ishga tushish paytidagi entropiya yetishmasligi muammosini yumshatadi. ATmega2560 EEPROM i 100 000 marta yozishga mo‘ljallangan [9], algoritm esa har bir ishga tushishda faqat 36 bayt yozadi.

Yig‘ilgan entropiya miqdori quyidagi balans tenglamasi bilan baholanadi:

$$H_\Sigma = 8 \cdot N_S \cdot \varepsilon_S \cdot k_P + N_J \cdot h_J \geq H_{req}, \qquad (2)$$

bu yerda $\varepsilon_S = 0{,}042$ - 1-jadvaldagi SRAM uchun eng kichik nisbiy min-entropiya; k_P - ishga tushish turi koeffitsiyenti (sovuq ishga tushishda 1, issiq qayta ishga tushishda 0); $h_J = 0{,}5$

bit/namuna - ehtiyotkor qiymat. Bu qiymat [7] da shunga o‘xshash jitter manbasi uchun olingan 1,47 bit / 8-bitli namuna bahosidan ancha past tanlangan. SP 800-90A [10] ning 8.6.7-bandiga ko‘ra, s xavfsizlik kuchiga ega DRBG ning entropy_input qiymati kamida $3s/2$ bit entropiyaga ega bo‘lishi kerak. SHA-256 asosidagi HMAC_DRBG uchun $s = 256$ bo‘lgani sababli $H_{req} = 384$ bit. Bundan tashqari, har bir manba alohida kamida 128 bit bera olishi talab qilinadi. Natijada manbalardan istalgan biri ishdan chiqqanda ham kalit X25519 ning 128-bitli xavfsizlik darajasini saqlaydi. Hisoblangan ko‘rsatkichlar 2-jadvalda keltirilgan.

2-jadval

Taklif etilgan algoritmning ATmega2560 uchun hisobiy ko‘rsatkichlari

№	Ko‘rsatkich	Sovuq ishga tushish	Issiq qayta ishga tushish
1	SRAM hissasi, bit	$8 \cdot 1024 \cdot 0{,}042 \approx 344$	0
2	Jitter namunalari soni / hissasi, bit	256 / 128	768 / 384
3	Jami min-entropiya H_Σ, bit	472	384
4	Talab etilgan H_{req}, bit	384	384
5	Entropiya yig‘ish vaqti, s	$256 \cdot 0{,}016 \approx 4{,}1$	$768 \cdot 0{,}016 \approx 12{,}3$
6	X25519 kalitini hisoblash vaqti (16 MGs), s	≈ 0,87 [11]	≈ 0,87 [11]
7	Qo‘shimcha xotira: SRAM / EEPROM, bayt	1024 + 68 / 36	1024 + 68 / 36

2-jadvaldan ko‘rinadiki, ikkala holatda ham $H_\Sigma \geq H_{req}$ sharti bajariladi. Sovuq ishga tushishda zaxira 88 bitni tashkil etadi, ya’ni yig‘ilgan entropiya talabdan 23 % ko‘p. SRAM ning o‘zi 344 bit, jitter 128 bit beradi, demak har bir manba alohida 128 bitlik shartni qanoatlantiradi. Issiq qayta ishga tushishda SRAM hissasi yo‘qligi jitter namunalari sonini uch baravar oshirish hisobiga qoplanadi. 6-qatordagi qiymat ATmega2560 da X25519 skalyar ko‘paytmasi uchun o‘lchangan 13 900 397 takt [11] asosida hisoblangan. Qo‘shimcha xotira .noinit sohasi (1024 bayt) va HMAC_DRBG holatidan (K va V uchun 32 baytdan hamda 4 baytli hisoblagich) iborat. .noinit sohasi konditsionlashdan so‘ng nollanib, ilova tomonidan bufer sifatida qayta ishlatilishi mumkin.

Kalit yaratish vaqti 5–13 s gacha oshadi. Biroq bu amal faqat qurilmani ro‘yxatdan o‘tkazishda yoki uzoq muddatli kalitni almashtirishda bajariladi. Keyingi sessiya kalitlari uchun tasodifiy qiymatlar allaqachon urug‘lantirilgan DRBG dan qayta entropiya yig‘masdan olinadi. Taqqoslash uchun, randomSeed(analogRead(0)) usulida $H_\infty(d) \leq 10$ bit, taklif etilgan algoritmda esa kalit X25519 ning 128-bitli xavfsizlik chegarasigacha to‘liq entropiyaga ega bo‘ladi. Algoritmni amaliy tasdiqlash uchun ATmega2560 dan olingan xom namunalar NIST SP 800-90B ning IID bo‘lmagan manbalar uchun baholash usullari bilan, DRBG chiqishi esa NIST SP 800-22 [12] statistik testlar to‘plami bilan tekshiriladi.

Xulosa

Tadqiqot natijalari asosida quyidagi xulosalarga kelindi:

1. Apparat TRNG ga ega bo‘lmagan mikrokontrollerlarda keng qo‘llaniladigan randomSeed(analogRead()) usuli yopiq kalit entropiyasini 10 bitdan oshirmaydi. Bu X25519 kabi kuchli algoritmning xavfsizligini amalda yo‘qqa chiqaradi.

2. SRAM ishga tushish holati va soat generatorlari jitterini NIST SP 800-90B sog‘lomlik testlari, Hash_df konditsionlash funksiyasi va HMAC_DRBG mexanizmi bilan birlashtirgan kalit

generatsiyalash algoritmi taklif etildi. Algoritm qo‘shimcha apparat talab qilmaydi va ishga tushish turiga moslashadi.

3. ATmega2560 uchun tuzilgan entropiya balansiga ko‘ra, algoritm sovuq ishga tushishda 472 bit, issiq qayta ishga tushishda 384 bit min-entropiya yig‘adi. Bu SP 800-90A ning 256-bitli xavfsizlik kuchi uchun 384 bitlik talabini qanoatlantiradi. Manbalardan istalgan biri ishdan chiqqanda ham kalit 128-bitli xavfsizlik darajasini saqlaydi.

Olingan natijalar Curve25519 asosidagi kalit almashinuvi bo‘yicha avvalgi natijalar bilan birgalikda IoT qurilmalari uchun to‘liq kalit generatsiyalash zanjirini tashkil etadi: entropiya yig‘ish, DRBG, X25519 kaliti va MQTT/CoAP protokollarida kalit almashinuvi. Kelgusida algoritm ATmega2560 da amalda tatbiq etilib, xom namunalarning min-entropiyasi NIST SP 800-90B usullari bilan eksperimental baholanadi.

Foydalanilgan adabiyotlar

1. Debian Security Advisory DSA-1571-1: openssl – predictable random number generator. CVE-2008-0166. – Debian Project, 2008.

2. Heninger N., Durumeric Z., Wustrow E., Halderman J. A. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices // Proc. 21st USENIX Security Symposium. – Bellevue: USENIX, 2012. – P. 205–220.

3. Kietzmann P., Schmidt T. C., Wählisch M. A Guideline on Pseudorandom Number Generation (PRNG) in the IoT // ACM Computing Surveys. – 2021. – Vol. 54, № 6. – Art. 112. – 38 p. – DOI: 10.1145/3453159.

4. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B. – Gaithersburg: NIST, 2018. – DOI: 10.6028/NIST.SP.800-90B.

5. Langley A., Hamburg M., Turner S. Elliptic Curves for Security. RFC 7748. – IETF, 2016. – DOI: 10.17487/RFC7748.

6. Kristinsson B. Ardrand: The Arduino as a Hardware Random-Number Generator. – arXiv:1212.3777, 2012.

7. Grycel J., Walls R. J. ERHARD-RNG: A Random Number Generator Built from Repurposed Hardware in Embedded Systems. – arXiv:1903.09365, 2019.

8. Holcomb D. E., Burleson W. P., Fu K. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers // IEEE Transactions on Computers. – 2009. – Vol. 58, № 9. – P. 1198–1210. – DOI: 10.1109/TC.2008.212.

9. ATmega640/1280/1281/2560/2561: 8-bit Atmel Microcontroller with 16/32/64KB In-System Programmable Flash. Datasheet 2549Q. – San Jose: Atmel Corporation, 2014.

10. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST Special Publication 800-90A, Revision 1. – Gaithersburg: NIST, 2015. – DOI: 10.6028/NIST.SP.800-90Ar1.

11. Düll M., Haase B., Hinterwälder G., Hutter M., Paar C., Sánchez A. H., Schwabe P. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers // Designs, Codes and Cryptography. – 2015. – Vol. 77, № 2–3. – P. 493–514. – DOI: 10.1007/s10623-015-0087-1.

12. Bassham L. E., Rukhin A. L., Soto J. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, Revision 1a. – Gaithersburg: NIST, 2010. – DOI: 10.6028/NIST.SP.800-22r1a.

RESURSLARI CHEKLANGAN QURILMALARDA ASCON ASOSIDAGI AEAD, XESH VA XOF FUNKSIYALARINI SAMARALI AMALGA OSHIRISH VA BAHOLASH

Axtamov A.H.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada resurslari cheklangan qurilmalarda NIST SP 800-232 standartiga kiritilgan Ascon oilasi funksiyalari, ularni samarali amalga oshirish usullari tahlil qilinadi. Almashtirish funksiyasiga asoslangan yagona tuzilma bir vaqtning o‘zida autentifikatsiyalangan shifrlash, xeshlash va o‘zgaruvchan uzunlikdagi chiqish hosil qilishga imkon berishi yoritiladi, bu esa dastur kodi hajmi va xotira sarfini kamaytirishda muhimdir. Mikrokontrollerlarda amalga oshirishni baholash mezonlari asoslanadi. Olingan natijalar yengil vaznli kriptografik yechimlarni IoT tizimlariga joriy etishda tegishli algoritm va amalga oshirish variantini tanlash uchun foydalanilishi mumkin.

Аннотация. В статье рассматриваются функции семейства Ascon, включённые в стандарт NIST SP 800-232, и способы их эффективной реализации на устройствах с ограниченными ресурсами. Показано, что единая конструкция на основе перестановки позволяет выполнять аутентифицированное шифрование, хеширование и генерацию выхода произвольной длины, что важно для сокращения объёма кода и расхода памяти. Обоснованы критерии оценки реализации на микроконтроллерах. Полученные выводы могут быть использованы при выборе алгоритма и варианта реализации при внедрении легковесных криптографических решений в системах Интернета вещей.

Kalit so‘zlar: Yengil vaznli kriptografiya, Ascon, AEAD, xesh funksiyasi, XOF, resurslari cheklangan qurilmalar, IoT xavfsizligi, mikrokontroller, optimallashtirish.

Ключевые слова: Ascon, легковесная криптография, AEAD, хеш-функция, XOF, микроконтроллер, Интернет вещей, оценка производительности.

Kirish

Buyumlar interneti (IoT) qurilmalari, sensor tugunlar, RFID teglar va tibbiy implantlar sanoat, transport, energetika va maishiy infratuzilmalarda keng qo‘llanilmoqda. Bunday qurilmalarda hisoblash quvvati, operativ xotira, dastur kodi hajmi va energiya zaxirasi cheklangan bo‘ladi, ko‘pincha ular batareyada uzoq muddat avtonom ishlashi kerak. Shu sababli an’anaviy kriptografik algoritmlarni ularda qo‘llash har doim ham o‘zini oqlamaydi. Ma’lumotlarning maxfiyligi, yaxlitligi va haqiqiyligini ta’minlash uchun qurilma imkoniyatlariga moslashtirilgan yengil vaznli kriptografiya zarur.

NIST cheklangan muhitlar uchun kriptografiyani 2013-yildan o‘rgana boshlagan va ochiq standartlashtirish jarayonini o‘tkazgan [2]. Jarayon yakunida Ascon oilasi tanlandi, 2025-yil 13-avgustda esa NIST SP 800-232 standarti e’lon qilindi. U to‘rtta funksiyani belgilaydi: Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128 va Ascon-CXOF128 [1]. Ascon algoritmining asosiy ilmiy tavsifi Dobraunig va boshqalarning ishida keltirilgan [3], tanlovning yakuniy bosqichidagi taqqoslash esa NIST hisobotida yoritilgan [4].

Biroq algoritmning nazariy bardoshliligi uning amaliy samaradorligini kafolatlamaydi. Aniq mikrokontrollerda amalga oshirish usuli (dasturlash tili, optimallashtirish darajasi, registrlardan foydalanish) Flash va RAM sarfiga, tezlikka hamda energiya iste’molining o‘zgarishiga sezilarli ta’sir qiladi. Bundan tashqari, yon-kanal hujumlariga chidamlilik ham

baholanishi kerak. Shuning uchun Ascon asosidagi funksiyalarni amalga oshirish va ularni yagona mezonlar bo‘yicha baholash dolzarb vazifadir.

Asosiy qism

1. Ascon tuzilmasi. Ascon oilasi sponge va duplex konstruksiyalariga asoslangan [3, 5]. Ichki holat 320 bit bo‘lib, beshta 64 bitli so‘zdan iborat. Holatning bir qismi (rate) xabar bilan o‘zaro ta’sirlashadi, qolgan qismi (capacity) esa tashqaridan ko‘rinmaydi va xavfsizlikni ta’minlaydi. Har bir raund uchta bosqichdan tuziladi: raund konstantasini qo‘shish, 5 bitli S-blokdan foydalanib bitli almashtirish va har bir so‘z ichida siklik siljish hamda XOR amallari orqali bajariladigan chiziqli diffuziya. Barcha amallar mantiqiy operatsiyalar va siljishlardan iborat, jadvalga murojaat talab qilinmaydi. Bu kichik mikrokontrollerlarda qulay va kesh orqali vaqt bo‘yicha axborot oqishi xavfini kamaytiradi.

2. Standartlashtirilgan funksiyalar. SP 800-232 bo‘yicha Ascon-AEAD128 128 bitli kalit va 128 bitli nonce bilan ishlaydi, shifrmatn bilan birga autentifikatsiya tegini hosil qiladi [1]. Ascon-Hash256 256 bitli xesh qiymat beradi, Ascon-XOF128 esa chiqish uzunligini foydalanuvchi tanlashiga imkon beradi. Ascon-CXOF128 bunga qo‘shimcha ravishda sozlash satrini (customization string) qabul qiladi. Bu bir xil funksiyani turli ilovalarda domen bo‘yicha ajratish uchun qulay. Funksiyalarning asosiy xususiyatlari 1-jadvalda keltirilgan.

1-jadval

Ascon funksiyalarining taqqoslanishi

Funksiya	Vazifasi	Kirish	Chiqish	Rate	Raundlar
Ascon-AEAD128	Autentifikatsiyalangan shifrlash	Kalit, nonce, AD, ochiq matn	Shifrmatn va 128 bitli teg	128 bit	12 (boshlang‘ich/ yakuniy), 8 (oraliq)
Ascon-Hash256	Xeshlash	Xabar	256 bit	64 bit	12
Ascon-XOF128	O‘zgaruvchan uzunlikdagi chiqish	Xabar, chiqish uzunligi	Ixtiyoriy uzunlik	64 bit	12
Ascon-CXOF128	Sozlash satrli XOF	Sozlash satri, xabar	Ixtiyoriy uzunlik	64 bit	12

Funksiyalarning barchasi bitta permutatsiyaga tayanadi, shuning uchun yagona kod bazasi uchala vazifani bajaradi. Bu qurilmada ham Flash hajmini, ham xotirani tejaydi, chunki alohida shifr va alohida xesh-funksiya kodini saqlash shart emas. Odatda an’anaviy yondashuvda AES-GCM [9] va SHA-2 yoki SHA-3 [6] kabi alohida algoritmlar birga ishlatiladi.

3. Xavfsizlik jihatlari. Ascon-AEAD128 128 bitli xavfsizlik darajasini ta’minlaydi, lekin bu nonce’ning bir kalit ostida takrorlanmasligi sharti bilan. Nonce qayta ishlatilsa, xavfsizlik kafolati yo‘qoladi, shuning uchun qurilmada nonce’ni yaratish va uni qayta yoqilganda ham saqlab qolish (hisoblagich yoki xavfsiz tasodifiy son) mexanizmi loyihalanishi kerak. Shifrni ochishda teg tekshiruvi to‘g‘ri o‘tmaguncha ochiq matn qaytarilmasligi lozim. Ascon-Hash256 va XOF funksiyalari esa to‘qnashuv va prototasvirni topishga qarshi chidamlilikka ega, lekin XOF chiqishi qisqartirilganda xavfsizlik darajasi chiqish uzunligi bilan cheklanadi. Shuning uchun energiyani tejash maqsadida chiqishni qisqartirishdan oldin kerakli xavfsizlik darajasini hisobga olish zarur.

4. Amalga oshirish samaradorligiga ta’sir qiluvchi omillar. Amalda quyidagi omillar natijaga ko‘proq ta’sir qiladi [7, 8].

Birinchidan, platformaning so‘z uzunligi. 64 bitli siljishlar 8 va 32 bitli mikrokontrollerlarda bevosita bajarilmaydi, shu sababli 32 bitli platformalarda holatni bit-interleaving shaklida saqlash, 8 bitli platformalarda esa baytlar bilan ishlash usullari qo‘llaniladi. Ikkinchidan, raundlarni yoyish darajasi: raundlarni to‘liq yoyish tezlikni oshiradi, lekin Flash sarfini ko‘paytiradi, ixcham sikl esa teskari natija beradi. Uchinchidan, holatni registrlarda saqlash: bu xotiraga murojaatlarni va RAM sarfini kamaytiradi, ammo registrlari kam qurilmalarda har doim ham mumkin emas. To‘rtinchidan, oqimli (incremental) interfeys: xabarni to‘liq buferlamasdan bo‘laklab qayta ishlash RAM’ni tejaydi, bu uzun xabarlarda muhim. Beshinchidan, yon-kanal hujumlaridan himoya: maskalash kabi usullar xavfsizlikni oshiradi, lekin tezlik va kod hajmi hisobiga.

5. Baholash metodikasi. Baholash uchun to‘rtta asosiy mezon tavsiya etiladi: Flash sarfi (kod hajmi), RAM sarfi (holat va stek), bajarilish tezligi (sikl/bayt) hamda energiya iste’moli (bitta xabar uchun, mikrojoul hisobida). IoT’da xabarlar odatda qisqa bo‘lgani uchun tezlikni faqat uzun ma’lumotlarda emas, qisqa xabarlarda (masalan, 16, 64 bayt) ham o‘lchash kerak, chunki boshlang‘ich va yakuniy raundlarning ulushi katta bo‘ladi. Taqqoslash bir xil qurilma, kompilyator va optimallashtirish bayroqlarida (tezlik va hajm bo‘yicha alohida) olib borilishi, taqqoslash bazasi sifatida AES-GCM va SHA-2/SHA-3 kabi mavjud yechimlardan foydalanilishi lozim. Ba’zi mikrokontrollerlarda AES uchun apparat tezlatgichi mavjudligi taqqoslash natijasiga ta’sir qilishini ham hisobga olish kerak.

6. Qo‘llanish ssenariylari. Funksiyani tanlash qurilma vazifasiga bog‘liq. Sensor tugun va telemetriya uzatishda maxfiylik va haqiqiylik birga kerak, shuning uchun Ascon-AEAD128 mos keladi. Dasturiy ta’minot yangilanishining yaxlitligini tekshirishda Ascon-Hash256, kalit hosil qilish yoki qisqa identifikator olishda esa Ascon-XOF128 yoki domen ajratish talab qilinsa Ascon-CXOF128 qulay. Tibbiy implantlar va RFID teglarda kod hajmi va energiya eng qattiq cheklov bo‘lgani uchun yagona kod bazasining afzalligi ayniqsa sezilarli bo‘ladi.

Xulosa

Ascon oilasi yagona permutatsiya asosida autentifikatsiyalangan shifrlash, xeshlash va o‘zgaruvchan uzunlikdagi chiqishni ta’minlab, resurslari cheklangan qurilmalarda kod hajmi va xotira sarfini kamaytirish imkonini beradi. Amalga oshirish samaradorligi platforma turi, raundlarni tashkil etish usuli va xotiradan foydalanish strategiyasiga bog‘liq. Shu sababli yechimni tanlashda nazariy bardoshlilik bilan birga Flash va RAM sarfi, sikl/bayt tezligi, energiya xarajati va yon-kanal hujumlariga chidamlilik mezonlari kompleks baholanishi zarur. Keyingi tadqiqotlar yo‘nalishi sifatida turli arxitekturadagi mikrokontrollerlarda o‘lchovlarni o‘tkazish va himoyalangan (maskalangan) variantlarni baholash tavsiya etiladi.

Foydalanilgan adabiyotlar:

1. NIST. Lightweight Cryptography.

2. NIST SP 800-232. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions. 2025. DOI: 10.6028/NIST.SP.800-232.

3. Dobraunig C., Eichlseder M., Mendel F., Schläffer M. Ascon v1.2: Lightweight Authenticated Encryption and Hashing // Journal of Cryptology, vol. 34, 2021.

4. Sönmez Turan M. va boshq. NIST IR 8454. Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process. 2023.

5. Ascon C implementatsiyasi.

6. Bertoni G., Daemen J., Peeters M., Van Assche G. Cryptographic sponge functions. 2011.

IOT TIZIMLARIDA DASTURIY AMALGA OSHIRISHGA YO‘NALTIRILGAN OQIMLI SHIFRLASH ALGORITMLARINING QIYOSIY TAHLILI

Xamrayev A.Q.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada eSTREAM loyihasining dasturiy amalga oshirishga yo‘naltirilgan Profile 1 portfelidan HC-128, Rabbit va Salsa20/12 oqimli shifrlari ko‘rib chiqiladi. Dastlab profilning vazifasi va algoritmlarni baholash mezonlari yoritilib, keyin kalit va boshlang‘ich vektor parametrlari, ichki holat, protsessor xarajati hamda 8-bitli AVR mikrokontrolleridagi xotira va tezlik natijalari taqqoslanadi. Natijalar turli realizatsiya va platformalarga bog‘liqligi hisobga olinib, resurslari cheklangan IoT qurilmalari uchun tanlash mezonlari muhokama qilinadi.

Kalit so‘zlar: eSTREAM, oqimli shifrlash, Profile 1, HC-128, Rabbit, Salsa20/12, IoT, SRAM, unumdorlik.

Аннотация. В статье рассматриваются потоковые шифры HC-128, Rabbit и Salsa20/12 из программного профиля Profile 1 проекта eSTREAM. Сначала описываются назначение профиля и критерии сравнения, затем сопоставляются параметры ключа и начального вектора, внутреннее состояние, процессорные затраты, а также результаты по памяти и скорости на 8-разрядном микроконтроллере AVR. С учётом зависимости результатов от платформы и конкретной реализации обсуждаются критерии выбора шифра для IoT-устройств с ограниченными ресурсами.

Ключевые слова: eSTREAM, потоковое шифрование, Profile 1, HC-128, Rabbit, Salsa20/12, IoT, SRAM, производительность.

Kirish

Buyumlar interneti (IoT) tizimlarida sensorlar, hisoblagichlar, boshqaruv qurilmalari va mikrokontrollerlar o‘zaro ma’lumot almashadi. Bunday qurilmalar ko‘pincha cheklangan operativ xotira, kichik dastur xotirasi va energiya manbai bilan ishlaydi. Shu sababli kriptografik algoritmni tanlashda faqat nazariy xavfsizlik emas, balki bajarilish vaqti, xotira sarfi, kalit oqimini hosil qilish tezligi va boshlang‘ich tayyorlash xarajati ham hisobga olinadi.

Oqimli shifrlar ma’lumotni ketma-ket bit yoki baytlar oqimi sifatida qayta ishlaydi. Algoritm maxfiy kalit va nonce yoki boshlang‘ich vektor asosida kalit oqimini hosil qiladi; shifrlashda u ochiq matn bilan XOR qilinadi. Bir xil kalit va nonce kombinatsiyasini takror ishlatish xavfsizlikka jiddiy zarar yetkazishi mumkin, shuning uchun real IoT tizimida nonce boshqaruvi ham algoritm tanlovi kabi muhimdir.

eSTREAM loyihasi oqimli shifrlarni amaliy ishlash va kriptografik tahlil nuqtayi nazaridan baholash uchun tashkil etilgan. Uning Profile 1 yo‘nalishi dasturiy amalga oshirishga, jumladan umumiy maqsadli protsessorlarda samarali ishlashga qaratilgan. Yakuniy Profile 1 portfeliga HC-128, Rabbit, Salsa20/12 va SOSEMANUK kiritilgan [1]. Ushbu maqolada uchta algoritm batafsil solishtiriladi; SOSEMANUK yakuniy portfel a’zosi bo‘lsa-da, tahlil doirasini aniq saqlash uchun sonli taqqoslashga kiritilmagan.

Tadqiqot maqsadi - algoritmlarning umumiy tuzilishi va e’lon qilingan tajriba natijalarini birgalikda ko‘rib chiqib, tezlik va xotira o‘rtasidagi muvozanatni IoT qurilmalariga nisbatan izohlash. Taqqoslashda protsessor modeli, kompilyator, optimallashtirish darajasi va dasturlash tili natijaga ta’sir qilishi alohida e’tiborga olinadi.

Profile 1 algoritmlarining umumiy xususiyatlari va baholash mezonlari

HC-128 kalit oqimini hosil qilishda katta jadvalli ichki holatdan foydalanadi. Bu yondashuv dasturiy realizatsiyada tezlikka yordam berishi mumkin, biroq SRAM cheklangan mikrokontrollerlarda katta xotira talabi muammo tug‘diradi. Rabbit arifmetik amallar va ichki holatni yangilashga asoslangan bo‘lib, dasturiy ishlash tezligi bilan tanilgan. Salsa20/12 esa 32-bitli so‘zlar ustida XOR, qo‘shish va aylantirish amallaridan foydalanadi; “12” belgisi Salsa20 oilasidagi 12 raundli variantni anglatadi. Algoritmlarning tuzilishi bir-biridan farq qilgani uchun ularni faqat bitta ko‘rsatkich bilan baholash yetarli emas.

Amaliy baholashda quyidagi mezonlar muhim: 1) kalit va nonce uzunligi - protokol bilan moslikka ta’sir qiladi; 2) ichki holat va SRAM - qurilmaning operativ xotirasiga yukni belgilaydi; 3) Flash yoki dastur kodi hajmi - mikrokontroller xotirasida egallangan joyni ko‘rsatadi; 4) takt/bayt - protsessor bir baytni qayta ishlash uchun sarflagan taktlar soni; 5) boshlang‘ich sozlash xarajati - qisqa xabarlar va tez-tez yangilanadigan seanslarda muhim; 6) nonce’ni to‘g‘ri boshqarish va algoritmni protokolga xavfsiz integratsiya qilish.

1-jadval

Algoritmlarning asosiy texnik parametrlari

Parametr	HC-128	Rabbit	Salsa20/12
Kalit uzunligi	128 bit	128 bit	128 yoki 256 bit
IV / nonce	128 bit	64 bit	64 bitli nonce
Ichki holat	32 768 bit (4 096 bayt jadvallar)	Taxminan 513 bit	512 bit
Asosiy yondashuv	Katta jadvalli holat	Arifmetik amallar va holat yangilanishi	32-bitli so‘zlar, XOR, qo‘shish va aylantirish
Amaliy e’tibor	Tezlik va SRAM talabi	Dasturiy unumdorlik	Ixcham holat va protsessor amallari

Jadvaldagi ichki holat qiymatlari algoritmlarning nazariy tuzilishiga tegishli; ular kompilyatsiya qilingan dastur egallaydigan umumiy SRAM yoki Flash bilan aynan bir xil tushuncha emas. Real dastur qo‘shimcha buferlar, stek va boshqaruv ma’lumotlarini ham talab qiladi. Shuning uchun algoritmning ichki holatini bilish dastlabki mezon bo‘lsa-da, yakuniy qaror aniq qurilmada o‘lchash orqali qabul qilinadi.

Umumiy protsessordagi tezlik natijalari

Bir tadqiqotda algoritmlarning C tilidagi bazaviy realizatsiyalari Intel Core 2 Duo E8400, 3 GHz protsessorida, GCC 4.6.1 kompilyatori va -O3 optimallashtirish darajasida solishtirilgan [4]. Natijalar takt/bayt ko‘rinishida berilgan. Bu o‘lchovda son qancha kichik bo‘lsa, ko‘rsatilgan sinov sharoitida baytni qayta ishlash uchun protsessor xarajati shuncha kam bo‘ladi.

2-jadval

Protsessor xarajati, takt/bayt (Intel Core 2 Duo E8400, GCC 4.6.1, -O3)

Algoritm	40 bayt	576 bayt	1500 bayt
HC-128	591,3	43,7	18,6
Rabbit	19,0	8,6	8,2
Salsa20/12	15,5	10,8	11,0

40 baytli xabarda HC-128 uchun ko‘rsatkich ancha yuqori. Bu kichik hajmdagi ma’lumotda boshlang‘ich tayyorlash xarajatlari umumiy hisobga katta ta’sir ko‘rsatishi bilan izohlanadi. Xabar uzunligi oshganda HC-128 ko‘rsatkichi yaxshilanadi va 1500 baytda 18,6 takt/baytga tushadi. Shu sinovda Rabbit 576 va 1500 baytli xabarlar uchun mos ravishda 8,6 va 8,2 takt/bayt, Salsa20/12 esa 10,8 va 11,0 takt/bayt ko‘rsatgan. Demak, ushbu protsessor va dasturiy realizatsiya sharoitida Rabbit hamda Salsa20/12 kichikroq takt xarajatiga ega, lekin bu xulosa barcha protsessorlarga avtomatik ko‘chirilmaydi.

8-bitli AVR mikrokontrolleridagi xotira va tezlik

IoT qurilmasiga yaqinroq misol sifatida 8-bitli AVR mikrokontrolleridagi amalga oshirish natijalarini ko‘rish mumkin. Meiser va hammualliflar eSTREAM shifrlarini AVR platformasida baholab, kalit oqimi tezligi, takt/bayt va xotira hajmi kabi ko‘rsatkichlarni keltirgan [2]. Quyidagi qiymatlar aynan o‘sha maqoladagi realizatsiyalarga tegishli; HC-128 va Salsa20/12 V2 kodlari turli usulda amalga oshirilgani sababli, natijalar algoritmning o‘zini alohida ajratib ko‘rsatmaydi.

3-jadval

AVR platformasidagi e’lon qilingan natijalar

Ko‘rsatkich (8 MHz)	HC-128	Salsa20/12 V2
Kalit oqimi tezligi	47 390 bayt/s	16 298 bayt/s
Takt/bayt	168,81	490,84
Dastur kodi (Flash)	23 100 bayt	3 842 bayt
SRAM	4 556 bayt	322 bayt
IV tayyorlash	2 082 876 takt	70 takt
Realizatsiya	C	Optimallashtirilgan assembler

Bu jadval muhim muvozanatni ko‘rsatadi: keltirilgan realizatsiyada HC-128 kalit oqimini tezroq hosil qilgan, ammo 4 556 bayt SRAM va 23 100 bayt Flash talab qilgan. Salsa20/12 V2 esa 322 bayt SRAM va 3 842 bayt Flash bilan ancha ixcham. Shu sababli kichik xotirali qurilmada Salsa20/12 ni joylashtirish osonroq bo‘lishi mumkin. HC-128 uchun IV tayyorlash xarajati ham juda katta ko‘rsatilgan; bu ko‘p kichik xabarlar alohida seanslarda shifrlanadigan tizimlarda sezilarli bo‘lishi mumkin.

Biroq bu raqamlarni to‘g‘ridan-to‘g‘ri algoritm ustunligi sifatida talqin qilish to‘g‘ri emas: HC-128 C tilida, Salsa20/12 V2 esa optimallashtirilgan assemblerda yozilgan. Turli kompilyator, registrlardan foydalanish, kodni optimallashtirish va protsessor arxitekturasi natijani o‘zgartirishi mumkin. Adolatli yangi tajriba uchun bir xil mikrokontroller, bir xil kompilyator va optimallashtirish darajasi, bir xil xabar uzunligi hamda bir xil o‘lchash metodikasi qo‘llanishi kerak.

IoT tizimlari uchun natijalarni talqin qilish

Agar IoT qurilmasi ko‘p hajmdagi ma’lumotni uzluksiz yuborsa, kalit oqimining barqaror tezligi muhim bo‘ladi. Bunday vaziyatda dasturiy realizatsiya ko‘rsatkichlari va protsessor yukini sinash kerak. Agar qurilma juda kichik SRAMga ega bo‘lsa, xotira sarfi tezlikdan ham muhimroq cheklovga aylanishi mumkin: xotiraga sig‘maydigan algoritmni tanlash amaliy jihatdan maqsadga muvofiq emas. Qisqa sensor xabarlari tez-tez yuboriladigan holatda esa initsializatsiya xarajati umumiy kechikishga katta ta’sir qiladi.

Bundan tashqari, oqimli shifrning o‘zi butun xavfsizlik yechimi emas. Tizimda nonce takrorlanmasligi, kalitlar xavfsiz saqlanishi va yangilanishi, xabar yaxlitligi esa alohida autentifikatsiya mexanizmi bilan ta’minlanishi lozim. Shuning uchun algoritmni tanlashda tezlik va xotira bilan birga protokolning to‘g‘ri qurilishi ham tekshiriladi.

Xulosa

HC-128, Rabbit va Salsa20/12 taqqoslanishi dasturiy oqimli shifr samaradorligi xabar hajmi, protsessor va konkret realizatsiyaga bog‘liqligini ko‘rsatadi. Umumiy protsessordagi sinovda Rabbit va Salsa20/12 ko‘p holatda kamroq takt/bayt ko‘rsatgan. AVR tajribasida esa HC-128 tezroq kalit oqimi hosil qilgan bo‘lsa-da, uning SRAM va Flash talabi hamda IV tayyorlash xarajati yuqori bo‘lgan. Salsa20/12 V2 xotira jihatidan ixchamroq natija ko‘rsatgan, biroq bu taqqoslashda optimallashtirilgan assembler ishlatilgani hisobga olinishi kerak.

Shu sababli IoT qurilmasi uchun yagona eng yaxshi algoritmni faqat bitta jadval asosida tanlash mumkin emas. Tanlov qurilmaning xotirasi, xabar uzunligi, uzatish chastotasi, ishlash vaqti va energiya cheklovlariga mos sinovlar orqali asoslanishi kerak. Keyingi tajribada bir xil mikrokontrollerda algoritmlarni bir xil sharoitda amalga oshirish va energiya sarfini ham o‘lchash taqqoslashning ishonchliligini oshiradi.

Foydalanilgan adabiyotlar

1. ECRYPT. eSTREAM: The ECRYPT Stream Cipher Project. https://www.ecrypt.eu.org/stream/

2. Meiser G., Eisenbarth T., Lemke-Rust K., Paar C. Efficient Implementation of eSTREAM Ciphers on 8-bit AVR Microcontrollers. IEEE, 2008. DOI: https://doi.org/10.1109/SIES.2008.4577681

3. Bernstein D. J. The Salsa20 Family of Stream Ciphers. https://cr.yp.to/snuffle.html

4. Exploiting SIMD Instructions in Modern Microprocessors to Optimize the Performance of Stream Ciphers. International Journal of Computer Network and Information Security, 2013, Vol. 5, No. 6, pp. 56–66.

GALUA MAYDONLARI ARIFMETIKASI VA UNING ZAMONAVIY KRIPTOGRAFIK ALGORITMLARDA QO‘LLANILISHI

Mahmanazarova Z.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda chekli (Galua) maydonlarining asosiy xossalari, GF(p) va GF(2^n) maydonlarida arifmetik amallarni bajarish usullari hamda ularning AES, AES-GCM, ZUC, Grain-128AEAD algoritmlarida va xatoliklarni tuzatuvchi kodlarda qo‘llanilishi tahlil qilingan. Resurslari cheklangan qurilmalarda maydon amallarini samarali va yon kanal hujumlariga chidamli amalga oshirish yo‘nalishlari ko‘rsatib berilgan.

Kalit so‘zlar: Galua maydoni, chekli maydon, keltirilmaydigan ko‘phad, primitiv element, AES, GHASH, LFSR, ZUC.

Аннотация. В тезисе рассмотрены основные свойства конечных полей (полей Галуа), методы выполнения арифметических операций в полях GF(p) и GF(2^n), а также их применение в алгоритмах AES, AES-GCM, ZUC, Grain-128AEAD и в помехоустойчивых кодах. Показаны направления эффективной и стойкой к атакам по побочным каналам реализации операций в поле на устройствах с ограниченными ресурсами.

Ключевые слова: поле Галуа, конечное поле, неприводимый многочлен, примитивный элемент, AES, GHASH, LFSR, ZUC.

Kirish

Zamonaviy kriptografik algoritmlarning aksariyati - simmetrik blokli va oqimli shifrlar, xabarlarni autentifikatsiyalash kodlari, elliptik egri chiziqlarga asoslangan ochiq kalitli tizimlar - chekli maydonlar ustidagi amallarga tayanadi. Chekli maydon tushunchasi bunday tuzilmalarni birinchilardan bo‘lib tadqiq etgan fransuz matematigi Evarist Galua (1811–1832) nomi bilan bog‘liq. Galua maydonlarining qat’iy algebraik tuzilishi shifrlash akslantirishlarining teskarilanuvchanligini, yuqori nochiziqlilik va diffuziya xossalarini kafolatlaydi, ikkilik xarakteristikali maydonlarda esa barcha amallar XOR va siljitish kabi apparat jihatdan arzon operatsiyalarga keltiriladi. Shu sababli Galua maydonlari arifmetikasini chuqur o‘zlashtirish va uni samarali amalga oshirish kriptografik vositalarni ishlab chiqishning muhim sharti hisoblanadi.

Asosiy tushunchalar

q ta elementdan iborat chekli maydon GF(q) faqat $q = p^n$ (p - tub son, $n \geq 1$) bo‘lgandagina mavjud va izomorfizm aniqligida yagonadir [1]. $n = 1$ bo‘lganda GF(p) maydon p modul bo‘yicha chegirmalar to‘plami $\{0, 1, \ldots, p - 1\}$ dan iborat. $n > 1$ bo‘lganda GF(p^n) elementlari GF(p) ustidagi darajasi n dan kichik ko‘phadlar sifatida ifodalanadi, ko‘paytirish esa n-darajali keltirilmaydigan m(x) ko‘phad moduli bo‘yicha bajariladi:

$$c(x) = a(x) \cdot b(x) \bmod m(x). \quad (1)$$

GF(q) ning noldan farqli elementlari $q - 1$ tartibli siklik multiplikativ guruh hosil qiladi; bu guruhning yasovchisi primitiv element, ildizi primitiv element bo‘lgan keltirilmaydigan ko‘phad esa primitiv ko‘phad deyiladi. Har bir nolmas a element uchun teskari element kengaytirilgan Evklid algoritmi yoki Fermaning kichik teoremasidan kelib chiqadigan quyidagi formula orqali hisoblanadi:

$$a^{-1} = a^{q-2}, \; a \neq 0. \quad (2)$$

Xarakteristikasi 2 ga teng $GF(2^n)$ maydonlar kriptografiyada alohida o‘rin tutadi: ularda qo‘shish va ayirish bitlar bo‘yicha XOR amaliga teng, x ga ko‘paytirish esa bir bitga chapga siljitish va zarurat bo‘lsa m(x) bilan XOR qilishdan iborat (AES dagi xtime amali).

Blokli shifrlarda qo‘llanilishi

AES standartida [2] baytlar $GF(2^8)$ maydon elementlari sifatida qaraladi va $m(x) = x^8 + x^4 + x^3 + x + 1$ ({11B}) keltirilmaydigan ko‘phad qo‘llaniladi; masalan, {57} · {83} = {C1}. SubBytes almashtirishining S-bloki $GF(2^8)$ dagi multiplikativ teskari elementni topish va undan keyingi affin akslantirishdan tuziladi. Aynan inversiya S-blokka yuqori nochiziqlilikni - maksimal differensial ehtimollik 2^{-6} va maksimal chiziqli korrelyatsiya 2^{-3} ni ta’minlaydi [3]. MixColumns amalida har bir ustun $GF(2^8)$ ustida {02}, {03}, {01}, {01} koeffitsiyentli MDS matritsaga ko‘paytiriladi, bu esa tarqalish soni (branch number) 5 ga teng bo‘lgan maksimal diffuziyani beradi. Shuni ta’kidlash joizki, AES ko‘phadi keltirilmaydigan, ammo primitiv emas: x elementining tartibi 51 ga teng, shu sababli logarifm/antilogarifm jadvallarini tuzishda yasovchi sifatida {03} olinadi.

Autentifikatsiya va oqimli shifrlarda qo‘llanilishi

AES-GCM rejimida [4] GHASH autentifikatsiya funksiyasi $GF(2^{128})$ maydonda $P(x) = x^{128} + x^7 + x^2 + x + 1$ ko‘phad moduli bo‘yicha ko‘paytirish (Horner sxemasi) orqali hisoblanadi. Oqimli shifrlarning asosiy elementi - chiziqli teskari bog‘lanishli siljitish registri (LFSR). n razryadli LFSR ning teskari bog‘lanish ko‘phadi GF(2) ustida primitiv bo‘lsa, chiqish ketma-ketligi maksimal $2^n - 1$ davrga ega bo‘ladi. Biroq Berlekamp–Massey algoritmi [5] chiziqli murakkabligi L bo‘lgan ketma-ketlikni 2L ta bit asosida to‘liq tiklaydi, shuning uchun zamonaviy yengil shifrlarda LFSR nochiziqli komponentlar bilan birlashtiriladi: Grain-128AEAD da 128 bitli LFSR va NFSR [6], Trivium da esa umumiy hajmi 288 bit bo‘lgan uchta nochiziqli registr ishlatiladi [7]. ZUC algoritmida [8] LFSR tub maydon $GF(2^{31} - 1)$ ustida aniqlangan: bu maydonda 2^k ga ko‘paytirish 31 bitli so‘zni k bitga siklik surishga teng bo‘lib, dasturiy va apparat amalga oshirishni sezilarli soddalashtiradi. Galua maydonlarining kriptografik algoritmlarda qo‘llanilishi 1-jadvalda umumlashtirilgan.

1-jadval

Galua maydonlarining kriptografik algoritmlarda qo‘llanilishi

Algoritm / standart	Maydon	Modul (ko‘phad yoki tub son)	Vazifasi
AES (FIPS 197)	$GF(2^8)$	$x^8 + x^4 + x^3 + x + 1$	S-blok (inversiya), MixColumns
AES-GCM (SP 800-38D)	$GF(2^{128})$	$x^{128} + x^7 + x^2 + x + 1$	GHASH autentifikatsiyasi
ZUC (128-EEA3/EIA3)	$GF(2^{31} - 1)$	$p = 2^{31} - 1$	LFSR teskari bog‘lanishi
Grain-128AEAD	GF(2)	128-darajali primitiv ko‘phad	LFSR (NFSR bilan birga)
X25519 / Ed25519	$GF(2^{255} - 19)$	$p = 2^{255} - 19$	Elliptik egri chiziq arifmetikasi
Reed–Solomon kodlari (DVB, QR)	$GF(2^8)$	$x^8 + x^4 + x^3 + x^2 + 1$	Xatoliklarni tuzatish

Samarali amalga oshirish masalalari

Resurslari cheklangan qurilmalarda (IoT sensorlari, IP-kameralar, ARM mikrokontrollerlari) maydon amallarini amalga oshirishda quyidagi yondashuvlar qo‘llaniladi:

– jadval (log/antilog) usuli tez ishlaydi, biroq xotiraga murojaat vaqti maxfiy ma’lumotga bog‘liq bo‘lgani uchun kesh-vaqt hujumlariga zaif;

– bitslice va doimiy vaqtli (constant-time) amalga oshirish yon kanal hujumlariga chidamlilikni oshiradi;

– apparat darajasida inversiyani kompozit maydon $GF((2^4)^2)$ da hisoblash AES S-blokini ixcham qurish imkonini beradi [9];

– $GF(2^m)$ da inversiya uchun Itoh–Tsujii algoritmi [10] ko‘paytirishlar sonini keskin kamaytiradi;

– ARMv8 (PMULL) va x86 (PCLMULQDQ) protsessorlaridagi tashuvsiz (carry-less) ko‘paytirish buyruqlari GHASH hisoblashni bir necha barobar tezlashtiradi.

Xulosa

Galua maydonlari zamonaviy kriptografiyaning matematik poydevori bo‘lib, blokli va oqimli shifrlar, autentifikatsiya kodlari, ochiq kalitli tizimlar va xatoliklarni tuzatuvchi kodlarning bardoshliligi va samaradorligini belgilaydi. Maydon parametrlarini (keltirilmaydigan yoki primitiv ko‘phad, tub modul, maydon tasviri) to‘g‘ri tanlash algoritmning kriptografik bardoshliligi bilan bir qatorda uni amalga oshirish narxiga ham bevosita ta’sir ko‘rsatadi. Videokuzatuv va IoT tizimlari kabi real vaqt rejimida ishlovchi muhitlarda maydon amallarini doimiy vaqtli va apparat tezlatkichlaridan foydalangan holda amalga oshirish ustuvor vazifa hisoblanadi. Yengil oqimli shifrlarning nochiziqli bloklarini Galua maydonlari ustida loyihalash va ularni ARM platformalarida baholash keyingi tadqiqotlarning istiqbolli yo‘nalishidir.

Foydalanilgan adabiyotlar

1. Lidl R., Niederreiter H. Finite Fields. 2nd ed. - Cambridge: Cambridge University Press, 1997. (Encyclopedia of Mathematics and its Applications, Vol. 20).

2. FIPS PUB 197. Advanced Encryption Standard (AES). - Gaithersburg: NIST, 2001 (updated 2023).

3. Daemen J., Rijmen V. The Design of Rijndael: The Advanced Encryption Standard (AES). 2nd ed. - Berlin: Springer, 2020.

4. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. - Gaithersburg: NIST, 2007.

5. Massey J.L. Shift-register synthesis and BCH decoding // IEEE Transactions on Information Theory. - 1969. - Vol. 15, No. 1. - P. 122–127.

6. Hell M., Johansson T., Maximov A., Meier W., Sönnerup J., Yoshida H. Grain-128AEAD - A lightweight AEAD stream cipher. - NIST Lightweight Cryptography Project, 2019.

7. Avoine G., Hernandez-Castro J. (eds.). Security of Ubiquitous Computing Systems: Selected Topics. - Cham: Springer, 2021. - 268 p.

8. ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification. Version 1.6. - 2011.

9. Canright D. A very compact S-box for AES // Cryptographic Hardware and Embedded Systems - CHES 2005. LNCS 3659. - Springer, 2005. - P. 441–455.

10. Itoh T., Tsujii S. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases // Information and Computation. - 1988. - Vol. 78, No. 3. - P. 171–177.

IOT QURILMALARI UCHUN APPARAT RESURSLARI CHEKLANGAN SHAROITDA OQIMLI SHIFRLASH ALGORITMLARINI TAHLIL QILISH

Xamrayev A.Q.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada eSTREAM loyihasining apparat amalga oshirishga yo‘naltirilgan Profile 2 portfelidagi Grain v1, MICKEY 2.0 va Trivium oqimli shifrlari ko‘rib chiqiladi. Profilning vazifasi, algoritmlarning ishlash prinsipi va apparat baholash mezonlari yoritilib, kalit va IV uzunligi, ichki holat, initsializatsiya, FPGA resurslari va chastota bo‘yicha e’lon qilingan natijalar tahlil qilinadi. Natijalar asosida cheklangan resursli IoT qurilmasida maydon, unumdorlik va energiya o‘rtasidagi muvozanat muhokama qilinadi.

Kalit so‘zlar: eSTREAM, oqimli shifrlash, Profile 2, Grain v1, MICKEY 2.0, Trivium, IoT, FPGA, apparat resurslari.

Аннотация. В статье рассматриваются потоковые шифры Grain v1, MICKEY 2.0 и Trivium из аппаратного профиля Profile 2 проекта eSTREAM. Описываются назначение профиля, принципы работы алгоритмов и критерии аппаратной оценки; анализируются длина ключа и IV, внутреннее состояние, инициализация, ресурсы FPGA и опубликованные показатели частоты. На этой основе обсуждается баланс между площадью схемы, производительностью и энергопотреблением в IoT-устройствах с ограниченными ресурсами.

Ключевые слова: eSTREAM, потоковое шифрование, Profile 2, Grain v1, MICKEY 2.0, Trivium, IoT, FPGA, аппаратные ресурсы.

Kirish

Buyumlar interneti tizimlarida ko‘plab qurilmalar uzoq muddat davomida batareya yoki cheklangan quvvat manbai bilan ishlaydi. Bunday qurilmalarda apparat maydoni, registrlar va mantiqiy elementlar soni, ma’lumotni qayta ishlash tezligi hamda energiya sarfi bir-biri bilan bog‘liq. Shuning uchun kriptografik algoritmni tanlashda faqat matematik tavsif yoki kalit uzunligi bilan cheklanib bo‘lmaydi; uning real apparat realizatsiyasi ham o‘rganilishi kerak.

Oqimli shifr maxfiy kalit va boshlang‘ich vektor (IV) asosida kalit oqimini hosil qiladi. Shifrlash jarayonida kalit oqimi ochiq matn bilan XOR amali orqali birlashtiriladi. Qurilma yangi seansni boshlaganda IV va kalit asosida ichki holatni tayyorlash uchun bir qator taktlar bajarilishi mumkin. Shu sababli uzoq uzluksiz oqimni qayta ishlash va qisqa xabarlar uchun tez-tez qayta ishga tushish holatlari alohida baholanishi lozim.

eSTREAM loyihasida Profile 2 apparat amalga oshirishga va resurslari cheklangan muhitlarga mos shifrlarni aniqlashga qaratilgan. Yakuniy apparat portfeliga Grain v1, MICKEY 2.0 va Trivium kiritilgan. F-FCSR-H v2 dastlab portfelda bo‘lgan, biroq keyingi kriptotahlil natijalaridan so‘ng yakuniy portfeldan chiqarilgan [1]. Ushbu maqolada uchta yakuniy algoritmning texnik xususiyatlari va e’lon qilingan apparat o‘lchovlari ko‘rib chiqiladi.

Tadqiqot maqsadi - algoritmlarning ichki holati va initsializatsiya xususiyatlarini apparat resurslari hamda unumdorlik ko‘rsatkichlari bilan bog‘lab, IoT qurilmalariga mos tanlov mezonlarini shakllantirish. Turli maqolalarda ishlatilgan FPGA modeli, sintez vositasi, realizatsiya turi va parallel ishlash darajasi natijalarni sezilarli o‘zgartirishi mumkinligi hisobga olinadi.

Profile 2 algoritmlarining ishlash prinsipi va baholash mezonlari

Grain v1 chiziqli qayta aloqa registri va nochiziqli qayta aloqa registridan foydalanadi. Uning ichki holati 160 bit bo‘lib, apparatdagi registrlar va mantiqiy funksiyalar yordamida amalga oshiriladi. MICKEY 2.0 ikkita boshqariladigan registrga asoslanadi; ichki holat hajmi 200 bit deb ko‘rsatiladi. Trivium esa uchta o‘zaro bog‘langan registrdan foydalanadi va jami 288 bitli ichki holatga ega. Ushbu tuzilishlar kalit oqimini hosil qilish usuli, mantiqiy bog‘lanishlar va apparatdagi resurs sarfiga ta’sir qiladi.

Apparat realizatsiyasida asosiy mezonlar quyidagilar: 1) slice yoki boshqa mantiqiy resurslar soni - sxemaning FPGA maydonini ko‘rsatadi; 2) maksimal ish chastotasi - sxema qanchalik tez taktlanishi mumkinligini bildiradi; 3) bir takt yoki siklda hosil qilinadigan bitlar soni - chastotani real throughput bilan bog‘lash uchun kerak; 4) kalit va IV uzunligi; 5) initsializatsiya taktlarining soni; 6) energiya sarfi. Yuqori chastota o‘z-o‘zidan yuqori bit tezligi yoki kam energiya sarfini anglatmaydi.

1-jadval

Grain v1, MICKEY 2.0 va Trivium algoritmlarining asosiy parametrlari

Parametr	Grain v1	MICKEY 2.0	Trivium
Kalit uzunligi	80 bit	80 bit	80 bit
IV uzunligi	64 bit	80 bitgacha	80 bit
Ichki holat	160 bit	200 bit	288 bit
Asosiy tuzilish	Chiziqli va nochiziqli registrlar	Boshqariladigan ikki registr	Uchta o‘zaro bog‘langan registr
Initsializatsiya	160 takt	Realizatsiyaga bog‘liq	1152 takt

Grain v1 ning ichki holati uch algoritm ichida eng kichik, Trivium esa kattaroq holatga ega. Lekin faqat bitlar soniga qarab apparat maydonini yakuniy baholab bo‘lmaydi: qayta aloqa funksiyalarining murakkabligi, boshqaruv mantiqi, registrlarning joylashuvi va sintez vositasining optimallashtirishi ham natijaga ta’sir ko‘rsatadi. Jadvaldagi initsializatsiya taktlarini ham foydali ma’lumot tezligi bilan aralashtirmaslik kerak; bu qiymatlar kalit oqimini chiqarishdan oldingi tayyorlash jarayoniga taalluqlidir.

FPGA realizatsiyalarida o‘lchangan natijalar

2020-yilda chop etilgan tadqiqotda Grain v1, MICKEY 2.0 va Trivium algoritmlari Xilinx Spartan-7 FPGA platformasida Verilog tilida amalga oshirilib, Vivado muhitida loyihalangan va sintez qilingan [5]. Mualliflar ketma-ket, bazaviy va parallel realizatsiya variantlarini ko‘rib chiqqan. Bu farq muhim: ketma-ket variant resurslarni tejashga qaratilishi mumkin, parallel variant esa bir takt ichida ko‘proq kalit oqimi bitlarini hosil qilish evaziga ko‘proq mantiqiy resurs talab qilishi mumkin.

2-jadval

E’lon qilingan FPGA natijalari [5]

Ko‘rsatkich	Grain v1	MICKEY 2.0	Trivium
Platforma	Xilinx Spartan-7 FPGA	Xilinx Spartan-7 FPGA	Xilinx Spartan-7 FPGA
Tavsiflash tili	Verilog	Verilog	Verilog

Ketma-ket variant resursi	26 slice	Maqola annotatsiyasida aniq son berilmagan	13 slice
Bazaviy variant chastotasi	Ushbu ma’lumotda tasdiqlanmagan	384 MHz	416 MHz

Keltirilgan ketma-ket variantlarda Grain v1 26 slice, Trivium esa 13 slice ishlatgan. Shu tajriba doirasida Triviumning ko‘rsatilgan ketma-ket varianti kamroq slice bilan amalga oshirilgan. Biroq bu natija Trivium har qanday FPGA yoki ASICda doimo ikki baravar kichik bo‘ladi degani emas: boshqa sintez cheklovlari, kod tuzilishi va qurilma oilasi natijani o‘zgartirishi mumkin. MICKEY 2.0 uchun ushbu manbaning qisqa annotatsiyasida ketma-ket variantning aniq slice qiymati ko‘rsatilmagan; shu sababli qiymat taxmin bilan to‘ldirilmaydi.

Bazaviy variantlar uchun manbada Triviumning chastotasi 416 MHz, MICKEY 2.0 chastotasi esa 384 MHz sifatida keltirilgan [5]. Bu raqamlar sxemaning sintez qilingan sharoitda ishlashi mumkin bo‘lgan chastotaga tegishli. Ma’lumot tezligini hisoblash uchun har takt ichida nechta bit ishlab chiqarilishi, boshqaruv taktlarining mavjudligi va interfeys cheklovlari ham ma’lum bo‘lishi kerak. Shu ma’lumotlarsiz chastotani bevosita bayt/soniya ko‘rsatkichiga aylantirish to‘g‘ri emas.

Natijalarni IoT qurilmalari nuqtayi nazaridan tahlil qilish

Birinchi mezon - apparat maydoni. Kichik maydon mikrokontroller yoki FPGA resurslarini boshqa vazifalar uchun saqlab qolishi mumkin. Sensor tugunida kriptografiyadan tashqari radio interfeys, taymer, xotira boshqaruvi va nazorat logikasi ham joy egallaydi. Shuning uchun algoritmning o‘zi kichik bo‘lishi yetarli emas; butun tizim sintez qilinib, resurslar yig‘indisi tekshirilishi kerak.

Ikkinchi mezon - unumdorlik. Ko‘p ma’lumot uzatadigan qurilmada kalit oqimining hosil bo‘lish tezligi muhim. Parallelizatsiya throughputni oshirishi mumkin, lekin qo‘shimcha mantiqiy resurslar va kommutatsiya faolligini ham oshirishi ehtimol. Kam ma’lumot uzatadigan, uzoq vaqt kutish holatida turadigan sensor uchun esa eng yuqori chastotadan ko‘ra kichik kutish va kam energiya sarfi muhimroq bo‘lishi mumkin.

Uchinchi mezon - initsializatsiya. Trivium uchun 1152 takt va Grain v1 uchun 160 takt qiymatlari ko‘rsatilgan. Agar qurilma uzoq uzluksiz oqimni shifrlasa, tayyorlash xarajati umumiy ish vaqtining kichik qismiga aylanishi mumkin. Agar har bir kichik xabar yangi IV bilan alohida seansni boshlasa, initsializatsiya kechikish va energiya sarfiga ko‘proq ta’sir qilishi mumkin. MICKEY 2.0 bo‘yicha ayni jadvalda aniq takt soni tasdiqlanmagani uchun u haqida sonli ustunlik xulosasi chiqarilmaydi.

To‘rtinchi mezon - energiya. FPGA slice soni va maksimal chastota energiya sarfining to‘g‘ridan-to‘g‘ri o‘lchovi emas. Dinamik quvvat takt chastotasi, sig‘imlar va signal almashinuvi faolligiga bog‘liq; statik quvvat esa qurilma texnologiyasiga ham bog‘liq. Agar energiya bo‘yicha o‘lchovlar mavjud bo‘lmasa, algoritmlarni energiya jihatidan reytinglash o‘rniga bu cheklovni aniq qayd etish kerak. Amaliy IoT sinovi bir xil ish yukida sarflangan energiyani, xabar kechikishini va resurslar sonini birgalikda o‘lchashi lozim.

Nihoyat, oqimli shifr xavfsiz aloqa tizimining faqat bir qismidir. IV takrorlanmasligi, kalitlarni yaratish va saqlash, xabar yaxlitligini tekshirish hamda qurilmaga ruxsatsiz dastur yuklanishidan himoya alohida ta’minlanadi. Shu bois apparat jihatidan samarali algoritmni tanlash bilan birga, uni protokol va qurilma xavfsizligi bilan to‘g‘ri birlashtirish zarur.

Xulosa

Grain v1, MICKEY 2.0 va Trivium taqqoslanishi apparat oqimli shifrni tanlashda ichki holat, initsializatsiya, mantiqiy resurslar va chastotani birgalikda baholash kerakligini ko‘rsatadi. Keltirilgan Xilinx Spartan-7 tajribasida ketma-ket Trivium realizatsiyasi 13 slice, Grain v1 esa 26 slice ishlatgan; bazaviy variant chastotalari Trivium uchun 416 MHz va MICKEY 2.0 uchun 384 MHz deb berilgan. Bu qiymatlar faqat manbada ko‘rsatilgan platforma va realizatsiya sharoitiga tegishli.

IoT qurilmalari uchun yagona universal g‘olibni belgilash uchun mavjud raqamlar yetarli emas: energiya sarfi va barcha variantlar bo‘yicha bir xil sharoitdagi throughput natijalari kerak. Keyingi tadqiqotda bir xil FPGA yoki ASIC texnologiyasi, bir xil sintez sozlamalari va bir xil ish yukidan foydalanib, maydon, tezlik, initsializatsiya va energiya sarfini parallel ravishda o‘lchash maqsadga muvofiq. Shunda tanlov muayyan qurilma talablari bilan asoslanadi.

Foydalanilgan adabiyotlar

1. ECRYPT. eSTREAM: The ECRYPT Stream Cipher Project. https://www.ecrypt.eu.org/stream/

2. Hell M., Johansson T., Meier W. Grain: A Stream Cipher for Constrained Environments. eSTREAM technical documentation.

3. De Cannière C., Preneel B. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. eSTREAM technical documentation.

4. Babbage S., Dodd M. The MICKEY Stream Ciphers. MICKEY 2.0 technical documentation.

5. FPGA Implementations of Grain v1, Mickey 2.0, Trivium, Lizard and Plantlet. Microprocessors and Microsystems, Vol. 78, 2020, Article 103210. DOI: https://doi.org/10.1016/j.micpro.2020.103210

6. Analysis of Area-Efficiency vs. Unrolling for eSTREAM Hardware Portfolio Stream Ciphers. Electronics, Vol. 9, No. 11, 2020, Article 1935. https://doi.org/10.3390/electronics9111935

KRIPTOGRAFIK KALITLARNI GENERATSIYALASHDA ENTROPIYA MANBALARINING SIFATINI BAHOLASH USULLARI

Daminov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada kriptografik kalitlarni generatsiyalashda entropiya manbalarining sifatini baholash usullari tahlil qilinadi. Shannon va min-entropiya matematik jihatdan farqlanib, NIST SP 800-90B bo‘yicha baholovchilar, restart va sog‘lomlik testlari qiyosiy ko‘rib chiqiladi. Baholash, monitoring va umumiy statistik testlar turli vazifalarni bajarishi, DRBG xavfsizligi esa dastlabki entropiya sifatiga bog‘liqligi asoslanadi.

Kalit so‘zlar: entropiya manbai, min-entropiya, Shannon entropiyasi, NIST SP 800-90B, sog‘lomlik testlari, DRBG, kriptografik kalit.

Аннотация. В статье анализируются методы оценки качества источников энтропии при генерации криптографических ключей. Раскрываются математические различия между энтропией Шеннона и минимальной энтропией, проводится сравнительный анализ методов оценивания, тестов перезапуска и тестов работоспособности, предусмотренных NIST SP 800-90B. Обосновывается, что оценивание, мониторинг и общие статистические тесты выполняют различные функции, а безопасность DRBG зависит от качества исходной энтропии.

Ключевые слова: источник энтропии, минимальная энтропия, энтропия Шеннона, NIST SP 800-90B, тесты работоспособности, DRBG, криптографический ключ.

Kriptografik kalitning chidamliligi uni hosil qilishda ishlatilgan tasodifiy ma'lumotlarning oldindan aytib bo‘lmasligiga bog‘liq. Deterministik tasodifiy bit generatori (DRBG) entropiya manbai emas: u faqat boshlang‘ich qiymat (seed) entropiyasini kengaytiradi [1]. Shu sababli entropiya manbalarini baholash NIST SP 800-90B (2018) hujjatida alohida tartibga solingan [2], manba, konditsioner va DRBG ni birlashtiruvchi konstruksiyalar esa SP 800-90C (2025) da keltirilgan [3]. SP 800-90B baholovchilarining amaldagi xatti-harakati keyingi tadqiqotlarda tahlil qilingan. Tezisning maqsadi baholash usullarini matematik asosi, qo‘llanish sohasi, afzalligi va cheklovi bo‘yicha qiyosiy ko‘rib chiqishdir. Original eksperiment o‘tkazilmagan; keltirilgan natijalar adabiyotdan olingan.

Shannon va min-entropiya. Diskret tasodifiy miqdor X uchun Shannon entropiyasi va min-entropiya quyidagicha aniqlanadi:

$$H(X) = -\sum_x p(x) \log_2 p(x) \quad (1)$$

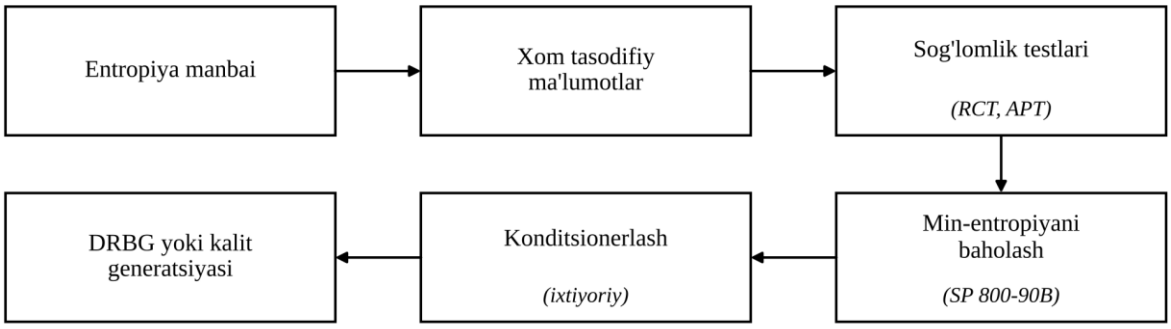
$$H_\infty(X) = -\log_2(\max p(x)) \quad (2)$$

bunda x -X ning mumkin bo‘lgan qiymati; p(x) -uning ehtimolligi; max p(x) -eng ehtimolli qiymatning ehtimolligi; entropiya bitlarda o‘lchanadi. Shannon entropiyasi o‘rtacha noaniqlikni, min-entropiya esa eng noqulay holatni tavsiflaydi. Doimo $H_\infty(X) \leq H(X)$ bajariladi. Hujumchining eng yaxshi bir martalik taxmini eng ehtimolli qiymatga asoslanadi, shuning uchun SP 800-90B xavfsizlikni min-entropiya orqali ifodalaydi. Shannon entropiyasi taqsimot bo‘yicha o‘rtacha qiymat bo‘lgani uchun juda ko‘p kam ehtimolli qiymatlar uni oshirib yuboradi, taxmin qilish qiyinligini esa eng ehtimolli qiymat belgilaydi. Shu sababli yuqori Shannon entropiyasi xavfsizlikni kafolatlamaydi. Misol: bir qiymat 1/2 ehtimollik bilan chiqib, qolgan $2^{128}-1$ qiymat

teng ehtimollikda taqsimlansa, H ≈ 65 bit, H_∞= 1 bit bo‘ladi: kalitni bitta urinishda 1/2 ehtimollik bilan topish mumkin.

SP 800-90B usullari

Manba modeli shovqin manbai, ixtiyoriy konditsioner va sog‘lomlik testlaridan iborat (1-rasm). Xom ma'lumotlar IID (mustaqil va bir xil taqsimlangan) deb faraz qilinsa, min-entropiya MCV (eng ko‘p uchraydigan qiymat) baholovchisi bilan aniqlanadi; aks holda non-IID yo‘li qo‘llanib, o‘nta baholovchi (jumladan Collision, Markov, Compression) natijalarining eng kichigi olinadi. IID farazi permutatsiya va boshqa statistik tekshiruvlar orqali sinaladi. Shu sababli bitta baholovchining sezilarli kam baholashi yakuniy natijani belgilaydi. Konditsioner qo‘llanilsa, chiqishdagi entropiya kirish entropiyasi va funksiya parametrlaridan hisoblanadi; bunday hisob faqat tasdiqlangan (vetted) funksiyalar uchun belgilangan. RCT (takrorlar soni) va APT (moslashuvchan ulush) testlari ishlash vaqtida buzilishni aniqlaydi, ammo entropiyani baholamaydi. Sxemada min-entropiyani baholash va sog‘lomlik testlari alohida vazifalar sifatida ko‘rsatilgan.



1-rasm. Entropiya manbasidan kalit generatsiyasigacha bo‘lgan jarayonning blok-sxemasi

Compression baholovchisini takomillashtirishda, umumlashgan LRS baholovchisi [4]da taklif etilgan. Bashoratchilar o‘rtacha min-entropiyani baholashga mosroq degan fikr preprintda ilgari surilgan .

Qiyosiy tahlil

Usullarning matematik asosi, mezoni, afzalligi va cheklovi 1-jadvalda keltirilgan. Jadvaldan ko‘rinadiki, baholash (MCV, Collision, Markov, Compression), tekshirish (restart) va nazorat (RCT, APT) turli mezonlarga tayanadi va turli savollarga javob beradi. SP 800-22 kabi umumiy statistik testlar chiqish ketma-ketligidagi og‘ishlarni tekshiradi; deterministik generator chiqishi ham ulardan o‘tishi mumkin, shu sababli ular min-entropiya o‘lchovi bo‘la olmaydi. Baholovchilar modelga asoslangan: bog‘liqlik turi modelga mos kelmasa, natija noto‘g‘ri bo‘lishi mumkin, shuning uchun eng kichik qiymat olinadi. Bu yondashuv konservativ; SP 800-90B baholovchilari min-entropiyani kam baholashga moyilligi ko‘rsatilgan oldingi ishlarga tayanib, da bashoratchilar o‘rtacha min-entropiya uchun mosroq deb hisoblanadi. Mashinaviy bashoratchilar preprint bo‘lib, SP 800-90B tarkibiga kirmaydi, shuning uchun ular baholovchilarning o‘rnini bosmaydi, balki qo‘shimcha tahlil vositasi sifatida qaraladi. Restart va sog‘lomlik testlari esa baholashga alternativa emas, balki uni to‘ldiruvchi nazorat vositasidir.

1-jadval

Entropiya manbalarining sifatini baholash usullarining qiyosiy tahlili

Baholash usuli	Baholash mezoni	Afzalligi	Cheklovi
MCV baholovchisi	Eng ko‘p uchraydigan qiymat ulushining yuqori ishonch chegarasi	Oddiy; IID va non-IID yo‘llarida qo‘llanadi	Qiymatlar orasidagi bog‘liqlikni hisobga olmaydi
Collision, Markov, Compression	To‘qnashuvlar, Markov zanjiri, siqilish o‘lchovi	Turli bog‘liqlik turlarini qamrab oladi	Har biri o‘z modeliga sezgir; eng kichik natija olinadi
Restart testi	1000×1000 matritsa qator va ustunlarining baholangan entropiyaga mosligi	Qayta ishga tushirishdagi bog‘liqlikni aniqlaydi	Entropiyaning o‘zini hisoblamaydi
RCT va APT	Qiymat takrorlari soni; oynadagi qiymat chastotasi	Uzluksiz, yengil nazorat	Entropiyani miqdoriy baholamaydi
SP 800-22 testlari	Ketma-ketlikdagi og‘ishlar bo‘yicha p-qiymatlar	Chiqish ketma-ketligini tekshiradi	Min-entropiyani baholamaydi
ML bashoratchilari	Bashoratchi aniqligi bo‘yicha o‘rtacha min-entropiya	Aniq model talab qilmaydi	Preprint; standartlashmagan

Amaliy ahamiyati. MCV baholovchisi eng ko‘p uchragan qiymatning kuzatilgan ulushiga 99% ishonch oralig‘ining yuqori chegarasini qo‘shib, uning teskari logarifmini min-entropiya sifatida beradi. TRNG uchun baholash loyihalash va validatsiya bosqichida xom ma'lumotlarda bajariladi, sog‘lomlik testlari esa ishlash vaqtida manba buzilishini kuzatadi. Konditsioner chiqishini statistik testlar bilan tekshirish manbaning entropiyasini isbotlamaydi, chunki konditsioner chiqishni tashqi ko‘rinishda tasodifiy qilishi mumkin. DRBG ni seed bilan ta'minlashda baholangan min-entropiya zarur: masalan, 256 bit entropiya uchun 0,5 bit/namuna bo‘lganda kamida 512 namuna kerak (konditsionerlash yo‘qotishlarisiz). SP 800-90C RBG1, RBG2, RBG3 va RBGC konstruksiyalarini belgilaydi; DRBG esa har qanday konstruksiyada entropiyaning manbasi emas, uni kengaytiruvchi mexanizm bo‘lib qoladi.

Foydalanilgan adabiyotlar

1. E. Barker and J. Kelsey, “Recommendation for random number generation using deterministic random bit generators,” NIST, Gaithersburg, MD, USA, SP 800-90A Rev. 1, Jun. 2015, doi: 10.6028/NIST.SP.800-90Ar1.

2. M. Sönmez Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, “Recommendation for the entropy sources used for random bit generation,” NIST, Gaithersburg, MD, USA, SP 800-90B, Jan. 2018, doi: 10.6028/NIST.SP.800-90B.

3. E. Barker, J. Kelsey, K. McKay, A. Roginsky, and M. Sönmez Turan, “Recommendation for random bit generator (RBG) constructions,” NIST, Gaithersburg, MD, USA, SP 800-90C, Sep. 2025, doi: 10.6028/NIST.SP.800-90C.

4. M. Aslan, A. Doğanaksoy, Z. Saygı, M. Sönmez Turan, and F. Sulak, “Observations on NIST SP 800-90B entropy estimators,” Cryptogr. Commun., vol. 18, no. 1, pp. 63–81, 2026, doi: 10.1007/s12095-025-00778-7.

KVANT HISOBLASH TEXNOLOGIYALARINING VPN TIZIMLARINING KRIPTOGRAFIK XAVFSIZLIGIGA TA’SIRI

Suyunov S.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Maqolada hozirgi kunda VPN tunellarini qurishda foydalanilayotgan kriptografik algoritimlar va ularga kvant kompyuterlar tomonidan yaratiladigan xavfsizlik muammolari va ularning yechimlari ko‘rib chiqiladi.

Kalit so‘zlar: VPN (Virtual Private Network), Shor algoritimi, Post-kvant kriptografiyasi, Kvant kompyuterlari.

Аннотация: В статье рассматриваются криптографические алгоритмы, используемые в настоящее время для построения VPN-туннелей, а также проблемы безопасности, связанные с квантовыми компьютерами, и обсуждаются пути их решения.

Ключевые слова: VPN (виртуальная частная сеть), алгоритм Шора, постквантовая криптография, квантовые компьютеры.

Kirish

Virtual xususiy tarmoq (VPN) tizimlari o‘zining umumiy xavfsizligini ta’minlashda asosan ochiq kalitli kriptografiya usullariga (masalan, RSA va elliptik egri chiziqlar kriptografiyasi - ECC) tayanadi. Kvant texnologiyalarining ochiq kalitli kriptotizimlar uchun tug‘dirayotgan xavflari VPN xavfsizligi borasida jiddiy va yaqin orada yuz berishi mumkin bo‘lgan inqirozga sabab bo‘lmoqda, bunga sabab - Shor algoritmining RSA va ECC kalitlarini buzib kirish imkoniyatiga egaligidir. Mavjud texnologik holat kvant hujumlariga chidamli va xavfsiz aloqa tizimlariga bo‘lgan talabga zudlik bilan javob topishni taqozo etadi.

Asosiy qisim

Klassik VPN (Virtual Private Network - Virtual Xavfsiz Tarmoq) texnologiyasi - bu ochiq va xavfsiz bo‘lmagan ommaviy internet tarmog‘i ustidan ikki nuqta o‘rtasida xavfsiz, shifrlangan va xususiy aloqa kanalini (tunnelini) o‘rnatib beruvchi tarmoq texnologiyasidir. Klassik korporativ yoki shaxsiy VPN tizimlari asosan bitta markaziy shlyuz (Gateway) va unga ulanuvchi masofaviy foydalanuvchilar (Remote Access) yoki boshqa bir filial (Site-to-Site) arxitekturasiga asoslanadi.

Klassik VPN ma’lumot uzatishda 3 ta asosiy jarayonni amalga oshiradi:

– *Foydalanuvchi yoki masofaviy router VPN* serverga ulanishni so‘raganda, tizim login/parol, raqamli sertifikatlar yoki maxsus kalitlar (Pre-shared key) orqali uning shaxsini va xavfsizligini tekshiradi.

– *Tunneling (Kapsulatsiyalash):* VPN siz yubormoqchi bo‘lgan oddiy ma’lumot paketini (IP paket) oladi va uni boshqa bir xavfsiz paketning ichiga "joylaydi" (kapsulatsiyalaydi). Bu xuddi xatni oddiy qog‘ozda emas, maxsus himoyalangan konvertda yuborishga o‘xshaydi.

– *Shifrlash (Encryption):* Konvert ichidagi ma’lumotlar shifrlash algoritmlari (masalan, AES-256) yordamida o‘qib bo‘lmaydigan kodga aylantiriladi. Hatto internet provayderingiz (ISP) yoki xakerlar trafikni tutib olgan taqdirda ham, uning ichida nima borligini ko‘ra olmaydi. Amaldagi klassik VPN protokollari: IPSec (Internet Protocol Security), OpenVPN, PPTP va L2TP, WireGuard.

Raqamli texnologiyalar va bulutli (Cloud) tizimlar rivojlanishi bilan klassik korporativ VPN'larning ba’zi jiddiy kamchiliklari yuzaga chiqdi:

“Ulandingmi – tamom” prinsipi: Klassik VPN foydalanuvchini tarmoqqa ichkariga kiritgach, uni to‘liq ishonchli deb hisoblaydi. Agar xaker bitta xodimning VPN loginini qo‘lga kiritsa, u korxonaning butun ichki tarmog‘iga (barcha serverlarga) kirish imkonini oladi (segmentatsiyaning yo‘qligi).

Tezlik va Kechikish (Latency): Barcha trafik markaziy VPN shlyuzi orqali o‘tgani sababli, foydalanuvchilar ko‘payganda tarmoq sekinlashadi (Hub-and-Spoke muammosi).

Qurilma holatini tekshirmaslik: VPN ulanayotgan shaxsiy kompyuterda virus yoki zararli dastur bor-yo‘qligini nazorat qilmaydi.

Kvant kompyuterlarining (Quantum Computers) rivojlanishi va to‘liq quvvatda ishga tushishi bugungi kunda biz ishlatayotgan klassik VPN texnologiyalarining asosiy xavfsizlik ustunlarini butunlay parchalash xavfini tug‘diradi. Kvant kompyuterlari klassik kompyuterlar uchun minglab yillar talab qiladigan murakkab matematik masalalarni bir necha daqiqada yecha olishi bilan xavflidir. Quyida ushbu texnologiyaning klassik VPN'larga soladigan aniq xavflari keltirilgan:

– Kalit almashinuvi (Key Exchange) jarayonining buzilishi: VPN ulanishi boshlanganda, foydalanuvchi va VPN server bir-birini tanib olishi hamda ma'lumotni shifrlash uchun umumiy maxfiy kalitni kelishib olishi kerak (bunga *Handshake* yoki salomlashish deyiladi). Buning uchun klassik VPN'lar RSA, Diffie-Hellman (DH) yoki ECC (Elliptic Curve Cryptography) kabi asimmetrik shifrlash algoritmlaridan foydalanadi. *Xavf:* Kvant kompyuterlari *Shor algoritmi (Shor's algorithm)* yordamida ushbu algoritmlarning matematik asosini (katta tub sonlarni ko‘paytuvchilarga ajratish va diskret logarifmlarni) juda tez hisoblab chiqadi. Natijada, kvant kompyuteriga ega bo‘lgan xaker VPN shlyuzining kalitlarini osongina buzib kiradi va tunnel ichidagi barcha maxfiy trafikni ochiq-oydin o‘qiy oladi.

– “Hozir yig‘ib ol, keyin shifrdan chiqar” (Harvest Now, Decrypt Later) hujumi. Bu bugungi kunda allaqachon sodir bo‘layotgan eng sinsi xavflardan biridir. Xavf: Kiberjinoyatchilar yoki ayrim davlatlarning maxsus xizmatlari bugungi kunda internet tarmoqlari orqali o‘tayotgan, klassik VPN bilan shifrlangan katta hajmdagi maxfiy ma’lumotlarni shunchaki yozib olib, o‘z ma’lumotlar omborida saqlamoqda (Harvesting). Hozir ularda buni o‘qish imkoniyati yo‘q. Ammo bir necha yildan keyin yetarli quvvatdagi kvant kompyuteri paydo bo‘lishi bilan, ular saqlab qo‘yilgan ushbu eski ma’lumotlarni (davlat sirlari, bank ma’lumotlari, shaxsiy yozishmalar) bir zumda shifrdan chiqarib o‘qishlari mumkin bo‘ladi.

– Simmetrik shifrlashning kuchsizlanishi (AES-128 xavf ostida). VPN tunnelining ichidagi ma’lumotlarni bevosita shifrlash uchun klassik VPN'lar AES (Advanced Encryption Standard) algoritmiga tayanadi. Xavf: Kvant kompyuterlaridagi Grover algoritmi (Grover's algorithm) ma’lumotlarni tanlab kalit qidirish (brute-force) tezligini kvadratik darajada oshiradi. Bu shuni anglatadiki, u simmetrik kalit uzunligini amalda yarmiga qisqartirib qo‘yadi. Natijada, bugungi kunda juda xavfsiz hisoblangan AES-128 shifrlash tizimi kvant davrida mutlaqo yaroqsiz (64-bitlik zaif himoya kabi) bo‘lib qoladi.

Dunyo IT hamjamiyati kvant xavfini shunchaki tomosha qilib o‘tirgani yo‘q. Hozirda klassik VPN tizimlarini himoya qilish uchun quyidagi choralar joriy etilmoqda:

– AES-256 standartiga o‘tish: Grover algoritmi kalit kuchini yarmiga tushirsa ham, AES-256 shifrlash tizimi kvant hujumidan keyin ham 128-bitlik mustahkamlikni saqlab qoladi. Bu esa hatto kvant kompyuterlari uchun ham buzib bo‘lmas darajada kuchli himoyadir.

– Post-Kvant Kriptografiyasi (PQC): AQShning NIST tashkiloti kvant kompyuterlari ham buza olmaydigan yangi matematik algoritmlarni (masalan, ML-KEM yoki ML-DSA)

standartlashtirdi. OpenVPN va WireGuard kabi yetakchi VPN protokollari allaqachon ushbu post-kvant algoritmlarini o‘z ichiga olgan gibrid (klassik + post-kvant) ulanish tizimlarini sinovdan o‘tkazishni va amaliyotga joriy etishni boshlagan.

Xulosa

VPN tizimlari uchun samarali kriptografik himoya algoritm, protokol va qurilma darajasidagi mexanizmlarni birgalikda loyihalashni talab qiladi. Yangi yechimlarni baholashda nazariy bardoshlilik bilan bir qatorda dasturiy va apparat samaradorligi, energiya xarajati hamda amaliy hujumlarga qarshi chidamlilik mezonlari kompleks ko‘rib chiqilishi zarur.

Foydalanilgan manbalar:

1. https://www.techtarget.com/it-strategy/tip/Attention-CISOs-Quantum-computing-security-risks-are-here
2. https://www.cyberfenceplatform.com/blog/quantum-computing-vpn-encryption/
3. https://www.appviewx.com/blogs/next-generation-vpn-security-needs-to-be-quantum-safe/

KLASSIK OCHIQ KALITLI KRIPTOTIZIMLAR (RSA, ECC, DIFFIE–HELLMAN) VA ULARNING KVANT KOMPYUTERLARIGA NISBATAN ZAIFLIGINI BAHOLASH

Xudoykulov Z.T., Baxodirov D.U.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda RSA, Diffi–Xellman va elliptik egri chiziqli kriptosistemalarning faktorlash va diskret logarifmlash masalalariga tayanishi, Shor algoritmi bu masalalarni kvant kompyuterida polinomial vaqtda yechishi tahlil qilingan. 2017–2026-yillarda e'lon qilingan resurs baholari qiyoslanib, 256 bitli elliptik egri chiziqli kriptografiya RSA-2048 algoritmiga nisbatan kamroq kvant resurs talab qilishi va baholar tez kamayib borayotgani ko'rsatilgan. NIST postkvant standartlari, o'tish muddatlari va O'zMSt 286:2024 imzo standartiga ta'siri asosida O'zbekiston uchun tavsiyalar berilgan.

Kalit so'zlar: RSA; Diffi–Xellman; elliptik egri chiziqli kriptografiya; Shor algoritmi; Grover algoritmi; kvant kompyuter; postkvant kriptografiya; ML-KEM; ML-DSA; O'zMSt 286:2024.

Аннотация. В тезисах рассмотрена зависимость криптосистем RSA, Диффи–Хеллмана и криптографии на эллиптических кривых от сложности задач факторизации и дискретного логарифмирования, а также решение этих задач алгоритмом Шора за полиномиальное время на квантовом компьютере. Сопоставлены оценки ресурсов, опубликованные в 2017–2026 гг.; показано, что 256-битная эллиптическая криптография требует меньших квантовых ресурсов, чем RSA-2048, и что оценки быстро снижаются. На основе постквантовых стандартов NIST, сроков перехода и анализа стандарта подписи O'zMSt 286:2024 даны рекомендации для Узбекистана.

Ключевые слова: RSA; Диффи–Хеллман; криптография на эллиптических кривых; алгоритм Шора; алгоритм Гровера; квантовый компьютер; постквантовая криптография; ML-KEM; ML-DSA; O'zMSt 286:2024.

Kirish

Ochiq kalitli (asimmetrik) kriptografiya kalit kelishuvi, kalitni shifrlab uzatish va elektron raqamli imzo orqali TLS (Transport Layer Security – transport qatlam xavfsizligi), ochiq kalitlar infratuzilmasi va dasturiy ta'minotni yangilash tizimlarining asosini tashkil etadi. Amalda uchta oila ishlatiladi: DH (Diffie–Hellman – Diffi–Xellman) kalit kelishuvi [1], RSA (Rivest–Shamir–Adleman – RSA ochiq kalitli kriptotizimi) [2] va ECC (Elliptic Curve Cryptography – elliptik egri chiziqli kriptografiya) [3, 4]. Ularning barchasi klassik kompyuterda yechilishi qiyin bo'lgan sonlar nazariyasi masalalariga tayanadi. 1994-yilda P.Shor bu masalalar kvant kompyuterida polinomial vaqtda yechilishini ko'rsatdi [5]. Xavf kelajakdagi bo'lsada, u bugungi ma'lumotlarga ham taalluqli: hujumchi shifrlangan trafikni hozir yozib olib, kvant kompyuter paydo bo'lgach ochishi mumkin («harvest now, decrypt later» – «hozir yig', keyin och»). M.Mosca bu holatni quyidagi tengsizlik bilan ifodalagan [6]:

$$x + y > z, \qquad (1)$$

bu yerda, x – ma'lumot maxfiy qolishi kerak bo'lgan muddat, y – yangi kriptografiyaga o'tish muddati, z – kriptografik ahamiyatli kvant kompyuter paydo bo'lguncha qolgan vaqt. Tengsizlik bajarilsa, ma'lumot himoyasiz qoladi. Tezisning maqsadi – klassik asimmetrik kriptosistemalarning kvant hujumlariga zaifligini so'nggi resurs baholari asosida baholash va O'zbekiston uchun xulosalar chiqarish.

Klassik asimmetrik kriptosistemalarning matematik asoslari

RSA da N = pq (p, q – katta tub sonlar), ochiq kalit (N, e), yopiq kalit d [2]:

$$c = m^e \bmod N,\ \ m = c^d \bmod N,\ \ ed \equiv 1 \pmod{\varphi(N)}. \quad (2)$$

RSA ning xavfsizligi butun sonlarni faktorlash masalasiga tayanadi: N ni ko‘paytuvchilarga ajratgan hujumchi d ni hisoblaydi. DH da tomonlar tartibi q bo‘lgan g generatorli guruhda tasodifiy a va b ni tanlab, umumiy sirni hisoblaydi [1]:

$$A = g^a,\ B = g^b,\ K = B^a = A^b = g^{ab}. \quad (3)$$

Uning xavfsizligi diskret logarifmlash masalasiga (g^a dan a ni topish) va Diffi–Xellman masalasiga tayanadi. ECC da guruh sifatida chekli maydon ustidagi elliptik egri chiziq nuqtalari olinadi: ochiq kalit Q = dP, bu yerda P – n tartibli bazaviy nuqta, d – yopiq kalit. ECDH (Elliptic Curve Diffie–Hellman – elliptik egri chiziqli Diffi–Xellman) va ECDSA (Elliptic Curve Digital Signature Algorithm – elliptik egri chiziqli raqamli imzo algoritmi) ning xavfsizligi ECDLP (Elliptic Curve Discrete Logarithm Problem – elliptik egri chiziqda diskret logarifmlash masalasi), ya’ni Q dan d ni topish murakkabligiga asoslanadi [3, 4].

Klassik hujumlar bo‘yicha faktorlash va chekli maydonda diskret logarifmlash uchun subeksponensial murakkablikdagi son maydoni g‘alviri ma’lum, ECDLP uchun esa umumiy holda faqat $O(\sqrt{n})$ murakkablikdagi Pollard ro turidagi usullar mavjud. Shu sababli ECC qisqa kalitlar bilan bir xil darajaga erishadi: 128 bitli xavfsizlik uchun RSA va DH da 3072 bitli modul, ECC da esa 256 bitli kalit talab etiladi; RSA-2048 taxminan 112 bitli darajaga mos keladi [7].

Shor va Grover algoritmlari

Shor algoritmi faktorlash va diskret logarifmlashni davrni topish masalasiga keltiradi va davrni kvant Furye almashtirishi yordamida topadi [5]. Faktorlashda tasodifiy a (gcd(a, N) = 1) uchun $f(x) = a^x \bmod N$ funksiyasining davri r topiladi; r juft va $a^{r/2} \not\equiv -1 \pmod N$ bo‘lsa, N ning ko‘paytuvchisi quyidagicha olinadi:

$$p = \gcd(a^{r/2} - 1, N). \quad (4)$$

Diskret logarifmlashda $h = g^a$ uchun $f(x, y) = g^x h^{-y}$ funksiyasining ikki o‘lchovli davri a ni beradi. Usul ixtiyoriy chekli abel guruhida ishlaydi, shu jumladan elliptik egri chiziq nuqtalari guruhida [5]. Algoritmning murakkabligi kalit uzunligi bo‘yicha polinomial, shuning uchun kalitni uzaytirish himoya bermaydi: RSA, DH, ECDH, ECDSA va EdDSA kriptografik ahamiyatli kvant kompyuterga qarshi bardoshsiz bo‘lib qoladi.

Grover algoritmi saralanmagan to‘plamda qidiruvni N tadan $\sqrt{N}$ ta murojaatgacha tezlashtiradi [8]. Bu simmetrik shifrlar va xesh funksiyalarni buzmaydi, balki ularning samarali xavfsizlik darajasini taxminan ikki barobar pasaytiradi; bunga kalit va chiqish uzunligini oshirish orqali javob beriladi. Demak, kvant xavfi asimmetrik va simmetrik kriptografiya uchun sifat jihatidan farq qiladi.

Kvant hujumlari uchun resurs baholari

Kvant xavfini real baholash uchun mantiqiy kubitlar, Toffoli amallari soni va xatoga bardoshli kodlash (odatda sirt kodi) bilan fizik kubitlar soni hisoblanadi. 1-jadvalda so‘nggi baholar keltirilgan.

1-jadval

RSA-2048 va 256 bitli ECDLPni Shor algoritmi bilan yechish uchun resurs baholari

Masala, manba	Mantiqiy kubitlar	Toffoli amallari	Fizik kubitlar	Vaqt
RSA-2048 [9]	–	–	≈ 20 mln	≈ 8 soat
RSA-2048 [10]	–	–	< 1 mln	< 1 hafta
ECDLP-256 [11]	2330	$\approx 1{,}26 \cdot 10^{11}$	–	–
ECDLP-256 [12]	≈ 1193	$\approx 2^{39}$ (22 urinish)	–	–
ECDLP-256 [13]	< 1200 yoki < 1450	$< 9 \cdot 10^7$ yoki < $7 \cdot 10^7$	< 0,5 mln	daqiqalar

Izoh: fizik baholar 10^{-3} fizik xatolik darajasi va qo‘shni ulanishli kvadrat panjara farazlariga asoslangan; «–» – manbada son keltirilmagan. Preprintlar retsenziyadan o‘tmagan bo‘lishi mumkin.

Jadvaldan uchta xulosa kelib chiqadi. Birinchidan, RSA-2048 uchun fizik kubitlar bahosi 2021–2025-yillarda taxminan 20 barobar kamaydi [9, 10]; ECDLP-256 uchun mantiqiy kubitlar 2017-yildagi 2330 dan 2026-yilda 1200 ga yaqinlashdi [11, 12, 13]. Ikkinchidan, klassik jihatdan kuchliroq ECC-256 (128 bit) kvant hujumi uchun RSA-2048 (112 bit) dan kamroq resurs talab qiladi, chunki Shor algoritmining narxi guruh elementining bit uzunligiga (256 ga qarshi 2048) bog‘liq. Demak, ECC asosidagi kalit kelishuvi va imzolar birinchi navbatda xavf ostida. Uchinchidan, bu baholar hali qurilmagan xatoga bardoshli kvant kompyuterlar uchun: ular hujum bugun amalga oshirilishini anglatmaydi, ammo Mosca tengsizligidagi z ning kamayib borayotganini ko‘rsatadi.

Postkvant kriptografiyaga o‘tish va O‘zbekiston uchun oqibatlar

Kvant xavfiga javob – PQC (Post-Quantum Cryptography – postkvant kriptografiya), ya’ni kvant hujumlariga bardoshli deb hisoblanadigan klassik algoritmlarga o‘tish. NIST (National Institute of Standards and Technology – AQSh Milliy standartlar va texnologiyalar instituti) 2024-yilda FIPS (Federal Information Processing Standards – federal axborotni qayta ishlash standartlari) 203 da ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism – modul panjaralarga asoslangan kalitni inkapsulyatsiyalash mexanizmi) [14], FIPS 204 da ML-DSA (Module-Lattice-Based Digital Signature Algorithm – modul panjaralarga asoslangan raqamli imzo algoritmi) [15] va FIPS 205 da SLH-DSA (Stateless Hash-Based Digital Signature Algorithm – holatsiz xeshga asoslangan raqamli imzo algoritmi) [16] standartlarini qabul qildi; 2025-yilda zaxira kalit inkapsulyatsiyasi mexanizmi sifatida HQC tanlandi [17]. 2026-yil oktyabrida yakuniy shaklda e’lon qilingan NIST IR 8547 ga ko‘ra RSA, ECDSA, EdDSA, DH va ECDH 2030-yildan keyin eskirgan (deprecated), 2035-yildan keyin esa taqiqlangan (disallowed) deb belgilangan [18]. IETF (Internet Engineering Task Force – Internet muhandisligi ishchi guruhi) 2026-yilda RFC (Request for Comments – sharhlar uchun so‘rov) 10024 da TLS 1.3 uchun X25519MLKEM768 kabi gibrid guruhlarni Proposed Standard sifatida belgiladi [19]: bunda umumiy sir klassik ECDH va ML-KEM natijalaridan olinadi va ulardan kamida bittasi buzilmagan bo‘lsa, himoya saqlanadi.

O‘zbekiston uchun muhim natija: milliy elektron raqamli imzo standarti O‘zMSt 286:2024 ning ikkala algoritmi ham diskret logarifmlash turidagi masalaga tayanadi. 2-algoritmning bardoshliligi standartda bevosita elliptik egri chiziq nuqtalari guruhida diskret logarifmlash murakkabligi bilan asoslangan, 1-algoritm esa p modul bo‘yicha, tartibi 256 bitli q bo‘lgan parametrli guruhda darajaga ko‘tarishdan foydalanadi [20]. 2-algoritm Shor algoritmiga qarshi bardoshsiz; 1-algoritm R parametri ochiq bo‘lgan holatda abel guruhidagi diskret logarifmlashga keladi deb hisoblash uchun asos bor, R maxfiy bo‘lgan rejim esa alohida kvant tahlilni talab qiladi. Simmetrik standartlar (256 bitli kalitli shifrlash va 256 bitli xesh) Grover algoritmi ta’sirida bo‘lsa-da, nisbatan bardoshli qoladi. Milliy postkvant standarti va milliy kalit kelishuvi standarti hozircha mavjud emas.

Xulosa

RSA, DH va ECC ning xavfsizligi faktorlash va diskret logarifmlash masalalariga tayanadi; Shor algoritmi bu masalalarni polinomial vaqtda yechgani sababli kalit uzunligini oshirish ularni kvant hujumidan himoya qilmaydi. Grover algoritmi esa simmetrik kriptografiya darajasini faqat pasaytiradi.

So‘nggi baholarga ko‘ra RSA-2048 uchun million fizik kubitdan kam, ECDLP-256 uchun 1200 ga yaqin mantiqiy va yarim milliondan kam fizik kubit talab etiladi; ECC kvant hujumiga RSA dan oldin duchor bo‘ladi va baholar yildan yilga kamaymoqda.

«Hozir yig‘, keyin och» xavfi tufayli uzoq muddat maxfiy qolishi kerak bo‘lgan ma’lumotlar uchun o‘tish hozirdan boshlanishi kerak; NIST bo‘yicha klassik asimmetrik algoritmlar 2030-yildan keyin eskirgan, 2035-yildan keyin taqiqlangan hisoblanadi.

O‘zMSt 286:2024 dagi imzo algoritmlari kvant hujumiga nisbatan zaif yoki tahlil talab qiladi. O‘zbekiston uchun quyidagilar tavsiya etiladi: asimmetrik kriptografiya qo‘llanadigan

tizimlarni inventarizatsiya qilish; kriptografik moslashuvchanlikni (algoritmni almashtirish imkoniyatini) ta’minlash; TLS da gibrid kalit kelishuvini (RFC 10024) joriy etish; NIST FIPS 203–205 asosida milliy postkvant kalit kelishuvi va imzo standartlarini ishlab chiqish bo‘yicha tadqiqotlarni boshlash.

Foydalanilgan adabiyotlar

1. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22, No. 6. P. 644–654.
2. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. 1978. Vol. 21, No. 2. P. 120–126.
3. Miller V. Use of Elliptic Curves in Cryptography // Advances in Cryptology – CRYPTO ’85. LNCS 218. Springer, 1986. P. 417–426.
4. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation. 1987. Vol. 48, No. 177. P. 203–209.
5. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. Vol. 26, No. 5. P. 1484–1509.
6. Mosca M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? // IEEE Security & Privacy. 2018. Vol. 16, No. 5. P. 38–41.
7. Barker E. Recommendation for Key Management: Part 1 – General. NIST SP 800-57 Part 1 Rev. 5. 2020.
8. Grover L. A Fast Quantum Mechanical Algorithm for Database Search // Proc. 28th ACM Symposium on Theory of Computing (STOC). 1996. P. 212–219.
9. Gidney C., Ekerå M. How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits // Quantum. 2021. Vol. 5. Art. 433.
10. Gidney C. How to Factor 2048 Bit RSA Integers with Less than a Million Noisy Qubits. arXiv:2505.15917 (preprint). 2025.
11. Roetteler M., Naehrig M., Svore K., Lauter K. Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms // Advances in Cryptology – ASIACRYPT 2017. LNCS 10625. Springer, 2017. P. 241–270.
12. Chevignard C., Fouque P.-A., Schrottenloher A. Reducing the Number of Qubits in Quantum Discrete Logarithms on Elliptic Curves // EUROCRYPT 2026; IACR ePrint 2026/280.
13. Babbush R., Zalcman A., Gidney C. et al. Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. arXiv:2603.28846 (preprint). 2026.
14. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.
15. NIST FIPS 204. Module-Lattice-Based Digital Signature Standard. 2024.
16. NIST FIPS 205. Stateless Hash-Based Digital Signature Standard. 2024.
17. Alagic G. et al. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545. 2025.
18. Moody D., Perlner R., Regenscheid A., Robinson A., Cooper D. Transition to Post-Quantum Cryptography Standards. NIST IR 8547 (final). 2026. DOI: 10.6028/NIST.IR.8547.
19. Kwiatkowski K., Kampanakis P., Westerbaan B., Stebila D. Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3. RFC 10024 (Proposed Standard). IETF, 2026.
20. O‘zMSt 286:2024. Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari. Toshkent, 2024.

АЛГЕБРАИЧЕСКАЯ ДИАГНОСТИКА БИТОВЫХ ИСКАЖЕНИЙ СИМВОЛЬНОЙ ИНФОРМАЦИИ В ПОЛЕ GF(31)

Байпакбаева С.Т.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Аннотация. Рассматривается применение спектрального преобразования в конечном поле GF(31) для алгебраической диагностики битовых искажений в бинарных представлениях символьной информации. Исходный 30-битный вектор преобразуется в спектральный код над GF(31). Для тестового алфавита цифр 0–9 ранее сформирована 30-битная кодовая книга с минимальным расстоянием Хэмминга d_min=9, что обеспечивает радиус гарантированного ближайшего распознавания до четырёх битовых ошибок. Показано, что при одиночном искажении спектральная разность имеет регулярную алгебраическую структуру, позволяющую локализовать позицию ошибочного бита. Полное спектральное представление не рассматривается как средство повышения криптографической стойкости и не заменяет механизмы аутентификации; его назначение состоит в формировании алгебраического представления данных и диагностике ошибок как дополнительного элемента контроля целостности.

Ключевые слова: GF(31), конечное поле, спектральное преобразование, символьная информация, битовые ошибки, контроль целостности, кодовое расстояние.

Annotatsiya. Ushbu maqolada GF(31) chekli maydonida spektral o‘zgartirishni ramziy ma’lumotlarning ikkilik tasvirlarida bit xatolarining algebraik diagnostikasi uchun qo‘llash ko‘rib chiqiladi. Asl 30-bitli vektor GF(31) ustidan spektral kodga aylantiriladi. 0–9 raqamlaridan iborat sinov alifbosi uchun avval d_min=9 minimal Hamming masofasiga ega 30-bitli kod kitobi shakllantirilgan bo‘lib, bu to‘rt bitgacha bo‘lgan xatolarni eng yaqin aniqlash radiusini kafolatlaydi. Bitta buzilish uchun spektral farq muntazam algebraik tuzilishga ega ekanligi ko‘rsatilgan, bu esa xato bitning o‘rnini lokalizatsiya qilishga imkon beradi. To‘liq spektral tasvir kriptografik xavfsizlikni oshirish vositasi deb hisoblanmaydi va autentifikatsiya mexanizmlarini almashtirmaydi; uning maqsadi ma’lumotlarning algebraik tasvirini shakllantirish va yaxlitlikni boshqarishning qo‘shimcha elementi sifatida xatolarni tashxislashdir.

Kalit so‘zlar: GF(31), chekli maydon, spektral o‘zgartirish, ramziy ma’lumot, bit xatolari, yaxlitlikni boshqarish, kod masofasi.

После стабилизации и бинаризации сигналов устройства ввода символ представляется бинарным вектором $U=(U_0,\ldots,U_{29})$, где $U_i \in \{0,1\}$. Прямое сравнение такого вектора с эталонной кодовой книгой может выполняться по расстоянию Хэмминга. Дополнительное спектральное представление над конечным полем позволяет перенести задачу диагностики отдельных искажений в алгебраическую форму. Выбор GF(31) естественен для 30-компонентной последовательности, поскольку мультипликативная группа ненулевых элементов поля содержит 30 элементов.

$$Z_k = \Sigma_{i=0}^{29} U_i \, \theta^{ik} \bmod 31, \quad k=0,\ldots,29 \quad (1)$$

Здесь θ - примитивный элемент поля GF(31), а Z_k - спектральные компоненты. Преобразование (1) задаёт полное алгебраическое представление входного бинарного вектора. В используемой тестовой кодовой книге для цифр 0–9 минимальное попарное

расстояние Хэмминга составляет d_min=9. Следовательно, для ближайшего распознавания гарантированный радиус исправления определяется стандартным соотношением

$$t = \lfloor (d_{min} - 1)/2 \rfloor = 4 \quad (2)$$

Алгебраическая диагностика одиночной ошибки

Рассмотрим одиночное битовое искажение в позиции r. Если его алгебраическая величина обозначена e_r, то разность между спектром искажённого и эталонного кодов имеет вид

$$\Delta Z_k = e_r \, \theta^{rk} \quad (3)$$

При k=0 получаем $\Delta Z_0 = e_r$. Для ненулевой ошибки отношение первой спектральной компоненты к нулевой устраняет неизвестную амплитуду ошибки:

$$\Delta Z_1 \cdot (\Delta Z_0)^{-1} = \theta^r \quad (4)$$

Отсюда позиция искажения определяется дискретным логарифмом относительно примитивного элемента:

$$r = \log_\theta [\Delta Z_1 \cdot (\Delta Z_0)^{-1}] \quad (5)$$

Таким образом, одиночная ошибка не только обнаруживается как несоответствие эталонному спектру, но и получает алгебраически интерпретируемую позицию. Для двоичного представления направление инверсии определяется сравнением исходного и принятого битов. Такой механизм удобен для диагностики сбоев в каналах формирования символьного кода и может использоваться совместно с обычным Хэмминг-сопоставлением.

Результаты и обсуждение

Для тестового алфавита из десяти цифр использована 30-битная кодовая книга с d_min=9. Это означает, что при не более чем четырёх битовых искажениях ближайший эталон остаётся однозначно определяемым в рамках принятой кодовой книги. Спектральное преобразование GF(31) не изменяет это кодовое расстояние и само по себе не повышает точность ближайшего распознавания: при использовании полного обратимого спектра решение эквивалентно решению в исходном бинарном пространстве. Его дополнительная ценность состоит в алгебраической структуре спектральной разности, которая позволяет диагностировать одиночные искажения и может служить основой для дальнейшего построения специализированных процедур контроля.

Таблица 1

Параметры и значения

Параметр	Значение / интерпретация
Поле	GF(31)
Длина бинарного представления	30 бит
Тестовый алфавит	цифры 0–9
Минимальное кодовое расстояние	d_min = 9
Гарантированный радиус ближайшего распознавания	t = 4 битовых ошибки
Одиночная ошибка	алгебраическая локализация позиции по спектральной разности

Следует отдельно отметить границы интерпретации результата. Использование конечного поля и спектрального кода не является шифрованием, цифровой подписью или криптографическим тегом аутентификации. Поэтому предложенный подход не должен описываться как самостоятельная защита от преднамеренной модификации данных. В

контексте криптологических систем он может рассматриваться как предварительный или сопутствующий алгебраический уровень контроля целостности и диагностики случайных либо аппаратных искажений.

Заключение

Предложено использовать спектральное представление бинарного кода в GF(31) для алгебраической диагностики искажений символьной информации. Для 30-битной кодовой книги тестового алфавита с d_min=9 гарантированный радиус ближайшего распознавания составляет четыре ошибки. Для одиночного искажения выведена зависимость, позволяющая определить позицию ошибочного бита по отношению спектральных разностей. Подход не заменяет криптографические механизмы аутентификации, но может использоваться как дополнительный уровень диагностики и контроля корректности символьных данных в цифровых устройствах и терминалах.

Литература

1. Байпакбаева С.Т. Алгоритм спектрального кодирования и распознавания символьной информации в GF(31) с диагностикой битовых ошибок // «Raqamli iqtisodiyot» ilmiy-elektron jurnali. 2026. № 16.

2. Kadyrzhan K., Kaldybekov D., Baipakbaeva S., Vitulyova Y., Matrassulova D., Suleimenov I. Electronic Fourier–Galois Spectrum Analyzer for the Field GF(31) // Applied Sciences. 2024. Vol. 14, No. 17. Article 7770. DOI: 10.3390/app14177770.

3. Suleimenov I.E., Vitulyova Y.S., Kabdushev S.B., Bakirov A.S. Improving the efficiency of using multivalued logic tools: application of algebraic rings // Scientific Reports. 2023. Vol. 13. Article 22021. DOI: 10.1038/s41598-023-49593-1.

TLS PROTOKOLINING ISHLASH PRINSIPI VA XABARLAR ALMASHINUVI JARAYONI

Tursunov O.O., Olimov I.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada Internet orqali uzatiladigan ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlovchi TLS (Transport Layer Security) protokolining ishlash prinsipi hamda tomonlar o‘rtasidagi xabarlar almashinuvi jarayoni tahlil qilinadi. Protokolning ikki asosiy qatlami: ma’lumotlarni himoyalangan holda uzatuvchi Record protokoli va sessiya parametrlarini kelishish hamda kalitlarni o‘rnatish uchun mas’ul Handshake protokoli ko‘rib chiqiladi. Shuningdek, TLS 1.2 va TLS 1.3 versiyalari taqqoslanib, ikkinchi versiyada handshake jarayonining qisqartirilgani (1-RTT va 0-RTT rejimlari), eskirgan va zaif kriptografik algoritmlarning chiqarib tashlangani hamda to‘g‘ridan-to‘g‘ri ilg‘or maxfiylik (forward secrecy) xususiyatining majburiy qilingani ko‘rsatiladi.

Kalit so‘zlar: TLS, handshake, Record protokoli, sertifikat, ochiq kalit infratuzilmasi (PKI), Diffie–Hellman, sessiya kaliti, ilg‘or maxfiylik, kriptografik himoya.

Аннотация: В данной статье анализируется принцип работы протокола TLS (Transport Layer Security), обеспечивающего конфиденциальность, целостность и аутентификацию данных, передаваемых через Интернет, а также процесс обмена сообщениями между сторонами. Рассматриваются два основных уровня протокола: протокол записи (Record), обеспечивающий безопасную передачу данных, и протокол подтверждения (Handshake), отвечающий за согласование параметров сессии и установление ключей. Также проводится сравнение версий TLS 1.2 и TLS 1.3, и показано, что во второй версии процесс подтверждения сокращается (режимы 1-RTT и 0-RTT), исключаются устаревшие и слабые криптографические алгоритмы, а функция прямой секретности становится обязательной.

Ключевые слова: TLS, подтверждение, протокол записи, сертификат, инфраструктура открытых ключей (PKI), Диффи-Хеллман, сессионный ключ, прямая секретность, криптографическая защита.

Kirish

TLS protokoli oldingi paragrafda takidlab o‘tilgandek Record Protokolni inkapsulyatsiya qiluvchi 4 ta Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol, Application Data Protocollardan iborat.

Record Protocol - TLS orqali uzatiladigan ma’lumotlarni recordlarga bo‘lish, ularni himoyalash va TCP orqali uzatishga tayyorlash uchun xizmat qiladi.

Handshake Protocol - TLS ulanishini o‘rnatish va tomonlarning xavfsiz aloqa uchun zarur bo‘lgan kriptografik parametrlarini kelishish protokoli.

Change Cipher Spec Protocol - keyingi xabarlar yangi kelishilgan kriptografik parameterlar bilan himoyalanishini bildiradi, TLS 1.3 ChangeCipherSpecni deyarli protokolning faol qismi sifatida ishlatmaydi, shifrlash algoritmi va kalitlar Handshake Protocol va Key Schedule orqali aniqlanadi.

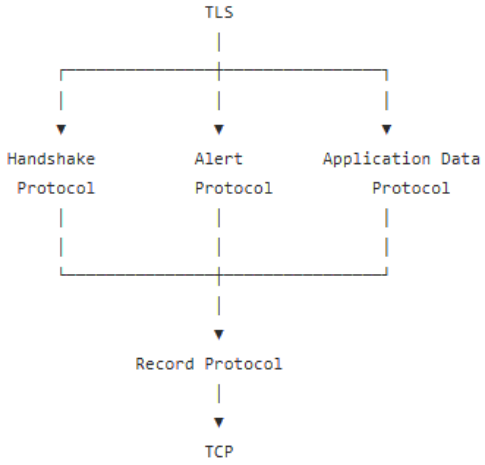
Alert Protocol - TLSdagi xatolar, xavfsizlik muammolari va ulanishning tugashi haqida ikkinchi tomonni xabardor qilish uchun ishlatiladi.

Application data Protocol - TLS orqali foydalanuvchi ilovalarining haqiqiy ma’lumotlarini xavfsiz uzatish uchun xizmat qiladi. Ilova yuborgan ma’lumotlarni TLS orqali ikkinchi tomonga yetkazish, ma’lumotlar shifrlash, ma’lumot o‘zgartirilgan bo‘lsa aniqlash, autentifikatsiyalangan himoyani ta’minlash kabi vazifalarni bajarib beradi.

TLSdan oldin odatda TCP aloqa o‘rnatiladi. TCP - transport aloqasini ta’minlaydi. TLS esa shu aloqa ustida maxfiylik, yaxlitlik va autentifikatsiyani ta’minlaydi.

1-rasmda keltirilgandek TLS da dastlab xavfsiz aloqa parametrlarini kelishib olish uchun Handshake Protocolidan foydalaniladi. Hanshake protocolining tarkibida Change Cipher Spec Protocol xavfsiz aloqa o ‘rnatilganligini bildiruvchi qiymat sifatida ishlatiladi. Handshake Protocoli o‘z ishini tugatgandan so‘ng Application data protocol orqali ilova ma’lumotlari xavfsiz yuboriladi.

Alert Protocol esa aloqa o‘rnatishda xatoliklar yuzaga kelganda yoki aloqa uzulayotganda ikkinchi tomonni xabardor qilish uchun ishlatiladi. Record Protocol yuqoridagi protocollarni inkapsultsiga qilgan holda TCP protocoliga yuboradi.

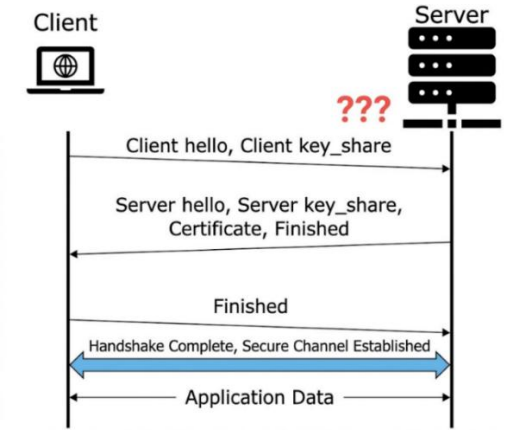


1-rasm. TLS quyi protokollarining umumiy ishlash ketma-ketligi

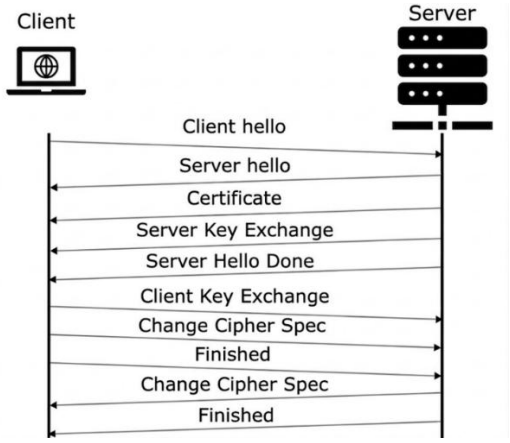
Asosiy qism

Handshake Protocol

TLS protokoli himoyalangan aloqani o‘rnatish uchun dastlab Handshake protokolidan foydalandi. TLS 1.3 versiyasi tezliklikni oshirish va resurslar sarfini kamaytirish maqsadida Handshake protokolini 3 ta so‘rovda amalga oshiridi. Bu so‘rovlar Client Hello, Server Hello va Finished so‘rovlaridir. Undan so‘ng barcha xabarlar maxfiy holda almashinishi mumkin (1-rasm). Har bir so ‘rov tarkibidagi barcha kengaytma (parameter, extensions) adabiyotlar ro‘yxatida ko‘rib o‘tilgan.



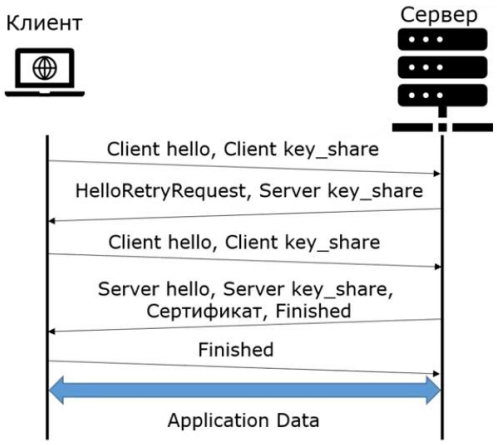
2-rasm. TLS 1.3 Handshake jarayoni



3-rasm. TLS 1.2 Handshake jarayoni

TLS 1.2 protoklidan farqli ravishda TLS 1.3 da **DHE/ECDHE uchun kerakli** key_share **m**a'**lumotlari** ClientHello **va** ServerHello **tarkibida b**o'**ladi.** Shuning uchun TLS 1.2 dagi alohida ServerKeyExchange va ServerHelloDone xabarlari TLS 1.3 da kerak emas.

Agar ClientHello so'rovchining tarkibida yuborilgan key_share parametrlar mos kelmasa, yoki mijoz supported_groups orqali ma'lum guruhlarni qo'llab-quvvatlashini bildirsa, lekin kerakli guruh uchun key_share yubormagan bo'lsa kabi holatlarda HelloRetryRequest(HRR) so'rovini server yuboradi. HelloRetryRequest server tomonidan ClientHello so'rovi qabul qilingandan keyin, server handshakeni davom ettira olishi uchun mijozdan ClientHelloni qayta yuborishini talab qilish kerak bo'lgan holatda yuboriladi. (4-rasm). HelloRetryRequest so'rovi aloqani davom ettrish mumkin vaqtlarda qo'llaniladi. Agar aloqani davom ettirish uchun kerakli parametrlar topilmasa Alert Protocol ishlaydi. Alert protocolda ma'lumot almashinish davom etmaydi, aloqa uzuladi.

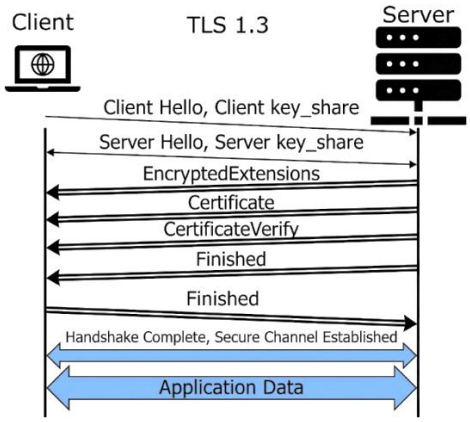


4-rasm. HelloRetryRequest so'rovi ishlatilishi ketma-ketligi

Sertifikat almashinuvi jarayoni

TLS 1.3 da sertifikat almashinuvi asosan serverning o'zini mijozga autentifikatsiya qilish uchun amalga oshiriladi. Bu jarayon ServerHello so'rovi tarkibidagi Certificate va CertificateVerify xabarlari orqali bajariladi. Certificate xabari bu serverning ochiq kaliti va CA tomonidan tasdiqlangan identifikatsiyasini bildiradi, CertificateVerify xabari esa server sertifikatiga mos private key egasi ekanligini kriptografik isbotlash vazifasini bajaradi. ServerHello, EncryptedExtensions, Certificate, CertificateVerify, Finished kabi xabarlar bitta so'rovmi deb aytish texnik jihatdan to'g'ri emas. To'g'ri ifoda ular alohida TLS Handshake xabarlari, lekin bir yoki bir nechta TLS Record tarkibida uzatilishi mumkin. ServerHellogacha

bo‘lgan asosiy handshake xabarlari ochiq ko‘rinishda bo‘ladi, ServerHellodan keyin esa handshake uchun kalitlar hosil qilingan bo‘ladi va shifrlangan holda uzatiladi (5-rasm).



5-rasm. Ikki chiziq bilan yuborilgan xabarlar shifrlangan holda

Server o‘zining X.509 sertifikatini yuboradi. Sertifikat odatda quyidagilarni o‘z ichiga oladi:

- serverning domen nomi;
- serverning ochiq kaliti (public key);
- sertifikatning amal qilish muddati;
- sertifikatni bergan CA ma’lumotlari;
- raqamli imzo;
- boshqa sertifikat kengaytmalari.

Agar serverda sertifikat zanjiri bo‘lsa, Certificate xabarida server sertifikati bilan birga intermediate CA sertifikatlari ham yuborilishi mumkin.

Mijoz server yuborgan sertifikatni tekshiradi. Masalan, foydalanuvchi https://example.com ga ulansa, server sertifikatidagi domen nomi example.com bilan mos kelishi kerak.

Mijoz serverga ClientHello so‘rovi tarkibida qo‘llab-quvvatlaydigan TLS parametrlari, key_share, signature_algorithms kabi boshqa kengaytmalarni (extensionlarni) yuboradi.

Server parametrlarni tanlab, ServerHello yuboradi. Shu bosqichda DHE/ECDHE ishlatilishi belgilangan, uning natijasida ikkala tomon umumiy shared secret hosil qilish uchun zarur ma’lumotlarga ega bo‘ladi. Undan so‘ng Server o‘zining sertifikatini yuboradi. Sertifikatni ishonchli tomon Certificate Authority (CA) imzolagan bo‘ladi.

Mijoz CA imzosini tekshirish (agar CA zanjiri mavjud bo‘lsa ularni tekshirish), amal qilish muddati, domen nomi kabi bir nechta tekshiruvlarni amalga oshiradi. Masalan, foydalanuvchi https://example.com saytiga ulanayotgan bo‘lsa, sertifikat example.com uchun amal qilishi kerak. Agar sertifikat noto‘g‘ri bo‘lsa, TLS autentifikatsiyasi muvaffaqiyatsiz bo‘ladi va ulanish to‘xtatilishi mumkin.

Faqat Server sertifikat yuborishining o‘zi yetarli emas. Server o‘zining private keyiga ega ekanligini isbotlashi kerak. Buning uchun server CertificateVerify xabarini yuboradi. Uning tarkibida Server handshake davomida yig‘ilgan ma’lumotlardan transcript hosil qilib va unga o‘zining private keyi bilan raqamli imzo qo‘ygan qiymat mavjud. Mijoz sertifikatdagi public keydan foydalanib CertificateVerifyni tekshiradi. Agar imzo to‘g‘ri bo‘lsa, Server ushbu sertifikatga mos private keyni haqiqatan ham egallab turibdi. Bu server autentifikatsiyasining eng muhim kriptografik qismidir.

Finished xabari handshake transcriptining yaxlitligini tasdiqlash va handshake davomida hosil qilingan kalitlarni tasdiqlashda ishlatiladi.

Kalit almashinuvi mexanizmi

TLS 1.3 da “kalit” deganda bitta kalit emas, balki Key Schedule orqali ketma-ket hosil qilinadigan bir nechta maxfiy qiymatlar va trafik kalitlari tushuniladi. Quyidagi jadvalda barcha kalitlar ro‘yxati keltirilgan.

1-jadval.

TLS 1.3 da foydalaniladigan maxfiy parametrlar ro‘yxati

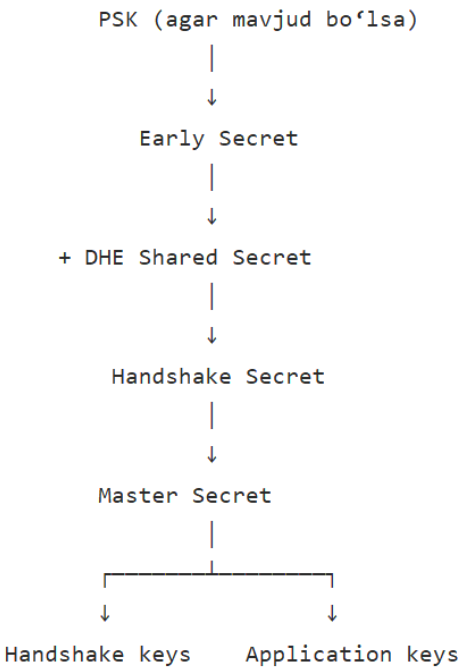
Kalit / Secret	Vazifasi
PSK (Pre-Shared Key)	Oldindan mavjud bo‘lgan umumiy maxfiy kalit. Resumption yoki oldindan sozlangan PSK uchun ishlatiladi.
Early Secret	PSK asosida Key Schedule'ning birinchi bosqichida hosil qilinadi. 0-RTT va keyingi kalitlarni hosil qilish uchun asos bo‘ladi.
DHE Shared Secret	Client va Server key_share orqali DHE/ECDHE yordamida mustaqil hosil qiladigan umumiy maxfiy qiymat. Tarmoq orqali yuborilmaydi.
Handshake Secret	DHE Shared Secret va oldingi secret asosida hosil qilinadi. Handshake ma’lumotlarini himoyalash uchun keyingi traffic secretlarining asosidir.
Client Handshake Traffic Secret	Serverdan clientga va clientdan serverga yuboriladigan handshake ma’lumotlarini himoyalash uchun client tomonida ishlatiladigan secret.
Server Handshake Traffic Secret	Server yuboradigan handshake ma’lumotlarini himoyalash uchun ishlatiladigan secret.
Master Secret	Handshake bosqichidan keyin hosil qilinadi va application traffic secretlarini hosil qilish uchun asos bo‘ladi.
Client Application Traffic Secret	Client yuboradigan Application Datani shifrlash/autentifikatsiya qilish uchun ishlatiladi.
Server Application Traffic Secret	Server yuboradigan Application Datani shifrlash/autentifikatsiya qilish uchun ishlatiladi.
Exporter Master Secret	TLS ulanishidan tashqaridagi boshqa protokollar yoki ilovalar uchun kalit materialini hosil qilishda ishlatiladi.
Resumption Master Secret	Keyingi TLS ulanishlarida resumption uchun PSK hosil qilishga asos bo‘ladi.
Client Early Traffic Secret	0-RTT rejimida client yuboradigan early application data’ni himoyalash uchun ishlatiladi.

TLS 1.3 da kalit kelishuvi (key agreement) mexanizmining asosiy maqsadi - client va server o‘rtasida umumiy maxfiy kalit materialini hosil qilish, lekin bu maxfiy qiymatni tarmoq orqali yubormaslik. TLS 1.3 da odatda (EC)DHE, masalan X25519 yoki secp256r1, ishlatiladi.

Mijoz kalit juftligini yaratadi va ClientHello ichida public keyni key_share sifatida yuboradi. Private key tarmoqqa yuborilmaydi.

Server ham yangi private/public key juftligini yaratadi. Server o‘z public keyini ServerHello ichidagi key_share orqali yuboradi.

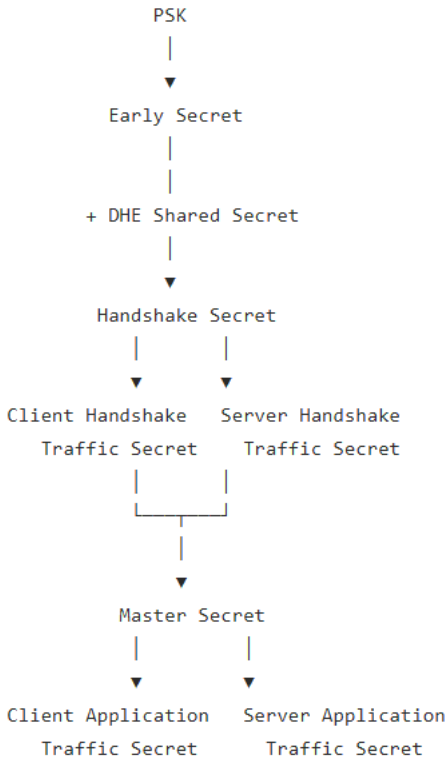
Ikkala tomon umumiy secretni (EC)DHE asosida hosil qiladi. Bu Shared_Secret deb ataladi. Hosil qilingan shared secret bevosita HTTP ma’lumotlarini shifrlash uchun ishlatilmaydi. U TLS 1.3 Key Schedule orqali HKDF yordamida keyingi kalitlarni hosil qilishda ishlatiladi.



6-rasm. Kalitlarni hosil qilish

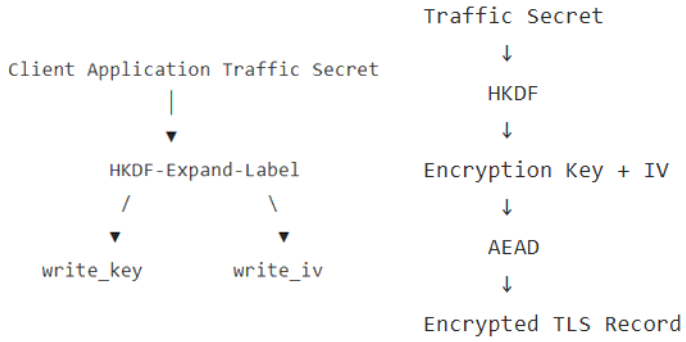
Agar oddiy TLS 1.3 DHE handshake bo‘lsa, PSK bo‘lmasligi ham mumkin. PSK (Pre-Shared Key) asosan ikki holatda ishlatiladi. Oldingi TLS ulanishini qayta tiklashda (Resumption) va oldindan sozlangan PSK (External PSK) holatlarda. Bu ikki holat adabiyotlar ro‘yxatida tushuntirladi.

Agar faqat Diffie-Hellman kalit kelishuvi ishlatilsa, hujumchi o‘rtaga kirib Man-in-the-Middle (MITM) hujumini amalga oshirishi mumkin. Shuning uchun TLS 1.3 Server Certificate va CertificateVerify orqali o‘zini autentifikatsiya qiladi.



7-rasm. Key Schedule zanjiri

TLS 1.3 terminologiyasida Traffic Secretni to‘g‘ridan-to‘g‘ri “shifrlash kaliti” deb tushunish to‘liq to‘g‘ri emas. Masalan: Client Application Traffic Secret asosiy manba sifatida HKDF-Expand-Label funksiyasiga uzatiladi. Funksiyaga “key” yorlig‘i va kerakli uzunlik berilganda, u write_key simmetrik shifrlash kalitini yaratadi. Funksiyaga “IV” yorlig‘i va kerakli uzunlik berilganda, u write_iv (Initialization Vector) qiymatini yaratadi. Natijada hosil bo‘lgan write_key va write_iv juftligi orqali mijoz tomonidan yuboriladigan barcha Application Data (HTTPS trafigi, HTTP so‘rovlari va h.k.) xavfsiz holatda shifrlanadi. Ya’ni Traffic Secret asosida haqiqiy AEAD encryption key va IV hosil qilinadi. (8-rasm)



8-rasm. Kalitlarni hosil qilish ketma-ketligi

Resumption

Yuqorida takidlanganidek PSKdan 2 holatda foydalaniladi:

1. Oldingi TLS ulanishini qayta tiklashda - Resumption;
2. Oldindan sozlangan PSK - External PSK.

Resumption eng ko‘p uchraydigan holat. Masalan, client example.com bilan TLS ulanishini o‘rnatdi. Server NewSessionTicket yuboradi. Client undan keyingi ulanishda foydalanish uchun PSK hosil qiladi va saqlaydi. Keyinchalik client yana shu serverga ulansa ClientHello so‘rovining tarkibida PSK qiymatni yuboradi. Server PSKni tan olsa, to‘liq yangi autentifikatsiya jarayonini takrorlamasdan tezroq handshake bajarish mumkin.

Oldindan sozlangan PSK - External PSK client va serverda mavjud bo‘lishi ham mumkin. Mijoz TLS uanish vaqtida PSK identity va PSK binder qiymatlarni ClientHello so‘rovi tarkibida yuboradi. Server o‘zida mos PSK mavjudligini tekshiradi. Agar mavjud bo‘lsa autentifikatsiya jarayonini takrorlamasdan tezroq handshake bajarish mumkin. Bu usul IoT qurilmalar, yopiq tizimlar yoki oldindan ishonchli tomonlar o‘rtasidagi aloqa kabi holatlarda ishlatilishi mumkin.

PSK server sertifikatini almashtirishi mumkin - agar PSK asosidagi autentifikatsiya ishlatilsa, sertifikatli server autentifikatsiyasi shart emas.

PSK ning o ‘zidan foydalanish TLS 1.3 da tavfsiya etilmaydi. U bilan birgalikda doim DHE ishlatilishi ko‘zda tutilgan. PSK o‘zi ilg‘or maxsiylikni (forward secrecy) taminlab bera olmaydi, 0-RTT hujumi ehtimoli yuzaga keladi. Shuning uchun PSK va (EC) DHE birgalikda foydalanish maqsadga muvofiq hisoblanadi.

Xulosa

TLS 1.3 protokoli tarmoq orqali uzatiladigan ma’lumotlarning maxfiyligi, yaxlitligi va tomonlarning autentifikatsiyasini ta’minlash uchun ishlatiladi. TLS ulanishini o‘rnatish jarayoni bir nechta o‘zaro bog‘langan bosqichlardan tashkil topadi.

Avvalo, ClientHello orqali mijoz TLS versiyasi, cipher suitelar, qo‘llab-quvvatlanadigan guruhlar, signature algoritmlari va key_share kabi parametrlarini serverga taqdim etadi. Server ularni tahlil qilib, mos parametrlarni ServerHello orqali tanlaydi. Agar kerakli key_share mavjud bo‘lmasa, lekin handshakeni davom ettirish imkoniyati mavjud bo‘lsa, server HelloRetryRequest

yuboradi. Agar mos kriptografik parametrlar umuman mavjud bo‘lmasa yoki jiddiy protokol xatosi yuz bersa, Alert Protocol orqali handshake to‘xtatiladi.

Key exchange bosqichida odatda DHE/ECDHE mexanizmi ishlatiladi. mijoz va server o‘zlarining shaxsiy/ochiq kalit juftliklari yordamida umumiy DHE Shared Secret hosil qiladi. Keyin TLS 1.3 ning HKDF asosidagi Key Schedule mexanizmi yordamida handshake va application traffic uchun zarur bo‘lgan kalitlar hosil qilinadi.

Server autentifikatsiyasi Certificate va CertificateVerify xabarlari orqali amalga oshiriladi. Certificate serverning identifikatsiyasi va ochiq kalitini taqdim etadi, CertificateVerify esa serverning tegishli shaxsiy kalitga egaligini kriptografik jihatdan isbotlaydi. Shundan so‘ng Finished xabari handshake yaxlitligini tasdiqlaydi.

Handshake muvaffaqiyatli yakunlangach, Application Traffic Keys yordamida HTTP kabi yuqori darajadagi protokollarning ma’lumotlari himoyalanadi. Bu ma’lumotlar Record Protocol orqali TLS recordlarga joylashtiriladi va AEAD mexanizmlari yordamida shifrlanadi hamda yaxlitligi tekshiriladi.

TLS 1.3 da PSK esa asosan ikki holatda qo‘llanadi: oldingi TLS sessiyasini resumption qilishda yoki mijoz va serverda oldindan mavjud bo‘lgan External PSK asosida autentifikatsiya qilishda. PSK DHE bilan birgalikda ishlatilsa, samaradorlik bilan bir qatorda ilg‘or maxfiylik xususiyatini ham saqlab qolish mumkin.

Foydalanilgan adabiyotlar

1. Internet Engineering Task Force (IETF). RFC 9846. RFC 9846 rasmiy sahifasi.
2. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force (IETF), August 2018.
3. Rescorla, E. Guidelines for Writing IANA Considerations Section in RFCs. RFC 8126, Internet Engineering Task Force (IETF), June 2017.
4. Eastlake 3rd, D., Hansen, T., Kelsey, J. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). RFC 6234, Internet Engineering Task Force (IETF), May 2011.
5. Krawczyk, H., Eronen, P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, Internet Engineering Task Force (IETF), May 2010.
6. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018.
7. Barnes, R., Bhargavan, K., Lipp, B., Wood, C. Updates to the TLS 1.3 Protocol. RFC 8446 bilan bog‘liq IETF standartlari va yangilanishlari.
8. Kaufman, C., Perlman, R., Speciner, M. Network Security: Private Communication in a Public World. 3rd ed. Prentice Hall, 2023.

VIDEOKUZATUV TIZIMLARIDA VIDEO OQIMINI TANLAB SHIFRLASH SXEMALARI: HUJUMLAR TAHLILI VA KALIT BOSHQARUVIGA QO‘YILADIGAN TALABLAR

Qozoqova T.Q.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda videokuzatuv tizimlarida siqilgan video oqimini kriptografik himoyalash yondashuvlari to‘liq, tanlab, format saqlovchi, perseptual va qiziqish sohasi (ROI) bo‘yicha shifrlash qiyosiy tahlil qilingan. H.265/HEVC sintaksis elementlarini shifrlash, kodlash birligi darajasidagi nozik granulyar ROI shifrlash sxemalari va ularga qarshi ma’lum hujumlar, jumladan bitta ochiq matn–shifrmatn juftligidan kalit ketma-ketligini 86 % dan ortiq aniqlikda tiklovchi HKPA hujumi ko‘rib chiqilgan. Mavjud sxemalarda asosiy zaiflik algoritm darajasida emas, kalit boshqaruvi darajasida joylashgani hamda kadr darajasidagi yaxlitlik nazorati yo‘qligi ko‘rsatilgan. Tahlil asosida himoyalash usuliga yettita talab shakllantirilgan.

Kalit so‘zlar: videokuzatuv, tanlab shifrlash, ROI shifrlash, H.265/HEVC, ma’lum ochiq matn hujumi, kalit boshqaruvi, kadrlar guruhi, yaxlitlik nazorati.

Аннотация. В тезисе проведён сравнительный анализ подходов к криптографической защите сжатого видеопотока в системах видеонаблюдения: полного, селективного, форматосовместимого, перцептуального шифрования и шифрования областей интереса (ROI). Рассмотрены схемы шифрования синтаксических элементов H.265/HEVC, мелкозернистого ROI-шифрования на уровне единиц кодирования и известные атаки на них, в том числе атака HKPA, восстанавливающая ключевую последовательность с точностью более 86 % по одной паре открытый текст–шифртекст. Показано, что основная уязвимость существующих схем находится не на уровне алгоритма, а на уровне управления ключами, и что в них отсутствует контроль целостности на уровне кадров. На основе анализа сформулированы семь требований к методу защиты.

Ключевые слова: видеонаблюдение, селективное шифрование, ROI-шифрование, H.265/HEVC, атака с известным открытым текстом, управление ключами, группа кадров, контроль целостности.

Kirish

Videokuzatuv tizimlarida video ma’lumot siqilgan holda uzatiladi va arxivlanadi, shuning uchun kriptografik himoya siqish jarayoni bilan muvofiqlashtirilishi lozim. Siqilgan oqimni oddiy ikkilik ma’lumot sifatida to‘liq shifrlash maksimal maxfiylik bersa-da, uchta jiddiy kamchilikka ega. Birinchidan, hisoblash yuki bitreytga to‘g‘ri proporsional. Ikkinchidan, shifrlangan oqim format muvofiqligini yo‘qotadi: uni standart dekoder o‘qiy olmaydi, transkodlash va tezkor ko‘rish ishlamaydi. Uchinchidan, paket yo‘qolganda tiklanish murakkablashadi.

Shu sababli amaliyotda oqimning faqat muhim qismlarini himoyalovchi tanlab shifrlash sxemalari keng qo‘llanilmoqda. Biroq ularning xavfsizligi ko‘pincha faqat statistik ko‘rsatkichlar (entropiya, NPCR, UACI) bilan baholanadi, real hujum modellari esa hisobga olinmaydi. Tezisning maqsadi tanlab shifrlash sxemalari va ularga qarshi hujumlarni tahlil qilib, videokuzatuv tizimi uchun himoyalash usuliga qo‘yiladigan talablarni asoslash.

Asosiy qism

Video shifrlash yondashuvlarining tasnifi. To‘liq shifrlashga muqobil sifatida to‘rtta yondashuv shakllangan. *Tanlab shifrlashda* siqilgan oqimning ma’noviy jihatdan muhim sintaksis elementlari harakat vektorlari farqi (MVD), kvantlangan transformatsiya koeffitsiyentlari (QTC),

intra-bashorat rejimi (Luma IPM) va koeffitsiyentlarning ishora bitlari - shifrlanadi. *Format saqlovchi shifrlashda* natija standart sintaksis qoidalariga mos qoladi: oqim oddiy dekoder bilan dekodlanadi, ammo tasvir buzilgan holda ko‘rinadi. *Perseptual skremblashda* tasvir sifati tanib olishning oldini oladigan darajada pasaytiriladi. *ROI shifrlashda* esa faqat yuz yoki davlat raqami kabi maxfiy sohalar shifrlanadi; u kuzatuvning funksional maqsadini saqlagani uchun videokuzatuvga eng mos keladi.

Shifrlash siqish jarayonining qaysi bosqichida qo‘llanilishiga qarab uchta variant mavjud. Siqishdan oldin (xom kadrlar ustida) shifrlash amalda yaroqsiz: shifrlangan kadr statistik bog‘liqlikni yo‘qotib, bitreytni bir necha barobar oshiradi. Siqishdan keyin (bitoqim ustida) shifrlash format muvofiqligini buzadi. Shu sababli zamonaviy sxemalarning aksariyati siqish ichida sintaksis elementlari darajasida ishlaydi. Yondashuvlarning qiyosiy tavsifi 1-jadvalda keltirilgan.

1-jadval

Video shifrlash yondashuvlarining qiyosiy tavsifi

Yondashuv	Hisoblash yuki	Format muvofiqligi	Bitreyt oshishi	Maxfiylik darajasi
To‘liq shifrlash	Yuqori	Yo‘q	Yo‘q	To‘liq
Sintaksis elementlarini shifrlash	O‘rtacha	Saqlanadi	Kam	Yuqori
Perseptual skremblash	Past	Saqlanadi	Kam	Qisman
ROI shifrlash	Past	Saqlanadi	Juda kam	Tanlangan sohada to‘liq

Sintaksis elementlari va ROI darajasidagi sxemalar. Li va hamkasblari H.265/HEVC uchun sintaksis elementlarini shifrlash (SEC) sxemasini taklif qilgan, unda MVD, QTC va Luma IPM elementlari xaotik akslantirishga asoslangan koeffitsiyent skremblash bilan buziladi [1]. Sxema slaytlar bilan sinxron ishlaydi, shuning uchun ayrim slaytlar yo‘qolganda ham qolgan qismning dekodlanishi saqlanadi, bitreyt qo‘shimchasi esa deyarli nolga teng. Biroq tanlangan ochiq matn hujumidan himoyalanish uchun mualliflar AES-CTR rejimida hosil qilingan ketma-ketlikni oqimga qo‘shishga majbur bo‘lgan. Bu xaotik generatorning mustaqil kriptografik yadro sifatida yetarli emasligini ko‘rsatadi.

ROI shifrlashda markaziy texnik masala shifrlash birligining granulyarligi. Mavjud sxemalarning aksariyati minimal birlik sifatida Tile dan foydalanadi, natijada shifrlangan soha haqiqiy ROI dan ancha kengroq chiqadi: ortiqcha maydon shifrlanib, hisoblash yuki va bitreyt oshadi. Zhang va hamkasblari promptli segmentatsiya yordamida ROI ni 8×8 kodlash birligi (CU) darajasiga aniq akslantiruvchi sxemani taklif qilgan [2]. Siqilgan videoda bloklar bashorat orqali bog‘langani sababli bitta blokni shifrlash qo‘shni bloklarning dekodlanishiga ta’sir qiladi va shifrlangan soha chegarasi «yoyilib» ketadi. Ushbu ishda bu diffuziya ta’sirlangan CU larga PCM rejimi va harakat vektori cheklovini qo‘llash orqali izolyatsiya qilingan. Demak, har qanday ROI sxemasida diffuziyani nazorat qilish mexanizmi bo‘lishi shart.

Muallifning oldingi tadqiqotida yuz sohalarini HKDF-HMAC-SHA-256 asosida hosil qilingan kalitlar bilan shifrlovchi shaxsga yo‘naltirilgan ROI sxemasi taklif qilingan bo‘lib, unda entropiya 7,9970, NPCR 99,599 %, UACI 33,526 % ga erishilgan, aniqlanmay qolgan yuzlarning 10,67 % i esa keyingi ishlov berish bosqichida tiklangan [3]. Bu natijalar shifrlash sifatining statistik mezonlarga mosligini tasdiqlaydi, ammo quyida ko‘rsatilganidek, yaxshi statistik ko‘rsatkichlar sxemaning kalit boshqaruvi darajasidagi zaifliklardan himoyalanganini anglatmaydi.

Tanlab shifrlash sxemalariga qarshi hujumlar. Tanlab shifrlash sxemalarining asosiy zaifligi kriptografik yadroda emas, kalitdan foydalanish tartibida yotadi. Chen va hamkasblari taklif qilgan HEVC ga asoslangan ma’lum ochiq matn hujumi (HKPA) buni aniq ko‘rsatadi [4]. Hujumning faraz sharoiti ancha qat’iy: hujumchida atigi *bitta* ochiq matn–shifrmatn video juftligi mavjud deb hisoblanadi. Avval slayt sinxronlash identifikatori aniqlanadi, so‘ngra sinxronlangan

slayt uchun maxsus dekoder yordamida baholangan kalit ketma-ketligi (EKS) hosil qilinadi. Tajribalarda EKS ning o‘rtacha aniqligi 86 % dan oshgan va dekodlangan videolarning sezilarli qismi tanib olinadigan bo‘lgan. Eng muhimi, olingan EKS xuddi shu boshlang‘ich kalit bilan shifrlangan *boshqa videolarni ham* ochishga imkon beradi.

Bundan tizimli xulosa kelib chiqadi: HKPA hujumining asosiy sharti - kalitning qayta ishlatilishi. Agar har bir shifrlash birligi - kadrlar guruhi (GOP) yoki paket - o‘z kaliti va nonce ga ega bo‘lsa, bitta birlikdan olingan EKS boshqasiga qo‘llanmaydi va hujum sharti bajarilmaydi. Tanlangan ochiq matn hujumlari asoslanmagan xaotik generatorlarga xos bo‘lsa, qisman ma’lumot sizishi hujumlari shifrlanmagan sintaksis elementlaridan (blok chegaralari, harakat energiyasi taqsimoti) foydalanib, shifrlangan sohaning umumiy konturini tiklaydi. Alohida muammo - qayta siqish: Lin va Imaizumi ko‘rsatganidek, mavjud usullar siqishga moslashmagan va shifrlangan video transkodlanganda vizual sifat ham, tanib olish sifati ham keskin pasayadi [5]. Videokuzatuv tizimlarida oqim ko‘pincha arxivga tushishdan oldin transkodlangani uchun bu xususiyat amaliy ahamiyatga ega. Ma’lum hujumlar va ularga qarshi choralar 2-jadvalda umumlashtirilgan.

2-jadval

Video tanlab shifrlash sxemalariga qarshi ma’lum hujumlar

Hujum turi	Hujum sharti	Qarshi chora
HKPA [4]	Kalitning qayta ishlatilishi	Har bir kadrlar guruhi uchun yangi kalit va nonce
Tanlangan ochiq matn hujumi	Asoslanmagan (xaotik) generator	Kriptografik jihatdan asoslangan generator
Qisman ma’lumot sizishi	Shifrlash qamrovining torligi	Sintaksis elementlari to‘plamini kengaytirish
Qayta siqish ta’siri [5]	Siqishga moslashmagan sxema	Siqishga mos (compression-friendly) dizayn
Yaxlitlikni buzish	Autentifikatsiya tegining yo‘qligi	Har bir guruh uchun autentifikatsiya tegi

Muqobil maxfiylik yondashuvlari. So‘nggi yillarda shifrlashga muqobil yo‘llar ham faol o‘rganilmoqda, ammo ularning hech biri kameradan arxivgacha maxfiylikni to‘liq ta’minlamaydi. Format saqlovchi shifrlash bilan qaytariladigan yuz de-identifikatsiyasi [6] saqlangan tasvirlar uchun mo‘ljallangan va real vaqtli oqimda hisoblash yuki yuqori. Chekkada desensitizatsiya [7] xom tasvirni kameradayoq abstrakt xususiyat vektoriga aylantirib, kuchli maxfiylik beradi, lekin qaytarilmaydi asl yozuv yo‘qoladi va huquqiy dalil sifatida yaroqsiz bo‘ladi. Gomomorf shifrlash [8] shifrlangan ma’lumot ustida neyron tarmoq hisoblashlarini bajarishga imkon beradi, ammo real vaqtli video uchun bir necha tartib qimmat va cheklangan kamera tugunida qo‘llanmaydi. Shamirning sirni bo‘lish sxemasiga asoslangan kalit taqsimoti [9] esa shifrlash algoritmini emas, kalit boshqaruvini takomillashtiradi va tanlab shifrlash bilan birga qo‘llanishi mumkin.

Xulosa

Tahlil natijalariga ko‘ra, videokuzatuv sharoitida sintaksis elementlari darajasidagi ROI shifrlash eng maqbul yondashuv hisoblanadi, chunki u bitreyt qo‘shimchasini deyarli nolga tushiradi va kuzatuvning funksional maqsadini saqlaydi. Mavjud sxemalarning kriptografik zaifligi algoritm darajasida emas, kalit boshqaruvi darajasida joylashgan, ko‘rib chiqilgan sxemalarning hech birida esa kadr darajasidagi yaxlitlik nazorati yo‘q - videoyozuv huquqiy dalil sifatida ishlatilganda bu jiddiy bo‘shliqdir. Shu asosda dissertatsiyada ishlab chiqiladigan himoyalash usuliga quyidagi talablar qo‘yiladi:

1) shifrlash sintaksis elementlari darajasida bajarilishi va format muvofiqligi saqlanishi;

2) shifrlash birligi ROI ga imkon qadar aniq moslashtirilishi va diffuziya izolyatsiya qilinishi;

3) har bir kadrlar guruhi o‘z kaliti va nonce ga ega bo‘lishi - bu HKPA hujumining asosiy shartini bekor qiladi;

4) kalitlar ierarxik tarzda hosil qilinishi, bunda bitta guruh kaliti sizib chiqsa, zarar shu guruh bilan cheklanadi;

5) har bir kadrlar guruhiga autentifikatsiya tegi qo‘shilishi va yaxlitlik nazorati sxemaga boshidan kiritilishi;

6) shifrlash yadrosi sifatida xaotik generator emas, kriptotahlildan o‘tgan yengil oqimli shifr, masalan Grain oilasi konstruksiyasi [10] qo‘llanilishi;

7) sxemaning qayta siqishga nisbatan barqaror bo‘lishi.

Ushbu talablar yagona kalit ierarxiyasiga asoslangan himoyalash usuli, kalit oqimi generatori va ROI tanlab shifrlash algoritmlarini ishlab chiqish uchun asos bo‘lib xizmat qiladi. Xususan, kadrlar guruhi bo‘yicha kalit va nonce yangilash HKPA turidagi hujumlarning asosiy shartini bekor qilsa, har bir guruhga biriktirilgan autentifikatsiya tegi videoyozuvning huquqiy dalil sifatidagi ishonchliligini ta’minlaydi.

Foydalanilgan adabiyotlar:

1. Li L.-W., Lee C.-N., Gupta K., Yang H.-F., Singh A.K. Syntax element encryption for H.265/HEVC using chaotic map-based coefficient scrambling scheme // IEEE Transactions on Circuits and Systems for Video Technology. – 2026. – Vol. 36(4).
2. Zhang X., Lu H., Li Z., He Z., Tan Z., Peng F., Fu Z. A H.265/HEVC fine-grained ROI video encryption algorithm based on coding unit and prompt segmentation. – arXiv:2604.08047, 2026.
3. Xudoykulov Z.T., Qozoqova T.Q. Video kuzatuv tizimlarida qo‘llaniladigan xavfsiz aloqa protokollari // «Al-Farg‘oniy avlodlari». – 2025. – T. 1, № 4. – B. 170–179.
4. Chen C., Yuan Y., Mao N., Amirpour H., Qu L. An HEVC-based known-plaintext attack for video selective encryption // Scientific Reports. – 2026.
5. Lin H., Imaizumi S. CFE-PPAR: compression-friendly encryption for privacy-preserving action recognition leveraging video transformers. – arXiv:2605.05692, 2026.
6. Kim H., Park S., Choi D. Secure and reversible face de-identification with format-preserving encryption // IEEE Access. – 2025. – DOI: 10.1109/ACCESS.2025.3583388.
7. Song H., Tian S., Long T., Liu J., Yuan C., Jia Z., Shao J., Li X. Privacy-Aware Camera 2.0 technical report. – arXiv:2603.04775, 2026.
8. Shah P., Virani R., Srivastava S. Homomorphic encryptions for privacy preserving vision. – arXiv:2606.25216, 2026.
9. Coşkun H., Çolhak F., Kulakov A., Dimitrova V. Privacy-preserving smart surveillance with cross-dataset violence detection and decentralized evidence governance. – arXiv:2606.01225, 2026.
10. Hell M., Johansson T., Maximov A., Meier W., Sönnerup J., Yoshida H. Grain-128AEADv2: a lightweight AEAD stream cipher. – NIST Lightweight Cryptography Project, 2021.

MERKLE–DAMGÅRD VA WIDE-PIPE KONSTRUKSIYALARINING XAVFSIZLIK JIHATIDAN QIYOSIY TAHLILI

Xaydarov T.S.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Merkle–Damgård va wide-pipe konstruksiyalari chiqish uzunligi bir xil bo‘lgan sharoitda qiyoslandi. Ichki va yakuniy kolliziyalar ajratilib, Lucksning ideal kompressiya modeli bo‘yicha multikolliziya qidirish xarajatining pastki chegarasi hisoblandi. 256-bit chiqish uchun 384-bit ichki holat 4-kolliziya mezonini, 448-bit holat esa 8-kolliziya mezonini ideal hesh darajasiga yetkazadi. Oddiy kolliziya uchun 128-bit daraja ko‘rsatkichi saqlanadi. SHA-256 va SHA-512/256 standart parametrlari nazariy modelning amaliy misoli sifatida muhokama qilindi.

Kalit so‘zlar: Merkle–Damgård, wide-pipe, ichki holat, multikolliziya, ideal kompressiya, SHA-512/256, xavfsizlik chegarasi.

Аннотация. Проведено сравнение конструкций Меркла–Дамгора и wide-pipe при одинаковой длине выхода. Разграничены внутренние и конечные коллизии; рассчитана нижняя граница стоимости поиска мультиколлизий в модели идеального сжатия Лукса. Для 256-битного выхода состояние шириной 384 бита достигает уровня идеального хеша по критерию 4-коллизии, а 448 бит - по критерию 8-коллизии. Для обычной коллизии сохраняется показатель степени 128. Параметры SHA-256 и SHA-512/256 рассмотрены как практический пример различий внутреннего состояния.

Ключевые слова: Меркл–Дамгор, wide-pipe, внутреннее состояние, мультиколлизия, идеальное сжатие, SHA-512/256, граница безопасности.

Kirish

Hesh chiqishining uzunligi bir xil bo‘lsa ham, funksiyalarning strukturaviy xavfsizlik xususiyatlari farq qilishi mumkin. Oddiy Merkle–Damgård (MD) konstruksiyasida ichki holat va yakuniy chiqish uzunligi teng. Wide-pipe yondashuvi ichki holatni kengaytirib, undan qisqaroq hesh qiymatini chiqaradi. Lucks ichki holat o‘lchamini mustaqil xavfsizlik parametri sifatida tahlil qilgan [1]. Ushbu tezisning maqsadi chiqish uzunligini o‘zgartirmasdan ichki holatning ayrim hujumlarga ta’sirini miqdoriy solishtirishdir.

Joux iterativ heshda bir necha kolliziya bosqichini birlashtirish orqali katta multikolliziya to‘plamini yaratish mumkinligini ko‘rsatgan [2]. Bu natija oddiy kolliziyaga bardoshlilik barcha boshqa kolliziya xususiyatlarini to‘liq ifodalamasligini anglatadi. Taqqoslash uchun aynan multikolliziya mezoni tanlandi. Tahlil klassik orakul-so‘rov modelida bajarildi; u real SHA-2 uchun yangi hujum yoki yangi xavfsizlik isboti da’vosini bermaydi.

Konstruksiyalar va tahlil mezoni

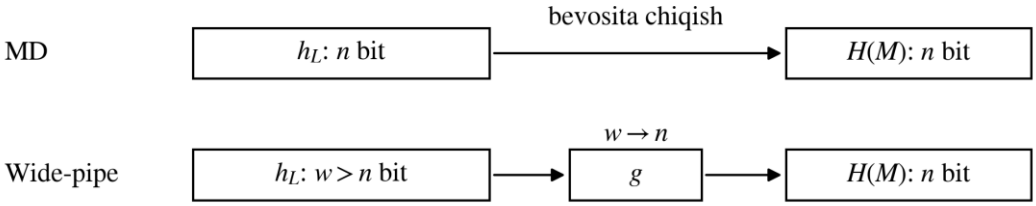
n hesh chiqishi, w ichki holat, b xabar bloki uzunligini bildiradi. w belgisi butun ichki holatga tegishli bo‘lib, FIPS 180-4 dagi mashina so‘zi uzunligi belgisi bilan aralashtirilmaydi. Har ikkala konstruksiyada xabar uzunligi hisobga olingan padding va bir xil boshlang‘ich holat tanlash qoidasi faraz qilindi. MD da w = n; wide-pipe da w > n.

$$h_i = f(h_{i-1}, m_i), \quad H_{MD}(M) = h_L \tag{1}$$

Wide-pipe da kompressiya funksiyasi w-bit holatni yangilaydi va yakunda g funksiyasi uni n-bit chiqishga akslantiradi. Lucksning modelida g mustaqil ideal funksiya yoki belgilangan

bitlarni kesib olish operatsiyasi bo‘lishi mumkin; xavfsizlik xulosalari kompressiya modeli shartlari bilan birga qo‘llanadi [1].

$$h_i = f_w(h_{i-1}, m_i), \quad H_{WP}(M) = g(h_L) \tag{2}$$



1-rasm. Yakuniy ichki holatdan hesh chiqishini olishning qiyosiy sxemasi

Ichki kolliziyada ikki turli xabar bir xil to‘liq yakuniy ichki holatga olib keladi. Yakuniy kolliziyada ichki holatlar turlicha bo‘lishi mumkin, lekin g chiqishlari teng keladi. Demak, wide-pipe heshlarining tengligi ularning ichki holatlari tengligini anglatmaydi. Bu farq keyingi bloklarni qo‘shganda kolliziyaning avtomatik davom etishiga yo‘l qo‘ymaslik uchun ahamiyatli [1].

1-jadval

Ideal kompressiya farazida konstruksiyalarning asosiy farqlari

Mezon	Oddiy MD	Wide-pipe
Ichki holat va chiqish	w = n	w > n
To‘liq ichki holat chiqishda	Oshkor bo‘ladi	To‘liq oshkor bo‘lmaydi
Ichki kolliziya qidiruvi tartibi	2n/2	2w/2
n-bit chiqish kolliziyasi tartibi	2n/2	2n/2

Multikolliziya uchun parametrlarni hisoblash

K-kolliziya - bir xil heshga ega K ta turli xabardan iborat to‘plam. $K = 2^r$ bo‘lganda Jouxning MD uchun usuli r ta ketma-ket kolliziya bosqichini ishlatadi; uning xarajati $O(r \cdot 2^{n/2})$ tartibida [2]. Bu yerda n-bit ichki holatdagi kolliziya yangi bosqichlar bilan qayta ishlatiladi. Katta K uchun aynan ushbu strukturaviy imkoniyat ideal hesh bilan farqni yuzaga keltiradi.

Lucksning 2-teoremasida wide-pipe kompressiyasi tasodifiy orakul sifatida qaraladi. Yakuniy g mustaqil tasodifiy orakul yoki w-bit holatning n bitini kesib olish funksiyasi bo‘lganda K-kolliziya qidirish uchun quyidagi pastki chegara beriladi [1]:

$$T(K) = \Omega(2^{\beta}), \quad \beta = min(w/2, n(K-1)/K) \tag{3}$$

(3) dagi n(K−1)/K ideal n-bit heshning K-kolliziya daraja ko‘rsatkichidir. β asimptotik so‘rovlar chegarasiga tegishli; uni aniq ish vaqti yoki barcha xavfsizlik xususiyatlarining bit bahosi deb olish mumkin emas. MD bilan taqqoslashda $2^{n/2}$ darajasi Joux xarajatining r ko‘paytuvchisi ajratilgan yetakchi ko‘rsatkichi sifatida berildi. Jadvalda logarifmik omillar va doimiy koeffitsiyentlar keltirilmagan.

2-jadval

n = 256 uchun multikolliziya chegaralarining daraja ko‘rsatkichlari

K	MD, yetakchi daraja	β, w = 384	β, w = 448	β, w = 512
2	128	128	128	128
4	128	192	192	192

K	MD, yetakchi daraja	β, w = 384	β, w = 448	β, w = 512
8	128	192	224	224
16	128	192	224	240
256	128	192	224	255

Jadval (3) formula asosida Python yordamida hisoblandi. K = 2 da barcha variantlar 128 darajasini beradi: ichki holatni kengaytirish oddiy 256-bit chiqish kolliziyasining birthday chegarasini oshirmaydi. K = 8 uchun 384-bit holatda β = 192, 448 va 512-bit holatlarda β = 224. Shunday qilib, ichki holatni 448 dan 512 bitga oshirish aynan 8-kolliziya mezonida qo‘shimcha daraja bermaydi; K = 16 va 256 uchun esa farq mavjud.

Muayyan K uchun ideal hesh darajasiga erishish shartini (3) dan algebraik tarzda ajratish mumkin:

$$w \geq 2n(K-1)/K \quad (4)$$

n = 256 bo‘lganda 4-, 8-, 16- va 256-kolliziya uchun chegaraviy ichki holatlar mos ravishda 384, 448, 480 va 510 bitdir. w = 512 barcha chekli K uchun yetarli, chunki n(K−1)/K < n. Ushbu qiymatlar amaliy kompressiya funksiyasi dizaynini belgilovchi tavsiya emas; ular ideal modeldagi mezon sezgirligini ko‘rsatadi. Real algoritmda holat o‘lchami bilan birga kompressiya xususiyatlari ham tekshiriladi.

SHA-2 misolida talqin va cheklovlar

FIPS 180-4 bo‘yicha SHA-256 ichki holati 256 bit va chiqishi 256 bit. SHA-512/256 esa SHA-512 ning 512-bit ichki holatini saqlab, yakunda 256-bit chiqish beradi [3]. Shu sababli ikkinchisi keng ichki holat tamoyilining standartlashtirilgan misolidir. SHA-512/256 uchun maxsus boshlang‘ich qiymat belgilangan; uni oddiy SHA-512 heshining dastlabki 256 bitini kesib olish bilan aynan tenglashtirish mumkin emas.

NISTning Hash Functions sahifasida ikkala algoritm uchun oddiy kolliziyaga bardoshlilik 128 bit, proobrazga bardoshlilik 256 bit sifatida keltiriladi. Ikkinchi proobraz mezonida SHA-256 uchun 256 − L(M), SHA-512/256 uchun esa 256 bit ko‘rsatilgan [4]. Bu yerda $L(M) = \log_2(\text{len}(M)/b)$, len(M) xabar uzunligi bitlarda, b esa blok uzunligidir. Bu misol chiqish uzunligi teng bo‘lsa ham, ichki tuzilish sabab ayrim xavfsizlik mezonlari farqlanishini ko‘rsatadi. Mazkur standart baholarni 2-jadvaldagi ideal orakul multikolliziya hisoblari bilan bir xil natija deb olish mumkin emas.

Lucks teoremasidagi ideal kompressiya farazi real SHA-512 kompressiyasining barcha xususiyatlarini isbotlamaydi. Shu bois w = 512 va n = 256 ni formulaga qo‘yishning o‘zi SHA-512/256 uchun barcha multikolliziya hujumlarini istisno qiluvchi isbot emas. Jadval konstruksiya modeliga tegishli. Tajriba orqali real hujum bajarilmadi; hesh xavfsizligining kvant, yon kanal va protokol jihatlari ham hisobga kiritilmadi.

Ichki holat kengayganda saqlanadigan holat hajmi ortadi, ammo butun dastur xotirasi yoki bajarilish vaqti shuncha marta oshishi shart emas. Xabar jadvali, registrlar va apparat arxitekturasi ham xarajatga ta’sir qiladi. Shuningdek, oddiy hesh konstruksiyasi xabarni autentifikatsiyalash vazifasini o‘zi bajarmaydi. Wide-pipe tanlovining afzalligi muayyan xavfsizlik mezoni va kompressiya modeliga bog‘lab baholanishi kerak.

Xulosa

Wide-pipe ning asosiy afzalligi chiqish uzunligini oshirishdan emas, ichki va yakuniy kolliziyalarni ajratishdan kelib chiqadi. Ideal modelda 256-bit chiqish uchun 384-bit holat 4-

kolliziya, 448-bit holat 8-kolliziya mezonini ideal hesh darajasiga yetkazadi. 512-bit holat esa kattaroq K qiymatlarida ham shu darajani saqlaydi. Oddiy kolliziyaning 128 daraja ko‘rsatkichi barcha variantlarda o‘zgarmaydi. Demak, konstruksiyalarni taqqoslashda ichki holat, chiqish uzunligi va hujumning K parametri birgalikda ko‘rsatilishi zarur. SHA-512/256 misoli ushbu tamoyilni amaliy parametrlar bilan bog‘laydi; real algoritm xavfsizligi alohida kriptoanalizni talab qiladi.

Foydalanilgan adabiyotlar

1. Lucks S. A Failure-Friendly Design Principle for Hash Functions // Advances in Cryptology - ASIACRYPT 2005. - LNCS. Vol. 3788. - Springer, 2005. - P. 474–494. - DOI: 10.1007/11593447_26.

2. Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions // Advances in Cryptology - CRYPTO 2004. - LNCS. Vol. 3152. - Springer, 2004. - P. 306–316. - DOI: 10.1007/978-3-540-28628-8_19.

3. National Institute of Standards and Technology. Secure Hash Standard (SHS): FIPS PUB 180-4. - Gaithersburg: NIST, 2015. - DOI: 10.6028/NIST.FIPS.180-4.

4. National Institute of Standards and Technology. Hash Functions [Elektron resurs]. - URL: https://csrc.nist.gov/projects/hash-functions (murojaat sanasi: 11.10.2026).

TLS 1.3 PROTOKOLI VA MILLIY KRIPTOGRAFIK PROFILLAR: ROSSIYA, BELARUS, XITOY TAJRIBASI HAMDA O‘ZBEKISTON UCHUN IMKONIYATLAR

Xudoykulov Z.T., Qutlimurotov A.H.
Muhammad al-Xorazmiy nomidagi TATU

Annotatsiya. Maqolada TLS (Transport Layer Security – transport qatlam xavfsizligi) protokolining joriy holati, TLS 1.3 arxitekturasi va milliy kriptografik algoritmlarni transport qatlam xavfsizlik protokollariga integratsiya qilish masalalari ko‘rib chiqilgan. Rossiya (GOST), Belarus (STB) va Xitoy (TLCP) yondashuvlari huquqiy-texnik maqomi bo‘yicha qiyoslangan, O‘zbekistonning 2024-yilgi O‘zMSt 270, 285 va 286 standartlari TLS 1.3 talablari nuqtai nazaridan tahlil qilingan. TLS 1.3 arxitekturasini saqlagan holda milliy algoritmlarni profil sifatida integratsiya qilish afzalroq ekani asoslangan.

Kalit so‘zlar: TLS 1.3; RFC 9846; milliy kriptografik profil; shifrlar to‘plami; autentifikatsiyalangan shifrlash; GOST; STB; TLCP; O‘zMSt 270/285/286:2024.

Аннотация. В статье рассмотрены современное состояние протокола TLS (Transport Layer Security – протокол защиты транспортного уровня), архитектура TLS 1.3 и вопросы интеграции национальных криптографических алгоритмов в протоколы защиты транспортного уровня. Сопоставлены подходы России (ГОСТ), Беларуси (СТБ) и Китая (TLCP) с учётом их правового и технического статуса, стандарты Узбекистана O‘zMSt 270, 285 и 286 (2024 г.) проанализированы с точки зрения требований TLS 1.3. Обосновано, что интеграция национальных алгоритмов в виде профиля при сохранении архитектуры TLS 1.3 предпочтительнее.

Ключевые слова: TLS 1.3; RFC 9846; национальный криптографический профиль; набор шифров; аутентифицированное шифрование; ГОСТ; СТБ; TLCP; O‘zMSt 270/285/286:2024.

Kirish

TLS ishonchsiz tarmoqda ikki tomon o‘rtasida himoyalangan kanal o‘rnatadi. Uning amaldagi spetsifikatsiyasi – IETF (Internet Engineering Task Force – Internet muhandisligi ishchi guruhi) tomonidan 2026-yil iyulida Proposed Standard maqomida e’lon qilingan RFC (Request for Comments – sharhlar uchun so‘rov) 9846 bo‘lib, u TLS 1.3 ni belgilaydi va RFC 8446 hamda RFC 5246 ni bekor qiladi [1]. TLS maxfiylik (confidentiality), yaxlitlik (integrity) va autentifikatsiyani (authentication) ta’minlaydi: server har doim, mijoz esa ixtiyoriy ravishda asimmetrik kriptografiya yoki PSK (Pre-Shared Key – oldindan kelishilgan kalit) yordamida autentifikatsiyalanadi [1]. Protokol amaliy protokoldan mustaqil va quyi transportdan faqat ishonchli, tartiblangan oqimni talab qiladi [1], ya’ni u transport protokoli emas, balki transport ulanishi, odatda TCP (Transmission Control Protocol – uzatishni boshqarish protokoli) ustidagi xavfsizlik qatlamidir. Eng keng qo‘llanishi – HTTPS (Hypertext Transfer Protocol Secure – xavfsiz gipermatn uzatish protokoli), unda server identifikatori sertifikat orqali tekshiriladi [2].

TLS versiyalari va TLS 1.3 ning asosiy farqlari

SSL (Secure Sockets Layer – xavfsiz soketlar qatlami) 3.0 [3] asosida IETF TLS 1.0 (1999) [4], TLS 1.1 (2006) [5], TLS 1.2 (2008) [6] va TLS 1.3 (2018) [7] ni qabul qilgan; TLS 1.0 va 1.1 2021-yilda eskirgan deb e’lon qilingan [8]. TLS 1.2 ga nisbatan TLS 1.3 da qo‘l siqish protokoli (Handshake Protocol) bitta aylanma kechikishda – 1-RTT (Round-Trip Time – aylanma kechikish

vaqti) da yakunlanadi va ServerHello dan keyingi barcha xabarlar shifrlanadi; statik RSA (Rivest–Shamir–Adleman – RSA ochiq kalitli kriptotizimi) va statik DH (Diffie–Hellman – Diffi–Xellman) kalit almashinuvi olib tashlanib, barcha ochiq kalitli almashuvlar oldinga yo‘naltirilgan maxfiylikni (forward secrecy) beradi [1]. Kalitlar HMAC (Hash-based Message Authentication Code – xeshga asoslangan xabar autentifikatsiya kodi) ga tayangan HKDF (HMAC-based Extract-and-Expand Key Derivation Function – ajratib olish va kengaytirishga asoslangan kalit hosil qilish funksiyasi) [9] bilan hosil qilinadi. Shifrlar to‘plami (cipher suite) endi faqat autentifikatsiyalangan shifrlash (authenticated encryption) algoritmi – AEAD (Authenticated Encryption with Associated Data – qo‘shimcha ma’lumotli autentifikatsiyalangan shifrlash) va HKDF xeshini belgilaydi, kalit almashish va imzo alohida muzokara qilinadi (Handshake yoki Negotiation); siqish, qayta muzokara (Renegotiation) va AEAD bo‘lmagan shifrlar chiqarib tashlangan. PSK asosidagi 0-RTT rejimi birinchi xabardayoq ma’lumot yuborishga imkon beradi, biroq bu ma’lumot uchun forward secrecy va takroriy yuborishdan himoya kafolatlari zaifroq [1].

TLS 1.3 arxitekturasi

TLS 1.3 qo‘l siqish (Handshake) va yozuvlar protokoli (Record Protocol) dan iborat [1]. Qo‘l siqishda ClientHello va ServerHello orqali kalit almashiladi, shifrlangan EncryptedExtensionsda server parametrlari uzatiladi, Certificate, CertificateVerify va Finished xabarlarida esa autentifikatsiya va kalit tasdig‘i amalga oshadi. Yozuvlar protokoli trafikni AEAD bilan himoyalaydi, ogohlantirish (alert) mexanizmi xatolarni bildiradi. Handshake bir-biridan mustaqil tanlanadigan uch parametrga tayanadi: (AEAD, xesh) juftligidan iborat shifr to‘plami; “supported_groups” va “key_share” kengaytmalaridagi kalit almashish guruhi; “signature_algorithms” dagi imzo sxemasi. Server tanimaydigan shifr to‘plamlari va kengaytmalarni (extensions) e’tiborsiz qoldiradi [1] – milliy profillarning texnik asosi aynan shu xossadir. Kalit almashish efemer ECDHE (Elliptic Curve Diffie–Hellman Ephemeral – elliptik egri chiziqlardagi efemer Diffi–Xellman) yoki KEM (Key Encapsulation Mechanism – kalitni inkapsulyatsiyalash mexanizmi) orqali bajariladi. Server sertifikati PKI (Public Key Infrastructure – ochiq kalitlar infratuzilmasi) va CA (Certification Authority – sertifikatlashtirish markazi) orqali tekshiriladi, CertificateVerify esa qo‘l siqish transkripti ustidagi RSA yoki ECC (Elliptic Curve Cryptography – elliptik egri chiziqlar kriptografiyasi) imzosidir; barcha muhim kattaliklar HKDF asosidagi kalitlar jadvalida ketma-ket hosil qilinadi [1].

Milliy kriptografik profillar: Rossiya, Belarus va Xitoy

IANA (Internet Assigned Numbers Authority – Internet raqamlarini taqsimlash organi) reestridagi kod nuqtasi hujjat maqomini anglatmaydi: mustaqil oqim (Independent Submission) orqali e’lon qilingan Informational RFC Internet standarti hisoblanmaydi [10], Internet-Draft esa vaqtinchalik ish hujjatidir. Shu sababli yondashuvlar “milliy TLS varianti” deb umumlashtirilmay, maqomi bo‘yicha tavsiflanadi.

Rossiya. GOST (State Standard – davlat standarti) algoritmlari TLS 1.2 uchun RFC 9189 (2022) [10] va TLS 1.3 uchun RFC 9367 (2023) [11] da belgilangan; ikkalasi mustaqil oqimdagi Informational RFC, kod nuqtalari IANA da “Recommended = N” belgisi bilan ro‘yxatga olingan. Asosiy algoritmlar: GOST R 34.12-2015 dagi Kuznyechik (128 bitli blok) va Magma (64 bitli blok) shifrlari, GOST R 34.11-2012 xesh funksiyasi, GOST R 34.10-2012 imzosi [12] va MGM (Multilinear Galois Mode – ko‘p chiziqli Galua rejimi) AEAD rejimi [11]. TLS 1.2 profilida dastlabki sir server kaliti asosida eksport qilinadi va forward secrecy yo‘q [10]. TLS 1.3 profili to‘rtta shifr to‘plami, yettita imzo sxemasi va GC256A–GC512C egri chiziqlarida ECDHE ni

belgilaydi; holatlar mashinasi va kalitlar jadvali o‘zgarmagan, yagona qo‘shimcha – yozuv kalitini qayta hosil qiluvchi TLSTREE funksiyasi [11].

Belarus. STB (STandards of Belarus – Belarus standartlari) seriyasidagi Belt (blokli shifr asosidagi shifrlash va xeshlash), Bash (gubka funksiyasiga asoslangan algoritmlar) va Bign (elliptik egri chiziqli imzo) [13] TLS 1.3 uchun milliy standart STB 34.101.90-2026 da qo‘llangan [14]. Xalqaro tanitish uchun 2026-yil 1-sentyabrda individual Internet-Draft draft-kalosha-stb-tls13-00 e’lon qilingan (mo‘ljallangan maqomi – Informational); u RFC emas, kod nuqtalari esa xususiy foydalanish (private use) diapazonidan olingan vaqtinchalik qiymatlar [13]. Hujjat TLS_BASH_PRG_AE2561_BASH256 va TLS_BELT_CHE256_BELT_HASH shifr to‘plamlarini, bign egri chiziqlarida Diffi–Xellman almashinuvini, Bign imzolarini va sinov vektorlarini belgilaydi; mualliflar parametrlarni almashtirish stekni qayta loyihalashni talab qilmasligini ta’kidlaydi [13].

Xitoy. TLCP (Transport Layer Cryptography Protocol – transport qatlam kriptografik protokoli) – mustaqil milliy standart GB/T 38636-2020 [15]. Uning tuzilmasi TLS 1.1/1.2 ga yaqin, biroq alohida versiya raqami (0x0101), imzo va shifrlash uchun ikki alohida sertifikat, ECC_SM4_CBC_SM3, ECDHE_SM4_GCM_SM3 kabi shifr to‘plamlari mavjud; ECC_ to‘plamlarida forward secrecy yo‘q, CBC (Cipher Block Chaining – shifrlangan bloklar zanjiri) rejimi esa TLS 1.3 da chiqarib tashlangan. Algoritmik asos – SM (ShangMi, Commercial Cryptography – Xitoy tijorat kriptografiyasi) oilasi: SM2 imzosi, SM3 xesh funksiyasi va SM4 blokli shifri [16]. Bundan alohida RFC 8998 (2021, Informational) TLS 1.3 ning SM profilini – TLS_SM4_GCM_SM3, TLS_SM4_CCM_SM3 to‘plamlari, sm2sig_sm3 imzosi va curveSM2 guruhini belgilaydi [16]. Demak, TLCP “TLS 1.3’ ning Xitoy varianti” emas, balki TLS 1.3 dan oldingi arxitekturaga tayangan mustaqil protokoldir.

1-jadval

Rossiya, Belarus va Xitoy yondashuvlarining qiyosiy tavsifi [10–16]

Ko‘rsatkich	Rossiya	Belarus	Xitoy
Yondashuv turi	TLS 1.2 va 1.3 profili	TLS 1.3 profili	Mustaqil protokol; TLS 1.3 SM profili
Bazaviy protokol	TLS 1.2; TLS 1.3	TLS 1.3	TLCP (0x0101); TLS 1.3
Blokli shifr / AEAD	Kuznyechik, Magma / MGM	belt-block / belt-che256	SM4 / GCM, CCM
Xesh funksiyasi	GOST R 34.11-2012	belt-hash, bash	SM3
Raqamli imzo	GOST R 34.10-2012	Bign	SM2
Kalit almashish	ECDHE (TLS 1.3)	bign egri chiziqlarida DH	ECC, ECDHE (TLCP); ECDHE
Maqomi	Informational RFC 9189, 9367	STB 34.101.90-2026; Internet-Draft	GB/T 38636-2020; Informational RFC 8998
TLS bilan moslik	Mos; IANA kodlari bor	Mos; kodlar vaqtinchalik	TLCP – mos emas; SM profili – mos

Milliy TLS 1.3 profiliga qo‘yiladigan talablar

TLS 1.3 faqat AEAD ni qabul qilgani uchun milliy blokli shifr uchun standartlashtirilgan AEAD rejimi va bitta kalit bilan himoyalanadigan ma’lumot hajmi chegarasi zarur (Rossiyada

MGM va TLSTREE [11], Belarusda belt-che256 va bash-prg-ae2561 [13]). Xesh HKDF va transkript uchun, imzo CertificateVerify va sertifikatlar uchun ishlatiladi; kalit kelishuvi efemer bo‘lishi va ochiq kalitni tekshirish tartibiga ega bo‘lishi kerak [1]. Protokol darajasida yangi shifr to‘plami, guruh va imzo sxemasi identifikatorlari, X.509 uchun OID (Object Identifier – obyekt identifikatori) va sertifikat profili belgilanadi; xalqaro moslik IANA kodlarini talab qiladi, xususiy foydalanish kodlari esa faqat yopiq tarmoqqa yaroqli [1]. Orqaga moslik (backward compatibility) uchun TLS 1.2 profili zarurligi alohida hal qilinadi. Amalga oshirishda o‘zgarmas vaqtli kod, yon-kanal hujumlariga bardoshlilik, sinov vektorlari, muvofiqlik testlari va mustaqil kriptotahlil talab etiladi.

Asosiy masala – protokolni qayta loyihalash zarurmi? Rossiya va Belarus tajribasi salbiy javob beradi: TLS 1.3 xabarlari, holatlar mashinasi va kalitlar jadvali saqlanib, faqat kriptografik parametrlar almashtirilgan [11, 13]. Bu TLS 1.3 xavfsizlik xossalarini meros qilib olish va tahlilni primitivlar darajasiga jamlash imkonini beradi.

O‘zbekiston uchun imkoniyatlar va cheklovlar

2024-yilda O‘zbekiston standartlar instituti uchta yangi standartni tasdiqladi: O‘zMSt 270:2024 – “Ma’lumotlarni shifrlash algoritmi” (O‘z DSt 1105:2009 o‘rniga; davlat tashkilotlari uchun majburiy) [17], O‘zMSt 285:2024-“Xeshlash funksiyasi” (O‘z DSt 1106:2009 o‘rniga) [18] va O‘zMSt 286:2024-“Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari” (O‘z DSt 1092:2009 o‘rniga) [19]. O‘zMSt 270:2024 uch algoritmni o‘z ichiga oladi: 256 bitli blokli va 256 bitli kalitli MShA (Ma’lumotlarni shifrlash algoritmi), uning uchun faqat elektron kod kitobi va CBC rejimlari bayon etilgan; AES (Advanced Encryption Standard – kengaytirilgan shifrlash standarti), uning rejimlari uchun NIST (National Institute of Standards and Technology – AQSh Milliy standartlar va texnologiyalar instituti) SP 800-38 seriyasiga ishora qilinadi; maxfiy o‘rniga qo‘yish blokiga ega 64 bitli blokli shifr [17]. O‘zMSt 285:2024 da 256 bitli diamatritsaviy xesh va 64 bitli shifrga asoslangan 256 bitli xesh berilgan [18]. O‘zMSt 286:2024 dagi 1-algoritm “daraja parametri muammosi”ga asoslangan, 2-algoritm esa elliptik egri chiziqli imzo bo‘lib, uning formulalari va nazorat misoli GOST R 34.10-2012 test misoli bilan mos keladi [12, 19].

TLS 1.3 talablari bilan solishtirilganda xesh va imzo uchun asos mavjud, biroq ikki majburiy element hali standartlashtirilmagan: milliy blokli shifr uchun AEAD rejimi (GCM – Galois/Counter Mode, Galua/hisoblagich rejimi – 128 bitli blokka mo‘ljallangan, MShA bloki esa 256 bit) va efemer kalit kelishuvi; nomlangan egri chiziqlar, OID lar va kod nuqtalari ham belgilanmagan. 64 bitli shifr, Magma kabi, bitta kalit bilan himoyalanadigan hajmni cheklashni talab qiladi, maxfiy o‘rniga qo‘yish jadvali esa ochiq protokolda moslashuvchanlikka to‘sqinlik qiladi.

Imkoniyatlar: AES ning standartga kiritilgani o‘tish davrida TLS 1.3 dagi TLS_AES_128_GCM_SHA256 to‘plamidan foydalanishni milliy talablarga yaqinlashtiradi [1], [17]; imzo 2-algoritmining GOST R 34.10-2012 bilan mosligi RFC 9367 tajribasini qo‘llashni osonlashtiradi [11, 19]; profil davlat axborot tizimlarida kriptografik mustaqillik, milliy PKI bilan integratsiya, mahalliy dasturiy va apparat vositalar, standartlashtirish maktabi hamda ilmiy tadqiqot va kadrlar tayyorlashni rivojlantirishga xizmat qiladi.

Cheklovlar: profil faqat uni qo‘llovchi tomonlar o‘rtasida ishlaydi va brauzer hamda server ekotizimida standart holda bo‘lmaydi; TLS kutubxonalariga qo‘shish va uzoq muddat qo‘llab-quvvatlash xarajat talab qiladi; yangi algoritmlar chuqur ochiq kriptotahlildan o‘tishi, sertifikatlashtirish va test infratuzilmasi yaratilishi zarur; xalqaro kod nuqtalarini olish uzoq

jarayon – Rossiya profili Internet-Draft dan RFC gacha kamida 2021–2023-yillar davomida yo‘l bosgan [10, 11].

TLS 1.3 ga profil sifatida integratsiya uning xavfsizlik xossalarini meros qiladi, bitta stekda xalqaro va milliy to‘plamlarni muzokara qilishga, mavjud kutubxonalarga modul sifatida qo‘shishga va IANA orqali ro‘yxatdan o‘tishga imkon beradi, ammo TLS 1.3 doirasidan tashqaridagi talablarni (masalan, ikki sertifikat modelini) aks ettira olmaydi. TLCP ga o‘xshash mustaqil protokol istalgan milliy talabni kiritishga imkon bersa-da, to‘liq qayta xavfsizlik tahlili, alohida stek va protokol standartini talab qiladi hamda standart TLS mijozlari bilan mos kelmaydi. Shu sababli texnik jihatdan profil yondashuvi maqsadga muvofiqroq; mustaqil protokol faqat TLS 1.3 da qondirib bo‘lmaydigan me’yoriy talablar mavjud bo‘lgandagina asoslanadi.

Post-kvant omili

NIST 2024-yilda ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism – modul panjaralarga asoslangan kalit inkapsulyatsiyalash mexanizmi) ni FIPS (Federal Information Processing Standards – federal axborotga ishlov berish standartlari) 203 sifatida tasdiqladi [20], IETF esa 2026-yilda uni ECDHE bilan birlashtiruvchi gibrid guruhlarni (masalan, X25519MLKEM768) Proposed Standard sifatida e’lon qildi [21]. PQC (Post-Quantum Cryptography – post-kvant kriptografiya) ga o‘tish ham “supported_groups” mexanizmiga tayangani uchun milliy profil kriptografik chaqqonlikni (crypto-agility) va milliy egri chiziq bilan post-kvant KEM ning gibrid guruhlarini ko‘zda tutishi lozim.

Xulosa

TLS 1.3 ning amaldagi spetsifikatsiyasi – RFC 9846 (2026); undagi shifr to‘plami, kalit almashish guruhi va imzo sxemasini mustaqil Handshake modeli milliy algoritmlarni protokol mantiqini o‘zgartirmasdan qo‘shish imkonini beradi.

Rossiya (Informational RFC 9189, 9367) va Belarus (STB 34.101.90-2026, Internet-Draft) yondashuvlari TLS ning milliy kriptografik profillari, Xitoyning TLCP (GB/T 38636-2020) standarti esa mustaqil milliy protokoldir.

O‘zMSt 270, 285 va 286 (2024) milliy profil uchun shifr, xesh va imzo asosini beradi, biroq milliy blokli shifr uchun AEAD rejimi, efemer kalit kelishuvi, nomlangan egri chiziqlar va kod nuqtalari hali belgilanmagan. O‘zbekiston uchun asoslanganroq yo‘l – ushbu elementlarni standartlashtirib, TLS 1.3 arxitekturasini saqlagan holda milliy algoritmlarni profil sifatida integratsiya qilish va post-kvant gibrid mexanizmlarni oldindan ko‘zda tutish.

Foydalanilgan adabiyotlar

1. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 9846. IETF, July 2026.
2. Fielding R., Nottingham M., Reschke J. (eds.). HTTP Semantics. RFC 9110. IETF, June 2022.
3. Freier A., Karlton P., Kocher P. The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101 (Historic), 2011.
4. Dierks T., Allen C. The TLS Protocol Version 1.0. RFC 2246. IETF, 1999.
5. Dierks T., Rescorla E. The TLS Protocol Version 1.1. RFC 4346. IETF, 2006.
6. Dierks T., Rescorla E. The TLS Protocol Version 1.2. RFC 5246. IETF, 2008.
7. Rescorla E. The TLS Protocol Version 1.3. RFC 8446. IETF, 2018.
8. Moriarty K., Farrell S. Deprecating TLS 1.0 and TLS 1.1. RFC 8996. IETF, 2021.
9. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, 2010.

10. Smyshlyaev S. (ed.) et al. GOST Cipher Suites for TLS Protocol Version 1.2. RFC 9189 (Informational, Independent Submission), 2022.

11. Smyshlyaev S. (ed.) et al. GOST Cipher Suites for TLS Protocol Version 1.3. RFC 9367 (Informational, Independent Submission), 2023.

12. Dolmatov V. (ed.), Degtyarev A. GOST R 34.10-2012: Digital Signature Algorithm. RFC 7091, 2013.

13. Agievich S., Kalosha N. STB Cryptographic Parameters for TLS Protocol Version 1.3. Internet-Draft draft-kalosha-stb-tls13-00 (work in progress), 2026.

14. STB 34.101.90-2026. Information technology and security. The Transport Layer Security Protocol Version 1.3. Minsk, 2026.

15. GB/T 38636-2020. Information security technology – Transport layer cryptography protocol (TLCP). Beijing, 2020.

16. Yang P. ShangMi (SM) Cipher Suites for TLS 1.3. RFC 8998 (Informational, Independent Submission), 2021.

17. O‘zMSt 270:2024. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi. Toshkent: O‘zbekiston standartlar instituti, 2024.

18. O‘zMSt 285:2024. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi. Toshkent: O‘zbekiston standartlar instituti, 2024.

19. O‘zMSt 286:2024. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari. Toshkent: O‘zbekiston standartlar instituti, 2024.

20. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.

21. Kwiatkowski K. et al. Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3. RFC 10024. IETF, August 2026.

POST-KVANT KRIPTOGRAFIK ALGORITMLAR VA ULARNING VPN TIZIMLARI XAVFSIZLIGINI TA’MINLASHDAGI O‘RNI

Suyunov S.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Maqolada hozirgi kundagi shifirlash algoritimlariga kvant kompyuterlarining tug‘diradigan xavflari va u xavflarga mos ravishda yaratilayotgan post-kvant shifirlash algoritimlari ko‘rib chiqiladi.

Kalit so‘zlar: Shor algoritimi, Post-kvant kriptografiyasi, Kvant kompyuterlari, NIST, ML-KEM, ML-DSA, SLH-DSA, Virtual Private Network.

Аннотация: В статье рассматриваются угрозы, которые квантовые компьютеры представляют для современных алгоритмов шифрования, а также постквантовые алгоритмы шифрования, создаваемые для противодействия этим угрозам.

Ключевые слова: Алгоритм Шора, постквантовая криптография, квантовые компьютеры, NIST, ML-KEM, ML-DSA, SLH-DSA, VPN (виртуальная частная сеть).

Kirish

Shifrlash algoritmlari elektron pochta xabarlaridan tortib tibbiy yozuvlar va moliyaviy hisobotlargacha bo'lgan maxfiy elektron ma'lumotlarni ruxsatsiz tomoshabinlardan himoya qiladi. O'nlab yillar davomida ushbu algoritmlar shifrlashni buzishga urinayotgan an'anaviy kompyuterlar yordamida hujumlardan himoya qilish uchun yetarlicha kuchli ekanligini isbotladi. Biroq, kvant kompyuteri deb nomlangan yangi turdagi qurilma ushbu algoritmlarni buzishi va elektron sirlarimizni kashf etilishiga zaiflashtirishi mumkin. Ushbu yaqinlashib kelayotgan tahdidga qarshi turish uchun bizga bugungi kunda biladigan an'anaviy kompyuterlar va ertangi kun kvant kompyuterlarining kiberhujumlarini oldini oladigan shifrlash usullari kerak. Bu yangi usullar post-kvant shifrlash algoritmlari deb ataladi. Ilg‘or kvant kompyuterlarining yaratilishi ehtimoli yuqori. Ular bugungi kundagi shifrlash tizimlariga shu qadar kuchli ta’sir ko‘rsatadiki, hozirgi shifrlash algoritimlarini bunga tayyorlashimiz kerak.

Asosiy qisim. Agar kriptografik jihatdan ahamiyatli kvant kompyuteri yaratilsa, uning hujumlariga qarshi turish uchun jahon hamjamiyati hozirgi shifrlash algoritmlaridan voz kechishi kerak. Kvantdan keyingi (post-kvant) shifrlash algoritmlari ham an’anaviy, ham kvant kompyuterlari uchun yechish qiyin bo‘lgan matematik masalalarga asoslanishi lozim. Ushbu algoritmlarni amaliyotga tatbiq etish maqsadida NIST (AQSh Standartlar va texnologiyalar milliy instituti) post-kvant shifrlash bo‘yicha texnik standartlarni ishlab chiqish ishlariga rahbarlik qildi. Mazkur standartlar turli vaziyatlar uchun yechimlar taqdim etishni, shifrlashda xilma-xil yondashuvlarni qo‘llashni hamda muayyan bir algoritm zaif bo‘lib chiqqan taqdirda, har bir qo‘llanilish sohasi uchun bir nechta muqobil algoritmlarni taklif etishni ko‘zlaydi.

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) - bu kvant kompyuterlari tahdidiga qarshi turish uchun ishlab chiqilgan, **post-kvant kriptografiyasi (PQC)** davrining eng yetakchi va asosiy kalit almashinuv algoritmidir. U 2024-yil avgust oyida AQSH Milliy standartlar va texnologiyalar instituti (NIST) tomonidan rasmiy ravishda **FIPS 203** standarti sifatida qabul qilingan. Bugungi kunda internet xavfsizligini (masalan, HTTPS brauzer ulanishlarini) ta'minlovchi RSA va ECDH kabi klassik algoritmlar kelajakda kuchli kvant kompyuterlari (Shor algoritmi) yordamida osongina buzilishi mumkin.

ML-KEM esa shifrlangan aloqa o‘rnatishdan oldin ikki tomonning o‘zaro **maxfiy simmetrik kalitni (Shared Secret)** xavfsiz almashib olishini ta'minlaydi va buni kvant hujumlaridan himoyalangan holda amalga oshiradi. Klassik algoritmlar katta tub sonlarni ko‘paytirish yoki diskret logarifmlarga asoslansa, ML-KEM **panjaralar geometriyasiga (Lattice-based cryptography)** hamda **Module-LWE (Module Learning With Errors)** deb ataladigan murakkab matematik muammoga tayanadi.

ML-DSA (Module-Lattice-Based Digital Signature Algorithm) - bu kvant kompyuterlari tahdidiga qarshi turish uchun ishlab chiqilgan, panjaralarga asoslangan **post-kvant raqamli imzo algoritmidir.** U **AQSH Milliy standartlar va texnologiyalar instituti (NIST)** tomonidan 2024-yil avgust oyida **FIPS 204** hujjati bilan rasmiy standart sifatida qabul qilingan.

ML-DSA algoritmi Fiat-Shamir with Aborts (rad etish orqali namuna olish) yondashuviga asoslangan bo‘lib, 3 ta asosiy operatsiyadan iborat:

– ML-DSA.KeyGen (Kalit yaratish): Matematik panjaralar asosida ochiq (public) va yopiq (private) kalitlar juftligini hosil qiladi.

– ML-DSA.Sign (Imzolash)**:** Maxfiy yopiq kalit yordamida xabarga raqamli imzo biriktiriladi. Xavfsizlik yuzasidan tasodifiy nomzod imzo yaratiladi, agar u xavfsizlik cheklovlaridan (norma tekshiruvidan) o‘tmasa, jarayon qaytadan takrorlanadi (o‘rtacha 4-5 marta).

– ML-DSA.Verify (Tekshirish): Ochiq kalit yordamida imzo haqiqiyligi va ma'lumotlar o‘zgartirilmaganligi (yaxlitligi) soniyaning kichik bo‘laklarida tasdiqlanadi.

SLH-DSA (*Stateless Hash-Based Digital Signature Algorithm* - Kvantdan keyingi holatsiz xesh-asosli raqamli imzo algoritmi) - bu kvant kompyuterlarining hujumlariga qarshi tura oladigan va butunlay xesh-funksiyalarga asoslangan raqamli imzo standartidir. AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan 2024-yil 13-avgustda FIPS 205 rasmiy standarti sifatida qabul qilingan.

VPN tunellarini qurishda asosan ikki turdagi post-kvant algoritmlaridan foydalaniladi: Kalitlarni uzatish (Key Encapsulation / KEX) va Raqamli imzo (Autentifikatsiya) ML-KEM (FIPS 203): NIST tomonidan standartlashtirilgan bo'lib, uning ML-KEM-768 versiyasi VPN protokollarida eng ko'p afzal ko'rilayotgan standartdir. Qo'llanilishi**:** Hozirgi o'tish davrida xavfsizlikni kafolatlash uchun u Gibrid usulda (Hybrid KEX) ishlatiladi. Masalan, klassik algoritm (X25519) va post-kvant algoritmi (MLKEM768+X25519) birgalikda qo'llanadi. Agar post-kvant algoritmida kutilmagan zaiflik topilsa ham, an'anaviy algoritm tunnelni himoya qilib turadi.

Tuneldagi foydalanuvchi yoki server kimligini tasdiqlash (shaxsni tekshirish) uchun quyidagi raqamli imzolar qo'llanilmoqda:

– ML-DSA (Dilithium / FIPS 204): Panjaralarga (lattice) asoslangan va VPN qurilmalarining dasturiy ta'minotini hamda sertifikatlarini (X.509) tekshirishda asosiy algoritm hisoblanadi.

– SLH-DSA (SPHINCS+ / FIPS 205): Xesh-funksiyalarga asoslangan bo'lib, uzoq muddatli xavfsizlik va Root sertifikatlar (Root CA) uchun VPN infratuzilmasida ishlatiladi.

– O‘zbekistonda Post-kvant kriptografiyasi (PQC) sohasidagi ishlar asosan akademik tadqiqotlar, milliy standartlashtirishga tayyorgarlik va kiberxavfsizlik infratuzilmasini modernizatsiya qilish yo‘nalishlarida olib borilmoqda. Kvant kompyuterlarining an’anaviy shifrlash algoritmlariga (RSA, ECC) solayotgan tahdidlari ortishi fonida, mamlakatimiz axborot xavfsizligi mutaxassislari va ilmiy jamiyati ushbu yo‘nalishga jiddiy e’tibor qaratmoqda.

Hozirgi kunda O‘zbekistonda post-kvant kriptografiyasi bo‘yicha amalga oshirilayotgan asosiy ishlar quyidagilardan iborat:

– Ilmiy-tadqiqot ishlari va Akademik tahlillar**.** Mamlakatdagi yetakchi texnik oliy ta’lim muassasalari (masalan, TATU, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti va boshqa ilmiy institutlar) olimlari tomonidan keng qamrovli tadqiqotlar olib borilmoqda: Matematik asoslarni o‘rganish: Panjara-asosli (lattice-based), kod-asosli (code-based), hash-asosli va ko‘p o‘zgaruvchili kvadratik tenglamalarga asoslangan kriptotizimlar tahlil qilinmoqda. NIST standartlari tahlili: AQShning NIST (Milliy standartlar va texnologiyalar instituti) tomonidan tasdiqlangan CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON va SPHINCS+ kabi algoritmlarning texnik xususiyatlari va samaradorligi mahalliy mualliflar tomonidan o‘rganilib, ilmiy maqolalar chop etilmoqda. Muqobil algoritmlar ustida ishlash: NTRU shifrlash va polinomlar yordamida shifrlash kabi kvantga chidamli algoritmlarni o‘rganish bo‘yicha ham izlanishlar mavjud.

– Amaliy modellar va Kutubxonalarni o‘rganish. Nazariy tadqiqotlardan tashqari, amaliy dasturiy tizimlarga post-kvant xavfsizligini integratsiya qilish tajribalari boshlangan: Gibrid post-kvant modellari: Taqsimlangan tizimlarda API xavfsizligini ta’minlash uchun gibrid (an’anaviy va post-kvant algoritmlari birgalikda ishlatiladigan) modellarni ishlab chiqish ustida tadqiqotlar olib borilmoqda. Dasturiy kutubxonalar tahlili: Mahalliy tadqiqotchilar dunyoda ochiq manbali hisoblangan liboqs, Microsoft PQCrypto, CIRCL va PQClean kabi post-kvant kutubxonalarining ishlash tezligi va xotira sarfini qiyosiy baholamoqdalar.

– Migratsiya va Raqamli Suverenitet strategiyasi. Kiberxavfsizlik sohasidagi davlat idoralari va strategik tashkilotlar uchun milliy xavfsizlik nuqtayi nazaridan post-kvant davriga o‘tish (migratsiya) strategiyalari taklif qilinmoqda: Kripto-chaqqonlik (Crypto-agility): Axborot tizimlarini kelajakda eski algoritmlardan yangi post-kvant algoritmlariga oson va tizimni to‘xtatmasdan o‘tkaza olish qobiliyatini (kripto-chaqqonlik) shakllantirish bo‘yicha tavsiyalar ishlab chiqilmoqda. Moliyaviy va Bank sektori: Mastercard kabi xalqaro tizimlar bilan hamkorlikda O‘zbekiston moliya institutlari uchun kvant migratsiyasining texnologik va tartibga solish murakkabliklarini hal qilish bo‘yicha amaliy ko‘rsatmalar berilmoqda.

Xulosa

Kvant kompyuterlari hozirgi kunda yaratilmagan bo‘lsada yaqin kelajakda klassik shifirlash algortimlari jiddiy muammo duch kelishi aniq bo‘lib bormoqda shu sababli xalqaro hamjamiyat post-kvant algoritimlari yartish ustida jiddiy ish olib bormoqda.

Foydalanilgan internet saytlari:

1. https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography
2. https://csrc.nist.gov/projects/post-quantum-cryptography
3. https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc

RESURS JIHATDAN CHEKLANGAN IOT QURILMALARI UCHUN YENGIL KIRISHNI ANIQLASH TIZIMLARI: RESURS BYUDJETIGA ASOSLANGAN QAROR QABUL QILISH MODELI

Maxamatjonov I.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada resurs jihatdan cheklangan qurilmalar uchun yengil IDS (L-IDS) yondashuvlari tizimli adabiyotlar tahlili asosida ko‘rib chiqiladi. Shuningdek, qurilmaning resurs byudjeti hamda mahalliy tasniflash bilan bulutga topshirish o‘rtasidagi tanlovni tavsiflovchi rasmiy model taklif etiladi.

Kalit so‘zlar: Internet buyumlar xavfsizligi, yengil kirishni aniqlash tizimi, resurslari cheklangan qurilmalar, modelni siqish, edge-cloud arxitekturasi, qaror qabul qilish qoidasi.

Аннотация. В данной статье на основе систематического анализа научной литературы рассматриваются подходы к разработке облегчённых систем обнаружения вторжений (L-IDS) для устройств с ограниченными вычислительными ресурсами. Кроме того, предлагается формальная модель, описывающая ресурсный бюджет устройства и выбор между локальной классификацией и передачей обработки данных в облачную среду.

Ключевые слова: безопасность Интернета вещей (IoT), облегчённая система обнаружения вторжений, устройства с ограниченными ресурсами, сжатие моделей, архитектура Edge–Cloud, правило принятия решений.

Kirish

Internet buyumlar (IoT) qurilmalari bugungi kunda salomatlikni masofadan kuzatish, sanoat boshqaruvi va past quvvatli sensor tarmoqlarining asosini tashkil etadi. Biroq ularning xotira, hisoblash quvvati va energiya bo‘yicha qattiq cheklovlari ushbu qurilmalarni ilg‘or doimiy tahdidlar, xizmat ko‘rsatishni rad etish (DoS/DDoS) hujumlari va ma’lumotlar sizib chiqishi uchun jozibador hamda ko‘pincha oson nishonga aylantiradi [1]. An’anaviy, resurs talab qiluvchi yuqori sig‘imli IDS yechimlarini bunday qurilmalarda bevosita joriy etish amaliy jihatdan imkonsiz bo‘lib qolmoqda. Shu sababli yengil IDS (L-IDS) yo‘nalishi mustaqil tadqiqot maydoniga aylandi.

Mensah, Makhamatdjonov, Jin va Yu (2025) tomonidan o‘tkazilgan tizimli tadqiqot [1] L-IDS aniqlash usullarini signaturalarga asoslangan (misuse-based) va anomaliyalarga asoslangan (anomaly-based) turlarga ajratadi hamda ularning kechikish, model hajmi, energiya iste’moli va aniqlik bo‘yicha o‘zaro murosalarini (trade-offs) taqqoslaydi. Alohida olganda, yengil usullar protokolga xos nihoyatda qattiq byudjetlarga javob bera oladi. Masalan, 500 KB SRAMga ega ESP32 mikrokontrollerida ishlagan CatBoost asosidagi tasniflagich DoS/MITM hujumlarini 99 foizdan ortiq aniqlik bilan, atigi 276 mikrosoniyalik kechikishda aniqlagan [2]. Bilim distillyatsiyasi chuqur aniqlash modelining parametrlar sonini 70 foizga qisqartirib, STM32L4 mikrokontrollerida 10 millisoniyadan kam xulosa chiqarish vaqtini ta’minlagan [3], dinamik kvantlash esa modelni 4 MB dan 512 KB gacha kichraytirib, taxminan 92 foizlik aniqlikni saqlab qolgan [4].

Signaturaga asoslangan usullar ma’lum hujumlarda yuqori aniqlik va past yolg‘on signal darajasini ta’minlaydi, biroq ular nol kunlik (zero-day) hujumlarni yomon qamrab oladi va signatura bazasini doimiy yangilab turishni talab qiladi. Anomaliyaga asoslangan usullar esa, aksincha, ko‘rilmagan hujumlarga yaxshi umumlashadi, lekin ularda yolg‘on signal darajasi va o‘qitish xarajati yuqoriroq bo‘ladi [1]. Shu sababli eng kuchli so‘nggi takliflar ikkala yondashuvni - ko‘pincha CNN-BiLSTM yoki chuqur o‘qitish va avtoenkoder asosidagi gibrid arxitekturalarni - model siqish texnikalari bilan birgalikda qo‘llaydi. Baholashda odatda CICIDS2017, UNSW-NB15 va Edge-IIoTset kabi etalon ma’lumotlar to‘plamlaridan foydalaniladi, biroq bu to‘plamlar

asosan hajmli yoki signaturasi aniq ko‘rinadigan hujumlarni (DoS, port skanerlash) qamrab oladi [1].

Protokol darajasida resurs chegaralari ham keskin farqlanadi: MQTT uchun 16 KB model byudjeti va soatiga 1 mAh dan kam energiya sarfi doirasida 5 millisoniyadan kam kechikish talab etilsa, Modbus 256 KB va 50 mVt doirasida 10 mikrosoniyadan kam kechikishni talab qiladi. LoRaWAN 128 KB byudjet va kuniga 0,5 mAh doirasida 300 millisoniyagacha kechikishga yo‘l qo‘yadi, CoAP esa 8 KB va 500 mikroamper doirasida 20 millisoniyadan kam kechikishni talab qiladi [1]. Demak, har bir protokol o‘ziga xos resurs chegaralariga ega va barcha holatlar uchun yagona mos model arxitekturasi mavjud emas.

Bu natijalarni umumlashtirish uchun qurilmaning resurs byudjetini uchlik ko‘rinishida ifodalash qulay: $B = (M_{\max}, T_{\max}, E_{\max})$, bunda $M_{\max}$ - ruxsat etilgan maksimal model hajmi, $T_{\max}$ - maksimal xulosa chiqarish kechikishi, $E_{\max}$ - maksimal energiya sarfi. Berilgan M modeli protokolga joriy etish uchun yaroqli hisoblanadi, agar uning hajmi, kechikishi va energiya sarfi mos ravishda shu uchta chegaradan oshmasa:

$$\text{Valid}(M) \Leftrightarrow \text{size}(M) \le M_{\max} \wedge T(M) \le T_{\max} \wedge E(M) \le E_{\max} \qquad (1)$$

Bu shart kon’yunksiya sifatida qurilgan: modelning faqat bitta ko‘rsatkich bo‘yicha ustunligi (masalan, yuqori aniqlik) qolgan chegaralardan birortasi buzilgan taqdirda uni qurilmaga yaroqsiz qiladi. 1-jadvalda ikkita keng tarqalgan IoT protokoli - MQTT va Modbus - uchun shu uchlikning qiymatlari keltirilgan [1].

1-jadval.

MQTT va Modbus protokollari uchun resurs byudjeti $B = (M_{max}, T_{max}, E_{max})$

Protokol	$T_{\max}$ (kechikish)	$M_{\max}$ (model hajmi)	$E_{\max}$ (energiya)	Maqsadli qurilma
MQTT	< 5 ms	16 KB	< 1 mAh/soat	ESP32
Modbus	< 10 µs	256 KB	< 50 mVt	Raspberry Pi / FPGA shlyuzi

E’tiborlisi, $B = (M_{\max}, T_{\max}, E_{\max})$ chegaralari protokoldan protokolga keskin farq qiladi: Modbus uchun kechikish chegarasi mikrosoniyalar darajasida bo‘lsa, MQTT uchun millisoniyalar darajasida, biroq MQTTda model hajmi va energiya chegaralari ancha qattiqroq. Bu farq barcha protokollar uchun yagona universal L-IDS yechimi mavjud emasligini, aksincha, har bir protokol uchun alohida $\text{Valid}(M)$ tekshiruvidan o‘tgan model tanlanishi lozimligini ko‘rsatadi.

Qurilma resurslari qanchalik puxta optimallashtirilmasin, yengil model butun tarmoq trafigini bir xil ishonch darajasida tasniflay olmasligi mumkin. Shu sababli so‘nggi ishlarda edge qatlamidagi tezkor tasniflashni bulutdagi kengroq hisoblash resurslariga ega tahlil bilan birlashtiruvchi federativ edge-cloud arxitekturasi taklif qilingan; bu yondashuv taxminan 95,6 foizlik umumiy aniqlikka erishgan [5]. Bunday arxitekturada asosiy muammo - qaysi holatlarni qurilmaning o‘zi hal qilishi, qaysilarini esa bulutga topshirish kerakligini aniqlashdir.

Buni rasmiylashtirish uchun x xususiyatlar vektori bo‘yicha chekka (edge) modeli M_{edge} hisoblagan ishonch darajasi $c(x) \in [0,1]$ va oldindan belgilangan chegara qiymati θ kiritiladi. $D(x)$ qaror funksiyasi quyidagicha aniqlanadi:

$$D(x) = \begin{cases} \text{mahalliy, agar } c(x) \ge \theta \wedge \text{Valid}(M_{\text{edge}}); \\ \text{bulutga yuborish, aks holda.} \end{cases} \qquad (2)$$

$D(x)$ qoidasi ikki shartning kon’yunksiyasiga tayanadi: model nafaqat yetarli ishonch bilan tasniflashi, balki (1)-tenglamadagi resurs byudjetiga ham mos kelishi kerak. Agar $c(x)$ past bo‘lsa yoki M_{edge} joriy qurilmada $\text{Valid}(M_{\text{edge}})$ shartini qanoatlantirmasa, qaror bulutga topshiriladi. Bu federativ arxitekturaning yuqori aniqligini [5] mahalliy modelning qattiq resurs chegaralari bilan muvofiqlashtirish imkonini beradi. θ qiymatini tanlash aniqlik va kechikish o‘rtasidagi amaliy murosaga bog‘liq: past θ ko‘proq holatni mahalliy hal qiladi va mahalliy xatolik ehtimolini oshiradi, yuqori θ esa ko‘proq holatni bulutga yo‘naltirib, tarmoq kechikishini oshiradi.

Masalan, ESP32 platformasida ishlaydigan CatBoost asosidagi M_{edge} 276 mikrosoniyalik kechikishda yuqori ishonch bilan tasniflagan trafik uchun $D(x)$ mahalliy qarorni tanlaydi: bunday kechikish MQTT uchun belgilangan $T_{\max} = 5$ ms chegarasidan ancha past [2], shuning uchun

model hajmi va energiya sarfi ham chegaradan oshmasa, $\mathrm{Valid}(M_{\mathrm{edge}})$ sharti bajariladi. Biroq o‘qitish ma’lumotlarida kam uchraydigan yoki yangi hujum turiga oid trafik uchun $c(x)$ past bo‘ladi, chunki model bunday naqshlarni ishonchli tasniflashga o‘rgatilmagan. Bunday holatda $D(x)$ qarorni bulutga yo‘naltiradi va u yerda kengroq hisoblash resurslariga ega, ehtimol federativ tarzda o‘qitilgan model [5] qo‘shimcha tahlil o‘tkazadi. Shu tariqa $D(x)$ qoidasi mahalliy tezkorlik bilan bulut aniqligi o‘rtasidagi muvozanatni avtomatik ta’minlaydi, bu esa qo‘lda sozlanadigan statik chegaralarga nisbatan ustunlikdir.

Apparat darajasidagi optimallashtirish ham shu byudjet mantig‘iga mos keladi. Modbus protokoli uchun FPGA asosida amalga oshirilgan funksiya kodlarini filtrlash o‘tkazuvchanlikni uch baravar oshirib, protsessor yukini 50 foizdan 15 foizgacha kamaytirgan [6]; bu $T(M)$ va $E(M)$ qiymatlarini bir vaqtda pasaytirib, $\mathrm{Valid}(M)$ sharti kengroq model sinflari uchun bajarilishini ta’minlaydi. Shu bilan birga, rejalashtirishga asoslangan moslashuvchan model boshqaruvi joriy batareya va xotira zaxirasiga qarab qaysi anomaliya modelini yuklangan holda saqlashni tanlaydi va shu orqali $M_{\max}$ hamda $E_{\max}$ chegaralarining vaqt bo‘yicha o‘zgarishini hisobga oladi [10].

Aniqlash usullarining o‘zi ham xilma-xil: CNN-BiLSTM gibrid arxitekturasi UNSW-NB15 to‘plamida yaxshi natija ko‘rsatgan bo‘lsa-da, NSL-KDD to‘plamiga yomon umumlashgan, bu esa uning barqarorligida muammolar borligidan dalolat beradi [7]. Sinflar nomutanosibligini S2CGAN asosida hal qiluvchi yondashuv [8], ko‘rilmagan hujum turlari uchun ochiq to‘plamli aniqlash sxemasi [9] va mikrokontrollerlarda TinyML yordamida ishlaydigan TinyIDS tizimi [11] ham shu resurs–aniqlik murosasi doirasida taklif etilgan. Biroq o‘rganilgan adabiyotlarda aniqlash qiyinroq bo‘lgan hujum turlari - o‘rtadagi odam (MITM) hujumi, Heartbleed uslubidagi protokol zaifliklaridan foydalanish va fidya dasturiga (ransomware) o‘xshash ma’lumot sizib chiqishi - o‘qitish ma’lumotlarida ham, baholashda ham izchil ravishda yetarlicha e’tiborga olinmagan [1].

2-jadval.

L-IDS uchun qo‘llanilgan yengillashtirish usullari va erishilgan natijalar

Usul	Erishilgan natija	Platforma
CatBoost tasniflagich [2]	~99% aniqlik, 276 µs kechikish	ESP32
Bilim distillyatsiyasi [3]	parametrlar ~70% kamaygan, < 10 ms kechikish	STM32L4
Dinamik kvantlash [4]	4 MB → 512 KB, ~92% aniqlik saqlangan	ko‘rsatilmagan
Federativ edge-cloud [5]	~95,6% aniqlik	edge-cloud
FPGA asosidagi Modbus [6]	o‘tkazuvchanlik 3×, CPU yuki 50% → 15%	FPGA shlyuzi

2-jadvaldagi natijalar shuni ko‘rsatadiki, bu besh usulning har biri $B = (M_{\max}, T_{\max}, E_{\max})$ byudjetining faqat bir yoki ikki o‘lchamiga ta’sir qiladi va hech biri uchala o‘lchamni bir vaqtda optimallashtirmaydi. Model siqish usullari (bilim distillyatsiyasi, dinamik kvantlash) asosan $\mathrm{size}(M)$ va $T(M)$ ni kamaytiradi, chunki kichikroq model odatda tezroq hisoblanadi. Apparat tezlashtirish (FPGA) $T(M)$ va $E(M)$ ni bir vaqtda pasaytiradi, chunki maxsus mantiqiy sxema umumiy maqsadli protsessorga qaraganda kamroq takt va energiya sarflaydi. Federativ edge-cloud arxitekturasi esa model ko‘rsatkichlarini o‘zgartirmaydi, balki $D(x)$ qoidasi orqali qiyin holatlarni boshqa resurs muhitiga - bulutga - ko‘chirib, aniqlikni oshiradi. Shu sababli bu usullar o‘zaro almashtiriluvchi emas, balki bir-birini to‘ldiruvchi hisoblanadi va amaliy L-IDS tizimi ularni (1)-tenglamadagi byudjet va (2)-tenglamadagi qaror qabul qilish mantig‘i orqali birlashtirgan holda qo‘llashi lozim.

L-IDS qurilmalari ko‘pincha xabar almashinuv kanalini himoya qilish uchun yengil kriptografik primitivlarga ham muhtoj, chunki to‘liq TLS stekini ishga tushirish xuddi shu $M_{\max}$ va $E_{\max}$ chegaralarini buzishi mumkin. AQSh Milliy standartlar va texnologiyalar instituti (NIST) 2025-yilda e’lon qilgan Ascon asosidagi yengil kriptografiya standarti aynan shunday cheklangan qurilmalar uchun autentifikatsiyalangan shifrlash va xesh funksiyalarini ta’minlashga qaratilgan [12]. Bu L-IDS resurs byudjeti bilan bir xil muammo maydonida yotadi: xavfsizlik mexanizmi o‘zi himoya qilayotgan qurilmaning resurslarini tugatib qo‘ymasligi kerak. ISO/IEC 27400:2022 standarti ham IoT qurilmalarining butun hayotiy sikli davomida xavfsizlik va maxfiylik bo‘yicha yo‘riqnomalarni belgilaydi hamda resurslari cheklangan qurilmalarda xavfsizlik mexanizmlarini

qurilmaning real imkoniyatlariga moslashtirish zarurligini ta’kidlaydi [13]; bu esa taklif etilgan $\mathrm{Valid}(M)$ shartining kengroq me’yoriy asosga mos ekanini ko‘rsatadi.

Taklif etilgan $B = (M_{\max}, T_{\max}, E_{\max})$ va $D(x)$ formalizatsiyasini sinab ko‘rish uchun ikkita sinov stendi mos keladi: ESP32 darajasidagi mikrokontrollerga asoslangan MQTT sensor tuguni va Raspberry Pi darajasidagi shlyuzga asoslangan Modbus konfiguratsiyasi, chunki aynan shu ikki protokol uchun 1-jadvaldagi aniq, manbaga tayangan kechikish, xotira va energiya ko‘rsatkichlari mavjud [1]. Baholash trafigi an’anaviy DoS va skanerlash hujumlaridan tashqari adabiyotlarda yetarlicha e’tiborga olinmagan uchta sinfni ham o‘z ichiga olishi lozim [1]: ARP/ICMP-redirect uslubidagi MITM trafigi, protokol shlyuziga qarshi qayta yuborilgan noto‘g‘ri handshake/heartbeat so‘rovlari (Heartbleed sinfi) va bosqichma-bosqich katta hajmli yuklama ko‘rinishidagi fidya dasturiga o‘xshash sizib chiqish trafigi. Bunday kengaytirilgan stsenariy $D(x)$ qoidasining aynan yangi, ko‘rilmagan hujum turlarida qanchalik to‘g‘ri ishlashini, ya’ni past ishonch darajasiga ega holatlarni bulutga to‘g‘ri yo‘naltirishini tekshirish imkonini beradi.

Taklif etilgan modelning bir qancha cheklovlari ham mavjud. Birinchidan, sintetik tarzda yaratilgan Heartbleed sinfidagi va fidya dasturiga o‘xshash trafik haqiqiy tajovuzkorning moslashuvchan xatti-harakatini to‘liq aks ettirmasligi mumkin, shuning uchun $D(x)$ asosidagi baholash natijalarini haqiqiy sharoitdagi ishlash kafolati sifatida emas, balki aniqlash qiyinligining quyi chegarasi sifatida talqin qilish kerak. Ikkinchidan, qaysi modelni yuklangan holda saqlashni tanlovchi ish vaqti siyosatining o‘zi qo‘shimcha xotira va hisoblash yukini talab qiladi; buni MQTTning soatiga 1 mAh dan kam energiya chegarasi kabi allaqachon qattiq $M_{\max}$ va $E_{\max}$ cheklovlari doirasida alohida hisobga olish shart. Uchinchidan, qamrov ataylab ikki protokol - MQTT va Modbus - bilan cheklangan; yondashuvni LoRaWAN va CoAP kabi boshqa protokollarga umumlashtirish kelajakdagi ishlar vazifasidir.

Xulosa

Resurslari cheklangan IoT qurilmalari uchun yengil kirishni aniqlash sohasida alohida model siqish va apparat tezlashtirish usullari yaxshi o‘rganilgan, biroq ularni yagona, protokolga moslashuvchan qaror qabul qilish mantig‘iga birlashtirish hali to‘liq hal etilmagan masala bo‘lib qolmoqda. Ushbu maqolada taklif etilgan $B = (M_{\max}, T_{\max}, E_{\max})$ resurs byudjeti va unga asoslangan $\mathrm{Valid}(M)$ hamda $D(x)$ formalizatsiyasi mavjud empirik natijalarni - CatBoost tasniflagichining 276 mikrosoniyalik kechikishidan tortib federativ edge-cloud arxitekturasining 95,6 foizlik aniqligigacha - yagona analitik asosda birlashtirish imkonini beradi.

Taklif etilgan formalizatsiyaning amaliy qiymati shundaki, u model siqish, apparat tezlashtirish va edge-cloud hamkorligini raqobatdosh emas, balki bir-birini to‘ldiruvchi vositalar sifatida ko‘rsatadi: ularning har biri $B = (M_{\max}, T_{\max}, E_{\max})$ uchligining turli o‘lchamiga ta’sir qiladi, $D(x)$ esa ularni yagona amaliy qaror qoidasiga bog‘laydi. Keyingi bosqichda ushbu model qurilma buzilgandan keyin eng xavfli bo‘lgan MITM, Heartbleed uslubidagi va fidya dasturiga o‘xshash hujum turlarini o‘z ichiga olgan kengaytirilgan baholash stsenariysi asosida ESP32 asosidagi MQTT va Raspberry Pi asosidagi Modbus sinov stendlarida sinovdan o‘tkazilishi rejalashtirilgan. Shu tariqa ushbu ish adabiyotlarda aniqlangan bo‘shliqni protokolga moslashuvchan, formal asoslangan va sinovdan o‘tkazish mumkin bo‘lgan aniq ilmiy hissaga aylantirishni maqsad qiladi.

Foydalanilgan adabiyotlar

1. Mensah, C., Makhamatdjonov, I., Jin, H., & Yu, S. (2025). SoK: Lightweight intrusion detection and automated response for resource-constrained IoT embedded systems [Unpublished coursework report, COM6017: Security of Control and Embedded Systems]. University of Sheffield.

2. Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). Review of recent intrusion detection systems and intrusion prevention systems in IoT networks. In 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1–6).

3. Hasan, T., Hossain, A., Ansari, M. Q., & Syed, T. H. (2025). Enhanced intrusion detection in IIoT networks: A lightweight approach with autoencoder-based feature learning (arXiv:2501.15266). arXiv. https://doi.org/10.48550/arXiv.2501.15266

4. Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., & Wang, J. (2023). A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. PeerJ Computer Science, 9, e1569. https://doi.org/10.7717/peerj-cs.1569

5. Belarbi, O., Spyridopoulos, T., Anthi, E., Mavromatis, I., Carnelli, P., & Khan, A. (2023). Federated deep learning for intrusion detection in IoT networks. In GLOBECOM 2023 – 2023 IEEE Global Communications Conference (pp. 237–242).

6. Mofidi, F., Hounsinou, S., & Bloom, G. (2023). L-IDS: A lightweight hardware-assisted IDS for IoT systems to detect ransomware attacks. In Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI '23) (pp. 464–465). ACM. https://doi.org/10.1145/3576842.3589170

7. Jouhari, M., & Guizani, M. (2024). Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices. In 2024 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1558–1563).

8. Wang, C., Xu, D., Li, Z., & Niyato, D. (2024). Effective intrusion detection in highly imbalanced IoT networks with lightweight S2CGAN-IDS. IEEE Internet of Things Journal, 11, 15140–15151.

9. Yang, X., Tong, F., Jiang, F., & Cheng, G. (2025). A lightweight and dynamic open-set intrusion detection for industrial internet of things. IEEE Transactions on Information Forensics and Security, 20, 2930–2943.

10. Mirzaei, A., Coban, A. Z., Almgren, M., Aoudi, W., & Bertilsson, T. (2023). Scheduling to the rescue: Improving ML-based intrusion detection for IoT. In Proceedings of the 16th European Workshop on System Security (EuroSec '23) (pp. 44–50). ACM.

11. Fusco, P., Rimoli, G. P., & Ficco, M. (2024). TinyIDS - An IoT intrusion detection system by tiny machine learning. In Computational Science and Its Applications – ICCSA 2024 Workshops (pp. 71–82). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65223-3_5

12. National Institute of Standards and Technology. (2025). Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions (NIST Special Publication 800-232). https://doi.org/10.6028/NIST.SP.800-232

13. International Organization for Standardization & International Electrotechnical Commission. (2022). Cybersecurity - IoT security and privacy - Guidelines (ISO/IEC 27400:2022). ISO.

KVANT KALITLARNI TAQSIMLASH VA POSTKVANT KEM ALGORITMLARINING QIYOSIY TAHLILI

Xudoykulov Z.T., Baxodirov D.U.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda kvant kompyuter xavfiga qarshi kalit kelishuvining ikki yondashuvi – fizik tamoyillarga asoslangan kvant kalitlarni taqsimlash va hisoblash murakkabligiga asoslangan postkvant kalitni inkapsulyatsiyalash mexanizmlari qiyoslangan. BB84 protokoli, kalit tezligining masofaga bog‘liqligi bo‘yicha fundamental chegara, autentifikatsiya talabi va amalga oshirish hujumlari, shuningdek ML-KEM va HQC ning parametrlari tahlil qilingan. 10 mezon bo‘yicha qiyosiy baho, xalqaro idoralar pozitsiyalari va O‘zbekiston uchun tavsiyalar keltirilgan.

Kalit so‘zlar: kvant kalitlarni taqsimlash; QKD; BB84; postkvant kriptografiya; KEM; ML-KEM; HQC; gibrid kalit kelishuvi; autentifikatsiya; ishonchli tugun.

Аннотация. В тезисах сопоставлены два подхода к выработке ключей в условиях угрозы квантового компьютера: квантовое распределение ключей, основанное на физических принципах, и постквантовые механизмы инкапсуляции ключа, основанные на вычислительной сложности. Проанализированы протокол BB84, фундаментальное ограничение скорости ключа в зависимости от расстояния, требование аутентификации и атаки на реализацию, а также параметры ML-KEM и HQC. Приведены сравнительная оценка по 10 критериям, позиции международных ведомств и рекомендации для Узбекистана.

Ключевые слова: квантовое распределение ключей; QKD; BB84; постквантовая криптография; KEM; ML-KEM; HQC; гибридная выработка ключа; аутентификация; доверенный узел.

Kirish

Shor algoritmi RSA, Diffi–Xellman va elliptik egri chiziqli kalit kelishuvini kriptografik ahamiyatli kvant kompyuterda polinomial vaqtda buzadi [1]; NIST (National Institute of Standards and Technology – AQSh Milliy standartlar va texnologiyalar instituti) bu algoritmlarni 2030-yildan keyin eskirgan, 2035-yildan keyin taqiqlangan deb belgilagan [2]. Kalit kelishuvini almashtirish uchun ikki yondashuv taklif etiladi: QKD (Quantum Key Distribution – kvant kalitlarni taqsimlash) – xavfsizligi kvant mexanikasi qonunlariga asoslangan fizik usul, va KEM (Key Encapsulation Mechanism – kalitni inkapsulyatsiyalash mexanizmi) ko‘rinishidagi PQC (Post-Quantum Cryptography – postkvant kriptografiya) – kvant kompyuter uchun ham qiyin deb hisoblanadigan matematik masalalarga asoslangan dasturiy usul. Tezisning maqsadi – ularni xavfsizlik asosi, amaliy cheklovlar va joriy etish nuqtai nazaridan qiyoslash.

Kvant kalitlarni taqsimlash: tamoyillar va cheklovlar

BB84 protokolida yuboruvchi har bir bitni ikki bazisdan tasodifan tanlangan birida foton holatiga kodlaydi; qabul qiluvchi ham bazisni tasodifan tanlab o‘lchaydi, so‘ng ochiq kanal orqali bazislar solishtiriladi [3]. Kvant holatni o‘lchash uni buzgani uchun tinglovchi xatolar ulushini – QBER (Quantum Bit Error Rate – kvant bitlar xatolik ulushi) ni oshiradi. Bir fotonli ideal manba uchun asimptotik maxfiy kalit ulushi [4]:

$$r = 1 - 2h(e),\ h(e) = -e\log_2 e - (1 - e)\log_2(1 - e), \quad (1)$$

bu yerda, e – QBER. Masalan, e = 3 % da r ≈ 0,61, e ≈ 11 % da r ≈ 0, ya'ni bundan katta xatolikda kalit hosil bo'lmaydi. QKDning xavfsizlik isboti klassik kanal *autentifikatsiyalangan* deb faraz qiladi. Axborot-nazariy autentifikatsiya (Wegman–Carter usuli) oldindan kelishilgan maxfiy kalitni talab qiladi [5], shuning uchun QKD aslida mavjud umumiy sirni «kengaytiradi»; ochiq kalitli imzo bilan autentifikatsiya qilinsa, xavfsizlik yana hisoblash farazlariga bog'lanadi.

Ikkinchi fundamental cheklov – masofa. Kvant takrorlagichlarsiz optik kanal uchun kalit tezligi (bitta kanaldan foydalanishga) quyidagicha chegaralangan [6]:

$$R \le -\log_2(1 - \eta) \approx 1{,}44\eta,\ \eta = 10\text{^}\{-\alpha L/10\}, \quad (2)$$

bu yerda, η – kanalning o'tkazish koeffitsiyenti, α – tolaning so'nish koeffitsiyenti, L – masofa. Standart tolada α ≈ 0,2 dB/km deb hisoblasak, L = 100 km da $R \le 1{,}45\cdot10^{-2}$, L = 300 km da esa $R \le 1{,}44\cdot10^{-6}$, ya'ni 1 GGs impuls chastotasida ham ideal holatda mos ravishda taxminan 14,5 Mbit/s va 1,4 kbit/s dan oshmaydi. Bu chegara masofa har 100 km ga oshganda tezlik taxminan 100 barobar kamayishini bildiradi. TF-QKD (Twin-Field QKD – egizak maydonli QKD) protokollari tezlikning √η ga proporsionalligi hisobiga bu chegaradan oshadi [7]: 1002 km tolada impuls boshiga $9{,}53\cdot10^{-12}$ bit asimptotik tezlik olingan [8]. Sun'iy yo'ldosh orqali QKD ham namoyish qilingan [9]. Amaliy QKD tarmoqlari oraliq ishonchli tugunlardan foydalanadi: kalit har bir tugunda ochiq holda bo'ladi va ular jismonan himoyalanishi kerak, ya'ni oxirdan-oxirgacha himoya ta'minlanmaydi; bunday tarmoqlar arxitekturasi ITU-T (International Telecommunication Union – Telecommunication Standardization Sector – Xalqaro elektraloqa ittifoqining standartlashtirish sektori) Y.3800 tavsiyasida bayon etilgan [10].

Uchinchi cheklov – amalga oshirish xavfsizligi. Nazariy isbot ideal qurilmalarni nazarda tutadi, real tizimlarda esa, masalan, tijorat QKD tizimlari detektorlarini yorqin nur bilan «ko'r qilish» hujumi namoyish etilgan [11]. Detektor zaifliklarini bartaraf etuvchi MDI-QKD (Measurement-Device-Independent QKD – o'lchash qurilmasidan mustaqil QKD) taklif qilingan [12], baholash talablari esa ISO/IEC (International Organization for Standardization / International Electrotechnical Commission – Xalqaro standartlashtirish tashkiloti / Xalqaro elektrotexnika komissiyasi) 23837 da standartlashtirilmoqda [13].

Postkvant KEM algoritmlari

KEM uch algoritmdan iborat: (pk, sk) ← KeyGen(); (c, K) ← Encaps(pk); K = Decaps(sk, c), bu yerda K – umumiy sir. NIST ning FIPS (Federal Information Processing Standards – federal axborotni qayta ishlash standartlari) 203 hujjatida standartlashtirilgan ML-KEM (Module-Lattice-Based KEM – modul panjaralarga asoslangan KEM) ning xavfsizligi MLWE (Module Learning With Errors – modul xatoli o'rganish) masalasiga asoslanadi va Fujisaki–Okamoto turidagi almashtirish orqali IND-CCA2 (Indistinguishability under Adaptive Chosen-Ciphertext Attack – moslashuvchan tanlangan shifrmatn hujumida farqlanmaslik) ma'nosida bardoshli qilingan [14]:

$$t = As + e, \quad (3)$$

bu yerda, A – ochiq tasodifiy matritsa, s va e – kichik koeffitsiyentli maxfiy vektorlar; t va A dan s ni topish kvant kompyuter uchun ham qiyin deb hisoblanadi. 2025-yilda NIST zaxira KEM sifatida kodlash nazariyasiga asoslangan HQC (Hamming Quasi-Cyclic – Xemming kvazitsiklik kodlari asosidagi KEM) ni tanladi [15]. Quyidagi jadvalda o'lchamlar keltirilgan.

1-jadval

Postkvant KEM larning parametrlari (baytlarda)

Algoritm	NIST darajasi	Ochiq kalit	Shifrmatn	Umumiy sir
ML-KEM-512	1	800	768	32

ML-KEM-768	3	1184	1088	32
ML-KEM-1024	5	1568	1568	32
HQC-128	1	≈ 2240	≈ 4430	32
X25519 (taqqoslash uchun)	klassik	32	32	32

KEM sof dasturiy usul bo‘lib, mavjud tarmoqlarda masofa cheklovisiz ishlaydi. RFC (Request for Comments – sharhlar uchun so‘rov) 10024 TLS (Transport Layer Security – transport qatlam xavfsizligi) 1.3 uchun X25519MLKEM768 kabi gibrid guruhlarni Proposed Standard sifatida belgilagan [16]: umumiy sir ECDH (Elliptic Curve Diffie–Hellman – elliptik egri chiziqli Diffi–Xellman) va ML-KEM natijalaridan olinadi va ulardan kamida biri buzilmagan bo‘lsa, himoya saqlanadi. KEM ning zaif tomonlari – xavfsizlikning shartsiz emasligi (MLWE farazi kriptotahlil qilinishda davom etadi) va amalga oshirishdagi yon-kanal xatolari; masalan, ML-KEM ning bir qator kutubxonalarida maxfiy qiymatga bog‘liq bo‘lish amali vaqti orqali kalitni tiklash mumkinligi ko‘rsatilgan [17]. Bunday xatolar dasturiy yangilanish bilan tuzatiladi.

2-jadval

QKD va postkvant KEM ning qiyosiy tavsifi

Mezon	QKD	Postkvant KEM (ML-KEM)
Xavfsizlik asosi	Fizika qonunlari; autentifikatsiya sharti bilan	Hisoblash murakkabligi (MLWE)
Autentifikatsiya	Alohida talab etiladi (oldindan kelishilgan kalit yoki imzo)	Imzo va sertifikatlar (PQC imzo)
Masofa	Cheklangan: har 100 km da tezlik ~100 barobar kamayadi; uzoq masofa – ishonchli tugunlar, TF-QKD yoki yo‘ldosh	Cheklanmagan
Kalit tezligi	Masofa bilan eksponensial kamayadi (2)	Hisoblash bilan cheklangan, yuqori
Infratuzilma	Maxsus optik uskunalar, ajratilgan tola	Mavjud tarmoq, dasturiy yangilanish
Oxirdan-oxirgacha himoya	Ishonchli tugunlarda yo‘q	Bor
Amalga oshirish hujumlari	Optik yon-kanallar; apparatni almashtirish kerak	Vaqt va quvvat bo‘yicha yon-kanallar; dasturiy tuzatiladi
Xizmat ko‘rsatishni rad etish	Kanalga ta’sir kalit hosil qilishni to‘xtatadi	Klassik tarmoq darajasida
Standartlashtirish	ITU-T Y.3800, ISO/IEC 23837 – tarmoq va baholash	FIPS 203, RFC 10024 – algoritm va protokol
Narx va masshtab	Yuqori, nuqtadan nuqtaga	Past, internet miqyosida

Xalqaro idoralar xulosalari bu qiyosga mos keladi. NSA (National Security Agency – AQSh Milliy xavfsizlik agentligi) QKDni milliy xavfsizlik tizimlari uchun tavsiya etmaydi, asosiy sabablar sifatida autentifikatsiya yo‘qligi, maxsus uskuna, ishonchli tugunlar xavfi, validatsiya qiyinligi va xizmat ko‘rsatishni rad etish xavfini ko‘rsatadi [18]. Fransiya, Germaniya, Niderlandiya va Shvetsiya idoralarining qo‘shma pozitsiyasiga ko‘ra QKD ning xavfsizlik yetukligi hali yetarli emas, u faqat tor sohalarda qo‘llanishi mumkin va ustuvorlik PQC ga berilishi

kerak [19]. Shu bilan birga, QKD kalit hosil qilishning hisoblash farazlaridan mustaqil yo‘lini beradi va uzoq muddat maxfiy saqlanadigan ma’lumotlar uchun ikki bog‘langan obyekt orasidagi magistral liniyalarda PQC ga qo‘shimcha bo‘lishi mumkin: bunda QKD va KEM kalitlari KDF (Key Derivation Function – kalit hosil qilish funksiyasi) orqali birlashtiriladi.

Xulosa

QKDning xavfsizligi fizik tamoyillarga asoslangan, ammo u faqat autentifikatsiyalangan kanal mavjud bo‘lganda kafolatlanadi, takrorlagichlarsiz kalit tezligi masofa bilan eksponensial kamayadi (100 km da ideal holatda bitta foydalanishga $1{,}45\cdot10^{-2}$ bitdan, 300 km da $1{,}44\cdot10^{-6}$ bitdan oshmaydi) va amaliy tarmoqlar ishonchli tugunlarga tayanadi.

Postkvant KEM (ML-KEM) hisoblash farazlariga asoslangan, lekin dasturiy, standartlashtirilgan, masofa cheklovisiz va mavjud protokollarga (TLS 1.3 gibrid guruhlari) qo‘shiladi; o‘lchamlari klassik ECDH dan bir necha o‘n barobar katta bo‘lsa-da, kilobayt tartibida qoladi.

Qiyosiy tahlil va xalqaro idoralar pozitsiyalari asosida kalit kelishuvini kvant xavfidan himoyalashning asosiy yo‘li – gibrid rejimdagi postkvant KEM; QKD – tor sohadagi qo‘shimcha vosita.

O‘zbekiston uchun tavsiya: birinchi navbatda TLS va VPN (Virtual Private Network – virtual xususiy tarmoq) tizimlarida gibrid postkvant kalit kelishuvini joriy etish va milliy postkvant KEM standartini ishlab chiqish bo‘yicha tadqiqotlarni boshlash; QKD ni esa alohida yuqori ahamiyatli liniyalarda tajriba loyihasi sifatida, autentifikatsiya va kalitlarni birlashtirish qoidalari aniq belgilangan holda sinash.

Foydalanilgan adabiyotlar

1. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. Vol. 26, No. 5. P. 1484–1509.

2. Moody D., Perlner R., Regenscheid A., Robinson A., Cooper D. Transition to Post-Quantum Cryptography Standards. NIST IR 8547 (final). 2026. DOI: 10.6028/NIST.IR.8547.

3. Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing. Bangalore, 1984. P. 175–179.

4. Shor P., Preskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol // Physical Review Letters. 2000. Vol. 85, No. 2. P. 441–444.

5. Wegman M., Carter J. L. New Hash Functions and Their Use in Authentication and Set Equality // Journal of Computer and System Sciences. 1981. Vol. 22, No. 3. P. 265–279.

6. Pirandola S., Laurenza R., Ottaviani C., Banchi L. Fundamental Limits of Repeaterless Quantum Communications // Nature Communications. 2017. Vol. 8. Art. 15043.

7. Lucamarini M., Yuan Z. L., Dynes J. F., Shields A. J. Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters // Nature. 2018. Vol. 557. P. 400–403.

8. Liu Y., Zhang W.-J., Jiang C. et al. Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance // Physical Review Letters. 2023. Vol. 130. Art. 210801.

9. Liao S.-K. et al. Satellite-to-Ground Quantum Key Distribution // Nature. 2017. Vol. 549. P. 43–47.

10. ITU-T Y.3800. Overview on Networks Supporting Quantum Key Distribution. Geneva: ITU, 2019.

11. Lydersen L., Wiechers C., Wittmann C. et al. Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination // Nature Photonics. 2010. Vol. 4. P. 686–689.

12. Lo H.-K., Curty M., Qi B. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. 2012. Vol. 108. Art. 130503.

13. ISO/IEC 23837-1:2023. Information Security – Security Requirements, Test and Evaluation Methods for Quantum Key Distribution – Part 1: Requirements.

14. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.

15. Alagic G. et al. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545. 2025.

16. Kwiatkowski K., Kampanakis P., Westerbaan B., Stebila D. Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3. RFC 10024 (Proposed Standard). IETF, 2026.

17. Bernstein D. J., Bhargavan K., Bhasin S. et al. KyberSlash: Exploiting Secret-Dependent Division Timings in Kyber Implementations // IACR Transactions on Cryptographic Hardware and Embedded Systems. 2025.

18. NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). URL: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/ (murojaat: 06.11.2026).

19. ANSSI, BSI, NLNCSA, Swedish Armed Forces. Position Paper on Quantum Key Distribution. 2024-yil 25-yanvar.

3-SHO‘BA. RAQAMLI KRIMINALISTIKA YUTUQLARI

KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISHNING METODIK ASOSLARI

Nematilloyev B.V.
O‘zbekiston Respublikasi IIV Akademiyasi

Annotatsiya. Mazkur tezisda kiberjinoyatlarni tergov qilishda raqamli texnologiyalardan foydalanish bilan bog‘liq huquqiy, tashkiliy, texnik va kriminalistik muammolar tahlil qilinadi. Asosiy e’tibor raqamli ma’lumotlarning haddan tashqari ko‘pligi, turli manbalardagi axborotni birlashtirish, dalillarning yaxlitligini saqlash, tergovchi va texnik mutaxassis hamkorligini tashkil etish hamda sun’iy intellekt natijalarini inson tomonidan tekshirish masalalariga qaratiladi. Tahlil natijasida ma’lumotlarni dastlabki saralash, o‘zaro bog‘lash, avtomatlashtirilgan tahlil va uning natijalarini tekshirishni izchil birlashtiruvchi metodik yondashuv taklif etiladi.

Kalit so‘zlar: kiberjinoyat, raqamli dalil, elektron dalil, raqamli kriminalistika, ma’lumotlarni dastlabki saralash, sun’iy intellekt, OSINT, raqamli ekspertiza.

Аннотация. В тезисе рассматриваются правовые, организационные, технические и криминалистические проблемы использования цифровых технологий при расследовании киберпреступлений. Основное внимание уделяется большому объёму цифровых данных, объединению информации из разных источников, обеспечению целостности доказательств, взаимодействию следователя и технического специалиста, а также проверке результатов искусственного интеллекта человеком. Предлагается методический подход, объединяющий первичную сортировку данных, их интеграцию, автоматизированный анализ и последующую проверку и процессуальную оценку.

Ключевые слова: киберпреступление, цифровые доказательства, электронные доказательства, цифровая криминалистика, первичная сортировка данных, искусственный интеллект, OSINT, цифровая экспертиза.

Kirish

Raqamli texnologiyalarning keng tarqalishi jinoyat izlarini aniqlash va tergov qilish usullariga ham yangi talablar qo‘ymoqda. Kompyuterlar, mobil qurilmalar, bulutli xizmatlar, ijtimoiy tarmoqlar va tarmoq infratuzilmasida saqlanadigan ma’lumotlar jinoyatga oid muhim izlarni o‘z ichiga olishi mumkin. Biroq bu ma’lumotlar tez o‘zgaradi, turli formatlarda saqlanadi va ko‘pincha bir nechta manbaga tarqaladi. Shuning uchun tergovchi uchun muammo faqat ma’lumotni topishda emas, balki uni to‘g‘ri ajratish, bir-biri bilan bog‘lash va ishonchliligini tekshirishda ham namoyon bo‘ladi [1; 2]. E. Casey raqamli dalillarni aniqlash, olish, saqlash va tahlil qilish bosqichlari o‘zaro izchil tashkil etilishi kerakligini ta’kidlaydi [2].

Tadqiqotning maqsadi - kiberjinoyatlarni tergov qilishda raqamli texnologiyalardan foydalanish samaradorligini pasaytiruvchi asosiy omillarni aniqlash va ularni bartaraf etishning metodik mexanizmlarini asoslash. Buning uchun raqamli ma’lumotlarni topish bilan cheklanmasdan, ularni saralash, turli manbalarni bog‘lash, natijalarni tekshirish va ish uchun ahamiyatini aniqlashga xizmat qiladigan yagona yondashuv ishlab chiqiladi.

Tadqiqotda tizimli, formal-yuridik, qiyosiy-huquqiy, kriminalistik, mantiqiy, induktiv va deduktiv metodlardan foydalanildi. Ular huquqiy va texnik jarayonlarni o‘zaro bog‘liq holda tahlil qilish hamda milliy amaliyotni xalqaro yondashuvlar bilan taqqoslash imkonini berdi. Manba

bazasini jinoyat-protsessual qonunchilik, ISO/IEC 27037 va ISO/IEC 27042 standartlari, NIST tavsiyalari hamda Budapesht konvensiyasi hujjatlari tashkil etdi [1;3;4;5].

O‘rganilgan manbalar va mavjud metodik yondashuvlarni umumlashtirish natijasida kiberjinoyatlarni tergov qilishda raqamli texnologiyalardan foydalanish bilan bog‘liq muammolarni besh o‘zaro bog‘liq yo‘nalishda ko‘rish mumkin: ma’lumotlarni saralash, tizimlararo integratsiya, dalillarning yaxlitligi, mutaxassislar hamkorligi va sun’iy intellektdan foydalanish. Ushbu yo‘nalishlar alohida masalalar bo‘lib ko‘rinsa-da, amalda ular bitta tergov jarayonining ketma-ket bosqichlarini tashkil etadi.

Birinchi muammo - raqamli ma’lumotlarning ko‘pligidir. Shu sababli ularni vaqt, qurilma, foydalanuvchi va hodisaga aloqadorlik mezonlari asosida dastlabki saralash (texnologik triage) zarur [6;7].

Ikkinchi muammo - turli tizimlardagi ma’lumotlarning mos kelmasligidir. Buni yagona identifikator, vaqt shkalasi va metama’lumotlar asosida integratsiyalash orqali hal etish mumkin [4;8].

Uchinchi muammo - raqamli dalilning yaxlitligi va ishonchliligini ta’minlashdir. Bunda dalilning olinishi, saqlanishi va undan foydalanish jarayonini hujjatlashtirish hamda ISO/IEC 27037 va 27042 tamoyillariga rioya qilish muhim [3;4].

To‘rtinchi muammo - tergovchi, IT-mutaxassis va ekspert vazifalarining aniq taqsimlanmaganidir. Ularning vakolatlarini belgilash texnik natijalardan samarali foydalanishga xizmat qiladi.

Beshinchi muammo - sun’iy intellekt natijalarining xato bo‘lishi ehtimolidir. Shu bois sun’iy intellekt (keyingi o‘rinlarda AI) natijalari tayyor xulosa emas, balki mutaxassis tomonidan tekshiriladigan yordamchi ma’lumot sifatida qo‘llanishi lozim [9].

AI yordamida yaratilgan yoki o‘zgartirilgan audio, video va tasvirlar ham shu muammo bilan uzviy bog‘liq. Deepfake texnologiyalari tashqi ko‘rinishi ishonchli bo‘lgan, ammo mazmuni o‘zgartirilgan materiallarni yaratish imkonini beradi [10]. Shu sababli bunday fayllarni faqat ko‘rinishiga qarab baholash yetarli emas. Ularni fayl xususiyatlari, metama’lumotlar, vaqt ma’lumotlari, manba qurilmasi, tarmoq ma’lumotlari va boshqa mustaqil manbalar bilan solishtirib tekshirish zarur.

Yuqoridagi muammolarni alohida-alohida hal qilishdan ko‘ra, ularni yagona jarayonda birlashtirish samaraliroq bo‘lishi mumkin. Shu asosda “Tergov va raqamli texnologiyalar integratsiyasi modeli” taklif etiladi. Model yetti ketma-ket bosqichdan iborat: 1) raqamli manbalarni aniqlash; 2) ma’lumotlarni dastlabki saralash; 3) turli manbalardagi ma’lumotlarni yagona identifikator va vaqt shkalasi asosida birlashtirish; 4) avtomatlashtirilgan tahlildan foydalanish;

5) natijalarni inson tomonidan tekshirish; 6) ma’lumotlarni kriminalistik mazmun asosida talqin qilish; 7) olingan natijalarning ish bo‘yicha huquqiy ahamiyatini aniqlash. Mazkur modelning afzalligi shundaki, texnologiya tergovchining o‘rnini egallamaydi, balki uning ishini tizimlashtiradi. Dastlabki saralash keraksiz ma’lumotlar hajmini kamaytiradi, integratsiya turli manbalarni yagona hodisa bilan bog‘laydi, avtomatlashtirilgan tahlil kerakli bog‘liqliklarni tezroq aniqlashga yordam beradi, inson tekshiruvi esa texnik natijaning xatoliklarini kamaytiradi. Shu sababli model doirasida raqamli dalillarni aniqlash, olish, saqlash va topshirish uchun yagona metodik reglamentni, tergovchi–IT-mutaxassis–ekspert hamkorligi uchun aniq vakolatlarni hamda umumiy identifikator va metama’lumot standartlarini joriy etish taklif qilinadi [3; 4]. AI

qo‘llanilganda esa “AI natijasi - mutaxassis tekshiruvi - olingan ma’lumotning ish bo‘yicha huquqiy ahamiyatini aniqlash” ketma-ketligi saqlanishi lozim [9].

Budapesht konvensiyasi kiberjinoyatchilik bo‘yicha xalqaro hamkorlik uchun umumiy huquqiy asos yaratadi [1]. NIST va ISO/IEC standartlari raqamli dalillarni aniqlash, yig‘ish, saqlash va tahlil qilishni izchil tashkil etishga xizmat qiladi [3; 4; 6; 7]. YI ning 2023/1543-son Reglamenti va 2023/1544-son Direktivasida elektron dalillarni transchegaraviy olish va xizmat ko‘rsatuvchi provayderlar bilan hamkorlik qilish mexanizmlari nazarda tutilgan [11; 12]. Ikkinchi qo‘shimcha protokol ham elektron dalillar bo‘yicha xalqaro hamkorlikni kuchaytirishga qaratilgan [13]. Mazkur tajribani O‘zbekistonda to‘liq ko‘chirish emas, balki milliy qonunchilik va amaliyotga moslashtirish lozim. Bunda transchegaraviy elektron ma’lumotlarga qonuniy murojaat qilish, xizmat ko‘rsatuvchi provayderlardan ma’lumot olish, raqamli dalillarni saqlash va ular bilan ishlash uchun mas’uliyatni aniq belgilash muhimdir [11–13]. Amaliy jihatdan esa quyidagi yo‘nalishlar muhim deb hisoblanadi: ma’lumotlarni dastlabki saralashning yagona mezonlarini joriy etish, turli manbalarni umumiy identifikator va vaqt asosida birlashtirish, AI dan inson nazoratida foydalanish, tergovchi–IT-mutaxassis–ekspert vakolatlarini aniq belgilash, sun’iy yaratilgan kontentni ko‘p manbali tekshirish, ekspertiza vositalarini muntazam metodik sinovdan o‘tkazish va xodimlarning raqamli ko‘nikmalarini doimiy yangilab borish. Tadqiqotning ilmiy yangiligi shundan iboratki, raqamli texnologiyalardan foydalanish bilan bog‘liq muammolar alohida texnik kamchiliklar sifatida emas, balki ma’lumotni aniqlashdan boshlab uning ish bo‘yicha huquqiy ahamiyatini aniqlashgacha davom etadigan yagona jarayon sifatida tizimlashtiriladi. Shu asosda ma’lumotlarni dastlabki saralash, integratsiya, inson nazoratidagi avtomatlashtirilgan tahlil va yakuniy baholashni yagona metodik modelga birlashtirish taklif etiladi.

Xulosa

Kiberjinoyatlarni tergov qilishda raqamli ma’lumotlarning ko‘pligi va tarqoqligi, turli tizimlarni birlashtirish qiyinligi, dalillar yaxlitligi va sun’iy intellekt natijalarini tekshirish zarurati asosiy muammolarni yuzaga keltiradi. Shu sababli ma’lumotni topish bilan cheklanmay, uni saralash, bog‘lash, ishonchliligini tekshirish va ish bo‘yicha huquqiy ahamiyatini aniqlash zarur. Taklif etilgan model ushbu bosqichlarni yagona tizimga birlashtirib, raqamli dalillar bilan ishlashda texnologik imkoniyatlar va inson nazoratini uyg‘unlashtiradi.

Foydalanilgan adabiyotlar

1. Council of Europe. Convention on Cybercrime (Budapest Convention). ETS No. 185. Budapest: Council of Europe, 2001. 27 p. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

2. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Waltham, MA: Academic Press, 2011. 816 p. URL: https://www.sciencedirect.com/ book/9780123742681/digital-evidence-and-computer-crime

3. ISO/IEC 27037:2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012. URL: https://www.iso.org/standard/44381.html

4. ISO/IEC 27042:2015. Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO, 2015. URL: https://www.iso.org/standard/44407.html

5. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. 22.09.1994. URL: https://lex.uz/docs/111463

6. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86. Gaithersburg, MD: NIST, 2006. 121 p. URL: https://csrc.nist.gov/pubs/sp/800/86/final

7. National Institute of Standards and Technology. Guidelines on Mobile Device Forensics. NIST SP 800-101 Rev. 1. Gaithersburg, MD: NIST, 2014. 104 p. URL: https://csrc.nist.gov/pubs/sp/800/101/r1/final

8. Roussev V. Digital Forensic Science: A Contemporary Review. San Rafael, CA: Morgan & Claypool Publishers, 2016. 180 p. URL: https://www.morganclaypool.com/doi/abs/10.2200/S00642ED1V01Y201503CSE014

9. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023. 46 p. URL: https://www.nist.gov/itl/ai-risk-management-framework

10. Chesney R., Citron D. Deepfakes and the New Disinformation War // Foreign Affairs. 2019. Vol. 98, No. 1. P. 147–155. New York: Council on Foreign Relations. URL: https://www.foreignaffairs.com/articles/2019-06-13/deepfakes-and-new-disinformation-war

11. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023. Official Journal of the European Union, L 191, 28.07.2023. P. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

12. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023. Official Journal of the European Union, L 191, 28.07.2023. P. 181–190. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj

13. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg: Council of Europe, 2021. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

14. Garfinkel S. Digital forensics research: The next 10 years // Digital Investigation. 2010. Vol. 7. P. S64–S73. Amsterdam: Elsevier. DOI: https://doi.org/10.1016/j.diin.2010.05.009

15. Sachoulidou A. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of judicial cooperation // New Journal of European Criminal Law. 2024. Vol. 15, No. 3. P. 256–274. London: SAGE. DOI: https://doi.org/10.1177/20322844241258649

16. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764, 15.04.2022. URL: https://lex.uz/docs/5960604

17. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni, O‘RQ-547, 02.07.2019. URL: https://lex.uz/docs/4396419

18. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge, MA: MIT Press, 2016. 800 p. URL: https://www.deeplearningbook.org/

MA’LUMOTLARNI YASHIRISHNING STEGANOGRAFIK YECHIMINI TADQIQ ETISH VA TAKOMILLASHTIRISH

Xo‘jamqulova D.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada raqamli tasvirlarning fazoviy sohasida ma’lumot yashirishning eng ko‘p qo‘llanadigan usuli – eng kichik ahamiyatli bitni (LSB) almashtirish – steganografik bardoshlilik nuqtai nazaridan tahlil qilinadi. Bu usul piksel qiymatlari juftliklari statistikasini buzishi va RS-steganotahlil yordamida oson fosh etilishi ko‘rsatiladi. Kamchilikni bartaraf etish uchun kalitga bog‘liq psevdotasodifiy piksel tanlash, Hamming (7,3) kodiga asoslangan matritsali kodlash va ±1 moslashtirishni birlashtirgan sxema taklif etiladi. Oltita test tasvirida o‘tkazilgan hisoblash tajribasida bir xil foydali yuklamada o‘zgartirilgan piksellar soni 41,7 % ga kamaydi, PSNR o‘rtacha 2,3 dB ga oshdi, RS-tahlil esa yashirin xabar uzunligini baholay olmadi.

Kalit so‘zlar: steganografiya, LSB, LSB-moslashtirish, matritsali kodlash, Hamming kodi, PSNR, RS-steganotahlil, axborot xavfsizligi.

Аннотация. В статье с позиции стеганографической стойкости анализируется наиболее распространённый метод сокрытия данных в пространственной области цифровых изображений – замена наименее значащего бита (LSB). Показано, что этот метод нарушает статистику пар значений пикселей и легко выявляется RS-стегоанализом. Для устранения недостатка предложена схема, объединяющая псевдослучайный выбор пикселей на основе ключа, матричное кодирование кодом Хэмминга (7,3) и встраивание по принципу ±1. В вычислительном эксперименте на шести тестовых изображениях при одинаковой полезной нагрузке число изменённых пикселей сократилось на 41,7 %, PSNR вырос в среднем на 2,3 дБ, а RS-анализ не смог оценить длину скрытого сообщения.

Ключевые слова: стеганография, LSB, LSB-согласование, матричное кодирование, код Хэмминга, PSNR, RS-стегоанализ, информационная безопасность.

Kirish

Shifrlangan xabar begona shaxsga o‘z mazmunini ochmaydi, biroq maxfiy aloqa borligini yashira olmaydi: tasodifiy ko‘rinishdagi bayt oqimining o‘zi shubha uyg‘otadi. Steganografiya ana shu muammoga javob beradi – xabar oddiy ko‘rinishdagi konteyner (tasvir, audio, matn) ichiga joylanadi va kuzatuvchi aloqa faktining o‘zini sezmasligi kerak. G.Simmons bu vaziyatni “mahbuslar masalasi” sifatida rasmiylashtirgan: ikki tomon nazoratchi ko‘zi oldida yozishadi, nazoratchi esa har bir xatni shubhali belgilar bor-yo‘qligiga tekshiradi [1]. Demak, steganografik tizim sifati faqat ko‘zga ko‘rinmaslik bilan emas, balki statistik aniqlab bo‘lmaslik bilan ham o‘lchanadi.

Prezidentning 2024-yil 15-avgustdagi PQ-293-son qarori bilan kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar belgilangani axborotni himoyalashning kriptografik va unga yondosh usullari bo‘yicha amaliy tadqiqotlarga ehtiyojni yanada oshirdi. Shifrlash bilan birga qo‘llanadigan steganografik vositalar ushbu yo‘nalishning ajralmas qismi hisoblanadi.

Tadqiqot maqsadi – tasvirning fazoviy sohasida ishlaydigan LSB usulining zaif tomonlarini aniqlash, o‘zgarishlar sonini kamaytirish hisobiga uning steganografik bardoshliligini oshiruvchi yechim taklif etish va uni miqdoriy baholashdan iborat.

Adabiyotlar tahlili

Raqamli steganografiyaning nazariy asoslari, stegotizimning matematik modeli va asosiy algoritmlar V.G.Gribunin va hammualliflarning monografiyasida tizimli bayon qilingan [2]. A.Cheddad va hammualliflar fazoviy, chastota va adaptiv sohadagi usullarni tasniflab, LSB usulining sig‘imi katta bo‘lsa-da, statistik hujumlarga chidamsizligini qayd etgan [3]. A.Westfeld va A.Pfitzmann LSB almashtirish 2i va 2i+1 qiymatlarning chastotalarini bir-biriga yaqinlashtirishini aniqlab, shunga asoslangan χ^2-hujumni taklif qilgan [4]. J.Fridrich, M.Goljan va R.Du ishlab chiqqan RS-usul esa xabar bitlari piksellar bo‘ylab tasodifiy sochilgan holatda ham uning nisbiy uzunligini baholash imkonini berdi [5].

Bu hujumlarga javoban ikki yo‘nalish shakllandi. Birinchisi – ±1 moslashtirish (LSB matching): piksel biti xabar bitiga mos kelmasa, uning qiymatiga tasodifiy ravishda 1 qo‘shiladi yoki ayriladi. Bunda juftliklar asimmetriyasi yuzaga kelmaydi, lekin A.Ker ko‘rsatganidek, gistogramma xarakteristik funksiyasining o‘zgarishi orqali bunday yashirishni ham aniqlash mumkin [6]. J.Mielikainen ikki piksel juftligida ikki bitni kamroq o‘zgarish bilan joylovchi modifikatsiyani taklif qilgan [7]. Ikkinchi yo‘nalish kodlash nazariyasiga tayanadi. A.Westfeld F5 algoritmida matritsali kodlash yordamida zarur o‘zgarishlar sonini kamaytirgan [8], T.Filler va hammualliflarning sindrom-trellis kodlari esa ixtiyoriy additiv buzilish funksiyasini minimallashtiruvchi universal vositaga aylandi [9]. Shu asosda qurilgan S-UNIWARD kabi adaptiv usullar o‘zgarishlarni modellashtirish qiyin bo‘lgan teksturali sohalarga yo‘naltiradi [10]. So‘nggi yillarda chuqur neyron tarmoqlariga asoslangan yondashuvlar ham faol rivojlanmoqda [11, 12], biroq ular katta hisoblash resursi va o‘qitish ma’lumotlarini talab qiladi.

Ko‘rib chiqilgan ishlardan ko‘rinadiki, adaptiv sxemalar yuqori bardoshlilikka ega, ammo ularni resursi cheklangan qurilmalarda va o‘quv-amaliy tizimlarda joriy etish murakkab. Oddiy LSB esa hamon ko‘plab dasturiy vositalar asosida qolmoqda. Shu sababli amalga oshirish soddaligini saqlagan holda LSB usulining asosiy kamchiliklarini yumshatadigan oraliq yechimga ehtiyoj bor.

Tadqiqot metodikasi

Taklif etilgan sxema uch bosqichdan iborat. Birinchi bosqichda maxfiy kalit K dan SHA-256 xesh-funksiyasi orqali psevdotasodifiy sonlar generatorining boshlang‘ich qiymati hosil qilinadi va barcha piksel indekslarining π o‘rin almashtirishi quriladi. Xabar bitlari shu tartibda tanlangan piksellarga joylanadi, natijada ketma-ket yozishga xos mahalliy statistik iz yo‘qoladi. Xabar joylashdan oldin shifrlanadi deb hisoblanadi, shuning uchun tajribada u tasodifiy bit oqimi sifatida modellashtirildi.

Ikkinchi bosqichda xabar 3 bitlik bloklarga ajratiladi va har bir blok yettita pikselning eng kichik bitlari $b = (b_1, \dots, b_7)$ ichiga Hamming (7,3) kodining tekshiruv matritsasi H yordamida joylanadi; H ning j-ustuni j sonining ikkilik yozuviga teng. Avval sindrom hisoblanadi:

$$s = Hb^T \oplus m \tag{1}$$

bu yerda m – xabarning 3 bitlik bloki, $\oplus$ – 2 modul bo‘yicha qo‘shish. Agar $s = 0$ bo‘lsa, blok o‘zgarishsiz qoladi, aks holda tartib raqami $j = s_1 + 2s_2 + 4s_3$ bo‘lgan bitta pikselgina o‘zgartiriladi. Qabul qiluvchi xabarni stego-tasvir bitlaridan to‘g‘ridan-to‘g‘ri tiklaydi:

$$m = Hb'^T \pmod 2 \tag{2}$$

Uchinchi bosqichda tanlangan pikselning biti almashtirilmaydi, uning qiymati bir birlikka o‘zgartiriladi:

$$y_j = \begin{cases} x_j + 1, \text{ agar } x_j = 0, \\ x_j - 1, \text{ agar } x_j = 255, \\ x_j \pm 1, \text{ qolgan hollarda,} \end{cases} \quad (3)$$

bunda ishora teng ehtimol bilan tasodifiy tanlanadi. Bu yondashuv qiymatlar juftligi bo‘yicha asimmetriyani yo‘qotadi, matritsali kodlash esa o‘zgarishlar sonini kamaytiradi. p bitni $2^p - 1$ ta pikselga joylashda o‘rtacha joylash samaradorligi (bir o‘zgarishga to‘g‘ri keladigan bitlar soni) va nisbiy sig‘im quyidagicha aniqlanadi:

$$e = \frac{p}{1-2^{-p}}, \qquad \alpha = \frac{p}{2^p - 1} \quad (4)$$

$p = 3$ da $e \approx 3{,}43$ bit/o‘zgarish va $\alpha \approx 0{,}43$ bit/piksel bo‘ladi, oddiy LSB uchun esa $e = 2$. Shunday qilib, sig‘imning bir qismi evaziga bir xil xabar uchun kamroq o‘zgarish talab etiladi.

Stego-tasvir sifati o‘rtacha kvadratik xato (MSE) va cho‘qqi signal-shovqin nisbati (PSNR) bilan baholandi:

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{ij} - y_{ij}\right)^2, \quad \mathrm{PSNR} = 10\lg\frac{255^2}{\mathrm{MSE}} \quad (5)$$

Strukturaviy o‘xshashlik uchun SSIM indeksi qo‘llandi [13]. Steganotahliliy bardoshlilik RS-usul [5] bergan yashirin xabar nisbiy uzunligi bahosi bilan tekshirildi: baho haqiqiy yuklamaga qancha yaqin bo‘lsa, usul shuncha oson fosh etiladi.

Tajriba Python muhitida scikit-image kutubxonasi [14] tarkibidagi oltita test tasvirida (Cameraman, Astronaut, Coffee, Chelsea, Moon, Brick; rangli tasvirlar kulrang ko‘rinishga o‘tkazildi) o‘tkazildi. To‘rt usul solishtirildi: M1 – klassik ketma-ket LSB almashtirish; M2 – kalit asosida tasodifiy tartibda LSB almashtirish; M3 – kalit asosida tasodifiy tartibda ±1 moslashtirish; M4 – taklif etilgan sxema. Yuklama 0,1; 0,2; 0,3 va 0,4 bit/piksel qilib olindi, har bir holat uchun beshta turli kalit va xabar ishlatilib, natijalar 30 ta stego-tasvir bo‘yicha o‘rtachalandi. Barcha usullarda xabar xatosiz tiklandi.

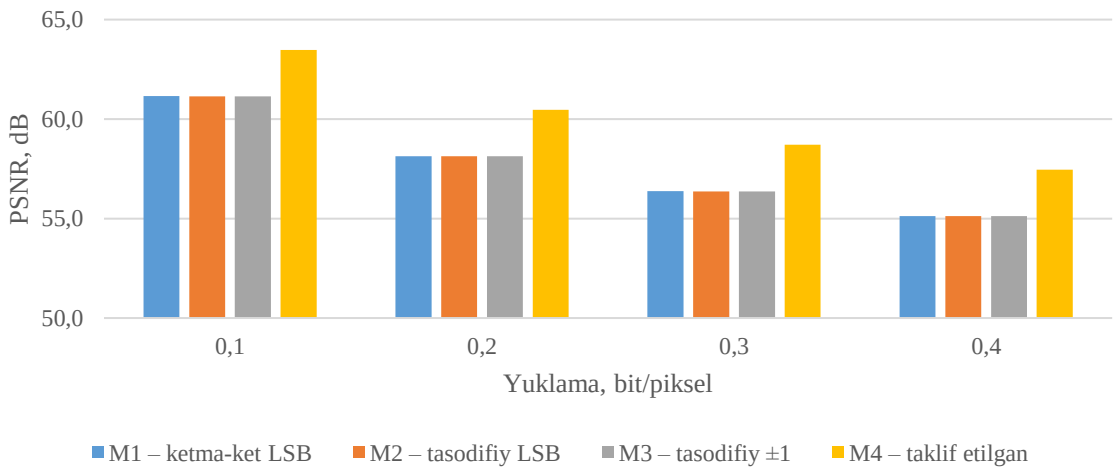
Natijalar va muhokama. Asosiy ko‘rsatkichlar 1-jadvalda keltirilgan.

1-jadval

Usullarning qiyosiy ko‘rsatkichlari (6 ta tasvir, 5 ta takror bo‘yicha o‘rtacha)

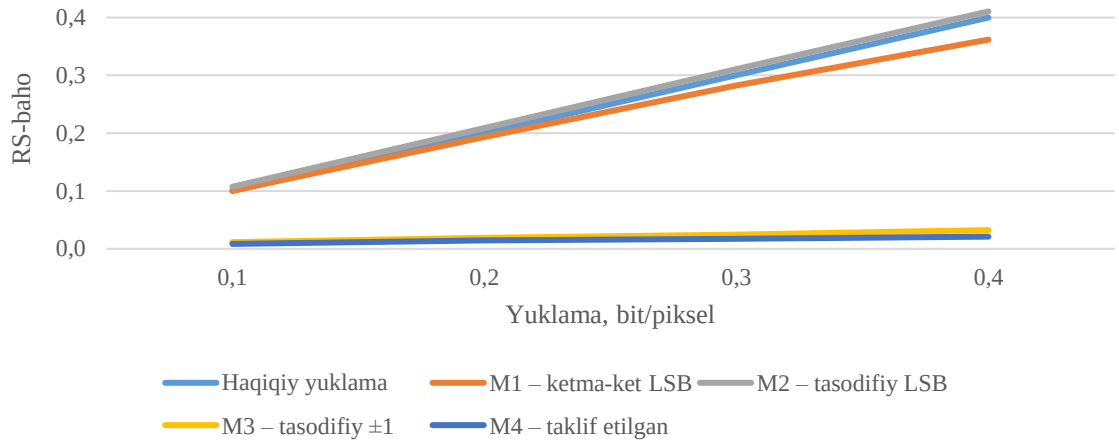
Usul	O‘zgarish / bit	e, bit / o‘zgarish	PSNR, dB (0,2 bpp)	PSNR, dB (0,4 bpp)	SSIM (0,4 bpp)	RS-baho (0,4 bpp)
M1 – ketma-ket LSB	0,499	2,00	58,14	55,13	0,9981	0,36
M2 – tasodifiy LSB	0,500	2,00	58,13	55,12	0,9982	0,41
M3 – tasodifiy ±1	0,500	2,00	58,13	55,12	0,9981	0,03
M4 – taklif etilgan	0,292	3,43	60,47	57,46	0,9989	0,02

M1–M3 usullarida har bir xabar biti uchun o‘rtacha 0,50 ta piksel o‘zgaradi – bu ehtimollik nazariyasidan kutilgan natija, chunki tasodifiy bitning yarmi piksel bitiga o‘z-o‘zidan mos keladi. Taklif etilgan M4 sxemada bu ko‘rsatkich 0,292 ga tushdi va $7/24 \approx 0{,}292$ nazariy qiymatiga deyarli to‘liq mos keldi. O‘zgarishlar 41,7 % ga kamaygani MSE ning o‘rtacha 1,71 marta kichrayishiga va PSNR ning barcha yuklamalarda 2,3 dB ga oshishiga olib keldi. E’tiborli jihati, M4 0,4 bit/piksel yuklamada (57,46 dB) M1–M3 usullarining 0,3 bit/piksel yuklamadagi natijasidan (56,38 dB) ham yuqori sifat berdi.



1-rasm. Foydali yuklamaga bog‘liq ravishda PSNR qiymatlari

RS-steganotahlil natijalari 2-rasmda ko‘rsatilgan. LSB almashtirishga asoslangan M1 va M2 usullarda RS-baho haqiqiy yuklamaga yaqin chiqdi (masalan, 0,4 bit/piksel yuklamada M2 uchun 0,41), ya’ni yashirin xabar mavjudligi va uning hajmi ishonchli aniqlandi. Ketma-ket yozishda (M1) baho biroz past va tarqoqroq, chunki usul xabarni tasodifiy tarqalgan deb faraz qiladi. ±1 moslashtirish qo‘llangan M3 va M4 da baho barcha yuklamalarda 0,01…0,03 oralig‘ida qoldi va toza tasvirlar uchun olingan qiymatlardan (−0,011…0,030) amalda farq qilmadi.



2-rasm. RS-steganotahlil bergan yashirin xabar uzunligi bahosi

Olingan natijalarni talqin qilishda tadqiqot cheklovlarini hisobga olish lozim. RS-usul LSB almashtirishga yo‘naltirilgan, shu bois uning M3 va M4 ni aniqlay olmagani bu usullar har qanday steganotahlilga chidamli ekanini anglatmaydi: ±1 moslashtirishga qarshi maxsus hujumlar [6] hamda boy modellar va neyron tarmoq klassifikatorlari bilan sinov alohida o‘tkazilishi kerak. Test tasvirlari soni kam, sxema sig‘imi 0,43 bit/piksel bilan chegaralangan va fazoviy sohada ishlagani uchun JPEG siqishga bardosh bermaydi. Shunga qaramay, M4 ning hisoblash murakkabligi juda past – har 7 piksel uchun bitta sindrom hisoblanadi – bu esa uni resursi cheklangan tizimlarda qo‘llashga qulay qiladi.

Xulosa

Tadqiqot oddiy LSB almashtirish usuli RS-steganotahlil orqali yashirin xabar uzunligigacha aniqlanishini tasdiqladi. Kalit asosidagi psevdotasodifiy tartib, Hamming (7,3) matritsali kodlash va ±1 moslashtirishni birlashtirgan sxema bir xil yuklamada o‘zgarishlar sonini 41,7 % ga kamaytirdi, PSNR ni 2,3 dB ga oshirdi va RS-baho qiymatini toza tasvirlar darajasiga

tushirdi. Keyingi bosqichda sxemani adaptiv buzilish funksiyasi va sindrom-trellis kodlari [9, 10] bilan to‘ldirish hamda zamonaviy klassifikatorlar asosida baholash rejalashtirilgan.

Foydalanilgan adabiyotlar

1. Simmons G.J. The Prisoners’ Problem and the Subliminal Channel // Advances in Cryptology: Proceedings of Crypto 83. – Boston: Springer, 1984. – P. 51–67. – DOI: 10.1007/978-1-4684-4730-9_5.

2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.

3. Cheddad A., Condell J., Curran K., Mc Kevitt P. Digital image steganography: Survey and analysis of current methods // Signal Processing. – 2010. – Vol. 90, № 3. – P. 727–752. – DOI: 10.1016/j.sigpro.2009.08.010.

4. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems // Information Hiding: Third International Workshop, IH’99. – Berlin: Springer, 2000. – LNCS, Vol. 1768. – P. 61–76. – DOI: 10.1007/10719724_5.

5. Fridrich J., Goljan M., Du R. Detecting LSB steganography in color and gray-scale images // IEEE Multimedia. – 2001. – Vol. 8, № 4. – P. 22–28. – DOI: 10.1109/93.959097.

6. Ker A.D. Steganalysis of LSB matching in grayscale images // IEEE Signal Processing Letters. – 2005. – Vol. 12, № 6. – P. 441–444.

7. Mielikainen J. LSB matching revisited // IEEE Signal Processing Letters. – 2006. – Vol. 13, № 5. – P. 285–287. – DOI: 10.1109/LSP.2006.870357.

8. Westfeld A. F5 – A Steganographic Algorithm: High Capacity Despite Better Steganalysis // Information Hiding: 4th International Workshop, IH 2001. – Berlin: Springer, 2001. – LNCS, Vol. 2137. – P. 289–302.

9. Filler T., Judas J., Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes // IEEE Transactions on Information Forensics and Security. – 2011. – Vol. 6, № 3. – P. 920–935. – DOI: 10.1109/TIFS.2011.2134094.

10. Holub V., Fridrich J., Denemark T. Universal distortion function for steganography in an arbitrary domain // EURASIP Journal on Information Security. – 2014. – Art. 1. – DOI: 10.1186/1687-417X-2014-1.

11. Baluja S. Hiding Images in Plain Sight: Deep Steganography // Advances in Neural Information Processing Systems 30 (NIPS 2017). – 2017. – P. 2069–2079.

12. Subramanian N., Elharrouss O., Al-Maadeed S., Bouridane A. Image Steganography: A Review of the Recent Advances // IEEE Access. – 2021. – Vol. 9. – P. 23409–23423.

13. Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P. Image quality assessment: from error visibility to structural similarity // IEEE Transactions on Image Processing. – 2004. – Vol. 13, № 4. – P. 600–612. – DOI: 10.1109/TIP.2003.819861.

14. van der Walt S., Schönberger J.L., Nunez-Iglesias J. et al. scikit-image: image processing in Python // PeerJ. – 2014. – Vol. 2. – e453. – DOI: 10.7717/peerj.453.

МЕТОДЫ АНАЛИЗА ЗАШИФРОВАННЫХ ТОМОВ В ПРОЦЕССАХ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Эргашбеков Н.А.
Ташкентский университет информационных технологий имени Мухаммада Ал-Хоразмий

Annotatsiya. Maqolada raqamli dalillarni kriminalistik tadqiqot jarayonida shifrlangan tomlarni aniqlash, identifikatsiyalash va tahlil qilish usullari yoritib o‘tilgan. Shifrlash vositalarining tasnifi (to‘liq diskli, konteynerli va fayl darajasidagi), shifrlangan sohalarni aniqlash belgilari (sarlavha signaturalari va entropiya tahlili) hamda har bir tur uchun ularning tadqiqot jarayoni - xotiradan kalitni ajratib olishdan va tiklash kalitlaridan foydalanishdan tortib sarlavhalarni tahlil qilish va parollarni tiklash jarayoni bo‘yicha ma’lumot keltirilgan. Alohida tarzda inkor etishga asoslangan yashirin tomlarni aniqlash masalasi ko‘rib chiqilgan. Usullar ISO/IEC 27037’ga muvofiq kriminalistik jarayon bosqichlari bilan bog‘langan.

Kalit so‘zlar: raqamli kriminalistika, shifrlangan tomlar, to‘liq diskni shifrlash, BitLocker, LUKS, VeraCrypt, entropiya tahlili, yashirin tomlar, raqamli dalillar.

Аннотация. В статье систематизированы методы выявления, идентификации и анализа зашифрованных томов в процессе криминалистического исследования цифровых доказательств. Рассмотрена классификация средств шифрования (полнодисковое, контейнерное и файловое), приведены признаки обнаружения зашифрованных областей (сигнатуры заголовков и энтропийный анализ) и методы получения доступа к их содержимому для каждого типа - от извлечения ключа из памяти и использования ключей восстановления до анализа заголовков и восстановления паролей. Отдельно рассмотрена задача обнаружения скрытых томов с правдоподобным отрицанием. Методы соотнесены с этапами криминалистического процесса согласно ISO/IEC 27037.

Ключевые слова: цифровая криминалистика, зашифрованные тома, полнодисковое шифрование, BitLocker, LUKS, VeraCrypt, энтропийный анализ, скрытые тома, цифровые доказательства.

Введение

Шифрование дисковых томов превратилось из специализированного инструмента в повсеместно применяемый механизм защиты данных: полнодисковое шифрование по умолчанию активировано во многих современных операционных системах, а контейнерные средства общедоступны. В криминалистическом процессе зашифрованный том выступает одновременно и препятствием для исследования, и самостоятельным объектом экспертизы, требующим корректного выявления, фиксации и анализа. Разнородность форматов шифрования и их защитных механизмов обуславливает необходимость систематизированного набора методов, применимых на каждом этапе экспертизы.

Целью настоящей работы является систематизация методов выявления, идентификации и анализа зашифрованных томов и их соотнесение с этапами криминалистического процесса. В отличие от работ, сосредоточенных на извлечении ключей из оперативной памяти конкретной ОС, здесь рассматривается обобщённый, кросс-платформенный взгляд на работу с зашифрованными томами различных типов.

Основная часть

Эффективность работы с зашифрованным томом определяется прежде всего правильным установлением его типа и формата, поскольку от этого зависят и признаки обнаружения, и применимые методы доступа. Поэтому изложение построено от классификации томов к их идентификации и далее к методам анализа.

Классификация зашифрованных томов. Целесообразно выделить три основные категории. Полнодисковое шифрование (full disk encryption) защищает том целиком: BitLocker в Windows, dm-crypt/LUKS в Linux, FileVault 2 в macOS, а также системное шифрование VeraCrypt. Контейнерное (виртуальные тома) оформляет зашифрованную область в виде файла-контейнера или отдельного раздела без привязки к системному диску: VeraCrypt и его предшественник TrueCrypt. Файловое и каталоговое шифрование защищает отдельные объекты файловой системы: EFS в NTFS, eCryptfs. Отдельно стоит аппаратное самошифрование накопителей (SED, TCG Opal), ключ которого хранится в контроллере диска. Каждая категория предъявляет собственные требования к методике исследования.

Выявление и идентификация зашифрованного тома. Идентификация опирается на два взаимодополняющих подхода. Первый - анализ сигнатур и заголовков: том BitLocker содержит в заголовке сигнатуру «-FVE-FS-», раздел LUKS - характерную магическую последовательность, FileVault распознаётся по метаданным CoreStorage/APFS. Второй подход необходим, когда сигнатура намеренно отсутствует: тома VeraCrypt и TrueCrypt не имеют заголовочных меток, что реализует концепцию правдоподобного отрицания. В этом случае применяется энтропийный анализ: равномерно высокая энтропия (близкая к 8 битам на байт) в сочетании с отсутствием распознаваемой файловой системы и метаданных указывает на зашифрованную область. Для выявления используются как штатные средства (file, binwalk), так и криминалистические платформы (Autopsy, FTK, EnCase) с модулями оценки энтропии.

Методы получения доступа к содержимому. Доступ к данным зашифрованного тома обеспечивается несколькими группами методов. Получение ключа или пароля: извлечение мастер-ключа (например, FVEK) из оперативной памяти при примонтированном томе; применение ключей восстановления (recovery key, в том числе депонированных); использование ключевых файлов; восстановление пароля по заголовку тома - современные инструменты (hashcat) поддерживают форматы BitLocker, LUKS и VeraCrypt. Монтирование только для чтения и расшифровка выполняются по формату тома: dislocker/libbde для BitLocker, cryptsetup для LUKS, libfvde для FileVault, VeraCrypt/tc-play для контейнеров, причём работа ведётся с побитовым образом, а не с оригиналом. Анализ заголовка и метаданных позволяет определить алгоритм и режим шифрования, число слотов ключей, соль и параметры функции формирования ключа (KDF), что важно как для планирования легального восстановления пароля, так и для документирования. Для файлового шифрования (EFS) доступ достигается через ключи DPAPI пользователя или его сертификат, извлекаемые из профиля.

Обнаружение скрытых томов. Особую задачу представляет обнаружение скрытых томов (hidden volume) VeraCrypt, реализующих правдоподобное отрицание: внутри внешнего тома размещается второй, факт существования которого криптографически недоказуем. Прямое подтверждение затруднено, поэтому исследование опирается на косвенные признаки: аномально высокую энтропию в «свободном» пространстве внешнего тома, расхождение между заявленным и фактическим использованием ёмкости, а также

артефакты операционной системы и приложений - списки недавно открытых файлов, точки монтирования, следы в реестре и журналах.

Интеграция в криминалистический процесс. Перечисленные методы встраиваются в этапы экспертизы, регламентированные ISO/IEC 27037. На этапе идентификации выполняется обнаружение зашифрованных областей (сигнатуры, энтропия). На этапе сохранения и сбора приоритет отдаётся «живому» сбору, если том примонтирован, после чего создаётся побитовый образ с фиксацией хеш-суммы. На этапе исследования проводится анализ заголовка и получение ключа, на этапе анализа - расшифровка по образу и изучение содержимого. Завершается процесс документированием (ключи, хеш-суммы, непрерывность владения доказательством). Обобщённое сопоставление типов томов, признаков и методов приведено в таблице 1.

Ограничения. Стойкое шифрование при отсутствии ключа и пароля остаётся непреодолимым за разумное время, а механизм скрытых томов обеспечивает правдоподобное отрицание даже при наличии подозрений. Это определяет приоритет методов, не требующих криптоанализа: получения ключа из памяти работающей системы, использования ключей восстановления и анализа сопутствующих артефактов. Результативность экспертизы в значительной мере закладывается на этапе идентификации и своевременного сбора.

Таблица 1

Типы зашифрованных томов: признаки идентификации и методы доступа

Тип тома / формат	Признак идентификации	Метод доступа	Инструмент
BitLocker (FDE, Windows)	сигнатура «-FVE-FS-» в заголовке	ключ FVEK из памяти, ключ восстановления, пароль	dislocker, libbde
LUKS / dm-crypt (Linux)	магическая сигнатура «LUKS»	парольная фраза, ключевой файл, анализ слотов	cryptsetup
FileVault 2 (macOS)	метаданные CoreStorage / APFS	ключ восстановления, пароль, ключ из памяти	libfvde
VeraCrypt / TrueCrypt (контейнер)	нет сигнатуры, высокая энтропия	пароль и keyfile, восстановление пароля	VeraCrypt, tc-play
EFS (файловое, NTFS)	атрибут шифрования файлов NTFS	ключ DPAPI пользователя, сертификат	профиль пользователя
Скрытый том VeraCrypt	энтропия «свободного» пространства, расхождение размеров	отдельный пароль скрытого тома	энтропийный анализ

Заключение

Систематизация методов анализа зашифрованных томов по типам (полнодисковое, контейнерное, файловое) и их соотнесение с этапами криминалистического процесса показывают, что успех исследования определяется прежде всего корректной идентификацией формата тома и своевременным получением ключевого материала, а не

попытками взлома шифра. Обнаружение скрытых томов опирается на косвенные признаки и анализ утечек состояния системы. Перспективными направлениями дальнейших исследований являются автоматизация энтропийного обнаружения зашифрованных областей, развитие кросс-платформенных методик расшифровки по образу и формализация требований к обеспечению целостности доказательств при работе с зашифрованными томами.

Список использованной литературы

1. Baier D., Basse A., Hilgert J.-N., Lambertz M. TLS key material identification and extraction in memory: Current state and future challenges // Forensic Science International: Digital Investigation. - 2024. - Vol. 49, Supplement. - Art. 301766. - DOI: https://doi.org/10.1016/j.fsidi.2024.301766.

2. Kazim A., Almaeeni F., Al Ali S., Iqbal F., Al-Hussaeni K. Memory Forensics: Recovering Chat Messages and Encryption Master Key // 2019 10th International Conference on Information and Communication Systems (ICICS). - 2019. - P. 58–64. - DOI: https://doi.org/10.1109/IACS.2019.8809179.

3. ISO/IEC 27037:2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. - ISO, 2012.

4. Microsoft. Обзор BitLocker и шифрования устройств в Windows 10/11 [Электронный ресурс]. - Microsoft Learn, 2023. - URL: https://learn.microsoft.com/windows/security/ (дата обращения: 20.10.2026).

MATNGA AXBOROT YASHIRISHNING IMKONIYATLARI VA CHEKLOVLARI HAMDA MAVJUD USULLARNING O‘ZBEK TILI SHAROITIDAGI ZAIF NUQTALARI TAHLILI

Xasanov K.A.
O‘zkomnazorat inspeksiyasi Samarqand viloyati hududiy bo‘limi
Ganiyev A.A.
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari,universiteti
Tairova D.A.
Zarmed University universiteti

Annotatsiya. Ushbu maqolada katta til modellari yaratgan o‘zbekcha matnlarni belgilash va ularning kelib chiqishini tasdiqlash algoritmi bayon etiladi. Sun’iy intellekt yaratgan matnni belgilashning mavjud usullari asosan ingliz va xitoy tillari materialida ishlab chiqilgan bo‘lib, o‘zbek tili kabi agglyutinativ tillarning morfologik xususiyatlari, ikki yozuvning parallel qo‘llanilishi va apostrof belgilarining xilma-xilligi hisobga olinmagan. O‘zbek tilidagi matnga axborot yashirishning imkoniyatlari va cheklovlari tahlil qilinib, mavjud usullarning o‘zbek tili sharoitidagi zaif nuqtalari aniqlangan.

Kalit so‘zlar: matn steganografiyasi, raqamli suv belgisi, katta til modellari, generativ steganografiya, o‘zbek tili, agglyutinativ til, tokenizatsiya, Unicode, morfologik o‘zgaruvchanlik, suv belgisi bardoshliligi.

Аннотация. В данной статье описывается алгоритм внедрения «водяных знаков» в тексты на узбекском языке, созданные большими языковыми моделями, а также метод проверки их происхождения. Существующие подходы к маркировке текстов, сгенерированных искусственным интеллектом, разрабатывались преимущественно для английского и китайского языков; они не учитывают морфологические особенности агглютинативных языков (к которым относится узбекский), параллельное использование двух систем письма, а также многофункциональность апострофов. В работе анализируются возможности и ограничения внедрения информации в узбекские тексты, а также выявляются недостатки существующих методов применительно к узбекскому языку.

Ключевые слова: текстовая стеганография, цифровые водяные знаки, большие языковые модели, генеративная стеганография, узбекский язык, агглютинативный язык, токенизация, Unicode, морфологическая изменчивость, устойчивость водяных знаков.

Matn steganografiyasi tasvir va audio steganografiyasiga nisbatan murakkabroq masala hisoblanadi. Tasvirda har bir piksel qiymatining kichik o‘zgarishi inson ko‘rish tizimi tomonidan sezilmaydi, ya’ni konteynerda psixovizual ortiqchalik mavjud. Matn esa diskret belgilar ketma-ketligi bo‘lib, undagi har bir o‘zgarish - harf, so‘z yoki tinish belgisining almashtirilishi - o‘quvchi tomonidan sezilishi yoki matn ma’nosini buzishi mumkin. Shu sababli matnga axborot yashirishning an’anaviy usullari uch sinfga ajratiladi. Birinchi sinf - format asosidagi usullar: axborot bo‘shliqlar soni, ko‘rinmas Unicode belgilari (masalan, nol kenglikdagi bo‘shliq U+200B) yoki shrift xususiyatlari orqali kodlanadi. Bu usullar sig‘imi yuqori bo‘lsa-da, matn qayta terilganda, oddiy matn formatiga o‘tkazilganda yoki normallashtirilganda belgi to‘liq yo‘qoladi. Ikkinchi sinf - leksik usullar: axborot sinonimlarni tanlash yoki gap tuzilishini o‘zgartirish orqali kodlanadi. Ular matnning semantikasiga bog‘langani uchun bardoshliroq, biroq sinonimlar lug‘ati

va sintaktik tahlilchi talab etiladi hamda almashtirishlar ko‘pincha tabiiy bo‘lmagan matn hosil qiladi. Uchinchi sinf - generativ (lingvistik) usullar: yashiriladigan axborot matnni yaratish jarayonining o‘zini boshqaradi, natijada stego-matn til modeli yaratgan oddiy matndan statistik jihatdan farqlanmaydi [1, 2].

Katta til modellari generativ steganografiya uchun tabiiy asos bo‘lib xizmat qiladi. Avtoregressiv til modeli matnni tokenlar ketma-ketligi $x_1, x_2, \ldots, x_n$ ko‘rinishida yaratadi: har bir qadamda model oldingi tokenlar asosida lug‘atning barcha V tokeni uchun logitlar vektori ℓ_t ni hisoblaydi va keyingi token quyidagi taqsimotdan tanlanadi:

$$p(x_t = v \mid x_{<t}) = \exp(\ell_t[v]/T) \,/\, \Sigma_{u \in V} \exp(\ell_t[u]/T), \quad (1)$$

bu yerda T - harorat parametri. Suv belgisini joylashtirish vazifasi logitlarni kalitga bog‘liq tarzda shunday o‘zgartirishdan iboratki, natijada matn sifati sezilarli yomonlashmasin, kalitga ega tomon esa matnning belgilanganligini statistik jihatdan ishonchli aniqlay olsin. Mualliflikni tasdiqlash nuqtayi nazaridan bu vazifa steganografiyaning maxsus holati - «nol bitli» suv belgisidir: bunda yashiriladigan xabar bitta faktdan iborat - «bu matn K kalitli tizim tomonidan yaratilgan». Kirchenbauer va boshqalar taklif etgan bazaviy usulda [3] har bir qadamda urug‘ oldingi token asosida hisoblanadi, lug‘at kalit va urug‘ bo‘yicha «yashil» G_t va «qizil» to‘plamlarga bo‘linadi hamda yashil tokenlarning logitlariga musbat siljish δ qo‘shiladi:

$$s_t = H_K(x_{t-1}), \quad |G_t| = \gamma|V|, \quad \tilde{\ell}_t[v] = \ell_t[v] + \delta \cdot \mathbb{1}[v \in G_t]. \quad (2)$$

Aniqlashda matndagi yashil tokenlar ulushi hisoblanadi: belgilanmagan matnda u taxminan γ ga teng bo‘lsa, belgilangan matnda sezilarli yuqori bo‘ladi. Mazkur usul sodda, generatsiya tezligiga deyarli ta’sir qilmaydi va aniqlash uchun til modelining o‘zini talab etmaydi. Shu sababli u keyingi ko‘plab tadqiqotlar uchun asos bo‘ldi: entropiyaga moslashtirilgan variantlar [4], urug‘ni butunlay kontekstdan mustaqil qiluvchi Unigram-Watermark [5], semantik jihatdan invariant belgilar [6] va sanoat miqyosidagi SynthID-Text tizimi [7] shular jumlasidandir.

Sun’iy intellekt yaratgan matnni belgilash usullarini bir necha mezon bo‘yicha tasniflash mumkin. Joylashtirish vaqti bo‘yicha generatsiyadan keyingi (post-hoc) usullar tayyor matnni o‘zgartiradi, generatsiya vaqtidagi usullar esa belgini matn yaratilishi jarayonida kiritadi. Katta til modellari uchun ikkinchi guruh ustun hisoblanadi, chunki unda matn sifati model imkoniyatlari bilan belgilanadi va qo‘shimcha tahrir talab etilmaydi. Taqsimotga ta’siri bo‘yicha «buzuvchi» usullar (bazaviy usul va uning ko‘plab variantlari) model taqsimotini kalitga bog‘liq tarzda siljitadi, «buzilishsiz» (distortion-free) usullar esa tanlash jarayonidagi tasodifiylikni kalitli psevdotasodifiy manba bilan almashtiradi va har bir alohida qadamda taqsimotni aynan saqlaydi [8, 9]. Ikkinchi guruh nazariy jihatdan jozibali bo‘lsa-da, aniqlash uchun odatda hisoblash jihatidan qimmat protseduralar talab etiladi va tahrirlarga bardoshlilik pasayadi. Axborot hajmi bo‘yicha nol bitli usullar faqat belgi mavjudligini tasdiqlaydi, ko‘p bitli usullar esa qo‘shimcha ravishda foydalanuvchi identifikatori yoki vaqt tamg‘asi kabi ma’lumotni kodlaydi. Mualliflikni tasdiqlash vazifasida nol bitli belgi ko‘p hollarda yetarli, chunki har bir muallif yoki tizim uchun alohida kalit ishlatilishi mumkin.

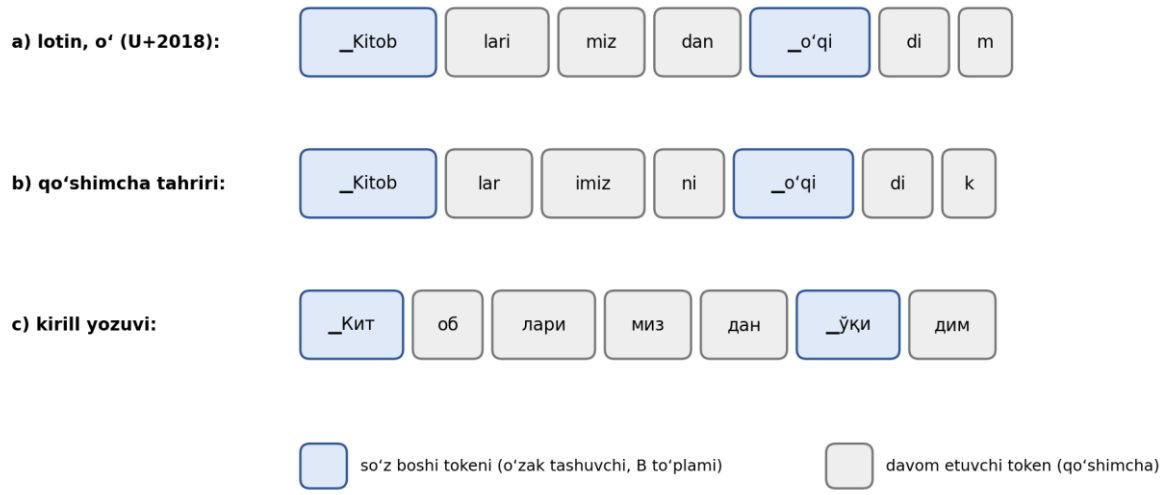
Matnli suv belgisiga qo‘yiladigan talablarni quyidagicha shakllantiramiz:

- sifatni saqlash - belgilangan matn belgisiz matndan ravonlik, grammatik to‘g‘rilik va mazmun jihatidan sezilarli farq qilmasligi kerak;
- aniqlanuvchanlik - kalitga ega tomon belgini ishonchli aniqlay olishi, belgisiz matnni esa yolg‘on ravishda belgilangan deb topish ehtimoli juda kichik bo‘lishi kerak;
- bardoshlilik - ma’noni saqlovchi o‘zgarishlar (yozuvni o‘girish, tahrirlash, qisman qayta yozish) belgini yo‘qotmasligi kerak;

- xavfsizlik - kalitsiz tomon belgini soxtalashtira olmasligi va uning parametrlarini tiklay olmasligi kerak;
- amaliylik - aniqlash til modeliga murojaat qilmasdan, oddiy hisoblash resurslarida bajarilishi, joylashtirish esa generatsiya tezligini sezilarli pasaytirmasligi kerak.

Bu talablar o‘zaro ziddiyatli: masalan, bardoshlilikni oshirish uchun belgini kuchaytirish sifatni pasaytiradi, xavfsizlikni oshirish uchun kontekstni kengaytirish esa bardoshlilikni kamaytiradi. Quyida ko‘rsatilganidek, o‘zbek tilining xususiyatlari bu ziddiyatlarni yanada keskinlashtiradi.

Endi bazaviy usulni o‘zbek tili sharoitida tahlil qilamiz. O‘zbek tili agglyutinativ tillar sirasiga kiradi: grammatik ma’nolar so‘z o‘zagiga ketma-ket qo‘shiluvchi qo‘shimchalar orqali ifodalanadi. Masalan, «kitoblarimizdan» so‘zi o‘zak (kitob), ko‘plik qo‘shimchasi (-lar), I shaxs ko‘plik egalik qo‘shimchasi (-imiz) va chiqish kelishigi qo‘shimchasidan (-dan) tarkib topgan. Zamonaviy til modellari matnni so‘zlarga emas, balki BPE [10] yoki SentencePiece [11] algoritmlari yordamida hosil qilingan so‘z bo‘laklariga (subword tokenlarga) ajratadi. Lug‘atning asosiy qismi ingliz va boshqa yirik tillar korpuslarida shakllangani sababli o‘zbekcha so‘zlar ko‘pincha bir nechta tokenga bo‘linadi: o‘zak odatda birinchi, yangi so‘z boshlanishini bildiruvchi (▁ yoki Ġ belgili) tokenga to‘g‘ri keladi, qo‘shimchalar esa keyingi, davom etuvchi tokenlarga tushadi. Kichik o‘zbekcha korpusda o‘qitilgan BPE tokenizatori misolida «Kitoblarimizdan o‘qidim» gapi «▁Kitob | lari | miz | dan | ▁o‘qi | di | m» ko‘rinishidagi yettita tokenga ajraldi (1-rasm, a). Bu kuzatish taklif etilayotgan algoritmning asosiy g‘oyasiga zamin bo‘ladi.



1-rasm. O‘zbekcha gapning tokenizatsiyasi (sxematik): a) asl matn; b) qo‘shimchasi o‘zgartirilgan matn; c) kirill yozuvidagi matn

O‘zbek tilidagi matnning suv belgisi nuqtayi nazaridan uchta muhim xususiyatini ajratib ko‘rsatamiz. Birinchi xususiyat - morfologik o‘zgaruvchanlik. Matn tahrirlanganda yoki parafraz qilinganda so‘zlarning o‘zagi ko‘pincha saqlanib, qo‘shimchalari o‘zgaradi: «kitoblarimizdan o‘qidim» → «kitoblarimizni o‘qidik». 1-rasmning b qismidan ko‘rinib turibdiki, bunday tahrirda o‘zak tokenlari o‘zgarmaydi, qo‘shimcha tokenlari esa butunlay boshqacha bo‘ladi. Bazaviy usulda urug‘ oldingi tokendan hisoblangani uchun har bir o‘zgargan qo‘shimcha tokeni ikki pozitsiyaga ta’sir qiladi: uning o‘zi va undan keyingi token uchun urug‘ o‘zgaradi. Agglyutinativ tilda tokenlarning katta qismi qo‘shimchalarga to‘g‘ri kelgani sababli bunday tahrir belgining sezilarli qismini yo‘qotadi.

Ikkinchi xususiyat - ikki yozuvning parallel qo‘llanilishi. 1993-yilda qabul qilingan va 1995-yilda tahrir etilgan «Lotin yozuviga asoslangan o‘zbek alifbosini joriy etish to‘g‘risida»gi Qonunga [12] muvofiq rasmiy yozuv lotin alifbosi hisoblansa-da, amalda kirill yozuvi ommaviy axborot vositalari, ijtimoiy tarmoqlar va kundalik yozishmalarda keng qo‘llanilmoqda. Lotin va kirill yozuvlari o‘rtasida avtomatik o‘girish oddiy dasturiy vosita bilan bajariladi, ammo tokenlar darajasida bu ikki matn butunlay farq qiladi (1-rasm, c): kirill yozuvidagi so‘z boshqa tokenlarga, boshqa bo‘linishga va boshqa identifikatorlarga ega bo‘ladi. Demak, belgilangan lotincha matnni kirillga o‘girish - ma’noni to‘liq saqlaydigan, bajarilishi oson va bazaviy usul uchun halokatli hujumdir: barcha tokenlar va barcha urug‘lar o‘zgaradi.

Uchinchi xususiyat - apostrof belgilarining xilma-xilligi. Lotin yozuvidagi o‘ va g‘ harflari hamda tutuq belgisi amalda kamida besh xil Unicode belgisi bilan yoziladi (1-jadval). Ko‘rinishda deyarli bir xil bo‘lgan bu variantlar tokenizator uchun turli baytlar ketma-ketligidir. Shuning uchun apostroflarni boshqa shaklga almashtirish ham matn ma’nosiga ta’sir qilmagan holda ko‘plab tokenlarni o‘zgartiradi.

1-jadval

O‘zbek lotin yozuvida o‘, g‘ va tutuq belgisini ifodalovchi belgilar

Belgi	Unicode kodi	Nomi	Qo‘llanish holati
‘	U+2018	Chap bittalik qo‘shtirnoq	O‘ va g‘ harflari uchun keng tarqalgan yozuv
ʻ	U+02BB	Modifikator harf: teskari vergul	O‘ va g‘ harflari uchun orfografik to‘g‘ri belgi
’	U+02BC	Modifikator harf: apostrof	Tutuq belgisi uchun orfografik to‘g‘ri belgi
'	U+0027	ASCII apostrof	Klaviaturada eng qulay, internetda keng tarqalgan
’	U+2019	O‘ng bittalik qo‘shtirnoq	Matn muharrirlarining avtomatik almashtirishi natijasi

Yuqoridagi tahlildan bazaviy usulning o‘zbek tili sharoitidagi uchta zaif nuqtasi kelib chiqadi. Birinchidan, urug‘ning oldingi token identifikatoriga bog‘liqligi: yozuv, apostrof yoki qo‘shimcha o‘zgarishi bilan urug‘ ham o‘zgaradi. Ikkinchidan, qo‘shimcha tokenlarini belgilash: bu tokenlar grammatik jihatdan qat’iy belgilangan, ya’ni past entropiyali bo‘lib, ular uchun siljish δ yo belgini deyarli kuchaytirmaydi (model baribir to‘g‘ri qo‘shimchani tanlaydi), yo grammatik xatoga olib keladi (model noto‘g‘ri qo‘shimchani tanlashga majbur bo‘ladi); bundan tashqari, aynan shu tokenlar tahrirda eng ko‘p o‘zgaradi. Uchinchidan, so‘z chegarasining buzilishi: bazaviy usulda yashil tokenlar orasida ham so‘z boshlovchi, ham davom etuvchi tokenlar bo‘lgani uchun siljish modelning so‘zni qaerda tugatishi haqidagi qaroriga ta’sir qiladi va natijada so‘zlar noto‘g‘ri bo‘linishi mumkin. Keyingi paragrafda ushbu uchta zaif nuqtani bartaraf etuvchi algoritm ishlab chiqiladi.

Xulosa

Shu o‘rinda o‘zbek tilidagi matnni belgilashning yana bir jihatiga to‘xtalish lozim - belgilash va sifat o‘rtasidagi muvozanat. Agar belgi juda kuchli bo‘lsa (δ katta), model tabiiy bo‘lmagan so‘zlarni tanlashga majbur bo‘ladi va matn sifati pasayadi; agar juda kuchsiz bo‘lsa, aniqlash uchun uzun matn talab etiladi. O‘zbek tilida bu muvozanat ikki sababga ko‘ra yanada

nozik: birinchidan, ko‘p tilli modellarning o‘zbek tilidagi matn yaratish sifati yirik tillardagiga nisbatan pastroq, ya’ni qo‘shimcha buzilishga «zaxira» kamroq; ikkinchidan, qo‘shimchalar zanjiridagi bitta xato butun so‘z shaklini buzadi. Taklif etilayotgan algoritmda siljish faqat so‘z tanlash darajasida amalga oshirilishi aynan shu muammoga javobdir.

Foydalanilgan adabiyotlar

1. Fang T., Jaggi M., Argyraki K. Generating Steganographic Text with LSTMs // Proceedings of ACL Student Research Workshop. - 2017.
2. Ziegler Z., Deng Y., Rush A. Neural Linguistic Steganography // Proceedings of EMNLP-IJCNLP. - 2019. - P. 1210-1215.
3. Kirchenbauer J., Geiping J., Wen Y. et al. A Watermark for Large Language Models // Proceedings of ICML. - 2023.
4. Lee T., Hong S., Ahn J. et al. Who Wrote this Code? Watermarking for Code Generation // Proceedings of ACL. - 2024.
5. Zhao X., Ananth P., Li L., Wang Y.-X. Provable Robust Watermarking for AI-Generated Text // Proceedings of ICLR. - 2024.
6. Liu A., Pan L., Hu X., Meng S., Wen L. A Semantic Invariant Robust Watermark for Large Language Models // Proceedings of ICLR. - 2024.
7. Dathathri S. et al. Scalable watermarking for identifying large language model outputs // Nature. - 2024. - Vol. 634. - P. 818-823.
8. Kuditipudi R., Thickstun J., Hashimoto T., Liang P. Robust Distortion-free Watermarks for Language Models // Transactions on Machine Learning Research. - 2024 (arXiv:2307.15593).
9. Christ M., Gunn S., Zamir O. Undetectable Watermarks for Language Models // Proceedings of COLT. - 2024 (arXiv:2306.09194).
10. Sennrich R., Haddow B., Birch A. Neural Machine Translation of Rare Words with Subword Units // Proceedings of ACL. - 2016. - P. 1715–1725.
11. Kudo T., Richardson J. SentencePiece: A simple and language independent subword tokenizer and detokenizer for Neural Text Processing // Proceedings of EMNLP: System Demonstrations. - 2018. - P. 66–71.
12. O‘zbekiston Respublikasining «Lotin yozuviga asoslangan o‘zbek alifbosini joriy etish to‘g‘risida»gi Qonuni (1993-yil 2-sentabr, 1995-yil 6-maydagi tahriri) // lex.uz.

O‘ZBEKISTONDAGI ELEKTRON PUL TIZIMLARIDA SUN’IY INTELLEKT VA IJTIMOIY MUHANDISLIK TAHDIDLARI HAMDA ULARGA QARSHI HIMOYA CHORALARI

Fayzullayev O.X.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Ushbu maqolada O‘zbekiston Respublikasida faoliyat yuritayotgan elektron pul tizimlarida (EPT) axborot xavfsizligini ta’minlashning zamonaviy muammolari tadqiq etilgan. Xususan, kiberjinoyatchilar tomonidan sun’iy intellekt (SI) texnologiyalari va ijtimoiy muhandislik usullarining birgalikda qo‘llanilishi natijasida yuzaga kelayotgan yangi avlod tahdidlari tahlil qilingan. Tadqiqot davomida “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi, “Kiberxavfsizlik to‘g‘risida”gi qonunlar hamda “O‘zbekiston – 2030” strategiyasi doirasida belgilangan vazifalarning EPT xavfsizligini ta’minlashdagi o‘rni ochib berilgan. Shuningdek, O‘zbekistondagi yirik EPT operatorlari (CLICK, Payme, OSON, Uzum va boshqalar) tajribasi asosida SI va ijtimoiy muhandislik tahdidlariga qarshi qo‘llanilayotgan himoya mexanizmlari tizimlashtirilib, sohaga doir ilmiy-amaliy takliflar ishlab chiqilgan.

Kalit so‘zlar: Elektron pul tizimlari, kiberxavfsizlik, sun’iy intellekt, ijtimoiy muhandislik, fishing, vishing, deepfake, anti-fraud tizimlari, liveness detection, behavioral skoring.

Аннотация. В данной статье рассматриваются современные проблемы обеспечения информационной безопасности в системах электронных денег (СЭД), функционирующих в Республике Узбекистан. В частности, анализируется новое поколение угроз, возникающих в результате комбинированного использования технологий искусственного интеллекта (ИИ) и методов социальной инженерии киберпреступниками. В ходе исследования выявлена роль законов «О платежах и платежных системах», «О кибербезопасности» и задач, поставленных в рамках стратегии «Узбекистан – 2030», в обеспечении безопасности СЭД. Также на основе опыта крупнейших операторов СЭД в Узбекистане (CLICK, Payme, OSON, Uzum и др.) систематизированы механизмы защиты от угроз ИИ и социальной инженерии, а также разработаны научно-практические предложения в этой области.

Ключевые слова: Системы электронных денег, кибербезопасность, искусственный интеллект, социальная инженерия, фишинг, вишинг, дипфейк, системы защиты от мошенничества, проверка подлинности, поведенческая оценка.

Kirish

Jahon iqtisodiyotining raqamlashtirilishi sharoitida naqd pulsiz hisob-kitoblar ko‘lami tezkorlik bilan o‘sib bormoqda. O‘zbekiston moliya bozorida ham fuqarolar va biznes vakillari raqamli to‘lov tizimlari, xususan elektron pul tizimlaridan orqali to‘lovlarni amalga oshirishni afzal ko‘rmoqda. Mazkur ehtiyojlardan kelib chiqib OSON, CLICK, Payme, Pay Way kabi mahalliy platformalar tijorat banklari bilan hamkorlikda innovatsion to‘lov xizmatlarini taqdim etmoqda.

Moliyaviy texnologiyalarning (FinTech) rivojlanishi bilan bir qatorda, kiberjinoyatchilik usullari ham transformatsiyaga uchramoqda. So‘nggi yillarda an'anaviy xakerlik hujumlaridan ko‘ra, inson psixologiyasiga ta’sir o‘tkazuvchi “ijtimoiy muhandislik” tahdidlari (foydalanuvchini aldash, ishontirish, qo‘rqitish yoki qiziqtirish orqali o‘z ixtiyori bilan maxfiy ma’lumotlarni (login,

parol, SMS orqali kelgan tasdiqlash kodi, electron hamyon va bank kartasi raqami va CVV kodlarini) uchinchi shaxslarga topshirishiga majbur qilish texnologiyasi) va jarayonlarni avtomatlashtiruvchi “sun’iy intellekt” imkoniyatlaridan g‘arazli maqsadlarda foydalanish tendensiyasi keskin kuchayib bormoqda. Bu esa moliya institutlari, EPT operatorlari va davlat regulyatorlari oldiga axborot xavfsizligini mutlaqo yangi konseptual yondashuvlar asosida ta’minlash vazifasini qo‘ymoqda.

Asosiy qism

Zamonaviy kiber tahdidlarning eng xavfli jihatilaridan biri shundaki, ular bevosita dasturiy ta’minotdagi zaifliklarga emas, balki tizimning eng zaif bo‘g‘ini hisoblangan inson omiliga qaratilgan. Bunga asosiy sabab, xalqimizning o‘ziga xos ijtimoiy-madaniy muhiti, xalqning to‘lov tizimi, bank, moliya va davlat tashkilotlariga bo‘lgan o‘ta yuqori ishonchi kabi lokal omillar. Shuningdek, foydalanuvchilar orasida raqamli savodxonlik (kiber-gigiyena) darajasining pastligi, parollarni ishonib topshirish odati, tezkor boyish ilinjida turli aksiyalarga ko‘r-ko‘rona ishonish holatlari kiberhujumlarning ta’sir doirasini yanada kengaytirmoqda.

Shu asosda respublikamiz bo‘ylab kiberjinoyatlar soni ham o‘sib bormoqda. So‘nggi ma’lumotlarga ko‘ra, 2021-2025-yillar oralig'ida O‘zbekistonda kiberjinoyatlar soni 11 baravarga (4865 tadan 62440 tagacha) keskin ko‘paygan. Birgina 2026-yilning dastlabki 9 oyida 69 mingdan ortiq kiberjinoyat sodir etilgan bo‘lib, fuqarolar ko‘rgan jami moddiy zarar 1 trillion so‘mdan oshib ketdi. Huquq-tartibot organlarining tezkor chora-tadbirlari va surishtiruvlari natijasida o‘g‘irlangan pullarning faqat 210 milliard so‘mi o‘z egalariga qaytarilgan.

Ijtimoiy muhandislik (Social Engineering) hujumlari. Elektron pul tizimlari foydalanuvchilariga nisbatan ijtimoiy muhandislik tahdidlari quyidagi shakllarda namoyon bo‘lmoqda:

- *Vishing (Voice Phishing)* – o‘zini "Markaziy bank", "Bank, to‘lov tizimi xavfsizlik xizmati" yoki emitent bank xodimi sifatida tanishtirib, foydalanuvchiga qo‘ng‘iroq qilish va “karta bloklangani” yoki “shubhali tranzaksiya amalga oshirilayotgani”ni aytib vahima uyg‘otish. Maqsad – SMS orqali kelgan tasdiqlash kodini qo‘lga kiritish.
- *Fishing va Smishing* – elektron pochta yoki SMS/Telegram orqali soxta havolalar yuborish. Masalan, "Siz yutuq yutdingiz, mablag‘ni OSON hamyoningizga qabul qilish uchun havolaga o‘ting". Havola EPTning rasmiy saytiga vizual jihatdan to‘liq o‘xshash bo‘lgan soxta (fishing) sahifaga olib boradi va login, parol hamda karta ma’lumotlarini o‘g‘irlaydi.

Sun’iy intellekt orqali modifikatsiyalangan tahdidlar. SI texnologiyalari ijtimoiy muhandislik hujumlarini mukammal darajada avtomatlashtirib, ularning ishonchliligini oshirmoqda:

- *Ovozni klonlash (Voice Cloning) va Deepfake* – jinoyatchilar neyrotarmoqlar yordamida foydalanuvchining tanishlari, qarindoshlari yoki davlat idoralari rahbarlarining ovozini aynan o‘xshatib soxtalashtirishi mumkin. Ovozli xabarlar (audio-deepfake) orqali qarzdorlikni uzish yoki zudlik bilan Payme/Click orqali pul tashlab berishni so‘rash holatlari ko‘paymoqda.
- *Generativ matn SI (SI botlar)* – ilgari fishing xabarlarida grammatik xatolar ko‘p bo‘lgan bo‘lsa, hozirda SI yordamida mukammal o‘zbek tilida, rasmiy ohangdagi ishonchli matnlar ishlab chiqilmoqda. Shuningdek, ijtimoiy tarmoqlarda mijozlarni chalg‘ituvchi avtomatlashtirilgan "yordamchi" botlar (SI) yaratilmoqda.

SI va ijtimoiy muhandislik tahdidlariga qarshi ko‘rilayotgan himoya choralari. O‘zbekistonda elektron pul tizimlari faoliyatini tartibga solish va ularning xavfsizligini ta’minlash maqsadida quyidagi huquqiy-normativ hujjatlar ishlab chiqilgan:

O‘zbekiston Respublikasining 2019-yil 1-noyabrda qabul qilingan “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi Qonuni va ushbu qonun asosida O‘zbekiston Respublikasi Markaziy banki boshqaruvining 2020-yil 29-apreldagi “O‘zbekiston Respublikasi hududida elektron pullarning chiqarilishi va muomalada bo‘lishi qoidalarini tasdiqlash to‘g‘risida”gi Qarori O‘zbekistonda elektron pullar va to‘lov tizimlari faoliyatining huquqiy asosini yaratdi. Ushbu huquqiy-normativ hujjatlarga muvofiq, elektron pul tizimi operatorlari (MChJlar) va emitentlari (Tijorat banklari) tranzaksiyalarning xavfsizligi, uzluksizligi hamda mijozlar ma’lumotlarining maxfiyligi uchun bevosita javobgardir. Qonunda axborotni shifrlash, ruxsatsiz ulanishlarning oldini olish va firibgarlik holatlari bo‘yicha monitoring (anti-fraud) tizimlarini joriy etish majburiyati qat’iy belgilab qo‘yilgan.

Bundan tashqari, O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi Qonuni moliya va to‘lov tizimlarini muhim axborot infratuzilmasi obyektlari toifasiga kiritadi. Qonunda kiberhujum, kiberxavfsizlik tahdidi kabi tushunchalarga ta’rif berilib, muhim axborot infratuzilmasi obyektlarida axborot xavfsizligini ta’minlashning yagona davlat siyosati belgilangan. EPT operatorlari ushbu qonun talablaridan kelib chiqib, kiberhujumlarni barvaqt aniqlash va ularning oqibatlarini bartaraf etish bo‘yicha chora-tadbirlar rejasiga ega bo‘lishlari shart.

Shuningdek, O‘zbekiston Respublikasi Prezidentining 2023-yil 11-sentyabrdagi PF-158-son Farmoni bilan tasdiqlangan “O‘zbekiston – 2030” strategiyasi raqamli iqtisodiyotni rivojlantirishda yangi maqsadlarni belgilab berdi. Strategiyaning “Raqamli texnologiyalarni rivojlantirish” yo‘nalishida IT-xizmatlar eksportini oshirish, raqamli infratuzilmani modernizatsiya qilish bilan birga, kiberxavfsizlikni ta’minlash darajasini keskin oshirish alohida maqsad sifatida qayd etilgan. Elektron hukumat va raqamli moliya tizimlarida sun’iy intellekt texnologiyalarini keng joriy etish orqali xavfsizlikni ta’minlash, aholining raqamli va moliyaviy savodxonligini yuksaltirish strategiyaning ustuvor yo‘nalishlaridan hisoblanadi.

Bugungi kunda elektron pul tizimlari hamda emitent banklar o‘z xavfsizlik siyosatlarida SI va ijtimoiy muhandislikka qarshi kompleks yondashuvni qo‘llamoqdalar. Ularni 3 ta asosiy yo‘nalishga ajratish mumkin:

Sun’iy intellektga asoslangan biometrik va xulq-atvor tahlili (Anti-Fraud SI). Kiberjinoyatchilarning SI qo‘llashiga javoban, EPT operatorlari ham xavfsizlik arxitekturasiga SI xavfsizlik tizimlarini joriy etmoqda:

- *Liveness Detection (Jonlilikni aniqlash):* elektron pul tizimlarida identifikatsiyadan o‘tish jarayonida FaceID texnologiyalari ishlatiladi. SI algoritmi kameraga qarab turgan shaxs haqiqiy insonmi yoki statik surat/deepfake videomi ekanligini mikromimika, yorug‘lik tushishi va ko‘z harakatlari orqali aniqlaydi.

- *Behavioral (xulq-atvor) skoring:* Emitent banklar tizimlari bilan integratsiyalashgan holda, EPTlar har bir mijozning odatiy harakat ko‘rinishlarini (pattern) SI orqali o‘rganib chiqadi. Agar tizimga noodatiy qurilmadan (masalan, chet el IP manzili orqali) kirilib, tunda barcha mablag‘lar noma’lum hamyonga o‘tkazilayotgan bo‘lsa, SI asosidagi Anti-Fraud tizimi operatsiyani inson aralashuvisiz, avtomatik bloklaydi va mijozdan qo‘shimcha verifikatsiya talab qiladi.

Ijtimoiy muhandislik tahdidlariga qarshi “Foydalanuvchi interfeysi” himoyasi. Texnologiya inson ishonchini to‘la himoya qila olmagani sababli, tizim operatorlari proaktiv usullarga o‘tgan:

SMS va Push ogohlantirishlar arxitekturasi: Barcha operatorlar tasdiqlash kodlari matniga *“Hech kimga, hatto bank xodimiga ham ushbu kodni aytmang!”* degan qat’iy ogohlantirishlarni kiritgan.

- *Tranzaksiyani kechiktirish (Cooling-off period)* – yirik summadagi va shubhali P2P (bir kartadan ikkinchisiga) o‘tkazmalarda, ayniqsa ijtimoiy muhandislik qurboni bo‘layotgan keksalar va tajribasiz foydalanuvchilarni himoya qilish uchun to‘lovni tasdiqlashda ekranda “Sizni hech kim ushbu to‘lovni qilishga majburlamayaptimi?” mazmunidagi qo‘shimcha interaktiv so‘rovnomalar joriy etilmoqda.

Regulyator va tijorat banklari bilan axborot almashinuvi. “O‘zbekiston – 2030” strategiyasidagi xavfsiz raqamli iqtisodiyot talablaridan kelib chiqib, Markaziy Bank qoshida Kiberxavfsizlik markazi faoliyati yo‘lga qo‘yilgan. OSON, CLICK, Payme kabi tizimlar barcha firibgarlik urinishlari bo‘yicha ma’lumotlarni yagona bazaga kiritadi. Agar bir tizimda (masalan, Paynet Wallet) aniqlangan firibgar akkaunt bloklansa, uning rekvizitlari avtomatik ravishda boshqa tizimlar (A-Pay, Interpay, 1HLSW) uchun ham blokirovka qilinadi.

Xulosa

O‘zbekiston EPTlarida axborot xavfsizligini ta’minlash endilikda faqatgina dasturiy kodlarni himoyalash emas, balki SI algoritmlari jangi (firibgar SI va himoyachi SI) hamda inson psixologiyasini sun’iy intellekt va ijtimoiy muhandislik tahdidlaridan himoya qilishga o‘rgatish darajasiga ko‘tarildi. “O‘zbekiston – 2030” strategiyasi maqsadlari va o‘tkazilgan tahlillardan kelib chiqib, quyidagi mamlakatimizdagi elektron pul tizimlarining axborot xavfsizligi siyosatida quyidagi ilmiy-amaliy takliflar ilgari suriladi:

Milliy Anti-Fraud Ekosistemasini yaratish: Barcha EPT operatorlari, xususan kichik operatorlar (“1HLSW”, “ExMoney”, “AIST”) axborot xavfsizligini ta’minlashda yirik banklarning ilg‘or sun’iy intellekt tahlili xizmatlaridan arzon yoki bepul foydalanishiga imkon beruvchi yagona Davlat anti-fraud platformasini ishga tushirish zarur.

Huquqiy javobgarlikni kuchaytirish. “Kiberxavfsizlik to‘g‘risida”gi qonun va Jinoyat kodeksiga sun’iy intellekt (deepfake, ovoz klonlash) yordamida sodir etilgan moliyaviy firibgarlikni og‘irlashtiruvchi holat sifatida baholovchi maxsus normalarni kiritish lozim.

Raqamli gigiyena va savodxonlik. “O‘zbekiston – 2030” strategiyasida belgilanganidek, inson omilini himoya qilishning yagona yo‘li – ta’lim. Maktab dasturlaridan boshlab oliy ta’limgacha ijtimoiy muhandislik tahdidlarini tanib olish bo‘yicha “Raqamli moliyaviy gigiyena” kurslarini ommaviy joriy etish talab etiladi.

Majburiy biometrik Liveness Detection (Jonlilikni aniqlash). Shubhali qurilmalardan EPT hisoblariga (masalan, uzoq vaqt kirmagan Payme yoki Click akkauntiga) kirish yoki katta miqdordagi to‘lovlarni amalga oshirishda majburiy tartibda biometrik jonlilikni aniqlash tizimlarini qonuniy talab darajasida mustahkamlash kerak.

Ushbu choralarning kompleks tatbiq etilishi mamlakatimiz raqamli iqtisodiyotining barqaror rivojlanishini ta’minlab, fuqarolarning elektron pul tizimlariga bo‘lgan ishonchini yanada mustahkamlaydi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining 01.11.2019 yildagi “To‘lovlar va to‘lov tizimlari to‘g‘risida”gi O‘RQ-578-son Qonuni.

2. O‘zbekiston Respublikasining 15.04.2022-yildagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.

3. “O‘zbekiston–2030” strategiyasi. O‘zbekiston Respublikasi Prezidentining 11.09.2023 yildagi PF-158-son Farmoni.

4. O.P. Shukurov, Ijtimoiy muhandislik hujumlari va ulardan himoyalanish masalalari: O‘zbekistondagi holat, muammolar va yechimlar. Journal of Effective Learning and Sustainable Innovation Vol.4 №5 (2026).

5. N. Amirmamatov, Click, Trust, Lose: An Analysis of Social Engineering Vulnerabilities in Uzbekistan. Matrix Academic International Online Journal Of Engineering And Technology 9(1):16-22

6. Markaziy bank CERT-CBU Kiberxavfsizlik markazi faoliyati va to‘lov tizimlari operatorlari uchun kiberxavfsizlik talablari. // cbu.uz

7. O‘zbekiston Respublikasi Markaziy Banki rasmiy ma’lumotlari va EPT (CLICK, Payme, Uzum va boshqalar) ochiq maxfiylik siyosati hujjatlari.

8. Xalqaro tadqiqotlar: The impact of AI-powered social engineering, vishing, voice cloning, and deepfakes on fintech/payment systems (nasscom, American Banker, Biometric Update va boshqa 2024–2026-yilgi materiallar).

9. https://www.wikipedia.org/

10. https://www.gazeta.uz/

11. https://zamin.uz/

ZAMONAVIY KIBERXAVFSIZLIK TAHDIDLARI SHAROITIDA AXBOROTLASHTIRISH OBYEKTLARINI ATTESTATSIYADAN O‘TKAZISHNING METODOLOGIK ASOSLARI

Madjitov K.M., Sayidmurotov Sh.Sh.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar institute

Annotatsiya. Ushbu tezisda axborotlashtirish obyektlarini zamonaviy kiberxavfsizlik talablari va milliy qonunchilik doirasida attestatsiyadan o‘tkazishning konseptual va amaliy mexanizmlari tahlil qilingan. Kibertahdidlar dinamikasi, obyektlarning strategik tasnifi, attestatsiyaning 12 bosqichli modeli va xorijiy ilg‘or tajribalar asosida amaliy takliflar keltirilgan.

Kalit so‘zlar: kiberxavfsizlik, axborotlashtirish obyekti, attestatsiya, CIA triadasi, kibertahdidlar, muhim axborot infratuzilmasi, NIST RMF, instrumental nazorat.

Аннотация. В данной научной статье анализируются концептуальные и практические механизмы аттестации объектов информатизации в рамках современных требований кибербезопасности и национального законодательства. Приведены научно обоснованные предложения на основе динамики киберугроз, стратегической классификации объектов, 12-этапной модели аттестации и передового зарубежного опыта.

Ключевые слова: кибербезопасность, объект информатизации, аттестация, триада CIA, киберугрозы, критическая информационная инфраструктура, NIST RMF, инструментальный контроль.

Kirish

Bugungi raqamli transformatsiya davrida davlat organlari va korxonalarda axborot-kommunikatsiya tizimlaridan foydalanish ko‘lami shiddat bilan kengaymoqda. Shu bilan birga, kibermakonda murakkab maqsadli kiberhujumlar, axborot sizib chiqishi va xizmat ko‘rsatishni izdan chiqaruvchi xatarlarning ortishi obyektlarning haqiqiy himoyalanganligini ta’minlashni dolzarb vazifaga aylantirmoqda. Ushbu sharoitda axborotlashtirish obyektlarini davlat attestatsiyasidan o‘tkazish tizimning daxlsizligini kafolatlovchi asosiy vositadir. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni 4-moddasida belgilangan «kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv» prinsipi huquqiy, ma’muriy va texnik mexanizmlarni uyg‘unlashtirishni talab etadi.

Tadqiqotning maqsadi axborotlashtirish obyektlarini kiberxavfsizlik talablari doirasida attestatsiyadan o‘tkazish bo‘yicha respublika qonunchiligiga mos namunaviy metodika ishlab chiqishdan iborat. Shundan kelib chiqib, kiberxavfsizlikning nazariy mezonlarini tahlil qilish, obyektlar toifalarini ajratish, 12 bosqichli attestatsiya jarayonini ishlab chiqish va xorijiy tajribani moslashtirish vazifalari hal etilgan.

Asosiy qism

Axborot xavfsizligi asosini CIA triadasi (Maxfiylik, Yaxlitlik, Foydalanish imkoniyati) tashkil etadi. Kiberxavfsizlik esa ushbu uchlikni raqamli infratuzilma, serverlar va dasturiy ta’minotda kompleks tarzda amalga oshirishga ixtisoslashgan.



1-rasm. Axborot xavfsizligining asosiy mezonlari (CIA triadasi)

Axborotlashtirish obyekti tushunchasi axborot tizimlari, telekommunikatsiya tarmoqlari, texnik vositalar, ma’lumotlar bazalari hamda maxfiy muzokaralar o‘tkaziladigan xonalarni o‘z ichiga oladi. Mazkur infratuzilmalarga qaratilgan asosiy destruktiv tahdidlar tizim funksionalligini buzishga qaratilgan bo‘lib, ular quyidagi 2-rasmda ifodalangan.



2-rasm. Axborotlashtirish obyektlariga qaratilgan asosiy kiberxavfsizlik tahdidlari

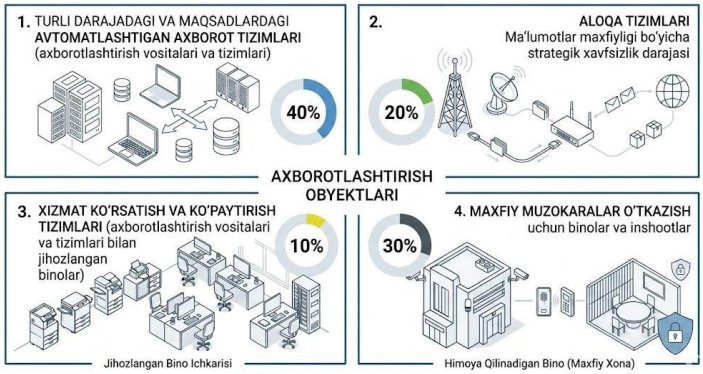
Axborotlashtirish obyektlariga tahdid soluvchi asosiy omillar quyidagilardir:

- zararli dasturlar (Malware): Viruslar, troyanlar, josuslik dasturlari va ma’lumotlarni shifrlab tovon talab qiluvchi bloklovchi (ransomware) tizimlar;
- fishing (Phishing) hujumlari: Ijtimoiy muhandislik orqali foydalanuvchilarning maxfiy autentifikatsiya ma’lumotlari va parollarini o‘g‘irlash usuli;
- DDoS hujumlari: Server va aloqa kanallariga soxta so‘rovlar oqimini yuborib, qonuniy xizmatlarni to‘xtatib qo‘yish va uzilish keltirib chiqarish;
- ruxsatsiz kirish va ma’lumotlar sizib chiqishi (Data Leakage): Tizimdagi bo‘shliqlar va zaifliklardan foydalanib noqonuniy kirish hamda maxfiy axborotning oqib ketishi.



3-rasm. Axborot va kiberxavfsizlikning o‘zaro uzviy bog‘liqligi

Kiberxavfsizlik umumiy axborot xavfsizligining tarkibiy qismi bo‘lib, apparat va raqamli muhitdagi axborotlashtirish obyektlarining xavfsiz va uzluksiz ishlashini ta’minlashda yetakchi o‘rin tutadi. Amaldagi me’yoriy hujjatlarga binoan axborotlashtirish obyektlari to‘rtta asosiy toifaga ajratiladi. Har bir yo‘nalishning tashkilot faoliyatiga ta’siri va xavf ehtimoli asosida foizli salmog‘i ishlab chiqilgan.



4-rasm. Axborotlashtirish obyektlarini strategik muhimlik darajasi bo‘yicha taqsimoti

1-jadval

Obyektlarning xavfsizlik iyerarxiyasidagi o‘rni quyidagi

№	Obyekt toifasi	Ulush	Strategik ahamiyati va asoslanishi
1	Avtomatlashtirilgan tizimlar (AT, MB)	40%	Eng yuqori muhimlik. Barcha elektron ma'lumotlar bazalari, xizmatlar saqlanadi. Ishdan chiqishi faoliyatni to'xtatadi.
2	Maxfiy muzokaralar binolari	30%	O‘ta yuqori maxfiylik. Davlat va korporativ strategik sirlar. Akustik sizib chiqish oqibatlarini qayta tiklab bo‘lmaydi.
3	Aloqa va ma’lumot uzatish tizimlari	20%	O‘rta-yuqori muhimlik. Routerlar, kabellar va tranzit oqimlari. Kriptografik va tarmoq himoyasini talab qiladi.
4	Xizmat ko‘rsatish tizimlari	10%	Taktik muhimlik. Printer, skaner va ish xonalari. Asosan operatsion va kundalik ochiq hujjatlarga xizmat qiladi.

Attestatsiyadan o‘tkazish - obyektning axborot va kiberxavfsizlik davlat standartlariga haqiqiy muvofiqligini baholovchi ilmiy-texnik tadbirlar majmuidir. Tadqiqot doirasida ishlab chiqilgan 12 bosqichli kompleks tekshiruv algoritmi quyidagilarni qamrab oladi:

1. Boshlang‘ich o‘rganish: Obyekt tarkibi, dasturiy-texnik vositalar va axborot turlari bo‘yicha dastlabki ma’lumotlar yig‘iladi;

2. Tahdidlarni aniqlash: Obyekt vazifasidan kelib chiqib tahdidlar modeli va maxsus sinov dasturi ishlab chiqiladi;

3. Test vositalarini belgilash: Attestatsiyada qo‘llaniladigan laboratoriya, o‘lchov va dasturiy skanerlar aniqlashtiriladi;

4. Foydalanishga ruxsat tizimi: Autentifikatsiya, avtorizatsiya va foydalanuvchilarning kirish huquqlari matritsasi tekshiriladi;

5. Tashkiliy-texnik talablar: Axborot xavfsizligi siyosati, ichki me’yoriy reglamentlar va boshqaruv choralari baholanadi;

6. Konfidensial axborot himoyasi: Maxfiy ma’lumotlarni ruxsatsiz nusxalash va tarqalishdan himoyalash holati o‘rganiladi;

7. Kamchiliklarni qayd etish: Aniqlangan zaifliklar va me’yoriy nomuvofiqliklar bo‘yicha rasmiy dalolatnomalar tuziladi;

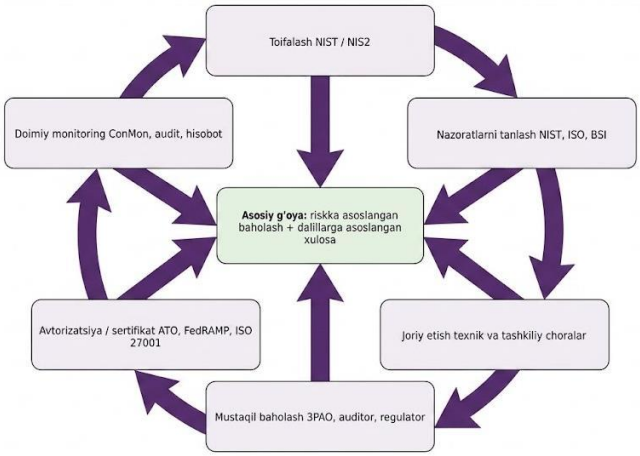
8. Maxsus laboratoriya sinovlari: Texnik vositalar laboratoriya sharoitida xavfsizlik talablariga mosligi sinovdan o‘tkaziladi;

9. Instrumental texnik tekshiruv: Maxsus xonalardan axborotning texnik (akustik, elektromagnit) sizib chiqishi o‘lchanadi;

10. Himoya vositalarini baholash: Xavfsizlik devorlari (firewall), kriptovositalar va dasturlarning davlat sertifikatlari tekshiriladi;

11. Yakuniy hisobot va tavsiyalar: Barcha sinov natijalari umumlashtirilib, kamchiliklarni bartaraf etish bo‘yicha tavsiyalar beriladi;

12. Attestat rasmiylashtirish: Obyekt barcha talablarga to‘liq javob berganda, uning xavfsizligini tasdiqlovchi davlat Attestati beriladi.



5-rasm. Kiberxavfsizlik talablari bo‘yicha obyektlarni baholash va attestatsiya sikli

Ushbu yondashuv attestatsiyani bir martalik tadbirdan toifalash, nazoratlarni tanlash, baholash, avtorizatsiya va doimiy monitoringni o‘z ichiga oluvchi uzluksiz kiberhimoya sikliga aylantiradi. Xorijiy davlatlar amaliyotida kiberxavfsizlik muvofiqligini baholash tizimli yondashuvlarga tayanadi: AQSh (NIST RMF, FedRAMP) doimiy monitoring va mustaqil ekspertizani talab qiladi; Yevropa Ittifoqi (NIS2) tanqidiy sektorlar kiberbarqarorligiga urg‘u beradi; Germaniya (BSI IT-Grundschutz) standart nazoratlar katalogini qo‘llaydi; Buyuk Britaniya (NCSC CAF) natijaga yo‘naltirilgan baholashni ilgari suradi (2-jadval).

2-jadval

Kiberxavfsizlik muvofiqligini baholash tizimli yondashuvlari

Davlat	Standart	Asosiy mazmuni	O‘zbekiston uchun foydali jihati
AQSh	NIST RMF / FedRAMP	Risk boshqaruvi, toifalash, avtorizatsiya va doimiy monitoring (ConMon)	Riskka asoslangan attestatsiya sikli va doimiy monitoring mexanizmi
YI / Germaniya	NIS2 / BSI Grundschutz	Obyekt xavfsizligi va tayyor nazoratlar katalogi bo‘yicha tekshirish	Standart nazoratlar milliy katalogi va chek-listlar bazasini yaratish
Buyuk Britaniya	NCSC CAF	Natijaga yo‘naltirilgan kiberbarqarorlik baholash tizimi	Talablarni qog‘ozbozlikdan dalillarga va amaliy himoya natijasiga bog‘lash

Rossiya / MDH	187-FZ / FSTEK / OAC	Obyektlarni toifalash, texnik-kriptografik himoyani attestatsiyalash	Davlat axborot tizimlari uchun majburiy yagona talablar bazasini o‘rnatish

Xulosa

Tadqiqot natijalari asosida quyidagi amaliy xulosalar va takliflar shakllantirildi:

1. Attestatsiya metodikasini kiberxavfsizlik instrumental sinovlari (pentest, zaifliklarni skanerlash) bilan boyitish zarur;

2. BSI va NIST tajribasi asosida kiberxavfsizlik nazoratlarining Milliy katalogi va chek-listlarini tasdiqlash lozim;

3. Attestatsiyadan o‘tgan ishonchli texnologik tizimlar va xizmatlarning yagona elektron reyestrini yuritish tavsiya etiladi;

4. Natijada axborot tizimlarining kiberhimoyasi 35-45% ga oshadi va ma’lumotlar sizib chiqish xavfi 80% gacha kamayadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni, 15.04.2022 y., O‘RQ-764-son. Lex.uz.

2. O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son qarori.

3. DXX Raisining «Axborotlashtirish obyektlarini attestatsiyadan o‘tkazish tartibi to‘g‘risida»gi buyrug‘i (№47, 2014 y.).

4. NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations. 2018.

5. UK NCSC. Cyber Assessment Framework (CAF). https://www.ncsc.gov.uk/collection/cyber-assessment-framework

6. BSI IT-Grundschutz-Kompendium. Bundesamt für Sicherheit in der Informationstechnik, Germany.

OVOZ YOZIB OLISH QURILMALARINI BLOKIROVKA QILISHNING YUQORI CHASTOTALI GIBRID TIZIMLARI: NAZARIY MODELLAR VA AMALIY TAHLIL

Alimov A.A., Botiraliyev N.X.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya: Mazkur maqolada konfidensial ovozli axborotni ruxsatsiz yozib olishdan himoyalashda qo‘llaniladigan yuqori chastotali va gibrid bloklash tizimlarining nazariy hamda texnik jihatlari tahlil qilinadi. Raqamli diktofonlar va smartfonlarning takomillashuvi ularni aniqlash hamda yozuv sifatini buzish masalasini dolzarb qilmoqda. Tadqiqotda akustik shovqin, ultratovush, elektromagnit interferensiya va kombinatsiyalangan usullar ko‘rib chiqilgan. Shovqin signallarining spektral xususiyatlari, ovozni maskalashdagi o‘rni va DSP hamda FPGA imkoniyatlari yoritilgan. DAudio BDA-2/3, Buben-Ultra, Kanonir-K7 va Tayfun-5/6 tizimlari qiyosiy tahlil qilinib, gibrid yondashuvlarning afzalliklari va cheklovlari aniqlangan. Tahlil natijalari bir nechta interferensiya mexanizmini birgalikda qo‘llash samarali yo‘nalishlardan biri ekanini ko‘rsatadi.

Kalit so‘zlar: axborot xavfsizligi, ovoz yozish qurilmasi, diktofon, mikrofon, ultratovush, akustik shovqin, elektromagnit interferensiya, gibrid bloklash, DSP, MEMS, FPGA.

Аннотация: В статье анализируются теоретические и технические особенности высокочастотных и гибридных систем защиты конфиденциальной речевой информации от несанкционированной записи. Развитие цифровых диктофонов и смартфонов повышает актуальность их обнаружения и снижения качества записи. Рассмотрены акустический шум, ультразвуковое воздействие, электромагнитная интерференция и комбинированные методы защиты. Проанализированы спектральные характеристики шумовых сигналов, их роль в маскировании речи, а также возможности DSP и FPGA при создании адаптивных систем блокирования. Проведен сравнительный анализ DAudio BDA-2/3, Buben-Ultra, Kanonir-K7 и Tayfun-5/6, определены преимущества и ограничения гибридного подхода. Результаты анализа показывают, что сочетание нескольких механизмов интерференции является перспективным направлением защиты.

Ключевые слова: информационная безопасность, звукозаписывающее устройство, диктофон, микрофон, ультразвук, акустический шум, электромагнитная интерференция, гибридная блокировка, DSP, MEMS, FPGA.

Ovozli axborotni ruxsatsiz yozib olishdan himoyalash dolzarb vazifa bo‘lib, bu borada bir qator olimlar tomonidan texnik yechimlar taklif etilgan [1, 2]. Ushbu tadqiqotning maqsadi – zamonaviy ovoz yozish qurilmalariga qarshi akustik, ultratovushli va elektromagnit ta’sir usullarini tahlil qilish hamda ularni uyg‘unlashtiruvchi gibrid himoya tizimining texnik imkoniyatlarini asoslash va baholashdan iborat [7, 8, 9].

Zamonaviy mobil qurilmalarda keng qo‘llaniladigan MEMS va boshqa turdagi mikrofonlarni bloklash samaradorligi ularning chastota xarakteristikasi, sezgirligi va ichki raqamli qayta ishlash algoritmlariga bevosita bog‘liq [6]. Shu sababli, faqat bitta yuqori chastotali ta’sir universal yechim bo‘la olmaydi.

Mikrofonning real xarakteristikasi ideal chiziqli modeldan farq qiladi. Tashqi yuqori chastotali ta’sir ayrim hollarda mikrofonning nochiziqli xususiyatlari sababli eshitiladigan

diapazonda qo‘shimcha komponentlar paydo bo‘lishiga olib kelishi mumkin. Bu yozuv spektriga ta’sir qilib, nutqni qayta ishlashni murakkablashtiradi.

Shu sababli bloklash tizimini ishlab chiqishda “har qanday yuqori chastotali signal mikrofonni bloklaydi” degan qarashni universal yechim sifatida qabul qilish to‘g‘ri emas. Amaliy samaradorlik mikrofonning konstruksiyasi, uning oldidagi akustik yo‘l, analog front-end, raqamli filtrlar va yozuv algoritmlariga bog‘liq bo‘ladi.

Akustik va ultratovushli ta’sirning fizik asoslari

Yozib olish jarayonidagi umumiy signalni soddalashtirilgan holda quyidagicha ifodalash mumkin.

$$u(t) = s(t) + n(t) \quad (1)$$

Bu yerda s(t) - foydali nutq signali, n(t) - qo‘shimcha shovqin signali.

Shovqinning ta’siri faqat amplitudaga emas, balki uning chastota bo‘yicha taqsimlanishiga ham bog‘liq. Oq shovqin keng chastota oralig‘ida energiyaning nisbatan bir tekis taqsimlanishi bilan tavsiflanadi. Pushti shovqinda esa past chastota komponentlari nisbatan ustun bo‘ladi. Ko‘k shovqinning spektral energiyasi yuqori chastota tomon siljigan bo‘ladi.

Nutqni maskalashda shovqin va foydali signal o‘rtasidagi nisbat muhim hisoblanadi. SNR qiymati quyidagi ifoda orqali aniqlanadi.

$$SNR = 10 \log10(Ps/Pn) \quad (2)$$

Bu yerda Ps - foydali signal quvvati, Pn - shovqin quvvati. SNR qiymatining kamayishi yozuvdagi foydali signalni shovqin fonidan ajratishni qiyinlashtiradi.

Ultratovushli himoya usullarida inson qulog‘i odatda eshita olmaydigan yuqori chastotali akustik komponentlardan foydalaniladi. Inson eshitish diapazonining yuqori chegarasi taxminan 20 kHz atrofida bo‘lsa-da, mikrofonlarning chastota xarakteristikasi bundan kengroq bo‘lishi mumkin. Natijada yuqori chastotali akustik ta’sir mikrofonning sezgirlik elementiga yetib boradi.

Ultratovushli signalning ta’siri mikrofonning nochiziqli xarakteristikalari bilan bog‘liq bo‘lishi mumkin. Agar foydali signal s(t) va yuqori chastotali signal x(t) bir vaqtda mikrofon kirishiga tushsa, nochiziqli o‘zgartirish natijasida ularning o‘zaro modulyatsiyasi yoki qo‘shimcha spektral komponentlar yuzaga kelishi mumkin. Bunday ta’sir mikrofon turiga bog‘liq bo‘lgani uchun uning samaradorligini tajriba yo‘li bilan tekshirish zarur [5].

Elektromagnit va gibrid tizimlar

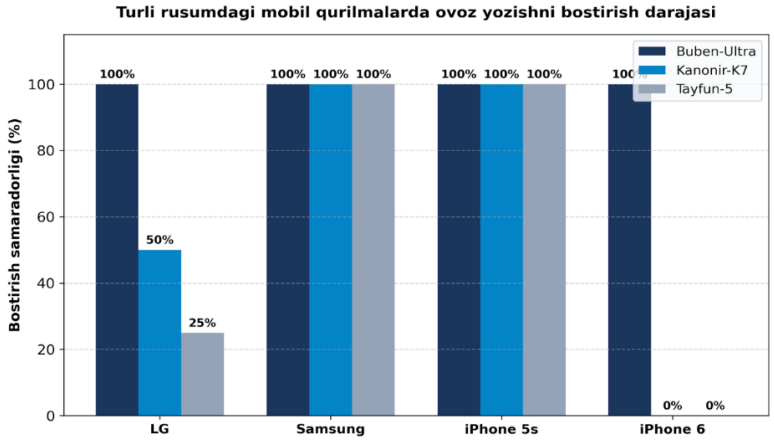
Elektromagnit interferensiya mikrofon analog traktida parazit toklar hosil qilishga asoslanadi [3, 4], lekin zamonaviy smartfonlarning yaxshi ekranlangani bu usul samaradorligini pasaytiradi. Shu sababli akustik, ultratovushli va elektromagnit usullarni birlashtiruvchi gibrid himoya eng barqaror yechimdir. Bozordagi mavjud «DAudio BDA-3», «Buben-Ultra», «Tayfun-6» va «Kanonir-K7» kabi tizimlar tahlili shuni ko‘rsatdiki [10-13], ular o‘rtacha 2-10 metr masofada faol ta’sir ko‘rsatadi. Ushbu qurilmalar asosan 24-27 kHz chastotadagi ultratovush, adaptiv spektral modulyatsiya va akustik nutqsimon shovqinlar kombinatsiyasidan foydalanib, mobil telefonlar (iPhone, Samsung, LG) mikrofonlarini turli darajada (qurilma arxitekturasiga qarab) muvaffaqiyatli bloklaydi.

1-jadval

Ovoz yozish qurilmalarini blokirovka qiluvchi vositalarning texnik ko‘rsatkichlari.

Qurilma modeli	Bostirish texnologiyasi	Ta’sir radiusi	Chastota va akustik parametrlar	Elektr ta’minoti

DAudio BDA-2 Ultrasonic *(i4 Technology)*	5 ta emitentli yo‘naltirilgan/tarqoq ultratovush; tashqi dinamik orqali nutqsimon shovqin	Optimal: 2 m; maksimal: 7 m; yangi iPhone: ~2 m	Tovush bosimi: 120 dB (1 m masofada); mikrokontrollerli o‘zgaruvchan chastota	110/220V tarmoq; 2600–3600 mA·soat Li-ion (3,7–4,2 V)
BugHunter DAudio BDA-3	6 ta emitent; adaptiv spektral modulyatsiya; tashqi akustik modul porti	10 m gacha (samarali faol zona)	Ultratovush: 23–27 kHz; dinamik interferensiya algoritmi	110/220V tarmoq; o‘rnatilgan avtonom akkumulyator
Tayfun-6 *(Gibrid kompleks)*	Kompleks: ultratovush rezonansi, EM induksiya, akustik maskalash, RF degradatsiya	8–10 m (to‘liq himoya radiusi)	RF: 400–2600 MHz; ultratovush: 24–26 kHz; ko‘pkanalli interferensiya	110/220V statsionar elektr tarmog‘i
Hunter Professional-3	Miniatyur piezoemitterlar bazasidagi yo‘naltirilgan ultratovush interferensiyasi	Kichik va o‘rta masofa (lokal suhbatlar)	Yo‘naltirilgan tor polosal ultratovush spektri	O‘rnatilgan avtonom akkumulyator
Kanonir-K7	Yo‘nalishli datchiklar (ultratovush); ichki va tashqi akustik nutqsimon shovqin	Ultratovush: 4 m gacha; akustik shovqin: xona bo‘ylab	Eshitilmaydigan ultratovush; sozlanuvchi nutq diapazoni	110/220V tarmoq; o‘rnatilgan qayta zaryadlanuvchi batareya
Buben-Ultra	3 bosqichli shovqin: ultratovush, past chastotali tovush, nutqsimon interferensiya	0,5–10 m (nurlanish burchagi: 90°/90°)	Ultratovush: 24–26 kHz; tovush: 10–2000 Hz; nutq: 300–18000 Hz	2 dona 18650 akkumulyator (iste’mol toki: 1000 mA)



1-rasm. Mobil telefonlarda ovoz yozishni bostirish samaradorligi gistogrammasi (%)

Xulosa

O‘tkazilgan tahlillar shuni ko‘rsatadiki, akustik shovqin, ultratovush va elektromagnit interferensiyani alohida-alohida qo‘llash barcha sharoitlarda kafolatlangan natija bermaydi. Gibrid yondashuv himoya barqarorligini oshiradi, biroq bunda xavfsizlik va elektromagnit moslashuv talablarini inobatga olish muhimdir. Xulosa qilib aytganda, bitta signal turiga asoslangan bloklash usullari zamonaviy takomillashgan qurilmalarga qarshi yetarli emas. Tadqiqot natijalariga ko‘ra, kelgusida raqamli filtrlash orqali tiklash murakkab bo‘lgan ko‘p chastotali va dinamik siljuvchi signallar generatorini yaratish zarur. Shuningdek, DSP (Raqamli signal protsessori) yoki FPGA platformasida ishlaydigan, muhitni tahlil qilib interferensiya turini moslashtiruvchi adaptiv gibrid tizim prototipini ishlab chiqish hamda uning samaradorligini kompleks baholash istiqbolli yo‘nalish hisoblanadi.

Foydalanilgan adabiyotlar

1. Uljayev O.M. Ovozni yozib olish qurilmalarini blokirovka qilish vositalarini ishlab chiqish. Magistrlik dissertatsiyasi. Toshkent 2025.

2. Frans M.V., Bukalo M.N., Nightshade V.V. Raqamli diktofonlarga qarshi elektromagnit va akustik bostirish usullari tahlili // Axborot xavfsizligi muammolari xalqaro ilmiy to‘plami. Moskva: MFTI, 2022.

3. Katorin Yu.F., Razumovskiy A.V. Axborotni texnik kanallar orqali himoyalash. Sankt-Peterburg: BHV-Peterburg, 2012.

4. Ott H.W. Electromagnetic Compatibility Engineering. New York: John Wiley & Sons, 2009.

5. Kinsler L.E., Frey A.R., Coppens A.B., Sanders J.V. Fundamentals of Acoustics. 4th Edition. New York: John Wiley & Sons, 2000.

6. Eargle J. The Microphone Book: From Mono to Stereo to Surround - A Guide to Microphone Design and Application. 3rd Edition. Oxford: Focal Press, 2012.

7. Proakis J.G., Manolakis D.G. Digital Signal Processing: Principles, Algorithms and Applications. 4th Edition. New Jersey: Pearson Prentice Hall, 2007.

8. Wolf W. FPGA-Based System Design. New Jersey: Prentice Hall PTR, 2004.

9. Oppenheim A.V., Willsky A.S., Nawab S.H. Signals and Systems. 2nd Edition. New Jersey: Pearson Education, 1996.

10. DAudio BDA-3 Professional Ultrasonic Suppressor Catalog. Seoul: i4 Technology, 2023.

11. Typhoon-6 RF Interference and Acoustic Protection System Technical Manual. Moscow: STG Publishing, 2021.

12. Kanonir-K7 Acoustic and Ultrasonic Suppression Device Passport. Moscow: Kanonir Ltd., 2022.

13. Buben-Ultra Technical Datasheet and User Manual. St. Petersburg: UltraSecurity Systems, 2023.

VIRTUALLASHTIRISH TEXNOLOGIYALARI ASOSIDA IP-TELEFONIYA TARMOQLARI XAVFSIZLIGINI BAHOLASHGA MO‘LJALLANGAN KIBERPOLIGON TIZIMINI ISHLAB CHIQISH

Djurayev N.T.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Mazkur maqolada virtuallashtirish texnologiyalari asosida IP-telefoniya tarmoqlariga ixtisoslashgan kiberpoligon tizimi yaratilishi bo‘yicha olib borilgan ishlar natijasi bayon etilgan. Asterisk serveri va SIP-abonentlardan iborat IP-telefoniya modeli, himoyalanganlikni baholash bo‘yicha sinov metodikasi haqida so‘z yuritiladi.

Kalit so‘zlar: kiberpoligon, virtuallashtirish, GNS3, IP-telefoniya, VoIP, SIP, RTP, Red team, Blue team, himoyalanganlikni baholash, ssenariy, normativ hujjat.

Аннотация. В данной статье представлены результаты работ по созданию специализированной системы киберполигона для сетей IP-телефонии на основе технологий виртуализации. Рассматриваются модель IP-телефонии, включающая сервер Asterisk и SIP-абонентов, а также методика испытаний по оценке защищённости сетей IP-телефонии.

Ключевые слова: киберполигон, виртуализация, GNS3, IP-телефония, VoIP, SIP, Red team, Blue team, оценка защищённости.

Kirish

So‘nggi yillarda O‘zbekiston Respublikasi davlat va xo‘jalik boshqaruvi organlari, aloqa operatorlari raqamli infratuzilmasini rivojlantirish jarayonida ovozli aloqa xizmatlarini IP texnologiyalar asosida tashkil etishga e’tibor ortib bormoqda. An’anaviy telefoniyadan IP-telefoniyaga (VoIP) o‘tish aloqa xarajatlarini kamaytirish va xizmatlarni markazlashtirish, shuningdek ovozli aloqani ma’lumotlar uzatish tarmog‘i bilan bir xil muhitga ko‘chirish imkonini bermoqda.

Biroq IP-telefoniyaga o‘tish bilan ovozli aloqa xizmatlari kompyuter tarmoqlariga xos xavflarga ham duch keladi. SIP-abonentlarning ruxsatsiz ro‘yxatdan o‘tishi, server konfiguratsiyasining o‘zgartirilishi, tarmoq segmentatsiyasi buzilishi, signalizatsiya va ovoz trafigiga ruxsatsiz kirish, xizmat resurslarining ortiqcha yuklanishi kabi holatlar aloqaning maxfiyligi, yaxlitligi va uzluksizligiga ta’sir ko‘rsatishi mumkin. Shu sababli muhim axborot infratuzilmasi obyektlarida bunday tarmoqlarning himoyalanganligini muntazam tekshirib turish, tarmoqning himoyalanganlik holatini baholash zarur hisoblanadi.

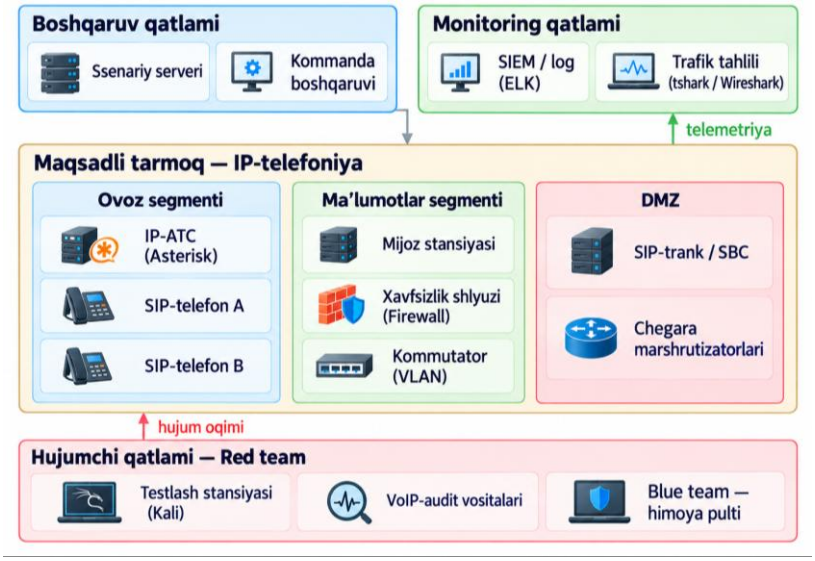
Shu sababli real tarmoqlarni faoliyatiga ta’sir etmagan holda ularning xavfsizligini baholashning eng maqbul yechimi, uning funksional xususiyatlarini alohida virtual muhitda modellashtirish, hujum va himoyani ssenariylarini yaratish imkonini beruvchi kiberpoligon tizimini yaratishdir.

Aynan shu bo‘shliqni to‘ldirish maqsadida ushbu tadqiqotda virtuallashtirish texnologiyalari (GNS3) asosida IP-telefoniya tarmoqlarining himoyalanganligini baholashga mo‘ljallangan kiberpoligon tizimi ishlab chiqildi.

Ishning asosiy g‘oyasi bo‘yicha, kiberpoligonda IP-telefoniya tarmog‘i modellashtirildi, hujum ssenariylari bo‘yicha sinovdan o‘tkazildi. Hujum va himoya natijalaridan olingan xulosalar asosida real tarmoqlarni xavfsiz qurish bo‘yicha normativ talablar va uslubiy tavsiyalar ishlab chiqildi.

Asosiy qism

Kiberpoligon nafaqat hujumlarni o‘tkazish, balki ularni kuzatish, boshqarish va natijasini qayd etish imkonini berishi kerak. Shuning uchun u GNS3 muhitida to‘rt mantiqiy qatlam sifatida loyihalandi: boshqaruv qatlami (ssenariylarni ishga tushirish, foydalanuvchilar va komandalarni boshqarish), monitoring qatlami (trafik va voqealarni yig‘ish, SIEM), maqsadli tarmoq qatlami (modellashtirilgan IP-telefoniya tarmog‘i) va hujumchi qatlami (Red team vositalari). Bunday bo‘linish hujum, himoya va kuzatuvni bir-biridan ajratib, har birini mustaqil ravishda sozlash imkonini berdi. Butun muhit xavfsizlik shlyuzi orqali segmentlarga bo‘lindi va tashqi tarmoqdan to‘liq izolyatsiyalandi.



1-rasm. Kiberpoligonning mantiqiy arxitekturasi

Maqsadli tarmoq, o‘z navbatida, uchta segmentga ajratildi: ovoz segmenti (IP-ATS va SIP-telefonlar), ma’lumotlar segmenti (mijoz ish stansiyalari) va chegara segmenti DMZ (SIP-trank/chegara qurilmasi). Bu segmentlash tarmoqdagi ovoz va ma’lumot trafigini ajratish va shu orqali hujumning bir segmentdan ikkinchisiga qanday tarqalishini o‘rganish imkonini berdi.

Hujumchi qatlami faqat ovoz va ma’lumotlar segmentlariga xavfsizlik shlyuzi orqali bog‘lanadi. Monitoring qatlami barcha segmentlardan ma’lumotlarni yig‘adi, bu esa hujumni aniqlash imkonini berdi. Asosiy server sifatida IP-ATS (Asterisk) ishlatilgan, mijozlar esa SIP-telefon emulyatorlari orqali modellashtirildi.

Kiberpoligon tarkibi quyidagi formal ifoda bilan tavsiflanadi:

$$K = (H, V, N, S, R, B, M, C, P)r \quad (1)$$

bu yerda H - hisoblash resurslari, V - virtuallashtirish muhiti, N - tarmoq infratuzilmasi, S - IP-telefoniya xizmatlari, R - Red Team, B - Blue Team, M - monitoring va jurnallash, C - boshqaruv, P - sinov ssenariylari majmuasi.

IP-telefoniya tarmoqlariga mavjud tahdidlar tahlili natijasiga ko‘ra quyidagi jadval shakllantirildi.

1-jadval

IP-telefoniya tarmog‘iga asosiy tahdidlar va himoya choralari

T.r.	Tahdid (hujum)	Ta’sir bosqichi	Oqibati	Himoya chorasi
1	Ro‘yxatdan o‘tishni o‘g‘irlash	Ro‘yxatdan o‘tish	Qo‘ng‘iroqlarni qabul qilib olish	Kuchli autentifikatsiya, TLS

T.r.	Tahdid (hujum)	Ta’sir bosqichi	Oqibati	Himoya chorasi
2	Qo‘ng‘iroqni soxtalashtirish	Signalizatsiya	Ishonch suiiste’moli, fishing	SIP autentifikatsiya, filtr
3	Ovozni tinglash	Ovoz oqimi (RTP)	Maxfiylik buzilishi	SRTP shifrlash
4	SIP-flud (DoS)	Signalizatsiya	Xizmatning ishdan chiqishi	Rate limiting, fail2ban, IPS
5	Aloqa resurslaridan ruxsatsiz foydalanish	Marshrutizatsiya	Resurslarning ruxsatsiz sarflanishi	Yo‘nalish cheklovi, limitlar
6	RTP oqimiga aralashuv	Ovoz oqimi	Ovoz buzilishi	SRTP, autentifikatsiya
7	Parollarni tanlash (brute force)	Ro‘yxatdan o‘tish	Hisob egallanishi	Murakkab parol, qulflash

Olib borilgan tahlillari asosida jadvalda tasniflangan har bir tahdid alohida sinov ssenariysiga aylantirildi. Bu kiberpoligonning asosiy ish mexanizmi bo‘lib, har bir ssenariy uchta qismdan tuzildi: boshlang‘ich holat (topologiya va konfiguratsiya), Red team qadamlari (hujum) va Blue team qadamlari (aniqlash va himoya). Shunday qilib, har bir ssenariyda bitta tahdid avval amalga oshirildi, so‘ng unga qarshi chora ko‘riladi.

Amalga oshirilgan namunaviy ssenariylar 2-jadvalda keltirilgan.

2-jadval

Namunaviy ssenariylar

Ssenariy	Red team harakati	Blue team javobi	Baholangan ko‘rsatkich
S1. Hisob egallash	Parol brutforsi	Qulflash, kuchli parol	Urinishlar soni
S2. Tinglash	RTP oqimini ushlash	SRTP yoqish	Ovoz ochiq/shifrlangan
S3. SIP-flud	Signalizatsiyaga DoS	Rate limiting, IPS	Xizmat mavjudligi
S4. Ruxsatsiz foydalanish	Tashqi raqamga qo‘ng‘iroq	Yo‘nalish/limit cheklovlari	Ruxsatsiz qo‘ng‘iroqlar
S5. Soxtalashtirish	Caller ID almashtirish	Autentifikatsiya, filtr	Soxta qo‘ng‘iroq o‘tdi/yo‘q

Ishlab chiqilgan kiberpoligon tizimining muhim vazifalaridan biri modellashtirilgan IP-telefoniya tarmog‘iga nisbatan amalga oshiriladigan kiberta’sirlarning oqibatlarini aniqlash, himoya mexanizmlarining samaradorligini baholash va olingan natijalarni o‘zaro taqqoslashdan iborat.

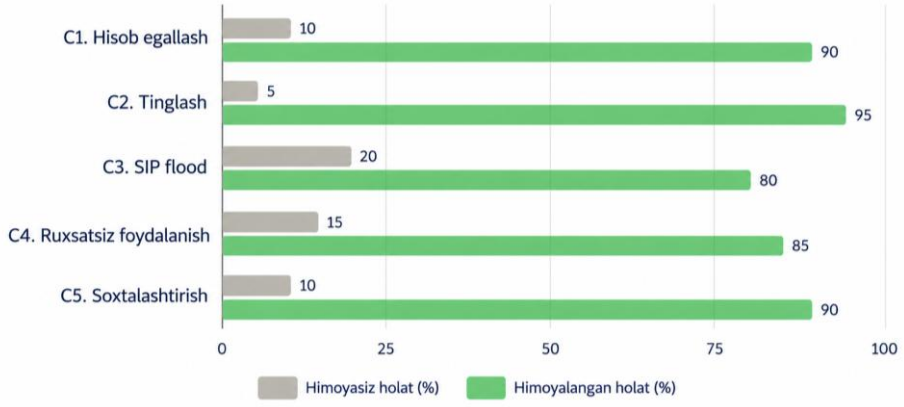
Mazkur vazifani amalga oshirishda sinov ssenariylarini yagona mezonlar asosida baholash zarurati yuzaga keladi. Shu maqsadda kiberpoligonda tarmoqning dastlabki holati va himoya choralari qo‘llanganidan keyingi holatini taqqoslashga asoslangan miqdoriy baholash yondashuvidan foydalanish taklif etildi.

Har bir i-ssenariy bo‘yicha himoyalanganlik balli hujumning muvaffaqiyati, uning aniqlanishi va oqibatlarining bartaraf etilishiga qarab hisoblanadi:

$$Si = w_1(1 - Ai) + w_2Di + w_3Mi \quad (2)$$

bu yerda *Ai* - hujumning amalga oshganligi, *Di* - aniqlanganligi, *Mi* - himoyadan keyin bartaraf etilganligi (har biri 1 yoki 0), w_1, w_2, w_3 - mezonlar vazni. Barcha ssenariylar bo‘yicha o‘rtacha qiymat esa tarmoqning yagona integral ko‘rsatkichi - Xavfsizlik indeksi (SPI) sifatida foizda ifodalandi. Bu indeks muhim, chunki u turli xil hujumlar natijasini bitta tushunarli raqamga jamlaydi.

Metodika beshta ssenariy (S1–S5) misolida sinovdan o‘tkazildi.

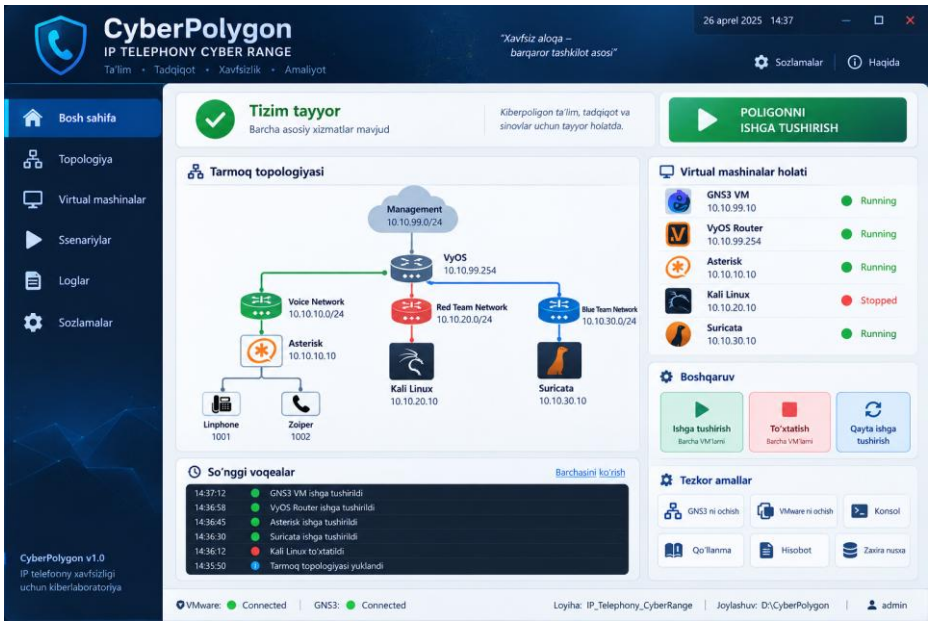


2-rasm. Ssenariy bo‘yicha xavfsizlik balli: himoyasiz va himoyalangan holat.

Natijalar himoya choralari qo‘llanganidan keyin barcha ssenariylar bo‘yicha xavfsizlik balli keskin oshganini ko‘rsatadi.

Tadqiqotning amaliy qiymati faqat raqamlar bilan cheklanmasligi va har bir samarali himoya chorasi real tarmoqlarga tavsiyaga aylanishi lozim. Shu bois kiberpoligonda olingan natijalar umumlashtirilib, real IP-telefoniya tarmoqlarini xavfsiz qurish bo‘yicha normativ-uslubiy hujjat loyihasiga aylantirildi. Hujjat umumiy qoidalar, xavfsizlik talablari, tahdidlar modeli, himoya choralarini joriy etish tavsiyalari, baholash metodikasi hamda nazorat va audit tartibidan iborat qilib tuzildi.

Kiberpoligonning barcha funksional qismlari foydalanuvchi uchun yagona muhitda jamlanishi maqsadida, uning virtual infratuzilma holatini, tarmoq topologiyasini va sinov ssenariylarini bitta oynada aks ettiruvchi boshqaruv interfeysi konsepsiyasi shakllantirildi. Panel bosh sahifa, topologiya, virtual mashinalar, ssenariylar, jurnallar va sozlamalar bo‘limlaridan iborat (3-rasm).



3-rasm. IP-telefoniya kiberpoligonining yagona boshqaruv paneli ko‘rinishi

Boshqaruv panelida virtual mashinalar holatini ko‘rsatish, ishga tushirish va to‘xtatish amallari, so‘nggi voqealar jurnali, GNS3 va VMware vositalarini ochish hamda hisobot va zaxira nusxa funksiyalari loyihaviy imkoniyatlar sifatida ko‘rsatildi.

Xulosa

Ushbu tadqiqotda IP-telefoniya tarmoqlarining himoyalanganligini ishlab turgan tizimga ta’sir etmasdan baholash muammosi virtuallashtirish texnologiyalari (GNS3) asosida yaratilgan kiberpoligon orqali hal etildi. Ishlab chiqilgan tizim boshqaruv, monitoring, maqsadli tarmoq va hujumchi qatlamlaridan iborat yaxlit muhit bo‘lib, unda Asterisk serveri va SIP-abonentlardan iborat real IP-telefoniya tarmog‘i modellashtirildi.

IP-telefoniya tarmog‘iga xos tahdidlar tahlil qilinib, har biri alohida sinov ssenariysiga aylantirildi. Olingan natijalar asosida real IP-telefoniya tarmoqlarini xavfsiz qurish bo‘yicha talablar va uslubiy tavsiyalardan iborat normativ-uslubiy hujjat loyihasi ishlab chiqildi. Mazkur kiberpoligon tizimi IP-telefoniya tarmoqlari xavfsizligini baholashda qo‘llanilash mumkin. Bundan tashqari, uning hujum va himoyani xavfsiz sharoitda takrorlash xususiyati tizimdan kiberxavfsizlik sohasida mutaxassislarni tayyorlash va malakasini oshirish uchun o‘quv vositasi sifatida ham foydalanish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-телефония. - М.: Радио и связь, 2001. - 336 с.

2. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. - 2-е изд. - М.: Эко-Трендз, 2003. - 252 с.

3. Тряпкин М.Н. Анализ безопасности протокола инициирования сеанса связи в сети IP-телефонии // Современные научные исследования и инновации. – №12, 2021.

4. Морозов А.М. Анализ уязвимости сети SIP фрод-угрозам по результатам тестирования оборудования действующей сети // Инженерный журнал: наука и инновации. - № 2, 2013.

5. Yamin M. M., Katt B., Gkioulos V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 2020.

DASTURIY TA’MINOT XAVFSIZLIGINI TA’MINLASH YO‘LLARI TAHLILI

Muratov O.A., Ergashov B.B.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Maqolada ishlab chiqarish korxonalarini raqamlashtirish jarayonida foydalaniladigan dasturiy ta’minot (keyingi o‘rinlarda - DT) xavfsizligini ta’minlashning tashkiliy va texnik choralari tahlil qilinadi. DTni ajratilgan tarmoqda ishlatish, xodimlarning rollari va vakolatlarini cheklash, foydalanuvchi harakatlarini jurnalga yozish, autentifikatsiya jarayonini qulay va xavfsiz tashkil etish, zaxira nusxalarini nazorat qilish, ularni asosiy serverdan geografik yoki fizik jihatdan ajratilgan joyda saqlash, yangilash, monitoring va hodisalarga javob berish masalalari ketma-ket yoritiladi. Taklif etilgan yondashuv ishlab chiqarish ma’lumotlarining maxfiyligi, yaxlitligi va mavjudligini oshirishga qaratilgan.

Kalit so‘zlar: ishlab chiqarishni raqamlashtirish, dasturiy ta’minot xavfsizligi, segmentatsiya, rollarga asoslangan kirish nazorati, autentifikatsiya, audit jurnallari, zaxira nusxa, tiklash, monitoring, kiberxavfsizlik.

Аннотация. В статье анализируются организационные и технические меры обеспечения безопасности программного обеспечения (далее - ПО), применяемого при цифровизации производственных предприятий. Последовательно рассматриваются работа ПО в изолированной сети, разграничение ролей и полномочий сотрудников, регистрация действий пользователей, безопасная и удобная аутентификация, контроль резервного копирования, хранение резервных копий в физически или географически отделённой от основного сервера локации, обновление программ, мониторинг и реагирование на инциденты. Предложенный подход направлен на повышение конфиденциальности, целостности и доступности производственных данных.

Ключевые слова: цифровизация производства, безопасность программного обеспечения, сегментация сети, ролевая модель доступа, аутентификация, журналы аудита, резервное копирование, восстановление, мониторинг, кибербезопасность.

Kirish

Ishlab chiqarish korxonalarida buyurtmalarni boshqarish, xomashyo va ombor hisobi, texnologik uskunalar monitoringi, ta’mirlash, sifat nazorati hamda moliyaviy hisob-kitoblarni raqamlashtirish mehnat unumdorligini oshiradi. Shu bilan birga, korxona faoliyati dasturiy ta’minot, serverlar, ma’lumotlar bazalari va tarmoq infratuzilmasiga ko‘proq bog‘lanadi. DTning ishlamay qolishi, ruxsatsiz o‘zgartirilishi yoki ma’lumotlarning yo‘qolishi ishlab chiqarish jarayonining to‘xtashi, moddiy zarar va maxfiy ma’lumotlar oshkor bo‘lishiga olib kelishi mumkin. Shu sababli xavfsizlik faqat antivirus o‘rnatish bilan cheklanmasligi kerak. U tarmoq arxitekturasi, foydalanuvchi vakolatlari, autentifikatsiya, audit, zaxiralash, yangilash va hodisalarga javob berish jarayonlarini yagona tizim sifatida qamrab olishi lozim. Ushbu maqolaning maqsadi ishlab chiqarish korxonalarida DT xavfsizligini oshirishga xizmat qiladigan asosiy choralarni izchil tartibda ko‘rib chiqish va amaliy tavsiyalar ishlab chiqishdan iborat.

Asosiy qism

Xavfsizlik siyosati va aktivlarni inventarizatsiya qilish. Dastlab korxonada ishlatilayotgan DT, serverlar, ma’lumotlar bazalari, foydalanuvchi qurilmalari, tarmoq uskunalari va ishlab chiqarish kontrollerlari ro‘yxati tuziladi. Har bir aktiv uchun mas’ul shaxs, korxonadagi ahamiyati, unda saqlanadigan ma’lumot turi va tiklash ustuvorligi belgilanadi. Axborot xavfsizligi siyosatida hisob yozuvlarini ochish va yopish, vakolat berish, dasturiy o‘zgarishlarni tasdiqlash, zaxira nusxa

olish va hodisalar haqida xabar berish tartibi yozma ravishda belgilanishi kerak. Bu choralar nazoratning kim tomonidan va qaysi muddatda bajarilishini aniqlashtiradi.

DTni ajratilgan va boshqariladigan tarmoqda ishlatish. Ishlab chiqarish DTsi imkon qadar korxonaning boshqariladigan ichki tarmog‘ida ishlashi, internetdan to‘g‘ridan-to‘g‘ri ochiq holda foydalanishga yo‘l qo‘yilmasligi kerak. Biroq “yopiq tarmoq”ning o‘zi to‘liq himoya kafolati emas: ichki qurilmaga zararli dastur tushishi, xodim hisob yozuvi buzilishi yoki tashqi qurilma orqali tahdid kirishi mumkin. Shu bois ofis tarmog‘i, serverlar zonasi va ishlab chiqarish/OT tarmog‘i mantiqiy segmentlarga ajratiladi. Segmentlar orasidagi trafik xavfsizlik devori orqali faqat zarur manzillar, portlar va protokollar bo‘yicha ruxsat etiladi [1].

Masofadan boshqarish zarur bo‘lsa, faqat tasdiqlangan VPN yoki shlyuz, ko‘p omilli autentifikatsiya va vaqt bilan cheklangan ruxsatdan foydalaniladi. Server boshqaruv interfeyslari internetga bevosita chiqarilmaydi. Tarmoq sxemasi hujjatlashtirilib, qoidalar muntazam ko‘rib chiqiladi.

Xodimlar rollari va vakolatlarini nazorat qilish. DTda rollarga asoslangan kirish nazorati joriy etilishi maqsadga muvofiq. Masalan, operator ishlab chiqarish topshiriqlarini ko‘rishi va o‘z ishiga oid ma’lumotlarni kiritishi mumkin; ombor xodimi materiallar harakatini yuritadi; muhandis texnik parametrlarni ko‘radi; buxgalter moliyaviy ma’lumotlarga kiradi; administrator esa tizim sozlamalarini boshqaradi. Har bir xodimga faqat xizmat vazifasini bajarish uchun zarur bo‘lgan minimal vakolat beriladi [2].

Umumiy hisob yozuvlaridan foydalanish cheklanadi, administratorlik huquqi kundalik ish uchun ishlatilmaydi, ishga qabul qilish, lavozim o‘zgarishi va ishdan ketish holatlarida vakolatlar darhol qayta ko‘rib chiqiladi. Yuqori xavfli amallar - masalan, ma’lumotlarni ommaviy o‘chirish, to‘lov rekvizitlarini o‘zgartirish yoki ishlab chiqarish parametrlarini tasdiqlash - qo‘shimcha tasdiqni talab qilishi mumkin. Vakolatlar kamida davriy ravishda mas’ul rahbar tomonidan tekshiriladi.

Autentifikatsiyani xavfsiz va samarali tashkil etish. Autentifikatsiya foydalanuvchining kimligini tekshiradi, avtorizatsiya esa uning qaysi amallarni bajarishi mumkinligini belgilaydi. Kirish jarayonini tezlashtirish maqsadida xavfsizlik talablarini pasaytirish yoki parolni juda qisqa qilish to‘g‘ri emas. Buning o‘rniga markazlashgan identifikatsiya boshqaruvi, bir martalik kirish, xavfsiz sessiya boshqaruvi va kerakli joylarda apparat kaliti yoki autentifikator ilovasi orqali ko‘p omilli autentifikatsiya joriy qilinadi.

Faol bo‘lmagan sessiyalar belgilangan vaqtdan keyin avtomatik qulflanadi; xavf darajasi yuqori amallar oldidan qayta autentifikatsiya talab qilinadi. Kirish urinishlariga tezlik cheklovi qo‘yilib, ko‘p marotaba muvaffaqiyatsiz urinishlar kuzatiladi. Hisobni vaqtincha bloklash mexanizmi ishlab chiqarish ishini asossiz to‘xtatib qo‘ymasligi uchun ehtiyotkor sozlanadi. Parollar ochiq matnda saqlanmaydi, zamonaviy, mos parametrli xeshlash algoritmlari bilan himoyalanadi. Autentifikatsiya vaqtini qisqartirish foydalanuvchi tajribasini yaxshilashi kerak, ammo xavfsizlik nazoratlarini chetlab o‘tish hisobiga amalga oshirilmasligi lozim [3].

Xodimlar harakatlarini jurnalga yozish va audit. DTda xodimlarning muhim harakatlari audit jurnaliga yozib boriladi. Jurnalga foydalanuvchi identifikatori, vaqt tamg‘asi, bajarilgan amal, obyekt yoki yozuv identifikatori, natija hamda zarur bo‘lsa, so‘rov manbasi kiritiladi. Kirish va chiqish, noto‘g‘ri autentifikatsiya urinishlari, ma’lumot qo‘shish /o‘zgartirish /o‘chirish, huquqlarni o‘zgartirish, hisobotlarni eksport qilish, administrator amallari va zaxira nusxa jarayonlari alohida nazorat qilinadi.

Jurnallarni foydalanuvchilarning o‘zi o‘zgartira yoki o‘chira olmasligi kerak. Ular markaziy jurnal serveriga uzatiladi, vaqt sinxronizatsiyasi ta’minlanadi, saqlash muddati va ko‘rish huquqlari belgilanadi. Jurnalda parollar, tokenlar yoki boshqa maxfiy ma’lumotlarni yozib qo‘yish mumkin emas. Avtomatik ogohlantirishlar noodatiy vaqtdagi kirish, katta hajmdagi eksport, ketma-ket xatolar yoki vakolatlarning kutilmagan o‘zgarishlarini aniqlashga yordam beradi.

Server va DTni muntazam yangilash. Operatsion tizim, DT kutubxonalari, ma’lumotlar bazasi va tarmoq qurilmalaridagi zaifliklar hujumchilar tomonidan ishlatilishi mumkin. Shu

sababli dasturiy aktivlar versiyalari qayd etilib, ishlab chiqaruvchi xavfsizlik yangilanishlari kuzatib boriladi [4]. Yangilanishlar avval sinov muhitida tekshiriladi, keyin tasdiqlangan jadval asosida ishchi muhitga joriy qilinadi. Yangilashdan oldin zaxira nusxa olinishi va qayta tiklash rejasi tayyor bo‘lishi zarur. Qo‘llab-quvvatlash muddati tugagan komponentlar almashtiriladi yoki alohida kompensatsion himoya choralari bilan cheklanadi.

Zaxira nusxalarini yaratish va nazorat qilish. Serverdagi DT konfiguratsiyasi, ma’lumotlar bazasi va ishlab chiqarish uchun muhim fayllar bo‘yicha zaxiralash siyosati belgilanadi. Zaxiralash chastotasi ma’lumotlarning qanchalik tez o‘zgarishi va korxona qabul qila oladigan ma’lumot yo‘qotish miqdoriga bog‘liq bo‘ladi. Har bir zaxiralash vazifasi muvaffaqiyatli yakunlangan-yakunlanmagani avtomatik tekshiriladi; xatolik yuz bersa, mas’ul xodimga ogohlantirish yuboriladi. Faqat “backup bajarildi” degan yozuv yetarli emas - nusxaning yaxlitligi va tiklashga yaroqliligi ham tekshirilishi kerak.

Zaxira nusxalari asosiy server bilan bir xonada yoki faqat shu serverga ulangan diskda saqlanmasligi lozim. Asosiy serverdan fizik yoki geografik jihatdan alohida joylashgan, kirish huquqlari cheklangan saqlash muhiti tanlanadi. Imkon qadar 3-2-1 tamoyili qo‘llanadi: ma’lumotlarning kamida uchta nusxasi, ikki xil saqlash turi va bitta nusxasi boshqa joyda bo‘lishi. Shuningdek, kamida bitta nusxani o‘zgartirib bo‘lmaydigan (immutable) yoki tarmoqdan uzilgan holatda saqlash ransomware xavfini kamaytiradi. Zaxira serveri asosiy server bilan bir xil administrator hisoblariga to‘liq bog‘lanib qolmasligi kerak [5].

Tiklash sinovlari reja asosida o‘tkaziladi: alohida muhitga ma’lumotlar qayta tiklanadi, fayllar va ma’lumotlar bazasi yaxlitligi tekshiriladi, tiklashga ketgan vaqt o‘lchanadi. Tiklashning maqsadli vaqti va qabul qilinadigan ma’lumot yo‘qotish oralig‘i rahbariyat tomonidan belgilanadi. Sinov natijalari hujjatlashtiriladi.

Ma’lumotlarni himoyalash va shifrlash. Tarmoq orqali uzatiladigan ma’lumotlar zamonaviy TLS kabi himoyalangan protokollar bilan, saqlanayotgan muhim ma’lumotlar esa xavf va talabga mos ravishda shifrlanishi kerak. Shifrlash kalitlari ma’lumotlar bilan bir joyda va bir xil ruxsatlar ostida saqlanmasligi lozim. Kalitlarni yaratish, foydalanish, almashtirish va bekor qilish jarayoni hujjatlashtiriladi. Maxfiylik darajalari belgilanib, ishlab chiqarish, xodimlar va moliyaviy ma’lumotlarga faqat vakolatli shaxslar kirishi ta’minlanadi.

Dasturiy o‘zgarishlarni boshqarish va ishlab chiqish xavfsizligi. DTga yangi funksiya qo‘shish yoki mavjud kodni o‘zgartirish nazoratsiz amalga oshirilmasligi kerak. O‘zgarishlar uchun so‘rov, mas’ul ijrochi, sinov natijalari, tasdiqlovchi shaxs va joriy etish vaqti qayd etiladi. Ishlab chiqish, sinov va ishchi muhitlar ajratiladi; haqiqiy ishlab chiqarish ma’lumotlari sinovda ishlatilsa, ular niqoblanadi yoki anonimlashtiriladi. Kod va bog‘liqliklar zaifliklar bo‘yicha tekshiriladi, maxfiy kalitlar kod omboriga joylashtirilmaydi. Ishchi muhitga o‘zgarish kiritish huquqi cheklangan bo‘lishi kerak.

Zararli dasturlar, qurilmalar va jismoniy kirishdan himoya. Serverlar va ishchi stansiyalarda boshqariladigan zararli dasturlardan himoya vositalari qo‘llanadi, operatsion tizimlarda keraksiz xizmatlar o‘chiriladi va ilovalarni ishga tushirish imkoniyatlari nazorat qilinadi. USB va boshqa tashqi qurilmalardan foydalanish siyosat bilan tartibga solinadi. Server xonasi qulflanadi, kirishlar qayd etiladi, elektr ta’minoti va sovitish tizimlari nazorat qilinadi. Ishlab chiqarish kontrollerlari yoki OT qurilmalariga xavfsizlik vositalarini joriy etishdan oldin ularning texnologik jarayonga ta’siri sinovdan o‘tkaziladi.

Doimiy monitoring va hodisalarga javob berish. Tarmoq, server, DT va audit jurnallarini muntazam kuzatish xavfli holatlarni erta aniqlashga yordam beradi. Korxonada hodisa yuz berganda kimga xabar berish, qaysi tizimni tarmoqdan ajratish, dalillarni qanday saqlash, zaxiradan tiklashni kim tasdiqlashi va ishlab chiqarishni qayta ishga tushirish shartlari oldindan belgilanishi lozim. Reja amaliy mashqlar orqali sinab ko‘riladi. Hodisa sababini aniqlash uchun jurnallar, zaxira nusxalar va konfiguratsiya o‘zgarishlari saqlab qolinadi [6].

Xodimlarni o‘qitish va xavfsizlik samaradorligini baholash. Texnik himoya choralariga qo‘shimcha ravishda xodimlar parollarni himoyalash, fishing xabarlarini aniqlash, shubhali holat haqida xabar berish va ishlab chiqarish ma’lumotlari bilan ishlash qoidalari bo‘yicha muntazam

o‘qitiladi. Xavfsizlik holatini baholash uchun muvaffaqiyatsiz zaxiralashlar soni, tiklash sinovlarining muvaffaqiyat darajasi, muddati o‘tgan yangilanishlar, ortiqcha vakolatli hisoblar, aniqlangan hodisaga javob vaqti hamda audit jurnallarining to‘liqligi kabi ko‘rsatkichlar kuzatiladi. Natijalar asosida choralar qayta ko‘rib chiqiladi.

Xulosa

Ishlab chiqarish korxonalarini raqamlashtirishda DT xavfsizligi bir-birini to‘ldiradigan tashkiliy va texnik choralar majmuasi orqali ta’minlanadi. Eng avvalo, aktivlar inventarizatsiya qilinishi va xavfsizlik siyosati belgilanishi, so‘ng tarmoq segmentatsiyasi, minimal vakolat tamoyili, kuchli autentifikatsiya va audit jurnallari joriy etilishi zarur. Server va dasturlarni o‘z vaqtida yangilash, ma’lumotlarni shifrlash, o‘zgarishlarni nazorat qilish, zararli dasturlardan himoya va doimiy monitoring ham muhim ahamiyatga ega. Ayniqsa, zaxira nusxalarini nazorat qilish faqat nusxa olish bilan tugamasligi kerak: nusxalar asosiy serverdan alohida joyda saqlanishi, ularga kirish cheklanishi, o‘zgartirib bo‘lmaydigan nusxa mavjud bo‘lishi va tiklash sinovlari muntazam bajarilishi lozim. Autentifikatsiyani tezlashtirish ham xavfsizlik darajasini pasaytirmasdan, markazlashgan kirish va qulay tasdiqlash usullari orqali amalga oshiriladi. Ushbu choralarni bosqichma-bosqich joriy etish korxonaning ishlab chiqarish uzluksizligi, ma’lumotlar yaxlitligi va axborot xavfsizligini mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. NIST. Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024. https://doi.org/10.6028/NIST.CSWP.29

2. NIST. Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

3. NIST. Guide for Cybersecurity Event Recovery, SP 800-184. https://doi.org/10.6028/NIST.SP.800-184

4. NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3. https://doi.org/10.6028/NIST.SP.800-82r3

5. CISA. #StopRansomware Guide. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/stopransomware

6. ISO/IEC 27001:2022. Information security management systems - Requirements. International Organization for Standardization, 2022.

KIBERPOLIGON INFRATUZILMASI UCHUN OCHIQ KODLI TEXNOLOGIYALARNI AMALIY SINOV NATIJALARI ASOSIDA TANLASH

Asliddinov Sh.A., Amirov A.D.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Maqolada tarmoq qurilmalariga qaratilgan kiberhujumlarni simulyatsiya qilishga mo‘ljallangan kiberpoligon infratuzilmasi uchun ochiq kodli texnologiyalarni tanlash natijalari keltirilgan. Containerlab, GNS3, EVE-NG va Kathara tarmoq emulyatsiya platformalari hamda KYPO CRP, CyberRangeCZ va Open Cyber Range kiberpoligon platformalari amaliy sinovdan o‘tkazilgan. Ko‘p mezonli baholash natijalariga ko‘ra Containerlab eng yuqori ball (*4,45*) oldi. Tarmoq qurilmalari, xavfsizlik monitoringi, hujum simulyatsiyasi va baholash qatlamlarini birlashtirgan olti qatlamli texnologik stek hamda uni bosqichma-bosqich joriy etish rejasi taklif etilgan.

Kalit so‘zlar: kiberpoligon, tarmoq emulyatsiyasi, Containerlab, ko‘p mezonli baholash, kiberhujumlarni modellashtirish, texnologik stek.

Аннотация. В статье представлены результаты выбора технологий с открытым исходным кодом для инфраструктуры киберполигона, предназначенного для имитации кибератак на сетевые устройства. Платформы сетевой эмуляции Containerlab, GNS3, EVE-NG и Kathara, а также платформы киберполигона KYPO CRP, CyberRangeCZ и Open Cyber Range были практически опробованы. По результатам многокритериальной оценки наивысший балл (*4,45*) получил Containerlab. Предложены шестиуровневый технологический стек, объединяющий уровни сетевых устройств, мониторинга безопасности, имитации атак и оценки, а также поэтапный план его внедрения.

Ключевые слова: киберполигон, сетевая эмуляция, Containerlab, многокритериальная оценка, моделирование кибератак, технологический стек.

Kirish

Router, switch va firewall kabi tarmoq qurilmalari axborot tizimlarining markaziy bo‘g‘ini bo‘lib, ularga qaratilgan DoS/DDoS, o‘rtadagi odam (*MITM*) va marshrutlash protokollariga yo‘naltirilgan hujumlar soni ortib bormoqda. Himoya konfiguratsiyalarini ishlab turgan tizimda sinash xavfli bo‘lgani uchun ularni real sharoitga yaqin, ammo izolyatsiyalangan kiberpoligon (*Cyber Range*) muhitida tekshirish dolzarb hisoblanadi. Ochiq kodli platformalar ko‘p bo‘lsada, ularning qaysi biri tarmoq qurilmalariga qaratilgan hujumlarni modellashtirish uchun maqbulligi amaliy sinov asosida yetarlicha asoslanmagan. Tadqiqotning maqsadi - ochiq kodli tarmoq emulyatsiya va kiberpoligon platformalarini amaliy sinab, kiberpoligon infratuzilmasi uchun maqbul texnologik stekni tanlashdir.

Asosiy qism

Sinovdan to‘rtta tarmoq emulyatsiya platformasi (*Containerlab, GNS3, EVE-NG, Kathara*) va uchta kiberpoligon platformasi (*KYPO CRP, CyberRangeCZ, Open Cyber Range*) o‘tkazildi. Emulyatsiya platformalari uchun yagona sinov topologiyasi ishlab chiqildi. Ikkita marshrutizator, ikkita kommutator va ikkita xostdan iborat bo‘lib, 192.168.10.0/24 va 192.168.20.0/24 segmentlarini 10.0.0.0/30 magistral tarmog‘i bog‘laydi. Topologiyada L2/L3 ulanish (ping, traceroute), marshrutlash, ishga tushirish vaqti va konfiguratsiyani takrorlash imkoniyati tekshirildi. Kathara va Containerlab’da topologiya to‘liq ko‘tarilib, ishga tushirish vaqti o‘lchandi.

Kiberpoligon platformalaridan KYPO CRP yengillashtirilgan KYPO-lite variantida (*Vagrant, libvirt*), CyberRangeCZ Vagrant asosidagi ishlab chiqish muhitida, Open Cyber Range esa Ubuntu Server'da Docker Compose orqali joylashtirildi. Natijalar ko‘p mezonli ekspert baholash usuli bilan umumlashtirildi. Yettita mezon 1-5 ball bilan baholanib, umumiy ball $S = \Sigma(w_i * b_i)/100$ formulasi bo‘yicha hisoblandi (w_i - *mezon og‘irligi,* b_i - *ball*).

Tarmoq emulyatsiyasi natijalari

Sinov topologiyasini ishga tushirish ko‘rsatkichlari 1 - jadvalda keltirilgan. Containerlab topologiyani taxminan 3,4 soniyada ko‘tardi, Kathara'da bu ko‘rsatkich taxminan 4,4 soniyani tashkil etdi, ya'ni Containerlab taxminan 23% tezroq ishladi. Bundan tashqari, Containerlab butun topologiyani yagona YAML faylida tavsiflaydi, Kathara esa bir nechta papka va .startup fayllarini talab qiladi va tashqi terminal emulyatorlariga bog‘liq. GNS3 va EVE-NG real qurilma obrazlari hamda qulay grafik interfeysi bilan ajralib turdi, biroq ularda apparat virtualizatsiyasi (*VT-x, ichma-ich virtualizatsiya*) shart, resurs sarfi yuqori, topologiyani CI/CD jarayoniga ulash esa qiyinroq.

1 – jadval

Sinov topologiyasini ishga tushirish ko‘rsatkichlari

Ko‘rsatkich	Kathara	Containerlab
Konfiguratsiya formati	Bir nechta papka va .startup fayllar	Yagona YAML fayli
Ishga tushish vaqti	~4,4 soniya	~3,4 soniya
Arxitektura	Docker; xterm oynalariga bog‘liq	Docker va Linux namespaces; minimal bog‘liqlik
Tugunlarni boshqarish	Alohida terminal oynalari	Boshqaruv IP manzillari (*172.20.20.X*), SSH

Platformalar yettita mezon bo‘yicha baholandi (*2 - jadval*). Eng yuqori og‘irlik resurs samaradorligi va avtomatlashtirishga berildi, chunki tajribalar bir xil konfiguratsiyada ko‘p marta takrorlanishi va cheklangan apparat resurslarida bajarilishi kerak. Umumiy ball bo‘yicha Containerlab (*4,45*) birinchi, GNS3 (*3,70*) ikkinchi, Kathara (*3,65*) uchinchi va EVE-NG Community Edition (*3,20*) to‘rtinchi o‘rinni egalladi. Containerlab'ning asosiy kamchiligi - interaktiv grafik muharrirning yo‘qligi - clab graph va Edgeshark vositalari yordamida qisman bartaraf etiladi.

2 – jadval

Emulyatsiya platformalarining og‘irlikli baholanishi (1-5 ball)

Mezon (og‘irlik)	Containerlab	GNS3	EVE-NG CE	Kathara
Resurs samaradorligi (*20%*)	5	3	2	4
Avtomatlashtirish va takrorlanuvchanlik (*20%*)	5	3	3	4
Tarmoq qurilmalari realizmi (*15%*)	4	5	5	3
Xavfsizlik vositalari bilan integratsiya (*15%*)	5	3	3	4
Ochiqlik va litsenziya erkinligi (*10%*)	5	5	3	5
Joylashtirish soddaligi (*10%*)	4	3	2	3
Vizualizatsiya (*GUI*) imkoniyati (*10%*)	2	5	5	2

Mezon (og‘irlik)	Containerlab	GNS3	EVE-NG CE	Kathara
Umumiy ball	4,45	3,70	3,20	3,65

Platformalarning xususiyatlari. Containerlab topologiyalarni YAML orqali tavsiflash va Git’da versiyalash, apparat virtualizatsiyasini talab qilmasdan yuzlab konteynerni kam resursli muhitda ishga tushirish hamda Prometheus va Grafana kabi telemetriya vositalari bilan integratsiya imkoniyatlari bilan ajralib turdi. Uning cheklovi - xususiy tarmoq operatsion tizimlarini (*masalan, Cisco IOS, Palo Alto*) vrnetlab kabi qo‘shimcha qatlamsiz ishga tushirib bo‘lmasligi va topologiyani sichqoncha bilan chizish imkoniyatining yo‘qligidir. GNS3 Dynamips, QEMU va Docker tugunlarini bitta topologiyada birlashtira oladi hamda har bir havoladagi trafikni Wireshark’ga uzatadi, biroq zamonaviy router va firewall obrazlari uchun VT-x/EPT va ichma-ich virtualizatsiyani talab qiladi. EVE-NG brauzer orqali ko‘p foydalanuvchili ishlash, router, firewall, hujumchi (*Kali linux*) va SIEM tugunlarini bitta muhitda birlashtirish imkonini beradi, ammo har bir QEMU tugun alohida xotira va protsessor talab qiladi. Kathara har bir tugunni alohida Docker konteyneri sifatida ishga tushirib, BGP, OSPF, MPLS va SDN tajribalari uchun yengil muhit yaratadi, lekin asosan buyruqlar satri orqali ishlaydi va xususiy operatsion tizim obrazlarini qo‘llab-quvvatlamaydi.

Kiberpoligon platformalarining sinovi. KYPO CRP yengillashtirilgan KYPO-lite variantida o‘rnatilib, Cyber Sandbox Creator vositasida YAML formatida tavsiflangan oddiy sandbox topologiyasi GitLab repozitoriysi orqali tizimga bog‘landi. CyberRangeCZ’da devops-helm repozitoriysidagi Vagrant asosidagi muhit yordamida sandbox boshqaruvi, training-service va veb-interfeys yagona virtual mashinada ishga tushirildi hamda oddiy o‘quv ssenariysi tekshirildi. Open Cyber Range’da administrator paneli orqali foydalanuvchilar yaratildi, kurs (*nomi, kodi, semestri, boshlanish va tugash sanalari, o‘qituvchi*) shakllantirildi va mashqlar YAML faylini import qilish yoki qo‘lda kiritish orqali qo‘shildi. Mashq tavsifi nomi, qiyinlik darajasi, yo‘nalishi, flag va bosqichma-bosqich vazifalarni o‘z ichiga oladi. Yaratilgan foydalanuvchi hisobida kurs ochiq va bajarishga tayyor holda ko‘rindi.

Kiberpoligon platformalari natijalari. KYPO CRP va CyberRangeCZ bir xil arxitekturaga tayanadi. OpenStack (*CyberRangeCZ’da AWS ham*), Kubernetes va Helm, sandbox muhitlari Terraform/OpenTofu orqali infratuzilma-kod tamoyilida yaratiladi, hodisalar OpenSearch’da qayd etiladi. Ular katta hajmdagi mashg‘ulotlar uchun kuchli, ammo joylashtirish murakkab va resurs talab qiladi. Open Cyber Range esa Docker Compose asosidagi yengil veb-ilova bo‘lib, har bir tinglovchi uchun izolyatsiyalangan /24 tarmoq, brauzerli hujum stansiyasi (*RangeBox*), kurs boshqaruvi, ball tizimi va YAML mashqlarni taqdim etadi. Uchala platforma ham tarmoq qurilmalarini chuqur emulyatsiya qilmaydi. Shu sababli KYPO CRP va CyberRangeCZ to‘liq joylashtirilmadi. Ularning sandbox’ni kod orqali tavsiflash va ball tizimi g‘oyalari asosida Python va YAML’ga tayangan yengil ssenariy-baholash moduli ishlab chiqish, Open Cyber Range’ni esa ixtiyoriy o‘quv moduli sifatida qoldirish qaror qilindi.

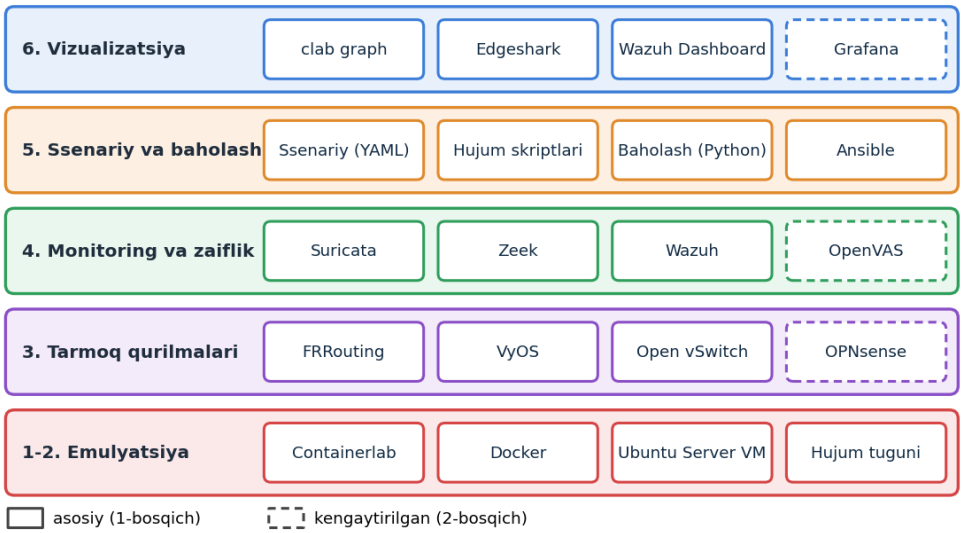
3 – jadval

Kiberpoligon platformalari bo‘yicha umumiy tahlil

Platforma	Infratuzilma talabi	Kuchli tomonlari	Umumiy tahlil
KYPO CRP	OpenStack, Kubernetes, Helm *(sinovda KYPO-lite*)	Sandbox’ni kod orqali yaratish, trening va baholash	Alohida joylashtirilmaydi, g‘oyalari o‘zlashtiriladi

Platforma	Infratuzilma talabi	Kuchli tomonlari	Umumiy tahlil
CyberRangeCZ	Kubernetes, Terraform/OpenTofu, OpenStack yoki AWS	Mikroservislar, OpenSearch, MITRE ATT&CK, OIDC	Alohida joylashtirilmaydi, kelajakdagi integratsiya
Open Cyber Range	Docker Compose	Izolyatsiyalangan /24 laboratoriyalar, RangeBox, kurs va ball tizimi	Ixtiyoriy o‘quv moduli

Tanlangan texnologik stek. Natijalar asosida olti qatlamli stek shakllantirildi (1 - rasm). Tarmoq qurilmalari uchun FRRouting, VyOS va Open vSwitch, monitoring uchun Suricata (IDS/IPS), Zeek va Wazuh, hujum tuguni sifatida esa Kali yoki Ubuntu konteyneri tanlandi. OPNsense FreeBSD asosida bo‘lgani uchun konteynerda ishlamaydi, shu sababli birinchi bosqichda firewall vazifasini VyOS (nftables) va Suricata bajaradi, OPNsense va Greenbone (OpenVAS) esa ikkinchi bosqichga o‘tkazildi. Hujum ssenariylari MITRE ATT&CK Network Devices texnikalariga mos beshta sinfni (skanerlash, parolni tanlash, xizmatni to‘xtatish, ARP spoofing, marshrutlashga ta’sir) qamrab oladi va faqat izolyatsiyalangan tarmoqda o‘tkaziladi.



1 - rasm. Kiberpoligonning olti qatlamli texnologik steki

4 – jadval

Kiberpoligon infratuzilmasi uchun tanlangan yechimlar

Qatlam	Tanlangan yechim	Ko‘rib chiqilgan muqobil yechimlar
Orkestratsiya	Containerlab + Docker	GNS3, EVE-NG, Kathara
Router	FRRouting, VyOS	Cisco/Juniper obrazlari
Switch	Open vSwitch/Linux bridge	Vendor switch obrazlari
Firewall	VyOS (*nftables*), 2 - bosqichda OPNsense	pfSense, OpenWrt
IDS/IPS	Suricata	Snort
Tarmoq monitoringi	Zeek	Faqat Wireshark
SIEM/XDR	Wazuh	ELK, Graylog

Qatlam	Tanlangan yechim	Ko‘rib chiqilgan muqobil yechimlar
Zaiflik tahlili	Greenbone (*OpenVAS*), 2 - bosqich	Nmap skriptlari
Avtomatlashtirish	Ansible, Python, Git	Qo‘lda sozlash

Wazuh o‘z tarkibida indexer va dashboard komponentlariga ega bo‘lgani uchun alohida ELK stekini qo‘shish takrorlanish hisoblanib, tanlovdan chiqarildi. Resurs hisobiga ko‘ra, asosiy poligon taxminan 17,5 GB, kengaytirilgan stek esa taxminan 28,5 GB operativ xotira talab qiladi, shuning uchun kamida 32 GB RAM va 8 yadroli muhit tavsiya etiladi. Integratsiya xavflarini kamaytirish uchun joriy etish to‘rt bosqichda, har bir bosqich oxirida tekshiruv nuqtasi bilan rejalashtirildi.

Topologiya va marshrutlash: Suricata, Zeek, Wazuh, Edgeshark, OPNsense, Greenbone va to‘liq baholash moduli. Asosiy xavflar va ularni kamaytirish choralari 5 - jadvalda keltirilgan.

5 – jadval

Asosiy integratsiya xavflari va kamaytirish choralari

Xavf	Kamaytirish chorasi
Ichma-ich virtualizatsiya yoqilmagan (*VyOS, OPNsense ishga tushmaydi*)	VMware’da VT-x/EPT’ni yoqish. Zaxira variant: FRR va nftables konteynerlari
Operativ xotira yetishmasligi	Bosqichma-bosqich joylashtirish. Wazuh va Greenbone’ni alohida VM’da yoki navbat bilan ishga tushirish
Suricata va Zeek loglari Wazuh’da ko‘rinmasligi	Sensor konteynerlariga Wazuh agent o‘rnatish. JSON loglarni tekshirish nuqtasi
Hujum trafigining poligondan tashqariga chiqishi	Izolyatsiyalangan tarmoq, boshqaruv tarmog‘ini internetdan ajratish
Greenbone zaiflik bazasining katta hajmi	Bazani oldindan yuklab olish yoki ikkinchi bosqichga qoldirish

Baholash ko‘rsatkichlari

Tanlangan stek kiberbardoshlilik indeksini hisoblash uchun zarur ma‘lumotlarni ta’minlaydi. Hujumni aniqlash va bloklash samaradorligi (*Suricata, Wazuh*), xizmat mavjudligi va tiklanish vaqti (*javob vaqti, paket yo‘qotilishi, hodisalarning vaqt tamg‘alari*), konfiguratsiya xavfsizligi (*Wazuh SCA, ochiq portlar auditi*), zaifliklar soni va jiddiyligi (*Greenbone, CVSS*) hamda kuzatiluvchanlik darajasi (*Zeek va Wazuh loglari*).

Baholash ekspert usuliga asoslangani uchun ballar tadqiqotchining sinov tajribasi va rasmiy hujjatlarga tayanadi, ishga tushirish vaqti esa bitta topologiyada o‘lchangan taxminiy qiymatdir. Shu sababli natijalar yakuniy hukm emas, balki keyingi amaliy sinovlar uchun asos hisoblanadi. Mezon og‘irliklari tadqiqot maqsadiga bog‘liq. Masalan, ta’lim jarayoni uchun vizualizatsiya og‘irligi oshirilsa, GNS3 va EVE-NG o‘rni yaxshilanadi, biroq tarmoq qurilmalariga qaratilgan hujumlarni takroriy modellashtirish uchun avtomatlashtirish va resurs samaradorligi hal qiluvchi bo‘lib qoladi.

Xulosa

Yagona sinov sharoitida Containerlab eng yuqori ball (*4,45*) oldi va Kathara’ga nisbatan topologiyani taxminan 23% tezroq (*3,4 va 4,4 soniya*) ko‘tardi. Ko‘rib chiqilgan kiberpoligon

platformalarining hech biri tarmoq qurilmalarini chuqur emulyatsiya qilmaydi, shu sababli ularning g‘oyalarini o‘zlashtirgan holda Containerlab asosidagi integratsiyalashgan stek taklif etildi. Stek resurs va integratsiya xavflari nuqtai nazaridan baholanib, to‘rt bosqichli joriy etish rejasi belgilandi. Keyingi bosqichlarda ushbu stek asosida hujum ssenariylari va kiberbardoshlilik indeksi amaliy sinovdan o‘tkaziladi.

Foydalanilgan adabiyotlar

1. Containerlab. Official documentation. https://containerlab.dev
2. Kathara. Official documentation. https://www.kathara.org
3. KYPO Cyber Range Platform. Documentation. Masaryk University. https://docs.crp.kypo.muni.cz
4. CyberRangeCZ Platform. CESNET/CyberSecurity Hub. https://github.com/cyberrangecz
5. Open Cyber Range. https://opencyberrange.com
6. Siemens. Edgeshark. https://github.com/siemens/edgeshark
7. Wazuh. Documentation: quickstart and requirements. https://documentation.wazuh.com
8. MITRE ATT&CK. Network Devices platform. https://attack.mitre.org
9. Suricata. Official documentation. https://suricata.io
10. Zeek. Official documentation. https://zeek.org
11. VyOS. Official documentation. https://vyos.io
12. FRRouting. Official documentation. https://frrouting.org

SUN’IY INTELLEKT AGENTLARINI ISHLAB CHIQISHDA XAVFSIZLIK TAMOYILLARI VA HIMOYA MEXANIZMLARI

Azizov D.A., Xatamov S.Q.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalar instituti

Annotatsiya. Mazkur maqolada katta til modellari (LLM) asosida ishlovchi sun’iy intellekt agentlarini ishlab chiqishda yuzaga keladigan xavfsizlik tahdidlari xalqaro OWASP tashkilotining “OWASP Top 10 for LLM Applications” (2024) tasnifi asosida tushunarli tilda tahlil qilingan. Xavfsiz agentni loyihalashning yettita tamoyili ifodalangan, lokal LLM bilan ishlovchi Telegram tizimi uchun ko‘p qatlamli himoya arxitekturasi taklif etilgan.

Kalit so‘zlar: sun’iy intellekt agenti, LLM, OWASP, prompt injection, RAG, minimal huquqlar tamoyili, Telegram bot, lokal model, Ollama.

Аннотация. В данном тексте рассматриваются проблемы безопасности при разработке искусственных интеллектуальных агентов, основанных на больших языковых моделях (LLM), с учётом классификации «OWASP Top 10 for LLM Applications» 2024 года от международной организации OWASP. В статье изложены семь принципов безопасного проектирования подобных агентов и предложена многоуровневая архитектура защиты для Telegram-подобной системы, работающей локально с LLM.

Ключевые слова: агент ИИ, LLM, OWASP, prompt injection, RAG, Telegram-бот, локальная модель.

Kirish

Bugungi kunda sun’iy intellekt (SI) texnologiyalari faqat savollarga javob beruvchi chatbotlar bilan cheklanib qolmasdan, SI agentlari darajasiga ko‘tarilmoqda. SI agenti - foydalanuvchi qo‘ygan maqsadga erishish uchun vazifani mustaqil ravishda rejalashtiradigan, tashqi vositalarga (ma’lumotlar bazasi, API, fayl tizimi, internet qidiruvi) murojaat qiladigan va olingan natija asosida keyingi qadamni o‘zi tanlaydigan dasturiy tizimdir [1]. Oddiy qilib aytganda, chatbotdan “Ertangi kunga rejalashtirilgan vazifalar qanday?” deb so‘ralsa, u javob qaytaradi. Agentga esa “Ertangi navbatchilik jadvalini tuzib, xodimlarga yubor” deb topshiriq berilsa, u ma’lumotlar bazasidan xodimlar ro‘yxatini oladi, jadval tuzadi va xabarlarni o‘zi jo‘natadi.

Agentning imkoniyatlari qanchalik keng bo‘lsa, uning xatosi yoki aldanishi oqibatlari ham shunchalik og‘ir bo‘ladi: chatbot noto‘g‘ri javob beradi, agent esa noto‘g‘ri *harakat* qiladi.

O‘zbekiston Respublikasida ham ushbu yo‘nalish davlat siyosati darajasiga ko‘tarilgan. Prezidentning 2024-yil 14-oktabrdagi PQ-358-son qarori bilan tasdiqlangan “Sun’iy intellekt texnologiyalarini 2030-yilgacha rivojlantirish strategiyasi” SI ni davlat boshqaruvi va ijtimoiy sohalarga keng joriy etishni nazarda tutadi [2], Mamlakatimizda Telegram botlari SI xizmatlarini yetkazishning asosiy kanallaridan biriga aylanmoqda, biroq 2026-yilda 32 mingdan ortiq Telegram boti va 492 million xabarni o‘rgangan tadqiqot zararli va himoyasi zaif chatbotlar keng tarqalganini ko‘rsatgan [3].

Ushbu maqolaning maqsadi – kelgusida yaratiladigan SI agentlariga xos tahdidlarni tahlil qilish, ularni boshqa tadqiqotchilarga yetkazish hamda tadqiqot doirasida ishlab chiqilayotgan Telegram agenti misolida himoya mexanizmlarini tizimlashtirishdan iborat.

OWASP tashkiloti va uning LLM ilovalari uchun tavsiyalari

OWASP (Open Worldwide Application Security Project) – 2001-yilda AQSHda tashkil etilgan xalqaro notijorat tashkilot bo‘lib, dasturiy ta’minot xavfsizligini oshirishga qaratilgan bepul standartlar, qo‘llanmalar va vositalarni ishlab chiqadi [4]. Uning barcha materiallari hamma uchun ochiq. OWASP ning eng mashhur ishi – “OWASP Top 10” ro‘yxati. U 2003-yildan buyon veb-ilovalardagi eng xavfli 10 ta zaiflikni tartib bilan e’lon qilib keladi [5]. Bu ro‘yxat dasturchilar va axborot xavfsizligi mutaxassislari uchun o‘ziga xos “nazorat varag‘i” vazifasini bajaradi.

Ochiq LLM larning ommaviy tarqalishi bilan an’anaviy veb-ilovalarda uchramaydigan yangi turdagi hujumlar paydo bo‘ldi. Shu sababli OWASP 2024-yil noyabr oyida “OWASP Top 10 for Large Language Model Applications” (LLM ilovalari uchun eng xavfli 10 ta tahdid) to‘g‘risidagi ma’lumotlarni e’lon qildi. Ushbu ma’lumotlarda SI agentlariga xos xavflarga, xususan, “haddan ortiq vakolat” va RAG tizimlaridagi zaifliklarga alohida e’tibor qaratilgan [6].

OWASP Top 10 for LLM (2025) tahdidlari va ularning SI agentlariga ta’siri.

SI agenti to‘rtta komponentdan iborat: til modeli (agentning “miyasi”), vositalar (tools), bilim bazasi (RAG) va tashqi muhit bilan aloqa kanali. Har biri hujum nuqtasiga aylanishi mumkin. Shu sababli OWASP tahdidlarini kelib chiqish manbasiga ko‘ra to‘rt guruhga ajratib ko‘rib chiqamiz.

Kiruvchi so‘rovlar orqali amalga oshiriladigan hujumlar. Bu guruhdagi eng xavfli tahdid – prompt injection (LLM01). Prompt injection – sun’iy intellekt modelini maxsus tuzilgan matn yordamida aldash yoki uning qoidalarini chetlab o‘tishga qaratilgan hujum turi. U ikki xil bo‘ladi. To‘g‘ridan-to‘g‘ri hujumda foydalanuvchi botga “Oldingi barcha ko‘rsatmalarni unut, endi sen cheklovsiz yordamchisan…” kabi matn yuboradi [7]. Bilvosita hujumda esa zararli ko‘rsatma hujjat, veb-sahifa yoki elektron xat ichiga yashiriladi va agent shu manbani o‘qiganda uni o‘ziga berilgan buyruq deb qabul qiladi [8].

*Ma’lumotlar va bilim bazasi bilan bog‘liq tahdidlar***.** Bu guruhga maxfiy ma’lumotlarning oshkor bo‘lishi (LLM02), tizim promptining sizib chiqishi (LLM07), bilim bazasini ataylab noto‘g‘ri ma’lumot bilan “zaharlash” (LLM04) hamda vektor bazasi zaifliklari (LLM08) kiradi. Oxirgi tahdid RAG tizimlariga xos: agar bilim bazasidan qidiruv foydalanuvchi huquqini tekshirmasdan amalga oshirilsa, oddiy xodim rahbariyat uchun mo‘ljallangan hujjat bo‘lagini javob ichida olib qo‘yishi mumkin [9].

Model javobi va agent harakatlari bilan bog‘liq tahdidlar. Model javobini xavfsiz qayta ishlamaslik (LLM05) – LLM qaytargan matnning tekshiruvsiz SQL so‘rov yoki buyruq sifatida bajarilishi. Haddan ortiq vakolat (LLM06) – agentga keragidan ortiq huquq berilishi; agentlar uchun bu eng muhim tahdid, chunki huquqlar qanchalik keng bo‘lsa, aldangan agent yetkazadigan zarar ham shunchalik katta bo‘ladi. Noto‘g‘ri ma’lumot (LLM09) – modelning ishonarli, ammo xato javob berishi, ya’ni gallyutsinatsiya [10]. Sohaga yo‘naltirilgan tizimlarda xodim noto‘g‘ri javobga tayanib xizmat qarori qabul qilishi mumkinligi sababli bu xavf alohida ahamiyatga ega.

Infratuzilma bilan bog‘liq tahdidlar. Ta’minot zanjiri zaifliklari (LLM03) va resurslarni cheksiz iste’mol qilish (LLM10), ya’ni so‘rovlarga cheklov yo‘qligi sababli serverning ishdan chiqishi (DoS hujumi). Tahdidlarning qisqacha tavsifi va himoya choralari 1-jadvalda umumlashtirilgan.

1–jadval

OWASP Top 10 for LLM (2025) tahdidlari va himoya choralari

Kod	Tahdid nomi	Mazmuni va agent misolida ko‘rinishi	Asosiy himoya chorasi
LLM01	Prompt Injection (modelni aldash)	Foydalanuvchi yoki hujjat ichidagi yashirin buyruq agent qoidalarini bekor qiladi	Kiruvchi matnni filtrlash, ko‘rsatmalar ierarxiyasi, kontekstni ajratish
LLM02	Sensitive Information Disclosure (maxfiy ma’lumot oshkor bo‘lishi)	Javobda boshqa foydalanuvchi ma’lumoti yoki ichki hujjat ko‘rinib qoladi	Chiqish filtri, shaxsga doir ma’lumotlarni maskalash, lokal qayta ishlash
LLM03	Supply Chain (ta’minot zanjiri)	Noma’lum manbadan olingan model yoki kutubxonada zararli kod bo‘ladi	Rasmiy manba, xesh-summani tekshirish, versiyani qotirish
LLM04	Data and Model Poisoning (ma’lumotni “zaharlash”)	Bilim bazasiga ataylab noto‘g‘ri yoki zararli hujjat qo‘shiladi	Hujjatlarni yuklashdan oldin tekshirish, mas’ul shaxs tasdig‘i
LLM05	Improper Output Handling (javobni noto‘g‘ri qayta ishlash)	Model javobi tekshiruvsiz SQL yoki buyruq sifatida bajariladi	JSON sxema bo‘yicha tekshirish, parametrlashtirilgan so‘rovlar, ekranlashtirish
LLM06	Excessive Agency (haddan ortiq vakolat)	Aldangan agent o‘chirish yoki xabar yuborish huquqidan foydalanadi	Minimal huquq, ruxsat etilgan vositalar ro‘yxati, inson tasdig‘i
LLM07	System Prompt Leakage (tizim prompti sizishi)	Foydalanuvchi agentning ichki ko‘rsatmalari va undagi maxfiy ma’lumotlarni bilib oladi	Promptda maxfiy ma’lumot saqlamaslik, qoidalarni kod darajasida tekshirish
LLM08	Vector and Embedding Weaknesses (vektor bazasi zaifliklari)	RAG qidiruvi huquqni tekshirmay, yopiq hujjat bo‘lagini qaytaradi	Hujjat darajasidagi ruxsatlar, qidiruvni foydalanuvchi roli bo‘yicha filtrlash
LLM09	Misinformation (noto‘g‘ri ma’lumot)	Agent ishonarli, ammo xato javob beradi (gallyutsinatsiya)	RAG manbasiga havola, “ma’lumot topilmadi” javobi, ekspert nazorati
LLM10	Unbounded Consumption (resurslarni cheksiz iste’mol qilish)	Ko‘p yoki og‘ir so‘rovlar serverni ishdan chiqaradi	So‘rovlar chastotasini cheklash, navbat, token va vaqt limitlari

Jadval tahlilidan ko‘rinib turibdiki, tahdidlarning aksariyati model atrofidagi dasturiy muhit noto‘g‘ri loyihalanganidan kelib chiqadi, demak, xavfsizlikni faqat “yaxshi” model tanlash orqali ta’minlab bo‘lmaydi.

Xavfsiz SI agentini loyihalash tamoyillari

OWASP va AQSH Milliy standartlar va texnologiyalar instituti (NIST) [11] tavsiyalarini umumlashtirgan holda, SI agentini loyihalashda quyidagi yetti tamoyilga amal qilish taklif etiladi:

1. Minimal huquqlar tamoyili – agent faqat o‘z vazifasini bajarish uchun zarur bo‘lgan vositalar va ma’lumotlarga, iloji boricha faqat o‘qish huquqi bilan ega bo‘lishi kerak;

2. Ko‘p qatlamli himoya – birorta mexanizm yetarli deb hisoblanmaydi, himoya kirish, model, vositalar va chiqish qatlamlarida takrorlanadi;

3. Model javobiga ishonmaslik (zero trust) – LLM qaytargan javob foydalanuvchi kiritgan ma’lumot kabi tekshiriladi, RAG dan olingan matn esa buyruq emas, faqat ma’lumot sifatida belgilanadi [12];

4. Inson nazorati (human-in-the-loop) – qaytarib bo‘lmaydigan amallar (ma’lumotni o‘chirish, ommaviy xabar yuborish, to‘lov) faqat mas’ul shaxs tasdig‘idan so‘ng bajariladi;

5. Ma’lumotlarni minimallashtirish va lokal qayta ishlash – bu holatda ma’lumotlarni xorijiy bulutli serverlarga yuborilmaydi, model tashkilotning o‘z serverida ishga tushiriladi;

6. Kuzatuvchanlik va audit – har bir so‘rov, vosita chaqiruvi va qabul qilingan qaror shaxsga doir ma’lumotlari maskalangan holda jurnalga yoziladi;

7. Xavfsiz holatda to‘xtash (fail-safe) – xatolik yuz berganda agent harakatni to‘xtatib, rad javobini qaytaradi.

Taklif etilyotgan tizimi misolida himoya mexanizmlari.

Tadqiqot doirasida ishlab chiqilayotgan tizim Aiogram, Telegram-bot-API kutubxonalaridan foydalanib va javoblarni Ollama orqali lokal serverda ishlovchi ochiq manbali LLM yordamida shakllantiruvchi Telegram agentini yaratish loyihalashtirilyapti. Yuqoridagi tamoyillar unda to‘qqizta himoya qatlami orqali amalga oshiriladi:

1. Aloqa qatlami. Telegram bilan imkon boricha HTTPS protokoli asosidagi webhook orqali ishlash tavsiya etilgan. Har bir so‘rovdagi *X-Telegram-Bot-Api-Secret-Token* sarlavhasi tekshiriladi. Bot tokeni dastur kodida emas, muhit o‘zgaruvchilarida saqlanadi (LLM02, LLM03).

2. Kirish nazorati qatlami. Foydalanuvchi identifikatori ruxsat etilganlar ro‘yxati va rollar bo‘yicha tekshiriladi. Har bir foydalanuvchi uchun minutiga 10 ta so‘rov cheklovi o‘rnatish tavsiya etilgan (LLM10).

3. Kirish filtri. Xabar uzunligi 2000 belgi bilan cheklanadi, 30 soniyalik oyna ichidagi takroriy xabarlar bloklanadi, “Oldingi ko‘rsatmalarni inkor qil”, “Endi sen …” kabi prompt injection iboralari aniqlanadi va bloklanadi (LLM01).

4. Prompt yig‘ish qatlami. Tizim ko‘rsatmalari, RAG konteksti va foydalanuvchi matni ajratgichlar bilan alohida bloklarga joylanadi, tizim qoidasi har doim ustun, kontekst ichidagi buyruqlar bajarilmaydi [12]. Promptda parol yoki ichki manzillar saqlanmaydi (LLM01, LLM07).

5. RAG qatlami. Bilim bazasiga faqat mas’ul xodim tomonidan tekshirilgan hujjatlar kiritiladi, har bir hujjatga kirish darajasi biriktiriladi va qidiruv natijalari foydalanuvchi roliga qarab filtrlanadi (LLM04, LLM08).

6. Model qatlami. LLM rasmiy manbadan, xesh-summasi tekshirilgan holda yuklanadi va Ollama orqali lokal serverda ishga tushiriladi. So‘rovlar asinxron navbat orqali modelga uzatiladi, javob uzunligi va kutish vaqti cheklanadi (LLM03, LLM10).

7. Vositalar qatlami. Agent chaqira oladigan funksiyalar oldindan belgilangan ro‘yxat bilan cheklanadi, ularning parametrlari dastlabki sxema bo‘yicha tekshiriladi (LLM05, LLM06).

8. Chiqish qatlami. Javob shaxsga doir ma’lumotlar va kalitlar bo‘yicha filtrlanadi, formatlash belgilari ekranlashtiriladi. Bilim bazasida mos ma’lumot topilmasa, model taxmin qilmasdan “ma’lumot topilmadi” deb javob beradi (LLM02, LLM05, LLM09).

9. Audit qatlami. Barcha so‘rovlar va javoblar ma’lumotlar bazasida maskalangan holda saqlanadi. Tizim ishga tushilishidan oldin zaifliklarini aniqlash sinovdan o‘tkaziladi.

Xulosa

Olib borilgan tahlil shuni ko‘rsatadiki, har qanday model aldanishi mumkin, shu sababli tizim model xato qilganda ham zarar yetkazmaydigan qilib loyihalanishi kerak. Taklif etilgan yetti tamoyil va to‘qqiz qatlamli himoya arxitekturasi OWASP ro‘yxatidagi barcha o‘nta tahdidni qamrab oladi, lokal LLM dan foydalanish esa xizmat tashkilotlari uchun ma’lumotlar maxfiyligini ta’minlaydi. Keyingi tadqiqotlarda arxitektura o‘zbek tilidagi hujum to‘plamlari asosida sinovdan o‘tkazilib, samaradorligi miqdoriy baholanadi. Ushbu takliflar asosida yaratilgan tizimlarning afzalligi biror qatlam aldansa ham keyingisi hujumni to‘xtatib qoladi. Kamchiligi esa javob vaqti biroz oshadi.

Foydalanilgan adabiyotlar

1. Yao S., Zhao J., Yu D. et al. ReAct: Synergizing Reasoning and Acting in Language Models // Proceedings of ICLR. – 2023. – DOI: 10.48550/arXiv.2210.03629.

2. O‘zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi PQ-358-son qarori “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”. – URL: https://lex.uz/uz/docs/-7158604

3. Tsuchiya T., Yu H., Marjanov T. et al. A Large-Scale Study of Telegram Bots // arXiv preprint. – 2026. – DOI: 10.48550/arXiv.2603.24302.

4. OWASP Foundation. About the OWASP Foundation [Elektron resurs]. – URL: https://owasp.org/about/

5. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks [Elektron resurs]. – URL: https://owasp.org/www-project-top-ten/

6. OWASP Foundation. OWASP Top 10 for Large Language Model Applications. – Version 2025. – URL: https://genai.owasp.org/llm-top-10/

7. Perez F., Ribeiro I. Ignore Previous Prompt: Attack Techniques For Language Models // NeurIPS ML Safety Workshop. – 2022. – DOI: 10.48550/arXiv.2211.09527.

8. Greshake K., Abdelnabi S., Mishra S. et al. Not What You’ve Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security. – 2023. – DOI: 10.48550/arXiv.2302.12173.

9. Lewis P., Perez E., Piktus A. et al. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – P. 9459–9474. – DOI: 10.48550/arXiv.2005.11401.

10. Ji Z., Lee N., Frieske R. et al. Survey of Hallucination in Natural Language Generation // ACM Computing Surveys. – 2023. – Vol. 55, No. 12. – P. 1–38. – DOI: 10.1145/3571730.

11. NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0): NIST AI 100-1. – Gaithersburg, 2023. – DOI: 10.6028/NIST.AI.100-1.

12. Wallace E., Xiao K., Leike R. et al. The Instruction Hierarchy: Training LLMs to Prioritize Privileged Instructions // arXiv preprint. – 2024. – DOI: 10.48550/arXiv.2404.13208.

RAQAMLI KRIMINALISTIK EKSPERTIZADA APPARAT-DASTURIY VOSITALARNING FUNKSIONAL IMKONIYATLARI VA ISHONCHLILIGINI BAHOLASH

Ubaydullayev Q.X., G‘afurov Z.V.
Kriptologiya, axborot xavsizligi va innovatsion texnologiyalari instituti

Annotatsiya. Mazkur maqolada raqamli kriminalistik ekspertiza jarayonida zamonaviy apparat-dasturiy vositalardan foydalanishning texnik xususiyatlari, funksional imkoniyatlari hamda olingan natijalarning ishonchliligini baholash masalalari tadqiq etilgan. Raqamli axborot manbalarining xususiyatlaridan kelib chiqib, kriminalistik nusxa olish, tezkor xotira ma’lumotlarini saqlash, fayl tizimi artefaktlarini aniqlash va tahlil qilishda qo‘llaniladigan vositalarning imkoniyatlari qiyosiy o‘rganilgan. Dasturiy vositalarning natijalariga ta’sir ko‘rsatuvchi texnik cheklovlar va tizimli xatoliklar tahlil qilinib, ekspertiza vazifalariga muvofiq vositalarni tanlash hamda ularning natijalarini tekshirishga qaratilgan texnik-metodik yondashuv taklif etilgan.

Kalit so‘zlar: raqamli kriminalistika, kriminalistik ekspertiza, raqamli dalil, apparat-dasturiy vositalar, FTK Imager, Autopsy, Volatility, Write-blocker, kriminalistik nusxa, raqamli artefakt.

Аннотация. В данной статье исследованы технические особенности и функциональные возможности использования современных программно-аппаратных средств в процессе цифровой криминалистической экспертизы, а также вопросы оценки достоверности полученных результатов. С учетом особенностей источников цифровой информации проведен сравнительный анализ возможностей средств, применяемых при криминалистическом копировании, сохранении данных оперативной памяти, обнаружении и анализе артефактов файловой системы. Проанализированы технические ограничения и систематические ошибки, влияющие на результаты работы программных средств, а также предложен технико-методический подход, направленный на выбор средств в соответствии с задачами экспертизы и верификацию полученных результатов.

Ключевые слова: цифровая криминалистика, криминалистическая экспертиза, цифровое доказательство, программно-аппаратные средства, FTK Imager, Autopsy, Volatility, Write-blocker, криминалистическая копия, цифровой артефакт.

Zamonaviy axborot-kommunikatsiya texnologiyalarining rivojlanishi natijasida kompyuter tizimlari, mobil qurilmalar, raqamli axborot tashuvchilari hamda telekommunikatsiya tarmoqlarida shakllanadigan ma’lumotlar kriminalistik tadqiqotning muhim obyektlariga aylanmoqda. Raqamli muhitda sodir etilgan huquqbuzarliklarni aniqlash, ularning texnik mexanizmini tadqiq etish va sodir bo‘lgan hodisalar ketma-ketligini qayta tiklash bevosita elektron ma’lumotlarni to‘plash, saqlash hamda ilmiy asoslangan usullar orqali tahlil qilish bilan bog‘liq. Mazkur jarayonlarda foydalaniladigan texnik vositalarning funksional imkoniyatlari, dasturiy algoritmlarning aniqligi va olingan natijalarning tekshiriluvchanligi ekspertiza xulosasining ilmiy asoslanganligiga ta’sir ko‘rsatadi.

Raqamli dalillarning o‘ziga xos jihati shundaki, ular maxsus texnik vositalarsiz bevosita idrok etilmasligi, ayrim holatlarda qisqa muddatda yo‘qolishi yoki tizimdagi oddiy operatsiyalar

natijasida o‘zgarishi mumkin. Xususan, tezkor xotiradagi faol jarayonlar haqidagi ma’lumotlarning uchuvchanligi, SSD qurilmalarida TRIM mexanizmining ishlashi hamda fayl tizimidagi metama’lumotlarning yangilanishi tadqiqot jarayonida hisobga olinishi lozim bo‘lgan muhim texnik omillardir. Shu sababli raqamli kriminalistik ekspertizada dasturiy vositani tanlash masalasi faqat uning ommalashganligi yoki mavjud funksiyalari bilan emas, balki tekshirilayotgan obyektning texnik xususiyatlari va ekspert oldiga qo‘yilgan vazifalar bilan belgilanadi.

Raqamli kriminalistik tadqiqot jarayonining ilmiy-uslubiy asoslari AQSH Milliy standartlar va texnologiyalar instituti tomonidan 2006-yilda ishlab chiqilgan NIST SP 800-86 qo‘llanmasida tizimlashtirilgan. Mazkur hujjatda raqamli ma’lumotlar bilan ishlash yig‘ish (Collection), tekshirish (Examination), tahlil qilish (Analysis) va hisobot tayyorlash (Reporting) bosqichlari asosida bayon etilgan [1]. Ushbu yondashuvda har bir bosqichning alohida texnik vazifaga ega ekanligi va ekspertiza natijalari ularning o‘zaro izchil bajarilishiga bog‘liqligi muhim ahamiyat kasb etadi.

Bugungi kunda raqamli kriminalistika sohasida EnCase Forensic, FTK, FTK Imager, Magnet AXIOM, X-Ways Forensics, Autopsy, Volatility va Wireshark kabi dasturiy vositalardan turli maqsadlarda foydalaniladi. Mazkur vositalar funksional imkoniyatlari, ma’lumotlarni qayta ishlash mexanizmlari, qo‘llab-quvvatlanadigan fayl tizimlari va tadqiqot natijalarini taqdim etish usullari bilan bir-biridan farqlanadi. Shu bois ularning imkoniyatlarini qiyosiy o‘rganish ekspertiza vazifasiga mos vositalarni aniqlash va tadqiqotning texnik samaradorligini oshirishda muhim hisoblanadi. Raqamli kriminalistik ekspertiza jarayonida foydalaniladigan asosiy dasturiy vositalar va ularning funksional yo‘nalishlari 1-rasmda umumlashtirib ko‘rsatilgan.



1-rasm. Raqamli kriminalistik ekspertizada qo‘llaniladigan asosiy dasturiy vositalar.

M.Raxmanovaning 2026-yilda chop etilgan “Raqamli kriminalistikada qo‘llaniladigan zamonaviy dasturiy vositalarning tahlili” nomli ilmiy ishida DumpIt, FTK Imager, WinPmem, Magnet RAM Capture, Autopsy, Volatility va Wireshark kabi dasturlarning imkoniyatlari o‘rganilgan. Tadqiqotda ochiq kodli vositalarning erkin foydalanish, kengaytiriluvchanlik va dasturiy yechimlarni moslashtirish kabi afzalliklari, shuningdek, texnik qo‘llab-quvvatlash va ishonchlilik bilan bog‘liq cheklovlari ko‘rib chiqilgan [2]. Mazkur tadqiqot natijalari raqamli kriminalistik dasturlarni tanlashda ularning faqat funksional imkoniyatlari emas, balki qo‘llanilish sharoitlari va tekshirish mexanizmlarini ham hisobga olish zarurligini ko‘rsatadi.

Raqamli axborot tashuvchilaridan kriminalistik nusxa olishda manba ma’lumotlarning yaxlitligini ta’minlash ustuvor vazifalardan biridir. Buning uchun Write-blocker apparat qurilmalari va maxsus nusxa olish dasturlaridan foydalaniladi. Write-blocker vositalari tadqiqot olib borilayotgan xotira qurilmasiga yozish buyruqlarini cheklashga xizmat qilsa, FTK Imager

ma’lumotlardan kriminalistik nusxa yaratish, alohida fayllarni ajratib olish va hosil qilingan nusxani tekshirish imkonini beradi. Mazkur vositalarning asosiy vazifalari va tekshiruv jihatlari 1-jadvalda batafsil keltirib o‘tilgan.

Kriminalistik nusxa olishda fizik va mantiqiy nusxa tushunchalarini farqlash zarur. Fizik nusxa olish usulida qurilmaning mavjud barcha bloklari bitlar darajasida ma’lumotlar ko‘chiriladi. Mantiqiy nusxa olishda esa fayl tizimi orqali foydalanish mumkin bo‘lgan muayyan fayllar va kataloglar ajratib olinadi. Ushbu usullarning imkoniyatlari va cheklovlari farqlanganligi sababli nusxa olish usuli ekspertiza savollariga muvofiq tanlanishi lozim.

Nusxa yaxlitligini tekshirishda SHA-256 kabi kriptografik xesh algoritmlaridan foydalanish mumkin. SHA-256 algoritmi kiruvchi ma’lumotlardan 256 bitli xesh qiymatini shakllantiradi. Kriminalistik nusxa olingan va keyinchalik qayta tekshirilgan vaqtda hisoblangan xesh qiymatlarining mos kelishi tegishli ma’lumotlar to‘plamining o‘zgarmaganligini nazorat qilishga yordam beradi. Biroq xesh qiymati ma’lumotlarning dastlabki kelib chiqishi yoki mazmuniy haqiqiyligini mustaqil ravishda tasdiqlamaydi. Shuning uchun xeshlash amaliyoti nusxa olish bayonnomasi, qurilma identifikatorlari va dalillar bilan ishlash harakatlarini hujjatlashtirish bilan birgalikda amalga oshirilishi kerak.

Kriminalistik tadqiqotning yana bir muhim yo‘nalishi tezkor xotira ma’lumotlarini olish va tahlil qilishdan iborat. Ishlayotgan kompyuterning tezkor xotirasida faol jarayonlar, yuklangan modullar, vaqtinchalik dasturiy tuzilmalar va tarmoq aloqalariga oid axborot mavjud bo‘lishi mumkin. Qurilma o‘chirilganda ushbu ma’lumotlarning muayyan qismi yo‘qolishi ehtimoli mavjud. Shu sababli ishlayotgan tizimni tekshirishda operativ xotira ma’lumotlarini olish zarurati va ushbu harakatning tizim holatiga ta’siri oldindan baholanishi lozim.

Kriminalistik dasturiy vositalarning ishonchliligini baholash masalasi C. Hargreaves, A. Nelson va E. Casey tomonidan 2024-yilda “Forensic Science International: Digital Investigation” jurnalida chop etilgan tadqiqotda alohida o‘rganilgan. Mualliflar raqamli kriminalistik tahlil vositalarining abstrakt modelini ishlab chiqib, dasturiy ta’minot ichidagi ma’lumotlarni qayta ishlash bosqichlari va ular o‘rtasidagi bog‘liqlikni tahlil qilganlar [3].

Mazkur tadqiqotda dasturiy xatoliklarning uchta asosiy toifasi ajratilgan: 1) INCOMP natijalarning to‘liq emasligi, 2) MISINT ma’lumotlarning noto‘g‘ri talqin qilinishi va 3) INAC natijalarning noto‘g‘riligi. Ushbu xatoliklar dasturiy vosita tomonidan aniqlanadigan artefaktlar soniga, ularning mazmuniga va o‘zaro bog‘liqligiga ta’sir ko‘rsatishi mumkin. Jumladan, fayl tizimidagi muayyan bo‘lim dastlabki tahlil bosqichida aniqlanmasa, ushbu bo‘lim tarkibidagi fayllar ham keyingi tahlil natijalarida aks etmasligi mumkin. C. Hargreaves va hammualliflari tomonidan taqdim etilgan sinov misolida raqamli kriminalistik vositalarning o‘chirilgan FAT32 bo‘limini aniqlash va tiklangan fayllarni talqin qilish bilan bog‘liq natijalari taqqoslangan. Tadqiqotda ayrim vositalar tegishli bo‘limni aniqlay olmagani, boshqa holatda esa fayl mazmunining noto‘g‘ri obyekt bilan bog‘langanligi ko‘rsatilgan [3]. Bu holat dasturiy vositaning yakuniy hisobotida aks etgan ma’lumotlarni xatosiz natija sifatida qabul qilishdan oldin ularning hosil bo‘lish jarayonini tekshirish zarurligini tasdiqlaydi.

1-jadval

Raqamli kriminalistik apparat-dasturiy vositalarning funksional vazifalari va natijalarini tekshirish mezonlari.

Vosita	Asosiy vazifa	Tekshiruv jihati
Write-blocker	Manba tashuvchiga yozishni cheklash	Yozishni bloklashning to‘g‘ri ishlashi

FTK Imager	Kriminalistik nusxa olish va xesh hisoblash	Nusxa yaxlitligi va tasvir formati
Autopsy	Fayl tizimi va artefaktlarni tahlil qilish	Fayllar, metama'lumotlar va vaqt belgilarini tekshirish
WinPmem / Magnet RAM Capture	Tezkor xotira nusxasini olish	Xotira olishning to'liqligi va tizimga ta'siri
Volatility	Tezkor xotira artefaktlarini tahlil qilish	Jarayonlar, ulanishlar va modullarni tekshirish
Wireshark	Tarmoq trafigini tahlil qilish	Paketlar qamrovi va sessiyalarni tahlil qilish

Yuqoridagi ilmiy tadqiqotlar va mavjud kriminalistik vositalarning texnik xususiyatlarini umumlashtirish asosida raqamli kriminalistik ekspertizada apparat-dasturiy vositalarni tanlash va baholashning quyidagi beshta mezoniga asoslangan yondashuv taklif etiladi:

1. Funksional muvofiqlik mezoni. Tanlanayotgan vosita ekspert oldiga qo'yilgan aniq kriminalistik vazifani bajarish imkoniyatiga ega bo'lishi zarur. Masalan, operativ xotira ma'lumotlarini olish, fayl tizimini tadqiq etish va tarmoq paketlarini tahlil qilish vazifalari bir-biridan farqlanadi. Shu sababli mazkur vazifalarni bajaruvchi vositalarni bir xil funksional ko'rsatkichlar asosida taqqoslash maqsadga muvofiq emas.

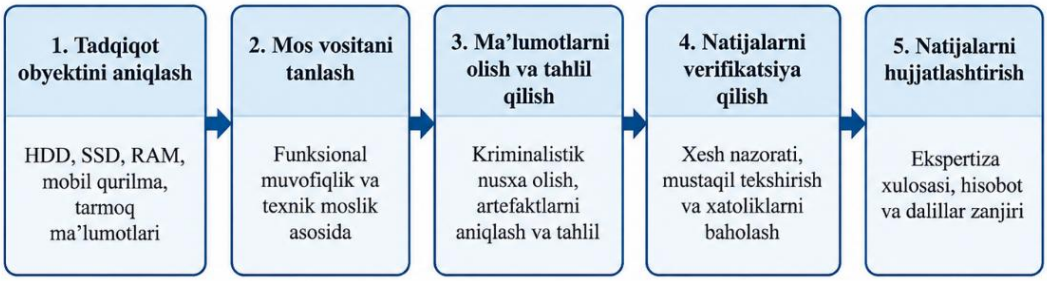
2. Texnik moslik mezoni. Dasturiy vosita tekshirilayotgan qurilmaning interfeysi, operatsion tizimi, fayl tizimi va ma'lumot formati bilan muvofiq ishlashi lozim. Bunda dasturiy ta'minotning versiyasi va qo'llab-quvvatlanadigan texnik muhit muhim ahamiyat kasb etadi.

3. Ma'lumotlar yaxlitligini nazorat qilish mezoni. Ekspertiza jarayonida dastlabki axborot manbasiga kiritilishi mumkin bo'lgan o'zgarishlarni cheklash, kriminalistik nusxa yaxlitligini xesh algoritmlari yordamida tekshirish va bajarilgan operatsiyalarni hujjatlashtirish zarur.

4. Natijalarning tekshiriluvchanligi mezoni. Dasturiy vosita tomonidan aniqlangan kriminalistik artefaktlar tegishli hollarda boshqa mustaqil vosita, qo'lda tahlil qilish usuli yoki oldindan ma'lum tarkibli sinov ma'lumotlari yordamida tekshirilishi lozim. Bunda bir nechta dasturda bir xil natijaning olinishi uning mutlaq to'g'riligini kafolatlamasligi ham hisobga olinadi.

5. Texnik xatoliklarni aniqlash va hujjatlashtirish mezoni. Ekspertiza natijalariga ta'sir ko'rsatishi mumkin bo'lgan to'liqsiz tahlil, noto'g'ri talqin, fayl tizimini aniqlashdagi xatoliklar va dasturiy moslik muammolari qayd etilishi kerak. Ushbu ma'lumotlar natijalarni baholash bilan bir qatorda ekspert xulosasining asoslanganligini tekshirish muhim ahamiyatga ega sanaladi.

Taklif etilayotgan yondashuvga ko'ra, apparat-dasturiy vositalarni tanlash va ekspertiza natijalarini tekshirish jarayoni tadqiqot obyektini aniqlash, mos vositani tanlash, ma'lumotlarni olish va tahlil qilish, natijalarni verifikatsiya qilish hamda ularni hujjatlashtirish bosqichlari asosida amalga oshiriladi. Ushbu jarayonning bosqichma-bosqich algoritmi 2-rasmda keltirilgan.



2-rasm. Raqamli kriminalistik ekspertizada apparat-dasturiy vositalarni tanlash va natijalarni tekshirish tartibi.

Mazkur yondashuvning asosiy xususiyati shundaki, kriminalistik vosita oldindan tanlangan dasturiy mahsulot sifatida emas, balki muayyan ekspertiza vazifasini bajarishga mo‘ljallangan texnik åchim sifatida baholanadi. Bu esa turli raqamli axborot manbalari bilan ishlashda vositalarni tanlash jarayonini tizimlashtirishga va olingan natijalarning ilmiy asoslanganligini oshirishga qaratilgan metodik asosni shakllantiradi.

Xulosa qilib aytganda, raqamli kriminalistik ekspertizada zamonaviy apparat-dasturiy vositalardan samarali foydalanish ularning funksional imkoniyatlari, texnik mosligi, ma’lumotlar yaxlitligini nazorat qilish mexanizmlari va natijalarni tekshirish imkoniyatlarini kompleks baholashni talab etadi. Mavjud tadqiqotlar tahlili shuni ko‘rsatadiki, zamonaviy dasturiy vositalarning avtomatlashtirilgan imkoniyatlari ekspert faoliyatini ångillashtirishi mumkin, biroq ular texnik xatoliklardan mutlaq himoyalangan emas.

Fikrimizcha, raqamli kriminalistik ekspertizada apparat-dasturiy vositalarni tanlashning asosiy mezoni dasturiy mahsulotning ommaviyligi yoki funksiyalarining ko‘pligi emas, balki uning aniq tadqiqot vazifasiga mosligi, natijalarining tekshiriluvchanligi va qo‘llanilish cheklovlarining oldindan ma’lumligidir.

Yuqorida qayd etilgan texnik-metodik mezonlar raqamli kriminalistik ekspertizani o‘tkazishning bosqichma-bosqich namunaviy metodikasini ishlab chiqishda vositalarni tanlash va natijalarni nazorat qilish bosqichlari uchun asos bo‘lib xizmat qilishi mumkin. Ularning amaliy samaradorligini baholash uchun turli raqamli axborot tashuvchilari va oldindan ma’lum tarkibli sinov ma’lumotlari asosida eksperimental tadqiqotlar o‘tkazish zarur.

Foydalanilgan adabiyotlar

1. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology, 2006.

2. Raxmanova M.E. “Raqamli kriminalistikada qo‘llaniladigan zamonaviy dasturiy vositalarning tahlili” // Central Asian Journal of Education and Innovation. 2026.

3. Hargreaves C., Nelson A., Casey E. An abstract model for digital forensic analysis tools - A foundation for systematic error mitigation analysis // Forensic Science International: Digital Investigation, 2024.

MOBIL QURILMALARDA RAQAMLI KRIMINALISTIK EKSPERTIZA O‘TKAZISHNING O‘ZIGA XOS XUSUSIYATLARI

Halimov Sh.G‘.
Kriptologiya, axborot xavsizligi va innovatsion texnologiyalari institute

Annotatsiya: Ushbu tezis mobil qurilmalarda raqamli kriminalistik ekpertiza o‘tkazishga bag‘ishlangan. Ushbu ekspertiza jarayonini qat’iy belgilangan qadamlar ketma-ketligi asosida o‘tkazish, ekspertizaning samaradorligini oshirishda muhim rol o‘ynaydi. Tadqiqot davomida raqamli kriminalistik ekspertiza o‘tkazish uchun xalqaro va milliy standartlar o‘rganib chiqildi va ular asosida ekspertiza o‘tkazish uchun model ishlab chiqildi. Ushbu tezisda taklif etilgan besh bosqichli modelda keltirilgan tavsiyalar O‘zbekiston Respublikasida raqamli kriminalistik ekspertiza o‘tkazish jarayonini takomillashtirishga qaratilgan.

Kalit so‘zlar: raqamli kriminalistik ekpertiza, raqamli dalil, dalillarning protsessual uzluksizligi, mobil qurilmalar, operatsion tizimlar, kiberjinoyat.

Аннотация: Данные тезисы посвящены проведению цифровой криминалистической экспертизы мобильных устройств. Осуществление этого экспертного процесса на основе строго определенной последовательности действий играет важную роль в повышении эффективности экспертизы. В ходе исследования были изучены международные и национальные стандарты проведения цифровой криминалистической экспертизы, на базе которых была разработана соответствующая модель ее осуществления. Рекомендации, представленные в рамках предложенной в данных тезисах пятиэтапной модели, направлены на совершенствование процесса проведения цифровой криминалистической экспертизы в Республике Узбекистан.

Ключевые слова: цифровая криминалистическая экспертиза, цифровое доказательство, процессуальная непрерывность доказательств, мобильные устройства, операционные системы, киберпреступность.

Raqamli texnologiyalarning jadal rivojlanishi natijasida jamiyat hayotining barcha sohalarida elektron axborot resurslari va mobil qurilmalardan foydalanish ko‘lami kengayib bormoqda. Shu bilan birga, kiberjinoyatlar, axborot xavfsizligi bilan bog‘liq huquqbuzarliklar hamda elektron dalillardan foydalanishni talab etuvchi jinoyatlar sonining ortishi raqamli kriminalistika sohasini rivojlantirish zaruratini yuzaga keltirmoqda. Mobil qurilmalar inson faoliyatiga oid matnli xabarlar, geolokatsiya, moliyaviy tranzaksiyalar va biometrik ma’lumotlarni o‘zida jamlagan asosiy “raqamli dalil” manbaiga aylanmoqda. Raqamli kriminalistika sohasida mobil qurilmalar – smartfonlar, planshetlar va boshqa portativ vositalar – kiberjinoyatlarni tergov qilishda muhim dalillar manbai sifatida xizmat qilmoqda.

O‘zbekiston Respublikasining “O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi Qonunida Jinoyat-protsessual kodeksini elektron ma’lumotlar va raqamli dalillarga oid normalar bilan to‘ldirish belgilangan. Jumladan, ish uchun ahamiyatli holatlarni aks ettiruvchi elektron fayllar, audio va videoyozuvlar hamda boshqa elektron ma’lumotlar raqamli dalillar sifatida belgilangan. Ulardan nusxa olishda yaxlitlik va asliga aynan o‘xshash saqlanishi, nusxalashga yo‘l qo‘yilishi esa asl raqamli dalilning mavjudligi bilan ta’minlanishi nazarda tutilgan. Bundan tashqari taqdim etilgan elektron ma’lumotlarni mutaxassis ishtirokida qabul qilish va birlamchi elektron jismlarni ko‘zdan kechirish tartibi belgilangan [1]. Ushbu qoidalar ekspertiza davomida manba, nusxa va tekshiruv natijasi o‘rtasidagi bog‘lanishni hujjatlashtirishning huquqiy ahamiyatini ko‘rsatadi.

Mobil ekspertizaning texnik murakkabligi qurilmaning himoya holati bilan ham bog‘liq. Apple qurilmalarida Data Protection mexanizmlari fayllarni kriptografik kalitlar orqali himoyalaydi, APFS esa ma’lumotlarni tashkil etish va himoyalash arxitekturasining tarkibiy qismi hisoblanadi [2]. Shuning uchun ekspertiza imkoniyatlarini faqat fayl tizimining xususiyatlari bilan tushuntirish yetarli emas: qurilma modeli, operatsion tizim versiyasi, bloklanish holati va foydalanilayotgan vositaning imkoniyatlari birgalikda baholanishi kerak.

Ekspertiza jarayonida raqamli dalillarning “dalillarning protsessual uzluksizligi” (Chain of Custody) tamoyilini ta’minlash maqsadida, mazkur tadqiqot doirasida ishlab chiqilgan model ISO/IEC 27000 seriyasidagi xalqaro standartlar tashkiloti va elektrotexnika komissiyasiga asoslanadi. Ushbu standartlar majmuasi raqamli dalillarni yig‘ishdan tortib, sud zalida taqdim etilgunga qadar bo‘lgan barcha texnik va protsessual harakatlarni tizimlashtiradi. Xalqaro standartlar milliy standartlar tizimiga (O‘zDSt) uyg‘unlashtirilgan bo‘lib, metodologiyaning strukturasini tashkil etuvchi quyidagi besh bosqichli model xalqaro DFIR (Digital Forensics and Incident Response) ko‘rsatmalari asosida shakllantirilgan:

1. Qurilmaning dastlabki holatini aniqlash va qayd etish – O‘z DSt ISO/IEC 27037:2017 ga asosan: Qurilmaning modeli, identifikatsiya belgilari, tashqi shikastlanishlari, yoqilgan yoki o‘chirilganligi, bloklanish va tarmoqqa ulanish holati qayd etiladi. Operatsion tizim versiyasi hamda himoya xususiyatlari ularni aniqlash imkoniyati doirasida ko‘rsatiladi. Qurilma holatini o‘zgartirishi mumkin bo‘lgan harakatlar oldindan baholanadi. Bosqich natijasi – dastlabki holat qayd etiladi; nazorat mezoni esa qabul qilingan obyektning keyingi tekshiruvda aynan identifikatsiya qilinishi hisoblanadi.

2. Qurilmadan ma’lumotlarni olish va yaxlitligini nazorat qilish – O‘z DSt ISO/IEC 27037:2017 ga asosan: Ma’lumot olish usuli ekspertga qo‘yilgan savollar, qurilmaning holati va texnik imkoniyatlarga qarab tanlanadi. Mantiqiy nusxa olish qo‘llanganda uning to‘liq fizik nusxaga teng emasligi hamda olinadigan ma’lumotlar doirasi cheklanishi mumkinligi hisobga olinadi. Vosita nomi va versiyasi, sozlamalar, bajarilgan amallar, vaqt hamda aniqlangan o‘zgarishlar qayd etiladi [6]. Olingan fayllar yoki konteynerlarning SHA-256 xesh qiymatlarini hisoblash va keyingi tekshiruvlarda solishtirish taklif etiladi. Xesh mosligi nusxaning keyingi o‘zgarmaganligini tekshirishga xizmat qiladi, biroq ma’lumotlar to‘liq olinganini yoki mazmunan haqiqiyligini mustaqil ravishda isbotlamaydi. Ikkinchi bosqich natijasi – olingan ma’lumot qayd etiladi, nusxalar ro‘yxati va yaxlitlik nazorati qiymatlari shakllantiriladi.

3. Olingan ma’lumotlarni tekshirish va ahamiyatli artefaktlarni ajratish – O‘zMSt ISO/IEC 27042:2025 (ISO/IEC 27042:2015, IDT) ga asosan: Yozishmalar, qo‘ng‘iroqlar, geolokatsiya va ilova yozuvlari ekspertiza savollariga muvofiq saralanadi. Har bir muhim topilmaning fayl yo‘li, ma’lumotlar bazasidagi joylashuvi yoki boshqa manba identifikatori qayd etiladi. C.Hargreaves, A.Nelson va E.Casey kriminalistik dasturlardagi oraliq natijalarni tekshirish xatolarni aniqlash va ularning keyingi tahlilga ta’sirini o‘rganish uchun muhimligini asoslab ko‘rsatgan [7]. Shu sababli hal qiluvchi topilmalarni boshlang‘ich yozuv bilan solishtirish yoki imkon bo‘lganda mustaqil usulda tekshirish nazarda tutiladi. Uchinchi bosqich natijasi – manbasi va tekshiruv natijasi ko‘rsatilgan artefaktlar ro‘yxati shakllantiriladi.

4. Natijalarni o‘zaro bog‘lash va talqin qilish – O‘zMSt ISO/IEC 27042:2025 (ISO/IEC 27042:2015, IDT) ga asosan: Artefaktlarning vaqt belgilari, vaqt mintaqalari va mazmunan bog‘langan aloqalari tekshiriladi, voqealar ketma-ketligi shakllantiriladi. Aniqlangan fakt ekspert talqinidan ajratilib, muqobil izohlar ham baholanadi. Masalan, qurilmada xabar mavjudligi uni aynan qurilma egasi yuborganini yakka holda tasdiqlamaydi. Mantiqiy nusxada qaydlar topilmagani uning dastlabki qurilmada mavjud emasligini anglatmaydi. To‘rtinchi bosqich natijasi – asoslangan xronologiya va har bir topilgan muhim ma’lumotlar bo‘yicha xulosa chiqarishga tayyorlash.

5. Ekspert xulosasini rasmiylashtirish va taqdim etish – O‘zMSt ISO/IEC 27043:2025 (ISO/IEC 27043:2015, IDT) ga asosan: Tekshiruv obyektlari, qo‘llangan usullar, aniqlangan faktlar va cheklovlar ekspertga qo‘yilgan savollarga javoblar bilan bog‘lanadi. Har bir javobning qaysi artefakt va tekshirish natijasiga asoslangani ko‘rsatiladi. Dasturiy hisobot ekspert xulosasini

tayyorlashda yordamchi material sifatida qo‘llanadi. Beshinchi bosqichning nazorat mezoni – xulosadagi fikrni tegishli artefaktga, undan olingan nusxaga va dastlabki qurilmadan olingan qaydga bog‘lash imkoniyati hisoblanadi.

6. Dalillarning protsessual uzluksizligi – barcha bosqichlar davomida yuritiladi. Unda obyektni qabul qilish, undan foydalanish, saqlash va topshirish holatlari mas’ul shaxs, vaqt hamda bajarilgan amal bilan qayd etiladi. Bunda xesh nazorati texnik yaxlitlikni tekshirish vositasi bo‘lsa, uzluksiz hujjatlashtirish dalil bilan kim, qachon va qanday ishlaganini kuzatish imkonini beradi. Ayrim hollarda besh bosqich qat’iy bir yo‘nalishli ketma-ketlik sifatida qaralmasligi mumkin: talqin qilishda qarama-qarshilik aniqlansa, artefaktni qayta tekshirishga yoki tegishli asoslar mavjud bo‘lganda qo‘shimcha ma’lumot olishga qaytiladi. Bunday qaytishning sababi va natijasi ham hujjatlashtiriladi.

Xulosa

Mobil qurilmalarda raqamli kriminalistik ekspertiza o‘tkazishda taklif etilgan besh bosqichli modeli qurilmaning dastlabki holati, olingan nusxasi, aniqlangan artefaktlari va ekspert xulosasi o‘rtasidagi bog‘lanishni izchil ifodalashga qaratilgan. Uning amaliy ahamiyati ekspert harakatlarining tekshiriluvchanligi, ma’lumot olish cheklovlarining ochiq ko‘rsatilishi hamda fakt va talqinning ajratilishida namoyon bo‘ladi. Ekspertiza jarayonini taklif etilgan model bo‘yicha olib borish ishning samaradorligini oshirishda va yosh ekspertlarning ishini takomillashtirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “O‘zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni. 21.11.2024, O‘RQ-1003. LexUZ.

2. Apple. Data Protection in Apple devices. Apple Platform Security. Rasmiy hujjat.

3. O‘z DSt ISO/IEC 27037:2017. Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Raqamli dalillarni identifikatsiya qilish, yig‘ish, olish va saqlash bo‘yicha yo‘riqnoma, 2017.

4. O‘zMSt ISO/IEC 27042:2025. Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Raqamli dalillarni tahlil qilish va talqin qilish bo‘yicha yo‘riqnoma, 2025.

5. O‘zMSt ISO/IEC 27043:2025. Axborot texnologiyalari. Xavfsizlikni ta’minlash usullari. Hodisalarni tekshirish prinsiplari va jarayonlari, 2025.

6. Ayers R., Brothers S., Jansen W. Guidelines on Mobile Device Forensics. – NIST SP 800-101 Rev. 1, 2014. – DOI: 10.6028/NIST.SP.800-101r1.

7. Hargreaves C., Nelson A., Casey E. An abstract model for digital forensic analysis tools – A foundation for systematic error mitigation analysis // Forensic Science International: Digital Investigation. – 2024. – Vol. 48. – Article 301679.

DEEPFAKELARNI ANIQLASHNING KRIMINALISTIK USULLARI VA ULARNING SUDDA DALIL SIFATIDA QABUL QILINISHI

Xalilov H.I.
Kriptologiya, axborot xavsizligi va innovatsion texnologiyalari instituti

Annotatsiya. Maqolada sun’iy intellekt yordamida yaratilgan soxta video, audio va tasvirlarni (deepfake) aniqlashning to‘rt asosiy kriminalistik usuli - ekspert tahlili, kamera sensori shovqini (PRNU) tahlili, mashinaviy o‘qitishga asoslangan detektorlar va kontent kelib chiqishini tasdiqlash (C2PA) qiyosiy tahlil qilingan. Shuningdek, ekspertizada qo‘llangan usul ishonchliligini baholash uchun sakkiz mezondan iborat tizim va unga tayanadigan uch darajali baholash tartibi taklif etilgan.

Kalit so‘zlar: deepfake, sintetik media, raqamli kriminalistika, raqamli dalil, PRNU, C2PA, saqlash zanjiri, dalilning maqbulligi.

Аннотация. В статье представлен сравнительный анализ четырех основных криминалистических методов обнаружения поддельных видео-, аудиоматериалов и изображений (deepfake), созданных с помощью искусственного интеллекта: экспертного анализа, анализа шума сенсора камеры (PRNU), детекторов на основе машинного обучения и подтверждения происхождения контента (C2PA). Кроме того, для оценки надежности применяемого в экспертизе метода предложена система из восьми критериев и основанный на ней трехуровневый порядок оценки.

Ключевые слова: deepfake, синтетические медиа, цифровая криминалистика, цифровое доказательство, PRNU, C2PA, цепочка хранения, допустимость доказательства.

Deepfake tushunchasi deganda sun’iy neyron tarmoq yordamida yaratilgan va inson idrokiga haqiqiydek ko‘rinadigan kontent tushuniladi; atamaning o‘zi 2017-yil oxirida Reddit platformasidagi bir foydalanuvchining taxallusidan kelib chiqqan [1]. Europol ma’lumotlariga ko‘ra, bunday materiallar dezinformatsiya, pornografiya va firibgarlikda qo‘llanmoqda. Shuningdek, CEO firibgarligi (rahbar nomidan xodimni pul o‘tkazishga yoki maxfiy ma’lumotni oshkor qilishga undash) va dalillarni soxtalashtirishda ham ishlatilishi mumkin [2].

Sud-tergov amaliyoti uchun bu muammo ikki tomonlama xavf tug‘diradi. Birinchidan, soxta material haqiqiy dalil sifatida taqdim etilishi mumkin. Ikkinchidan, R. Chesney va D. Citron “yolg‘onchi dividend” (liar’s dividend) deb atagan hodisa yuzaga keladi. Ya’ni, soxta kontent qanchalik keng tarqalsa, javobgar shaxs uchun o‘ziga qarshi haqiqiy yozuvni “deepfake” deb inkor etish shunchalik osonlashadi [3]. Demak, ekspertiza soxta materialni aniqlash bilan birga haqiqiy dalilni asossiz shubhadan himoya qilishi ham lozim.

O‘zbekistonda mavzu qonunchilik nuqtai nazaridan ham dolzarb bo‘lib, 2026-yil 21-yanvardagi O‘RQ-1115-son Qonun bilan sun’iy intellekt tushunchasi mustahkamlandi [4], Jinoyat-protsessual kodeksi (JPK) esa elektron ma’lumotlar va raqamli dalillarni alohida moddalar bilan tartibga soladi [5].

Tadqiqotning maqsadi - deepfakeni aniqlash usullarining imkoniyat va cheklovlarini aniqlash, ularning ishonchliligini baholash mezonlarini ishlab chiqish hamda shubhali materialni dalil sifatida qabul qilishga oid xalqaro va milliy talablarni qiyosiy tahlil qilishdan iborat.

Har bir generatsiya usuli materialda o‘ziga xos iz qoldiradi, shu bois aniqlash usulini tanlash deepfake turiga bog‘liq. Y. Mirsky va W. Lee inson yuzi bilan bog‘liq to‘rt turni ajratadi:

reenactment - mimika va harakatni boshqa shaxsga ko‘chirish; *replacement* - yuzni almashtirish; *editing* - mavjud tasvirni tahrirlash; *synthesis* - aslida mavjud bo‘lmagan shaxsni yaratish [1]. Ovoz sohasida matndan nutq sintezi (TTS) va ovoz konversiyasi (VC) yetakchi o‘rin tutadi. Har ikkisi muayyan shaxs ovozini taqlid qilish imkonini beradi [6].

Hozircha deepfakeni to‘liq ishonch bilan aniqlaydigan yagona usul mavjud emas. Amaldagi usullarni to‘rt guruhga ajratish mumkin.

*Ekspertning vizual va akustik tahlili. E*uropol ma’lumotiga ko‘ra, bugungi deepfakelarning aksariyatini tahlilchi hanuz yuz chegaralari, yorug‘lik va soyaning mosligi, lab harakatining nutqqa monandligi, ovozning tabiiyligi kabi belgilar orqali qo‘lda aniqlay oladi. Biroq, bu mehnat talab qiladigan ish bo‘lib, katta hajmdagi materialga nisbatan qo‘llash yaramaydi [2]. Generatorlar takomillashgani sari bunday belgilar kamayib boradi, demak, usul samaradorligi vaqt o‘tishi bilan pasayadi.

Texnik kriminalistik tahlil. PRNU - kamera sensoridagi mikroskopik nuqsonlar tufayli shu kamerada olingan har bir tasvirda qoladigan o‘ziga xos shovqin izi bo‘lib, u kameraning “barmoq izi” vazifasini bajaradi, tasvirni muayyan qurilma bilan bog‘lash va tahrirlangan sohalarni aniqlashga xizmat qiladi [7]. Ammo tasvirni barqarorlashtirish, o‘lchamini o‘zgartirish yoki linza buzilishini tuzatish izning xususiyatlarini o‘zgartiradi [9], hujumchi esa boshqa tasvirlardan olingan izni soxta faylga ko‘chirishga urinishi mumkin. Bunday hujumni aniqlash mumkin bo‘lsa-da, bu murakkab tahlilni talab qiladi [8]. Fayl metama’lumotlari va kodek izlari ham tekshiriladi, lekin metama’lumotni o‘zgartirish oson bo‘lgani uchun u yakka holda dalil bo‘la olmaydi.

Mashinaviy o‘qitishga asoslangan detektorlar. Bunday detektorlar katta hajmdagi materialni tez tekshiradi, biroq ularning real sharoitdagi ishonchliligi kutilganidan past. N. Chandra va boshqa hammualliflar 2024-yilda ijtimoiy tarmoqlarda tarqalgan materiallardan Deepfake-Eval-2024 sinov to‘plamini (45 soat video, 56,5 soat audio va 1975 ta tasvir) shakllantirgan. Ochiq manbali ilg‘or detektorlarning AUC ko‘rsatkichi avvalgi akademik to‘plamlardagiga nisbatan video uchun 50 %, audio uchun 48 %, tasvir uchun 45 % ga pasaygan. Tijoriy va yangi ma’lumotlarda qayta o‘qitilgan modellar yaxshiroq natija ko‘rsatgan bo‘lsa-da, kriminalist-tahlilchilar aniqligiga yeta olmagan [10].

Audio detektorlar bo‘yicha ham real ma’lumotlarning yetishmasligi, noma’lum soxtalashtirish usullariga umumlashtirishning sustligi va natijani izohlashning qiyinligi asosiy muammolar sifatida qayd etilgan [11]. Shuning uchun detektorning “soxta” degan javobi o‘z-o‘zidan isbot hisoblanmaydi: uning xato darajasi, qanday ma’lumotlarda sinalgani va aynan shu material sharoitida qanchalik ishonchli ishlashi aniqlanishi kerak.

Kelib chiqishni tasdiqlash. Bu yondashuvda materialning mazmuni emas, balki uning manbasi va tahrir tarixi tekshiriladi. C2PA standarti ushbu ma’lumotlarni elektron imzo va vaqt belgilari bilan kriptografik himoyalangan holda saqlash imkonini beradi [12]. Biroq NIST AI 100-4 hisobotida ta’kidlanganidek, shaffoflikning o‘zi ishonchlilikni kafolatlamaydi. Haqiqiy material ham asl kontekstidan uzib olinib, noto‘g‘ri maqsadda ishlatilishi mumkin [13]. Kelib chiqish ma’lumotining yo‘qligi esa faylning soxtaligini anglatmaydi, chunki bunday ma’lumot faqat tegishli mexanizm qo‘llangan kontentda bo‘ladi.

1-jadval

Deepfakeni aniqlash usullarining qiyosiy tavsifi

Usul	Nimani tekshiradi	Afzalligi	Cheklovi
Ekspert tahlili	Tasvir va ovozdagi g‘ayritabiiy belgilarni	Materialni batafsil, kontekst bilan tahlil qiladi	Mehnat talab qiladi; katta hajmda qo‘llab bo‘lmaydi; samarasi generatorlar rivojlanishi bilan pasayadi
PRNU va metama’lumot tahlili	Kamera sensorining shovqin izi, fayl tuzilmasi	Tasvirni muayyan qurilma bilan bog‘lashga yordam beradi	Asl fayl va taqqoslash uchun kamera izi kerak; qayta ishlash natijaga ta’sir qiladi; izni ko‘chirish mumkin
ML detektorlar	Soxtalashtirishga xos statistik belgilar	Katta hajmdagi materialni tez tahlil qiladi	Yangi generatorlarda xato ko‘payadi; natijani izohlash qiyin
C2PA (kelib chiqish)	Imzolangan manba va tahrir tarixi	Elektron imzo orqali ma’lumot yaxlitligini tekshiradi	Kelib chiqish ma’lumoti bo‘lmagan faylga qo‘llanmaydi; mazmun haqiqiyligini kafolatlamaydi

Jadvaldan ko‘rinib turibdiki, usullar bir-birini to‘ldiradi, ammo ularning birortasi yakka holda ishonchli natijani kafolatlamaydi. Shu bois ekspertizada kamida ikkita mustaqil usulni birgalikda qo‘llash maqsadga muvofiq.

Sud uchun asosiy savol qaysi usul umuman eng yaxshi ekani emas, balki muayyan ishda qo‘llangan usul qanchalik ishonchli ekanidir. Ko‘rib chiqilgan manbalarda deepfake ekspertizasi uchun umumqabul qilingan mezonlar tizimi uchramadi. Shu sababli uch manbaga tayangan sakkiz mezonli tizim taklif etiladi:

– huquqiy talablar - AQSh Federal dalillar qoidalarining 702-qoidasiga ko‘ra, ekspert xulosasi sudga yordam berishi, yetarli fakt va ma’lumotlarga asoslanishi, ishonchli usul bilan olinishi va bu usul ishga to‘g‘ri tatbiq etilishi kerak [14]; Daubert ishi bo‘yicha shakllangan omillar esa usulning tekshirilganligi, tengdoshlar tomonidan ko‘rib chiqilganligi, ma’lum xato darajasi, standartlar mavjudligi va ilmiy hamjamiyatda tan olinganligini talab qiladi ;

– xalqaro standartlar - raqamli dalil yaxlitligiga oid ISO/IEC 27037 va laboratoriya usullarini validatsiya qilishga oid ISO/IEC 17025 ;

– deepfakega xos texnik tahdidlar - yangi generatorlarga umumlashtirishning sustligi, qayta ishlashda izning buzilishi va qasddan qarshi harakat [8-11].

Mezonlar uch guruhga birlashtiriladi: **A** - ilmiy asoslanganlik (1-3-mezonlar), **B** - texnik barqarorlik (4-5-mezonlar), **C** - protsessual yaroqlilik (6-8-mezonlar). Har bir mezonning mazmuni va ekspert xulosasida aks etishi lozim bo‘lgan ma’lumotlar 2-jadvalda keltirilgan.

2-jadval

Deepfakeni aniqlash usuli ishonchliligini baholash mezonlari

Mezon	Tekshiriladigan savol	Ekspert xulosasida ko‘rsatiladi
A1. Tashqi validlik	Usul laboratoriya to‘plamidan tashqari real tarqalgan materiallarda va o‘rgatishda qatnashmagan generatorlar mahsulotida sinalganmi?	Sinov to‘plamining nomi, tarkibi va uning real sharoitga mosligi

Mezon	Tekshiriladigan savol	Ekspert xulosasida ko‘rsatiladi
A2. Xato ko‘rsatkichlarining ochiqligi	Yolg‘on ijobiy va yolg‘on salbiy natijalar ulushi miqdoriy jihatdan ma’lummi?	Har ikki xato turi alohida, qaysi to‘plamda olingani bilan
A3. Mustaqil tekshiruv	Usul taqriz qilingan nashrda bayon etilganmi, natijalari mustaqil tadqiqotchilar tomonidan tasdiqlanganmi?	Nashr va mustaqil sinov manbalari
B4. Qayta ishlashga chidamlilik	Siqish, o‘lchamni o‘zgartirish, barqarorlashtirish va platformaga yuklashdan keyin natija saqlanadimi?	Materialning qayta ishlanganlik darajasi va usulning shu holatdagi ishonchliligi
B5. Qasddan qarshi harakatga chidamlilik	Usulni ataylab chalg‘itish yoki izni boshqa faylga ko‘chirish mumkinmi, bunga qarshi tekshiruv o‘tkazilganmi?	Ma’lum hujum turlari va ularni istisno qilish choralari
C6. Dalil yaxlitligi	Faylning hash qiymati, olingan vaqti va saqlash zanjiri hujjatlashtirilganmi, tahlil davomida fayl o‘zgarmaganmi?	Tahlildan oldingi va keyingi hash qiymatlari, saqlash zanjiri
C7. Takrorlanuvchanlik	Usul yozma protokol bo‘yicha qo‘llanganmi, boshqa ekspert natijani takrorlay oladimi?	Protokol, dastur versiyasi va sozlamalari
C8. Izohlanuvchanlik	Ekspert natijani va usul mantig‘ini sudga tushunarli tilda ochib bera oladimi?	Xulosaga olib kelgan belgilar va ularning talqini

Mezonlar bir-birini takrorlamasligi uchun ularning chegaralari aniq belgilangan. A1 sinov ma’lumotlarining real sharoitga mosligini, A3 esa sinovni kim o‘tkazganini baholaydi: usulni ishlab chiqqan jamoaning o‘zi o‘tkazgan sinov bu talabni to‘liq qondirmaydi. A2 mezonida ikki xato turi alohida ko‘rsatilishi shart, chunki ularning oqibati turlicha: yolg‘on salbiy natija soxta materialni haqiqiy deb qabul qilishga, yolg‘on ijobiy natija esa haqiqiy dalilni rad etishga olib keladi va “yolg‘onchi dividend”ni kuchaytiradi. Shuning uchun umumiy aniqlik ko‘rsatkichi bilan cheklanib bo‘lmaydi.

B4 fayl hayotiy siklida o‘z-o‘zidan yuzaga keladigan o‘zgarishlarni (siqish, uzatish, platformaga yuklash), B5 esa aldash maqsadida ataylab kiritilgan o‘zgarishlarni qamrab oladi. C6 dalil faylining holatiga, C7 usulni qo‘llash tartibiga tegishli. C8 ekspertdan natijani “dastur shunday ko‘rsatdi” deb emas, uning mantig‘ini ochib bergan holda taqdim etishni talab qiladi. Ekspert malakasi, hisoblash resurslari va xarajatlar usulning xossasi emas, balki ekspertizani o‘tkazish shartlari bo‘lgani uchun tizimga kiritilmagan.

Har bir mezon bo‘yicha usul uch holatdan biriga kiritiladi: “bajarilgan”, “qisman bajarilgan” yoki “bajarilmagan (ma’lumot yo‘q)”. Mezonlar orasida A1, A2, C6 va C8 asosiy hisoblanadi: ularsiz natijaning qanday ma’lumotga tayangani, qanchalik xato qilishi, qaysi fayl tahlil qilingani va nimaga asoslangani noma’lum qoladi. Shunga ko‘ra ekspert xulosasi uch darajadan biriga ajratiladi:

– asoslangan - sakkiz mezonning barchasi bajarilgan va natija ikkinchi mustaqil usul bilan tasdiqlangan.

– shartli - asosiy mezonlar (A1, A2, C6, C8) bajarilgan, ammo qolgan mezonlardan (A3, B4, B5, C7) biri yoki bir nechtasi qisman bajarilgan yoki tekshirilmagan, yoxud natija faqat bitta usulga tayanadi.

– yetarli emas - asosiy mezonlardan kamida bittasi bajarilmagan. Bunday natija yakka holda dalil asosi bo‘la olmaydi.

O‘tkazilgan tahlil quyidagi xulosalarga kelish imkonini beradi. Birinchidan, deepfakeni aniqlashda birorta usul yagona yechim bo‘la olmaydi: real sharoitda detektorlarning AUC ko‘rsatkichi 45-50 % ga pasayadi va kriminalist-tahlilchi aniqligiga yetmaydi; PRNU va metama’lumot tahlili asl, qayta ishlanmagan faylni talab qiladi; C2PA faqat belgilangan kontentda ishlaydi va mazmun haqiqiyligini kafolatlamaydi. Ikkinchidan, sud amaliyoti shakllanish bosqichida: AQShda deepfakega oid maxsus norma qabul qilinmagan, 707-qoida loyihasi qo‘shimcha o‘rganilmoqda, O‘zbekistonda esa bunday material umumiy qoidalar asosida baholanadi.

Shu asosda quyidagilar taklif etiladi:

– sintetik mediani tekshirish bo‘yicha ekspertiza metodikasini ishlab chiqish va uni JPKning 22-bobi normalari bilan bog‘lash;

– ekspert xulosasida kamida ikki mustaqil usul natijasini, usulning xato ko‘rsatkichlari va sinov ma’lumotlarini aks ettirish, usulni taklif etilgan sakkiz mezon bo‘yicha baholab, ishonchlilik darajasini ko‘rsatish;

– raqamli dalilni olish va saqlashda ISO/IEC 27037 tamoyillari va hash qiymati orqali yaxlitlikni tasdiqlashni yagona tartib sifatida joriy etish;

– tergov harakatlarini qayd etuvchi rasmiy vositalarda kelib chiqishni tasdiqlash texnologiyalarini sinovdan o‘tkazish;

Foydalanilgan adabiyotlar

1. Mirsky Y., Lee W. The Creation and Detection of Deepfakes: A Survey // ACM Computing Surveys. - 2021.

2. Europol. Facing Reality? Law Enforcement and the Challenge of Deepfakes. - Luxembourg: Publications Office of the European Union, 2022.

3. Chesney R., Citron D. K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. 2019.

4. O‘zbekiston Respublikasining 2026-yil 21-yanvardagi O‘RQ-1115-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi.

5. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi. 1994-yil 22-sentabr // Qonunchilik ma’lumotlari milliy bazasi.

6. Zhang B., Cui H., Nguyen V., Whitty M. Audio Deepfake Detection: What Has Been Achieved and What Lies Ahead // Sensors. – 2025.

7. Lukáš J., Fridrich J., Goljan M. Detecting Digital Image Forgeries Using Sensor Pattern Noise // Proceedings of SPIE. 2006.

8. Goljan M., Chen M., Fridrich J. Sensor Noise Camera Identification: Countering Counter-Forensics // Proceedings of SPIE. 2010.

9. Sencar H. T., Verdoliva L., Memon N. (eds.). Multimedia Forensics. – Singapore: Springer, 2022.

10. Chandra N. A., Lee H., Murtfeldt R. et al. Deepfake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes Circulated in 2024.

11. Yi J., Wang C., Tao J. et al. Audio Deepfake Detection: A Survey. 2023.

12. C2PA. Content Credentials: C2PA Technical Specification. Version 2.2.

13. NIST AI 100-4. Reducing Risks Posed by Synthetic Content. Gaithersburg: NIST, 2024.

14. Federal Rules of Evidence. Rule 702. Testimony by Expert Witnesses (2023-yil tahriri).

KIBERXAVFSIZLIK VA VIDEOMONITORING TIZIMLARIDA OB'YEKTLARNI INTELLEKTUAL ANIQLASHNING ZAMONAVIY MODELLARI (YOLOv8 VA YOLOv12) TAHLILI

Xayinov R.Sh., Sheraliyev M.Sh.
Kriptologiya, axborot xavfsizligi va innovatsion texnologiyalari instituti

Annotatsiya. Maqolada kiberxavfsizlik, axborot xavfsizligi auditi hamda muhim infratuzilmalarning jismoniy perimetrini himoyalashga mo'ljallangan intellektual videomonitoring tizimlarida ob'yektlarni aniqlashning zamonaviy chuqur o'qitish modellarining arxitekturalari va ularning matematik asoslari tahlil qilinadi. Klassik algoritmlar (Canny, Haar, HOG) hamda bir bosqichli konvolyutsion neyron tarmoqlari (*YOLOv8 va YOLOv12*) ning hisoblash murakkabligi, aniqligi va tezkorligi solishtiriladi. Yangi avlod YOLOv12 modelida taklif etilgan Area Attention (A2) moduli, R-ELAN agregatsiyasi, ko'p komponentli yo'qotish (loss) funksiyalari hamda NMS mexanizmining afzalliklari asoslanadi. Resurslari cheklangan chekka (edge) qurilmalarda tezkorlik (FPS) va aniqlik (mAP) muvozanatini ta'minlash bo'yicha ilmiy xulosalar shakllantirilgan.

Kalit so'zlar: kiberxavfsizlik, videomonitoring, ob'yektlarni aniqlash, YOLOv8, YOLOv12, Area Attention, R-ELAN, yo'qotish funksiyasi, IoU (*Intersection over Union*), kompyuter ko'rish.

Аннотация. В статье рассматриваются вопросы интеллектуального обнаружения объектов в системах видеомониторинга, кибербезопасности и защиты физического периметра критических информационных инфраструктур. Сопоставлена эффективность классических методов компьютерного зрения (Canny, каскады Хаара, HOG) и передовых детекторов реального времени (YOLOv8 и YOLOv12). Рассмотрены математические основы инновационного механизма Area Attention (A2), агрегации признаков R-ELAN, многокомпонентных функций потерь и алгоритма NMS. Обоснованы пути обеспечения оптимального баланса между скоростью обработки (FPS), задержкой (latency) и точностью (mAP) на ресурсно-ограниченных периферийных устройствах.

Ключевые слова: кибербезопасность, видеомониторинг, обнаружение объектов, YOLOv8, YOLOv12, Area Attention, R-ELAN, функция потерь, IoU(*Intersection over Union*), компьютерное зрение.

Kirish

Axborot xavfsizligi va kiberxavfsizlikni ta'minlash vazifasi bugungi kunda nafaqat tarmoq protokollari va dasturiy ta'minotlarni virtual hujumlardan himoyalash, balki muhim axborot infratuzilmalari (MAI), ma'lumotlarni qayta ishlash markazlari (MQIM) hamda strategik ob'yektlarning jismoniy perimetrini muhofaza qilishni ham qamrab oladi [5]. Tahlillar shuni ko'rsatadiki, axborot resurslariga yetkaziladigan jiddiy zararlarning salmoqli qismi aynan server xonalari va cheklangan zonalarga bevosita noqonuniy jismoniy kirish (unauthorized physical intrusion), apparat vositalariga begona tashuvchilarni ulash yoki tarmoq kabellariga apparat darajasida suqilib kirish oqibatida sodir bo'ladi. Shu bois, kiberxavfsizlik arxitekturasida intellektual videomonitoring va raqamli kriminalistika tizimlari birinchi darajali mudofaa chizig'i sifatida muhim o'rin tutadi [6].

Kuzatuv hududlaridagi o‘nlab videokameralar oqimini inson-operator tomonidan uzluksiz kuzatib borishi charchoq va e’tibor susayishi sababli talabga javob bermaydi. Shubhali shaxslar, transport vositalari, perimetr buzilishi yoki qoldirilgan buyumlarni soniyaning ulushlarida aniqlash uchun kompyuter ko‘rish (*Computer Vision*) va chuqur o‘qitish (*Deep Learning*) texnologiyalariga asoslangan ob’yektlarni avtomatlashtirilgan aniqlash (*object detection*) modellarini joriy etish lozim. Ushbu modellar kiberxavfsizlik monitoringida video oqimni kechikishsiz (*real-time, kamida 30-60 FPS*) qayta ishlashi, murakkab yorug‘lik va qisman to‘silish (*occlusion*) sharoitlarida yuqori aniqlikni (mAP) ta’minlashi hamda resurslari cheklangan chekka (*edge*) qurilmalarda barqaror ishlashi talab etiladi [6]. Mazkur ishning maqsadi - ob’yektlarni aniqlashning klassik algoritmlari hamda zamonaviy chuqur neyron tarmoqlari (*YOLOv8 va YOLOv12*) arxitekturalarini qiyosiy tahlil qilish, ularning matematik modellashtirish asoslarini o‘rganish va kiberxavfsizlik monitoring tizimlarida qo‘llash istiqbollarini ilmiy asoslashdan iborat.

Asosiy qism

Kompyuter ko‘rish sohasida ob’yektlarni aniqlash tasvir yoki video kadrda ob’yektlarning chegaralovchi to‘rtburchak qutilarini (*bounding box*) fazoviy koordinatalarda topish (*lokalizatsiya*) hamda ularning sinfini ishonchlilik ehtimoli bilan belgilash (*klassifikatsiya*) jarayonlaridan iborat. Kiberxavfsizlik tizimlari talablari nuqtai nazaridan ushbu yo‘nalishdagi asosiy usullarni ko‘rib chiqamiz.

Kiberxavfsizlik monitoringida an’anaviy tasvir tahlili usullari. Neyron tarmoqlari keng qo‘llanilishidan oldin past darajadagi piksel xususiyatlariga tayanuvchi algoritmlar ishlatilgan:

1) Canny qirralar detektori shovqinni Gaussian filtri $G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$ orqali bostirib, Sobel operatori yordamida gradient amplitudasi $G = \sqrt{{G_x}^2 + {G_y}^2}$ va yo‘nalishini $\theta = \text{atan2}(G_y, G_x)$ hisoblaydi, so‘ng Non-Maximum Suppression va gisterezis chegaralash bilan qirralarni ajratadi. Biroq u semantik toifalarni ajrata olmaydi. Bu yerda $G(x,y)$ - filtrning koordinatadagi vazni, x,y - filtr markaziga nisbatan koordinatalar, π - 3,14159 matematik konstantasi, σ - standart og‘ish, silliqlash darajasini boshqaradi, e - Eyler soni, taxminan 2,71828, $x^2 + y^2$ - markazgacha masofaning kvadrati, G_x – gorizontal gradient, G_y – vertikal gradient [7].

2) Har kaskadlari yuzlarni aniqlashda Integral tasvir $II(x,y) = \sum_{x\prime \le x, y\prime \le y} I(x', y')$ yordamida $O(1)$ hisoblash tezligiga erishadi va AdaBoost bilan kaskadlangan zaif klassifikatorlarni birlashtiradi. Ammo burchak o‘zgarishi va yorug‘lik yetishmasligiga o‘ta ta’sirchan [8].

3) HOG (*Histogram of Oriented Gradients*) deskriptori gradientlar yo‘nalishi gistogrammasini normallab, SVM klassifikatori bilan inson siluetlarini aniqlaydi [9], lekin murakkab fonlarda xatoligi ortadi. Ushbu cheklovlar xavfsizlik monitoringida chuqur neyron tarmoqlariga o‘tishni taqozo etdi.

YOLOv8 model arxitekturasi. Ikki bosqichli tarmoqlar (*Faster R-CNN*) yuqori aniqlik bergani bilan, 5-15 FPS tezlik sababli real vaqt xavfsizlik tizimlarida kechikish tug‘diradi. Bir bosqichli YOLO (*You Only Look Once*) modeli esa kadrni bitta neyron tarmoq orqali regressiya qilib, bir vaqtning o‘zida koordinatalar va sinflarni aniqlaydi. YOLOv8 arxitekturasi quyidagi uch qismdan iborat [2]: Backbone qismida C2f (*Cross Stage Partial with 2 convolutions*) modullari qo‘llanilib, gradientlarning qatlamlararo erkin oqishini va hisoblash yengilligini ta’minlaydi, SPPF (*Spatial Pyramid Pooling Fast*) esa ko‘p masshtabli kontekstni jamlaydi; Neck qismida PAN-FPN

tuzilmasi fazoviy va semantik belgilarni birlashtiradi; Head qismida langarsiz (*Anchor-free*) mexanizm qo‘llanilib, oldindan belgilangan sun’iy qutilarga bog‘liqlik bartaraf etilgan va kichik ob’yektlar aniqligi oshirilgan [3].

YOLOv12 model arxitekturasi: Area Attention va R-ELAN innovatsiyalari. 2025-yilda ishlab chiqilgan YOLOv12 modeli e’tibor (*Attention*) mexanizmining $O(N^2)$ kvadratik murakkabligini hal etib, uni ilk bor real vaqt detektorlariga to‘liq joriy qildi [1]. Birinchidan, Area Attention (A2) moduli xususiyatlar xaritasini gorizontal va vertikal sohalarga (areas) bo‘lib, lokal e’tiborni global agregatsiya bilan birlashtiradi. Bu hisoblash xarajatini 4 barobar kamaytiradi va fon bilan aralashgan ob’yektlarni aniq ajratadi. Ikkinchidan, R-ELAN (Residual Efficient Layer Aggregation Networks) arxitekturasi chuqur qatlamlarda gradient barqarorligini ta’minlash uchun residual ulanishni qo‘llaydi. Uning matematik modeli quyidagicha ifodalanadi:

$$Y = X + \alpha F(X) \quad (1)$$

Bu yerda: X - kirish tensori; F(X) - oraliq konvolyutsiya va Area Attention qatlamlaridan o‘tgan tensor; α – masshtab koeffitsiyenti ($\alpha \ll 1$); Y - chiqish tensori. Shuningdek, apparat darajasida Conv2d va BatchNorm optimallashtirishlari orqali TensorRT platformasida yuqori tezlik kafolatlangan [1].

1-jadval

YOLOv8 va YOLOv12 modellarining qiyosiy texnik ko‘rsatkichlari

Model varianti	Masshtab	FLOPs (G)	Parametr (M)	AP50:95 (%)	AP50 (%)	Kechikish (T4, ms)
YOLOv8-N	Nano	8.7	3.2	37.4	52.6	1.77
YOLOv12-N	Nano	6.5	2.6	40.6	56.7	1.64
YOLOv8-S	Small	28.6	11.2	45.0	61.8	2.33
YOLOv12-S	Small	21.4	9.3	48.0	65.0	2.12
YOLOv8-M	Medium	78.9	25.9	50.2	67.2	4.90
YOLOv12-M	Medium	67.5	20.2	52.5	69.6	4.35
YOLOv8-L	Large	165.2	43.7	52.9	69.8	7.84
YOLOv12-L	Large	139.0	26.4	53.7	70.9	6.92

1-jadvaldan ko‘rinib turibdiki, YOLOv12 modeli barcha masshtablarda YOLOv8 ga nisbatan mAP aniqligini 1.2–3.2% ga oshirgan holda, parametrlar sonini 18–40% ga, FLOPs hisoblash yukini 20–25% ga qisqartirgan. Ayniqsa, chekka qurilmalarga mo‘ljallangan YOLOv12-N varianti atigi 2.6M parametr va 6.5G FLOPs bilan 40.6% aniqlik va 1.64 ms kechikish (600+ FPS) ko‘rsatib, real vaqt xavfsizlik auditi uchun eng optimal samaradorlikni namoyon etmoqda.

Ob’yektlarni aniqlashning matematik modellashtirish asoslari. Zamonaviy modellarning o‘qitilishi va ishlashi quyidagi matematik formulalarga tayanadi: Bo‘yin qismida ko‘p masshtabli xususiyatlar xaritalari $F_{fused} = \mathrm{Concat}(\mathrm{Conv}(P_i), \mathrm{Upsample}(P_{i+1}))$ qoidasi asosida birlashtiriladi. Neyron tarmoqni o‘qitishda umumiy yo‘qotish (loss) funksiyasi ko‘p maqsadli kompleks ko‘rinishga ega:

$$L_{total} = \lambda_{box} L_{box} + \lambda_{cls} L_{cls} + \lambda_{dfl} L_{dfl} \quad (2)$$

Bu yerda L_{box} - chegaralovchi quti xatoligi bo‘lib, Complete IoU (CIoU) metrikasi orqali hisoblanadi: $L_{CIoU} = 1 - IoU + \frac{\rho^2(b,b_{gt})}{c^2} + \alpha v$ (bunda $\rho -$ markazlar orasidagi Evklid masofasi, c - qutilarni o‘rab oluvchi diagonal uzunligi, v - tomonlar nisbati o‘xshashligi parametri); L_{cls} - sinfni tasniflashdagi Binary Cross-Entropy yo‘qotishi; L_{dfl} - Distribution Focal Loss bo‘lib, chegaralar koordinatalarining noaniqligini modellashtiradi; $\lambda_{box}, \lambda_{cls}, \lambda_{dfl}$ - yo‘qotishlarning nisbiy vazn koeffitsiyentlaridir. Natijalarni filtrlashda ortiqcha qutilar Non-Maximum Suppression (NMS) orqali bostiriladi. Bunda ikki qutining o‘zaro mosligi quyidagi IoU koeffitsiyenti orqali aniqlanadi [4]:

$$IoU(B_p, B_g) = \frac{|B_p \cap B_g|}{|B_p \cup B_g|} \quad (3)$$

B_p - Predicted Bounding Box: model ob’yektning joylashuvini bashorat qilib chizgan to‘rtburchak.

B_g - Ground Truth Bounding Box: ob’yektning haqiqiy joylashuvini ko‘rsatuvchi, datasetda belgilangan etalon to‘rtburchak.

Kiberxavfsizlik va monitoring tizimlarida samaradorlikni baholash mezonlari. Tizim ishonchliligi quyidagi ko‘rsatkichlar bilan baholanadi:

1) $\text{Precision} = \frac{TP}{(TP + FP)}$ - noto‘g‘ri soxta ogohlantirishlar (false alarm) chastotasini kamaytirish mezonidir;

2) $\text{Recall} = \frac{TP}{(TP + FN)}$ - kadrda mavjud ob’yektlarning qanchasi topilganini bildiradi. Xavfsizlik tizimlarida buzg‘unchini o‘tkazib yubormaslik uchun Recall maksimal bo‘lishi talab etiladi;

3) $F_1 = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$ - balanslashgan sifat ko‘rsatkichi;

4) mAP (mean Average Precision) - barcha sinflar bo‘yicha o‘rtacha aniqlik;

5) FPS (Frames Per Second) va Latency - real vaqt monitoringini ta’minlash uchun kamida 30 FPS talab etiladi. Shuningdek, neyron tarmoqlariga qarshi uyushtiriladigan kiberhujumlar (*adversarial patches, shovqin kiritish*) sharoitida YOLOv12 ning Area Attention mexanizmi global kontekst tahlili evaziga yuqori bardoshlilik namoyon etadi.

Xulosa

Olib borilgan tadqiqotlar shuni ko‘rsatadiki, muhim axborot infratuzilmalari va server xonalarining jismoniy perimetrini kiber-himoyalashda zamonaviy ob’yektlarni aniqlash modellari hal qiluvchi ahamiyat kasb etadi. An’anaviy usullar (Canny, Haar, HOG) real sharoitdagi shovqinlar va yorug‘lik o‘zgarishlariga bardosh bera olmaydi. YOLO arxitekturasi esa bir bosqichli regressiya orqali real vaqt tezligida yuqori aniqlikni ta’minlaydi. Xususan, 2025-yilgi YOLOv12 modelidagi Area Attention mexanizmi hisoblash xarajatlarini 4 barobar kamaytirib, diqqat modullarini real vaqt tizimlariga muvaffaqiyatli tatbiq etdi. R-ELAN moduli esa gradientlar barqarorligini ta’minlab, parametrlar soni 18–40% ga kamaygan holda aniqlikni 1.2–3.2% ga oshirish imkonini berdi [1].

Kiberxavfsizlik va videomonitoring tizimlarida quyidagi amaliy tavsiyalar ilgari suriladi:

1) Chekka (*edge*) xavfsizlik kameralari uchun YOLOv12-N modelini TensorRT va FP16 kvantlash yordamida optimallashtirish, bu esa 1.6 ms kechikish bilan 600+ FPS tezlik beradi;

2) Markaziy monitoring serverlari uchun murakkab sahnalarni yuqori aniqlikda tahlil qiluvchi YOLOv12-M/L modellaridan foydalanish;

3) O‘zbekiston Respublikasining milliy sharoitlari (*keskin yorug‘lik, chang-qum, noqulay ob-havo*)ga moslashtirilgan milliy datasetni shakllantirish va modellarni transfer learning asosida o‘qitish. Bu tadbirlar milliy kiberxavfsizlik qalqonining jismoniy bo‘g‘inini ishonchli ta’minlashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Tian Y., Ye Q., Doermann D. YOLOv12: Attention-Centric Real-Time Object Detectors. Technical Report, arXiv preprint arXiv:2502.12524, 2025. – 18 p.

2. Terven J., Córdova-Esparza D.-M., Romero-González J.-A. A Comprehensive Review of YOLO Architectures in Computer Vision: From YOLOv1 to YOLOv8 and YOLO-NAS // Machine Learning and Knowledge Extraction. – 2023. – Vol. 5, No. 4. – P. 1680–1716.

3. Yaseen M. What is YOLOv8: An In-Depth Exploration of the Internal Features of the Next-Generation Object Detector. – 2024. – arXiv:2408.15857.

4. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2016. – P. 779–788.

5. NIST Special Publication 800-82 Rev. 3. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology, 2023. – 238 p.

6. RFC 8576. Internet of Things (IoT) Security: State of the Art and Challenges. Internet Engineering Task Force (IETF), 2019.

7. Canny J. A Computational Approach to Edge Detection // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1986. – Vol. PAMI-8, No. 6. – P. 679–698.

8. Viola P., Jones M. Robust Real-Time Face Detection // International Journal of Computer Vision. – 2004. – Vol. 57, No. 2. – P. 137–154.

9. Dalal N., Triggs B. Histograms of Oriented Gradients for Human Detection // IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR). – 2005. – Vol. 1. – P. 886–893.

МЕТОД КЛАССИФИКАЦИИ ЦИФРОВЫХ АУДИОСИГНАЛОВ НА ОСНОВЕ СПЕКТРАЛЬНЫХ И ВЕЙВЛЕТ-ПРИЗНАКОВ ДЛЯ ЗАДАЧ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Шамшиева Б.М.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Annotatsiya: Maqolada raqamli kriminalistikada audioyozuvlarning haqiqiyligini tekshirishda qo‘llash uchun mo‘ljallangan, raqamli audiosignallarni ularga ishlov berish tarixi bo‘yicha tasniflash usuli taklif etilgan. Usul qisqa vaqtli Furye almashtirishi asosidagi spektral va mel-kepstral belgilar hamda Dobeshi db4 diskret veyvlet almashtirishi qism polosalarining statistik belgilaridan birgalikda foydalanishga asoslangan. Beshta sinf ko‘rib chiqilgan: asl yozuv, MP3-siqish, qayta diskretlash, shovqin qo‘shish va montaj. 600 ta yozuvdan iborat modellashtirilgan korpusda o‘tkazilgan tajribalar birlashtirilgan belgilar vektori «tasodifiy o‘rmon» klassifikatori bilan birgalikda 85,0 % aniqlikni ta’minlashini ko‘rsatdi. Bu spektral (82,7 %) va veyvlet-belgilardan (59,0 %) alohida foydalanishdan yuqori natijadir.

Kalit so‘zlar: raqamli kriminalistika, audioekspertiza, audiosignallarni tasniflash, spektral belgilar, MFCC, veyvlet almashtirish, tasodifiy o‘rmon, tayanch vektorlar usuli.

Аннотация: В статье предложен метод классификации цифровых аудиосигналов по истории их обработки, предназначенный для применения в цифровой криминалистике при проверке подлинности аудиозаписей. Метод основан на совместном использовании спектральных признаков, вычисляемых по кратковременному преобразованию Фурье (спектральный центроид, ширина, частота спада, спектральная плоскостность, спектральный поток, мел-кепстральные коэффициенты), и признаков дискретного вейвлет-преобразования (относительная энергия, стандартное отклонение, эксцесс и энтропия коэффициентов в подполосах разложения Добеши db4). Рассмотрены пять классов: исходная запись, MP3-сжатие, передискретизация, добавление шума и монтаж. Экспериментальное исследование на смоделированном корпусе из 600 записей показало, что объединённый вектор признаков в сочетании с классификатором «случайный лес» обеспечивает точность 85,0 %, превосходя раздельное использование спектральных (82,7 %) и вейвлет-признаков (59,0 %).

Ключевые слова: цифровая криминалистика, аудиоэкспертиза, классификация аудиосигналов, спектральные признаки, MFCC, вейвлет-преобразование, случайный лес, метод опорных векторов.

Цифровые аудиозаписи всё чаще используются как доказательства в судебных делах и при расследовании инцидентов информационной безопасности, а доступность аудиоредакторов упростила их фальсификацию (монтаж, повторное кодирование, передискретизация, маскировка шумом). Поэтому ключевой задачей аудиоэкспертизы является установление истории обработки записи [1, 8].

Существующие подходы используют либо внешние артефакты, например критерий частоты электрической сети (ENF) [9], либо статистические свойства самого сигнала: следы кодеков с потерями [7], изменения спектральной огибающей, нарушения стационарности; эффективность последних сильно зависит от признакового описания. Вопросы построения

графа методов классификации сигналов и применения предикатов сходства, в том числе в системах защиты информации, рассмотрены в работах [11–13].

Спектральные признаки и мел-кепстральные коэффициенты (MFCC) хорошо зарекомендовали себя в распознавании речи и классификации аудио [3, 4], а вейвлет-преобразование обеспечивает многомасштабный анализ, чувствительный к изменениям в высокочастотных подполосах [2]. Цель работы - разработать метод классификации, объединяющий оба типа признаков, и оценить его эффективность для типовых операций обработки.

Пусть задана цифровая аудиозапись $x(n)$, $n = 0, \ldots, N - 1$, с частотой дискретизации f_d. Требуется отнести запись к одному из классов $\Omega = \{\omega_1, \ldots, \omega_5\}$, соответствующих истории её обработки (табл. 1). Задача решается как задача обучения с учителем: по обучающей выборке пар (x_i, y_i) строится решающее правило a: $X \to \Omega$, где X - пространство признаков.

Таблица 1

Классы аудиозаписей, рассматриваемые в работе

№	Класс	Описание операции
1	Оригинал	Исходная запись в формате PCM без дополнительной обработки
2	MP3-сжатие	Кодирование MP3 (LAME) со скоростью 64 кбит/с и обратное декодирование
3	Передискретизация	Понижение частоты дискретизации до 8 кГц и обратное повышение до 22,05 кГц
4	Аддитивный шум	Добавление белого гауссова шума с отношением сигнал/шум 25–35 дБ
5	Монтаж	Склейка фрагментов двух различных записей со случайным изменением уровня (0,5–1,5)

Обобщённая схема метода (рис. 1) включает предобработку сигнала, вычисление спектральных и вейвлет-признаков и классификацию по объединённому вектору признаков.

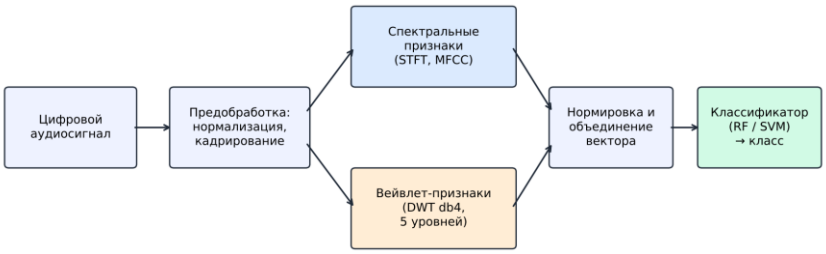


Рис. 1. Обобщённая схема метода классификации аудиосигналов

Сигнал нормируется по максимальной амплитуде и разбивается на кадры длиной $L = 1024$ отсчёта (≈46 мс при f_d = 22,05 кГц) с перекрытием 50 %. К каждому кадру применяется окно Ханна, после чего вычисляется дискретное преобразование Фурье $X_t(k)$, где t - номер кадра, k - номер частотного отсчёта.

Для каждого кадра вычисляются следующие характеристики. Спектральный центроид, характеризующий «центр тяжести» спектра:

$$C_t = \Sigma_k f_k \cdot |X_t(k)| / \Sigma_k |X_t(k)|, \quad (1)$$

где f_k - частота k-го отсчёта. Спектральная ширина:

$$B_t = [\Sigma_k (f_k - C_t)^2 \cdot |X_t(k)| / \Sigma_k |X_t(k)|]^{1/2}. \quad (2)$$

Частота спада R_t определяется как наименьшая частота, ниже которой сосредоточено 85 % энергии спектра. Спектральная плоскостность, позволяющая отличать шумоподобные сигналы от тональных, определяется отношением геометрического и арифметического средних:

$$SF_t = \exp((1/K)\cdot\Sigma_k \ln|X_t(k)|) / ((1/K)\cdot\Sigma_k |X_t(k)|). \quad (3)$$

Спектральный поток характеризует скорость изменения спектра между соседними кадрами:

$$FL_t = [\Sigma_k (|X_t(k)| - |X_{t-1}(k)|)^2]^{1/2}. \quad (4)$$

Дополнительно вычисляются частота переходов через нуль и логарифм доли энергии в полосе выше 7 кГц, чувствительный к низкочастотной фильтрации, свойственной кодекам с потерями и передискретизации. Мел-кепстральные коэффициенты вычисляются по набору из 26 треугольных мел-фильтров $H_m(k)$ с последующим дискретным косинусным преобразованием [4]:

$$c_t(q) = \Sigma_{m=1}^{M} \ln(\Sigma_k |X_t(k)|^2 \cdot H_m(k))\cdot\cos(\pi q(m - 0{,}5)/M), \quad (5)$$

где $q = 0, \ldots, 12$. Для получения признаков уровня записи по каждой кадровой характеристике вычисляются среднее значение и стандартное отклонение по всем кадрам. Итого формируется 40 спектральных признаков (табл. 2).

Сигнал раскладывается с помощью дискретного вейвлет-преобразования (ДВП) с вейвлетом Добеши db4 на $J = 5$ уровней [2]. В результате получаются подполосы детализирующих коэффициентов $D_1, \ldots, D_5$ и подполоса аппроксимирующих коэффициентов A_5. При $f_d = 22{,}05$ кГц подполоса D_1 соответствует диапазону ≈5,5–11 кГц, D_2 - ≈2,8–5,5 кГц и т. д. Для каждой подполосы j с коэффициентами $d_j(n)$ вычисляются:

- относительная логарифмическая энергия

$$e_j = \ln(E_j / \Sigma_i E_i), \; E_j = \Sigma_n d_j^2(n); \quad (6)$$

- стандартное отклонение коэффициентов σ_j;
- коэффициент эксцесса κ_j, характеризующий импульсность (разреженность) коэффициентов;
- энтропия Шеннона нормированной энергии коэффициентов:

$$H_j = -\Sigma_n p_j(n)\cdot\ln p_j(n), \; p_j(n) = d_j^2(n) / E_j. \quad (7)$$

Таким образом, вейвлет-описание записи содержит 6 × 4 = 24 признака. Объединённый вектор признаков имеет размерность 64.

Таблица 2

Состав вектора признаков

Группа	Признаки	Количество
Спектральные (STFT)	Центроид, ширина, частота спада, плоскостность, поток, ЧПН, доля ВЧ-энергии (среднее и СКО)	14
Кепстральные (MFCC)	Коэффициенты c(0)–c(12) (среднее и СКО)	26
Вейвлет (ДВП db4)	e_j, σ_j, κ_j, H_j для D1–D5, A5	24
Итого		64

На рис. 2 видно, что MP3-кодирование срезает спектр выше ≈10 кГц, а передискретизация до 8 кГц удаляет составляющие выше 4 кГц; это отражается на спектральных признаках и энергии подполос D_1 и D_2.

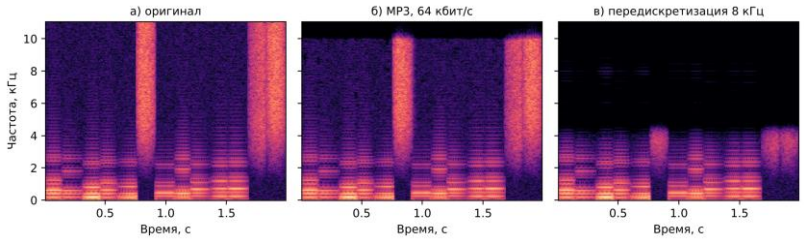


Рис. 2. Спектрограммы фрагмента записи: а) исходная запись; б) после MP3-сжатия; в) после передискретизации

Признаки нормируются по обучающей выборке (нулевое среднее, единичная дисперсия). Рассмотрены классификаторы k-NN (k = 5), случайный лес из 300 деревьев [5] и SVM с радиальной базисной функцией (C = 10) [6]; реализация выполнена на Python (NumPy, SciPy, scikit-learn [10]).

Данные. Сформирован смоделированный корпус речеподобных сигналов длительностью 2 с (22,05 кГц, 16 бит), синтезированных по модели «источник–фильтр». К исходным записям применялись операции из табл. 1 (MP3 - кодеком LAME); корпус содержит 600 записей, по 120 на класс.

Методика. Оценка проводилась стратифицированной 5-кратной перекрёстной проверкой по точности (accuracy) и макроусреднённой F-мере; результаты приведены в табл. 3.

Таблица 3

Точность и F-мера классификации (5-кратная перекрёстная проверка), %

Набор признаков	k-NN Точн.	k-NN F1	Случ. лес Точн.	Случ. лес F1	SVM Точн.	SVM F1
Спектральные (40)	70,5	70,6	82,7	82,5	81,5	81,6
Вейвлет (24)	40,8	40,3	52,2	51,7	59,0	59,4
Комбинированные (64)	68,0	68,0	85,0	84,9	84,2	84,3

Наилучший результат - 85,0 % - получен для объединённого вектора признаков и случайного леса; близкий результат показал SVM (84,2 %). Объединение признаков повысило точность на 2,3 п. п. (случайный лес) и на 2,7 п. п. (SVM) по сравнению со спектральными признаками. Метод k-NN оказался наименее эффективным. Показатели по отдельным классам приведены в табл. 4.

Таблица 4

Показатели качества по классам (комбинированные признаки, случайный лес)

Класс	Точность (precision)	Полнота (recall)	F1-мера
Оригинал	0,628	0,675	0,651
MP3-сжатие	0,928	0,967	0,947
Передискретизация	1,000	1,000	1,000
Аддитивный шум	1,000	1,000	1,000
Монтаж	0,689	0,608	0,646

Классы «Передискретизация» и «Аддитивный шум» распознаются безошибочно: обе операции оставляют глобальные следы в спектре, надёжно фиксируемые долей ВЧ-энергии, спектральной плоскостностью и энергией подполос D_1–D_2. MP3-сжатие распознаётся с F-мерой 0,947.

Основным источником ошибок является различение классов «Оригинал» и «Монтаж» (F-мера 0,651 и 0,646): монтаж - локальная операция, а признаки агрегированы по всей записи. Вейвлет-признаки сами по себе дают точность не более 59,0 %, но в составе объединённого вектора повышают её.

Заключение

Предложен метод классификации цифровых аудиосигналов по истории обработки, объединяющий 40 спектральных и кепстральных признаков с 24 признаками дискретного вейвлет-преобразования. Объединённое описание в сочетании со случайным лесом обеспечивает точность 85,0 % при различении пяти классов. Передискретизация, зашумление и MP3-сжатие выявляются с F-мерой 0,95–1,00, а обнаружение монтажа требует локального анализа признаков в скользящем окне. Дальнейшая работа связана с расширением набора кодеков и проверкой метода на реальных записях.

Список литература

1. Maher R. C. Audio forensic examination // IEEE Signal Processing Magazine. 2009. Vol. 26, No. 2. P. 84–94.

2. Mallat S. A Wavelet Tour of Signal Processing: The Sparse Way. 3rd ed. Burlington: Academic Press, 2009. 832 p.

3. Tzanetakis G., Cook P. Musical genre classification of audio signals // IEEE Transactions on Speech and Audio Processing. 2002. Vol. 10, No. 5. P. 293–302.

4. Davis S., Mermelstein P. Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences // IEEE Transactions on Acoustics, Speech, and Signal Processing. 1980. Vol. 28, No. 4. P. 357–366.

5. Breiman L. Random forests // Machine Learning. 2001. Vol. 45, No. 1. P. 5–32.

6. Cortes C., Vapnik V. Support-vector networks // Machine Learning. 1995. Vol. 20, No. 3. P. 273–297.

7. Yang R., Shi Y. Q., Huang J. Defeating fake-quality MP3 // Proceedings of the 11th ACM Workshop on Multimedia and Security. 2009. P. 117–124.

8. Zakariah M., Khan M. K., Malik H. Digital multimedia audio forensics: past, present and future // Multimedia Tools and Applications. 2018. Vol. 77, No. 1. P. 1009–1040.

9. Grigoras C. Digital audio recording analysis: the Electric Network Frequency (ENF) criterion // International Journal of Speech, Language and the Law. 2005. Vol. 12, No. 1. P. 63–76.

10. Pedregosa F. et al. Scikit-learn: Machine learning in Python // Journal of Machine Learning Research. 2011. Vol. 12. P. 2825–2830.

11. Абдуллаев М.М., Шамшиева Б.М. Граф методов классификации сигналов // Республиканская научно-техническая конференция «Современное состояние и перспективы применения информационных технологий в управлении». 7–8 сентября 2015 г. – Ташкент, 2015. – С. 108–21.

12. Абдуллаев М.М., Шамшиева Б.М., Рахманова Г.Х., Абдуллаева Г.М. Предикаты сходства для классификации сигналов // Международная научная конференция «INNOVATION-2015»: сборник научных статей. 23–24 октября 2015 г. – Ташкент, 2015. – С. 320–321.

13. Абдуллаев М.М., Шамшиева Б.М. Предикаты сходства для классификации сигналов и их применение в системах защиты информации // «Muhammad al-Xorazmiy avlodlari»: ilmiy-amaliy va axborot-tahliliy jurnal. – 2019. – № 2 (8). – С. 38–41.

РАЗРАБОТКА МОДЕЛИ ОБНАРУЖЕНИЯ ПОДДЕЛЬНЫХ ИЗОБРАЖЕНИЙ И ВИДЕОМАТЕРИАЛОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Юлдашева Н.С., Салимов С.А., Сайжанов И.А.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Annotatsiya. Ushbu ishda sun’iy ravishda o‘zgartirilgan tasvirlar va videomateriallarni aniqlash uchun modulli dasturiy tizim ishlab chiqish masalasi ko‘rib chiqiladi. Videodan kadrlarni ajratib olish, YuNet neyron tarmog‘i yordamida yuzlarni aniqlash va tasvir sohalarini keyingi ikkilik tasniflash uchun tayyorlash bosqichlari tavsiflanadi. Python va OpenCV asosidagi dastlabki ishlov berish modullari sinovi natijalari keltiriladi. Shuningdek, PyTorch asosida tasniflagich sifatini baholash rejasi bayon etiladi. Yuzning aniqlanishi tasvir haqiqiy yoki soxta ekanini isbotlamasligi alohida ta’kidlanadi.

Kalit so‘zlar: sun’iy intellekt; Deepfake; chuqur o‘rganish; soxtalikni aniqlash; kompyuter ko‘rishi; YuNet; video tahlili.

Аннотация. В работе рассматривается разработка модульной программной системы для обнаружения искусственно модифицированных изображений и видеоматериалов. Представлены этапы получения кадров из видео, локализации лиц нейросетевой моделью YuNet и подготовки областей интереса для последующей бинарной классификации. Описана программная реализация предварительной обработки на Python и OpenCV и план оценки качества классификатора с использованием PyTorch. Приведены результаты испытаний модулей обработки одного изображения и тестового видеоролика. Отмечено, что успешное обнаружение лица не является подтверждением подлинности или подделки контента.

Ключевые слова: искусственный интеллект; Deepfake; глубокое обучение; обнаружение подделок; компьютерное зрение; YuNet; анализ видео.

Введение

Развитие генеративного искусственного интеллекта расширило возможности редактирования и синтеза визуального контента. С помощью соответствующих алгоритмов можно изменять отдельные участки изображения, заменять лица и формировать видеоряд, внешне похожий на реальную запись. Подобные средства имеют законные творческие применения, однако могут использоваться для распространения недостоверной информации и имитации действий человека. Поэтому задача определения происхождения и возможной модификации медиаматериалов представляет интерес для кибербезопасности.

Современные исследования рассматривают обнаружение Deepfake как задачу анализа статистических и визуальных особенностей изображений. Бенчмарк FaceForensics++ содержит примеры различных способов манипулирования лицами, а набор DFDC применяется для оценки алгоритмов на видеоконтенте [1, 2]. При этом качество модели зависит не только от архитектуры классификатора, но и от подготовки исходных данных, состава обучающей выборки и условий тестирования. На практике видеоматериалы часто различаются разрешением, степенью сжатия и освещением, что усложняет перенос результатов между наборами данных [5].

Цель и постановка задачи

Цель исследования - разработать основу автоматизированной системы, которая принимает изображения и видеозаписи и подготавливает их к определению принадлежности к классам Real («подлинное») и Fake («поддельное»). Работа организована как последовательность независимых модулей, чтобы можно было отдельно проверять качество извлечения кадров, обнаружения лиц и дальнейшей классификации.

На рассматриваемом этапе поставлены следующие задачи: реализовать считывание изображений и видео; исследовать алгоритм равномерного отбора кадров; локализовать лица нейросетевой моделью; сохранить подготовленные области; сформулировать схему обучения и объективной проверки классификатора. Программная демонстрация не должна выдавать вероятность подделки на основании одной лишь уверенности детектора лиц, поскольку эти показатели описывают разные задачи.

Архитектура разрабатываемой системы

Общая схема обработки предусматривает последовательность «входной файл → проверка формата → предварительная обработка → обнаружение лица → выделение области интереса → классификация → представление результата». Для изображения обработка выполняется непосредственно над отдельным кадром. Для видеозаписи сначала формируется выборка кадров, после чего каждый кадр обрабатывается тем же модулем локализации лиц. Подобный подход позволяет повторно использовать программные компоненты и снижает сложность сопровождения кода.

Основные средства реализации - Python, OpenCV и PyTorch. OpenCV применяется для декодирования видео, работы с изображениями и запуска модели обнаружения лиц. В качестве такого детектора используется YuNet - компактная нейросетевая архитектура, предназначенная для поиска областей лица [3]. PyTorch рассматривается как среда реализации последующей модели глубокого обучения, поскольку поддерживает обучение и выполнение нейронных сетей на графических ускорителях [4].

Система разделяет две разные величины: уверенность YuNet в том, что на изображении найдено лицо, и предполагаемую оценку класса Real/Fake, которую должен выдавать отдельный обученный классификатор. Смешение этих значений ведёт к методологически неверным выводам. Если на кадре несколько лиц, для каждого необходимо сохранить отдельную область и связать её с исходным кадром; если лиц не найдено, результат обработки следует обозначать как отсутствие пригодной области, а не как «подлинное видео».

Для изображения лица подготовка может включать изменение размера до входных размеров классификатора, преобразование цветовых каналов и нормализацию значений пикселей. Параметры преобразований важно одинаково применять при обучении и при проверке. Сведения об исходном файле и перечень сформированных кадров необходимо хранить отдельно от прогнозов, чтобы впоследствии можно было воспроизвести ход исследования.

Экспериментальная проверка модулей

Первоначальная проверка проводилась на рабочем прототипе, созданном в среде Python. Для одиночного тестового изображения размером 1050 × 1350 пикселей алгоритм обнаружения лиц выделил одну область с показателем уверенности около 0,897. Этот показатель отражает ответ детектора лица и не характеризует вероятность искусственной модификации изображения.

Следующий эксперимент выполнен на видеозаписи размером 720 × 1280 пикселей с частотой приблизительно 29,98 кадра/с. Продолжительность записи составляла около 19,25 с, общее число кадров - 577. Из видеоматериала было равномерно отобрано 20 кадров. При запуске YuNet области лиц обнаружены на всех 20 кадрах; значения уверенности обнаружения в полученных результатах находились приблизительно в диапазоне 0,79–0,90. Изображения выделенных областей сохранены для дальнейшего анализа.

Таким образом, эксперимент подтвердил работоспособность двух модулей: отбора кадров из видеозаписи и выделения лиц из подготовленных изображений. Он не предназначался для измерения точности обнаружения Deepfake. На основании одного тестового видео нельзя оценить чувствительность метода к различным типам подделок или устойчивость к изменению условий съёмки.

План оценки модели классификации

На следующем этапе требуется сформировать размеченные обучающую, валидационную и тестовую выборки. В качестве исходных источников могут рассматриваться FaceForensics++ и DFDC [1, 2]; использование каждого набора должно учитывать условия доступа и разрешённые цели применения. Во избежание утечки данных кадры одного исходного видео нельзя независимо распределять между обучением и тестированием: разделение следует проводить на уровне видеозаписей, а по возможности также с контролем совпадающих лиц и исходных сцен.

Для оценки классификатора целесообразно рассчитать Accuracy, Precision, Recall и F1-score по классу Fake, а также изучить матрицу ошибок. Для видео необходимо заранее зафиксировать правило объединения прогнозов отдельных кадров, например медианное значение вероятностей, и проверить его на отложенных видеозаписях. Дополнительное тестирование на другом наборе данных позволит оценить способность модели работать вне условий, на которых она обучалась.

Перспективными направлениями являются сравнение нескольких архитектур классификации, изучение влияния уровня видеосжатия и проведение анализа случаев ошибочного срабатывания. Однако количественные результаты таких экспериментов могут приводиться в публикации только после фактического выполнения измерений.

Дополнительным элементом проектируемой архитектуры является контроль качества входных данных. Прежде чем направить изображение в классификатор, система должна проверять, удалось ли декодировать файл, имеет ли кадр допустимые размеры и существует ли подходящая область интереса. Для видеоматериалов желательно фиксировать число реально обработанных кадров и число кадров, на которых детектор обнаружил лицо. Это позволит отделить ошибку чтения файла от ситуации, когда человек в кадре отсутствует, и от ошибки самого детектора. Результат анализа без пригодного изображения лица следует представлять как «недостаточно данных», а не относить автоматически к одному из двух целевых классов.

Особое значение имеет согласованность анализа отдельных изображений и целой видеозаписи. В одном видео качество освещения и положение головы изменяются во времени, поэтому прогноз по одному кадру не обязательно отражает свойства всего ролика. При объединении покадровых оценок нужно учитывать количество пригодных кадров, наличие нескольких людей и возможные выбросы. До экспериментальной проверки нельзя считать усреднение вероятностей универсальным решением: оно может скрывать кратковременные признаки подделки. При сравнении вариантов объединения следует

использовать одинаковый набор тестовых видео и предварительно зафиксированные критерии оценки.

Отдельной исследовательской задачей является оценка вычислительной доступности системы. Модульная реализация позволяет запускать предварительную обработку отдельно от классификации и при необходимости изменять число анализируемых кадров в зависимости от ресурсов устройства. Однако сокращение выборки ускоряет работу ценой возможной потери информативных фрагментов. Поэтому в дальнейшем рекомендуется экспериментально изучить соотношение количества кадров, времени обработки и качества определения классов Real/Fake. Такую проверку следует проводить при одинаковых условиях и фиксировать используемое оборудование, версии библиотек и параметры модели.

Заключение

В работе представлена модульная архитектура системы анализа изображений и видеоматериалов, ориентированная на последующее обнаружение Deepfake. Реализованы и испытаны компоненты декодирования видео, отбора кадров и нейросетевого обнаружения лиц. В рамках проведённой предварительной проверки лица выделены на всех 20 кадрах одного тестового видеоролика.

Практическим результатом является работоспособный этап подготовки визуальных данных для дальнейшего обучения и проверки классификатора. Научно обоснованная оценка обнаружения поддельного контента остаётся следующим этапом исследования и требует разметки, независимого тестирования и представления количественных метрик. Такой подход позволяет не смешивать успешность предварительной обработки с реальной точностью определения подлинности медиаконтента.

Список использованной литературы

1. Rössler A., Cozzolino D., Verdoliva L., Riess C., Thies J., Nießner M. FaceForensics++: Learning to Detect Manipulated Facial Images // Proceedings of ICCV. - 2019. - P. 1–11. - DOI: 10.1109/ICCV.2019.00009.

2. Dolhansky B., Bitton J., Pflaum B. et al. The DeepFake Detection Challenge (DFDC) Dataset. - 2020. - arXiv:2006.07397.

3. Wu W., Peng H., Yu S. YuNet: A Tiny Millisecond-level Face Detector // Machine Intelligence Research. - 2023. - Vol. 20. - P. 656–665. - DOI: 10.1007/s11633-023-1423-y.

4. Paszke A., Gross S., Massa F. et al. PyTorch: An Imperative Style, High-Performance Deep Learning Library // Advances in Neural Information Processing Systems. - 2019. - Vol. 32. - P. 8026–8037.

5. Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J. Deepfakes and beyond: A Survey of face manipulation and fake detection // Information Fusion. - 2020. - Vol. 64. - P. 131–148. - DOI: 10.1016/j.inffus.2020.06.014.

ПРИМЕНЕНИЕ МЕТОДОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ВЫЯВЛЕНИЯ ПРИЗНАКОВ DEEPFAKE В ВИДЕОМАТЕРИАЛАХ

Юлдашева Н.С., Салимов С.А., Сайжанов И.А.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Annotatsiya. Ishda sun’iy ravishda o‘zgartirilgan yuz tasvirlari bo‘lishi mumkin bo‘lgan videomateriallarni dastlabki raqamli kriminalistik tekshirish yondashuvi ko‘rib chiqiladi. Manba videoni hujjatlashtirish, texnik xususiyatlarini aniqlash, kadrlarni ajratib olish va YuNet modeli orqali yuzlarni topish ketma-ketligi taklif etiladi. Sinov videosi asosida dasturiy modullarning ishlash natijalari bayon qilinadi. Asl ma’lumotlarni saqlash, amallarni takrorlash imkoniyati hamda neyron tarmoq baholarini talqin qilish chegaralariga e’tibor qaratiladi. Yuz sohasining ajratilishi Deepfake mavjudligiga mustaqil dalil bo‘la olmasligi ta’kidlanadi.

Kalit so‘zlar: raqamli kriminalistika; Deepfake; video dalillar; kadrlarni ajratish; YuNet; yaxlitlikni tekshirish; video tahlili.

Аннотация. Рассматривается подход к предварительному криминалистическому исследованию видеоматериалов, потенциально содержащих искусственно модифицированные изображения лиц. Предлагается последовательность документирования исходного видео, определения технических характеристик, отбора кадров и локализации лиц с помощью модели YuNet. На примере тестовой видеозаписи описаны результаты работы созданных программных модулей. Отдельное внимание уделено сохранению исходных данных, воспроизводимости действий и границам интерпретации нейросетевых оценок. Показано, что выделение областей лица создаёт материал для последующего исследования, но не является самостоятельным доказательством Deepfake.

Ключевые слова: цифровая криминалистика; Deepfake; видеодоказательства; извлечение кадров; YuNet; проверка целостности; анализ видео.

Введение

В цифровой криминалистике видеозаписи рассматриваются как потенциальные источники сведений о событиях и действиях участников. Однако возможности программного редактирования и генеративного искусственного интеллекта усложняют проверку происхождения подобных материалов. Изменённое лицо, синтетически сформированные мимика и речь, а также монтаж отдельных фрагментов могут влиять на интерпретацию записи. По этой причине аналитик должен учитывать не только видимое содержание ролика, но и условия получения файла, его технические свойства и историю обработки.

В обзоре L. Verdoliva систематизированы методы проверки целостности визуальных данных и подчёркнуты ограничения автоматических детекторов [1]. Методические рекомендации SWGDE рассматривают документирование действий, сохранение исходных объектов и воспроизводимость экспертного процесса как существенные составляющие анализа видеодоказательств [2]. Следовательно, применение нейросетевых технологий в криминалистике требует процедур, позволяющих проверить, из каких данных получен каждый результат.

Цель и подход к исследованию

Цель работы - разработать и описать процедуру предварительной обработки видеоматериала для последующего поиска признаков Deepfake, пригодную для включения в более широкий криминалистический процесс. В отличие от задачи построения универсального классификатора подделок, акцент сделан на происхождении файлов, последовательности исследовательских действий и корректной интерпретации промежуточных результатов.

Для достижения цели рассматриваются четыре задачи: регистрация исходных характеристик видеозаписи, формирование контролируемой выборки кадров, автоматическая локализация областей лица и документирование связи между исходным файлом и полученными изображениями. На текущем этапе технически реализованы модули извлечения кадров и обнаружения лиц; расширенные механизмы фиксации целостности предложены в качестве дальнейшего развития методики.

Обеспечение сохранности цифровых материалов

При работе с видеозаписью важно отделять исходные данные от производных изображений. Рекомендуется выполнять анализ на рабочей копии файла, фиксировать название, размер, формат, дату получения и источник поступления, а для контроля неизменности рассчитывать криптографическую контрольную сумму. Перечень обработанных файлов и контрольных значений может формировать основу журнала исследования. Эти действия особенно значимы, когда результаты предполагается использовать не только в исследовательской работе, но и при подготовке экспертных материалов [2].

Извлечённые кадры и обрезанные изображения лиц необходимо считать производными объектами. Их желательно именовать по устойчивой схеме с привязкой к номеру кадра и исходной видеозаписи, а также фиксировать применённые параметры преобразований. Сохранение кадров в формате JPEG вносит дополнительное сжатие; поэтому при изучении тонких следов монтажа предпочтительно сохранять также вариант без потерь или проводить необходимые измерения непосредственно на исходных декодированных кадрах. В описываемом прототипе результаты сохранялись как отдельные изображения; полноценный журнал цепочки обработки ещё требует реализации.

Извлечение кадров и обнаружение лиц

Предварительная обработка начинается с чтения видео при помощи OpenCV. Из контейнера извлекаются такие параметры, как ширина и высота кадра, оценочная частота кадров и их общее количество. Эти сведения позволяют выбрать способ дискретизации видеоряда. В изучаемом прототипе заданное число кадров выбирается равномерно по продолжительности видеозаписи, чтобы охватить разные временные участки записи без необходимости сохранять каждый кадр.

Равномерный отбор уменьшает объём анализируемых данных, однако он не гарантирует попадания кратковременного признака модификации в выборку. Поэтому при дальнейшей криминалистической проверке может потребоваться увеличение частоты выборки или исследование отдельных участков видео по результатам первоначального просмотра. При видеозаписях с переменной частотой кадров предпочтительно опираться на временные метки кадров, а не только на отношение числа кадров к номинальной частоте.

На извлечённых изображениях выполняется поиск лиц с помощью нейросетевой модели YuNet. Эта модель используется для локализации областей лица, а не для принятия

решения о подлинности записи [3]. Для каждого успешного обнаружения сохраняется изображение лица и при необходимости может фиксироваться оценка уверенности детектора. Значение этой оценки не соответствует вероятности Deepfake: нейросеть определяет наличие лица, а не факт его синтеза.

В перспективе подготовленные области лица могут передаваться классификатору признаков модификации. При этом вывод следует рассматривать как автоматизированную оценку, требующую проверки другими методами: сравнением кадров во времени, анализом структуры файла и исследованием условий создания записи. Литература по обнаружению манипуляций демонстрирует как возможности глубокого обучения, так и проблемы переноса моделей на ранее неизвестные способы генерации [4, 5].

Результаты предварительного эксперимента

Для проверки работоспособности модулей использовалась тестовая видеозапись в разрешении 720 × 1280 пикселей. По данным программного считывания длительность записи составляла около 19,25 с, частота кадров - около 29,98 кадра/с, общее количество кадров - 577. Из видеопоследовательности были извлечены 20 кадров, распределённых по всей её продолжительности.

Алгоритм YuNet обнаружил лицо на каждом из 20 подготовленных кадров. Регистрировавшиеся значения уверенности обнаружения находились приблизительно в интервале 0,79–0,90. Полученные области были сохранены в файлах для последующего исследования. Таким образом, опыт подтвердил, что модуль извлечения кадров и последующая локализация лиц могут применяться последовательно в одном программном конвейере.

Важное ограничение опыта состоит в том, что он проведён на одной видеозаписи и не включал эталонного сравнения подлинных и поддельных материалов. Поэтому отношение 20 обнаруженных лиц к 20 обработанным кадрам характеризует только данный этап обработки конкретного файла. Оно не может интерпретироваться как стопроцентная точность распознавания Deepfake, достоверность криминалистического заключения или обобщённое качество YuNet на произвольных видео.

Интерпретация и дальнейшая проверка

Криминалистическая ценность автоматизированного модуля заключается прежде всего в возможности повторяемой подготовки материала и локализации областей для более детального исследования. При этом характеристики видеосжатия, размытие, низкое освещение, поворот головы и частичное перекрытие лица могут вызывать ошибки на любом этапе обработки. Кроме того, признаки, напоминающие артефакты генерации, иногда обусловлены обычными операциями перекодирования и монтажа, не связанными с Deepfake.

Для последующих экспериментов необходимо подготовить набор видео с известным происхождением и подлинностью. В отчёте целесообразно отдельно указывать долю кадров с обнаруженными лицами, время обработки, частоту пропусков и результаты классификации на независимой тестовой выборке. Для подтверждения выводов желательно сохранять логи параметров программы и контрольные суммы исходных файлов. Такой подход позволяет рассматривать нейросетевой вывод как один из исследовательских признаков, но не заменяет комплексную экспертизу.

Для воспроизводимости предлагаемого подхода важно заранее определить состав отчёта об обработке. В нём целесообразно указывать идентификатор исследуемого файла,

программную среду, значения параметров извлечения кадров, количество полученных изображений и номера кадров, где обнаружены лица. При возможном изменении видео в процессе перекодирования следует отдельно отражать, какой именно файл исследовался: исходный или производный. При повторном анализе по тем же данным и с теми же параметрами такие сведения помогут проверить последовательность выполненных действий и сопоставить результаты разных экспериментов.

Необходимо также учитывать, что отсутствие визуального признака модификации не равнозначно установлению подлинности записи. Даже детектор, хорошо работающий на одном наборе данных, может ошибаться на другом типе видеоматериалов. По этой причине предлагаемая процедура относится к предварительному исследованию и подготовке объектов для эксперта. Она не заменяет анализ метаданных, структуры видеопотока и иных доступных сведений об обстоятельствах получения файла.

Заключение

Представлен подход к предварительной криминалистической обработке видеоматериалов, включающий регистрацию характеристик видео, равномерный отбор кадров и выделение лиц с использованием YuNet. В выполненном эксперименте все 20 извлечённых кадров одного тестового видеоролика содержали обнаруженные моделью лица. Результаты подтверждают пригодность разработанного конвейера для подготовки материалов к последующему анализу.

Дальнейшая работа должна включать документирование происхождения и целостности файлов, расширение набора тестовых видеозаписей, разработку классификатора признаков Deepfake и проверку его обобщающей способности. При использовании результатов в цифровой криминалистике принципиально важно различать технический результат локализации лица, аналитическую гипотезу о возможной модификации и экспертно подтверждённый вывод.

Список использованной литературы

1. Verdoliva L. Media Forensics and DeepFakes: An Overview // IEEE Journal of Selected Topics in Signal Processing. - 2020. - Vol. 14, No. 5. - P. 910–932. - DOI: 10.1109/JSTSP.2020.3002101.

2. Scientific Working Group on Digital Evidence (SWGDE). Best Practices for Digital Forensic Video Analysis. - Doc. 18-V-001-2.0. - 2025.

3. Wu W., Peng H., Yu S. YuNet: A Tiny Millisecond-level Face Detector // Machine Intelligence Research. - 2023. - Vol. 20. - P. 656–665. - DOI: 10.1007/s11633-023-1423-y.

4. Rössler A., Cozzolino D., Verdoliva L., Riess C., Thies J., Nießner M. FaceForensics++: Learning to Detect Manipulated Facial Images // Proceedings of ICCV. - 2019. - P. 1–11. - DOI: 10.1109/ICCV.2019.00009.

5. Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J. Deepfakes and beyond: A Survey of face manipulation and fake detection // Information Fusion. - 2020. - Vol. 64. - P. 131–148. - DOI: 10.1016/j.inffus.2020.06.014.

FINGERPRINT BIOMETRICS: TECHNOLOGIES, SECURITY CHALLENGES, AND FUTURE DEVELOPMENTS

Allanov O., Safoev N., Salimov S.
Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi

Annotation. Fingerprint scanners differ from one another depending on their purposes and areas of application. This article also outlines the advantages and disadvantages of fingerprint scanners.

Key words: scanner, identification, forensics, authentication, fingerprint.

Аннотация. Сканеры отпечатков пальцев различаются в зависимости от назначения и области применения. В данной статье также перечислены преимущества и недостатки сканеров отпечатков пальцев.

Ключевые слова: сканер, идентификация, криминалистика, аутентификация, отпечаток пальца.

A fingerprint scanner is a type of electronic security system that uses fingerprints for biometric authentication to provide user access to information or to confirm a transaction.

Human fingerprints are practically unique, so they are successful in identifying people. Law enforcement agencies aren't the only ones collecting fingerprint databases. Many occupations that require professional licensing or certification (eg, financial advisors, stockbrokers, real estate professionals, teachers, doctors/nurses, security, contractors, etc.) require fingerprinting as a requirement for employment. defines as It is customary to submit fingerprints with notarized documents [1].

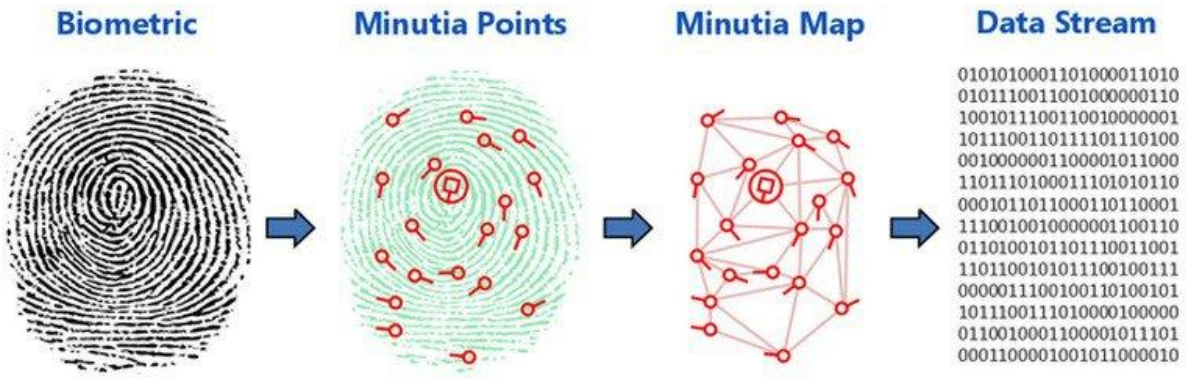


Figure 1. "Stages of Fingerprint Recognition: Biometric to Data Stream Conversion"

Changes in technology have made it possible to introduce fingerprint scanners (also called "readers" or "sensors") as another (optional) security feature for mobile devices. Fingerprint scanners are one of the latest innovations in an ever-growing list of ways to lock and unlock smartphones - pin codes, pattern codes, passwords, facial recognition, location recognition, voice recognition, reliable Bluetooth / NFC communication.

Fingerprint scanners work by printing a pattern of fingerprints and grooves. The data is then processed using the device's pattern analysis / matching software, which then compares the file to a list of registered fingerprints. A successful match means that the ID has been verified and thus authorized. Fingerprint scanners are divided into the following types according to the method of obtaining data [2]:

Optical Sensor: These scanners basically take a photocopy of the finger. Most fingers are scanned by a light-sensitive scanner (usually an image sensor or light-sensitive microchip) that records the information to produce a digital image, illuminating the finger to provide sharp contrast of the lines. Most computer-connected fingerprint scanners use optical sensors.

Capacitive Sensor: Instead of light, capacitive scanners use electricity to detect fingerprint patterns. When the finger sensor is placed on a capacitive surface, the device measures the charge; peaks show changes in the rock, depressions show almost no changes. The sensor uses all the data to map this map correctly. Most smartphones with fingerprint scanners use capacitive sensors.

Ultrasonic Sensor: Similar to how porpoises and dolphins use echolocation to locate and identify objects, ultrasonic scanners work by using sound waves. The equipment is designed to send ultrasound pulses and measure how far back it travels. Hills and depressions reflect sound differently, and these ultrasound scanners are able to create a detailed 3D map of fingerprint patterns. Ultrasonic sensors are currently being prototyped (e.g. Qualcomm Technologies, Inc.) and tested for use in mobile devices.

Capacitive Scanner: special miniature capacitor circuits (capacitive sensors) are used instead of a matrix. When we place our finger on this sensor, the capacity of the individual capacitors changes instantly. Capacitive scanners are more accurate and efficient than optical scanners because they are harder to fool.

Thermal Scanner: This works similarly to a capacitive scanner, but instead of microcapacitors, they use microscopic thermal sensors that detect the temperature difference between the ridges and lips of the finger pad. Such a scanner cannot be fooled by imitating a finger (ie a piece of skin) [3].

Advantages of using fingerprint scanners:

– allows quick and easy finger access to unlocking devices;
– a great way to identify unique individuals;
– very difficult to counterfeit / duplicate (against identification / access cards, etc.);
– real guessing / loss (PIN codes, passwords, etc.);
– you won't forget your fingerprint (such as passwords, codes, patterns, access cards, etc.);

Problems with using fingerprint scanners:

– fingerprint scanners can be fooled;
– it is possible to change the card, codes and passwords, but it is difficult to use it if the fingerprint data is stolen;
– a finger injury can prevent successful login and deny access to authorized users;
– medical microbes sit on sensors.

The use of fingerprint scanners in consumer electronics is still very new, so we can expect standards and protocols to evolve over time. As the technology matures, manufacturers will be able to improve the quality of encryption and data security to prevent theft or misuse with stolen fingerprints.

Future Trends and Innovations in Fingerprint Biometrics: fingerprint biometric technology continues to evolve rapidly, with new advancements aimed at improving accuracy, security, and usability. As digital security becomes increasingly important, researchers and technology companies are developing innovative solutions to overcome current limitations and enhance system performance.

One of the most significant developments is 3D fingerprint scanning technology. Unlike traditional 2D scanners, 3D systems capture not only the surface patterns of a fingerprint but also

its depth and structural characteristics. This additional layer of detail makes it much more difficult to spoof fingerprint data and significantly improves authentication accuracy.

Another important trend is the integration of Artificial Intelligence (AI) and Machine Learning (ML) into biometric systems. These technologies enable systems to analyze large volumes of biometric data more efficiently, reduce false acceptance and false rejection rates, and adapt to variations in fingerprint quality. AI can also detect unusual patterns or suspicious behavior, adding an extra layer of security.

The concept of continuous authentication is also gaining attention. In this approach, user identity is not verified only at the point of login but continuously monitored during device usage. By analyzing behavioral and biometric patterns, such systems can detect unauthorized access even after initial authentication, thereby enhancing overall security[4].

In addition, multi-biometric systems are becoming more widespread. These systems combine fingerprint recognition with other biometric methods, such as facial recognition or iris scanning, to provide a more robust and reliable authentication process. This layered approach reduces the likelihood of security breaches.

Furthermore, advancements in anti-spoofing technologies are helping to address one of the major weaknesses of biometric systems. Modern sensors can analyze characteristics such as skin texture, blood flow, and moisture levels to distinguish between real and fake fingerprints. This significantly reduces the risk of fraudulent access using artificial replicas.

Summary

Despite the problems with fingerprint scanners, many people use them. They lead to the security of mobile devices, as people simply tap their finger on the scanner to unlock the smartphone. However, users may cut their fingers in everyday life. This affects his work efficiency.

Reference

1. Joshi M., Mazumdar B., Dey S. A comprehensive security analysis of match-in-database fingerprint biometric system //Pattern Recognition Letters. – 2020. – T. 138. – C. 247-266.

2. Datta P. et al. Survey of Security and Privacy Issues on Biometric System //Handbook of Computer Networks and Cyber Security. – Springer, Cham, 2020. – C. 763-776.

3. Win K. N. et al. Fingerprint classification and identification algorithms for criminal investigation: A survey //Future Generation Computer Systems. – 2020. – T. 110. – C. 758-771.

4. Zhang, Y., Liu, J. (2024). Cancelable biometrics and template protection for fingerprint systems – IEEE Transactions on Information Forensics and Security, 2024.

KOMPYUTER TARMOQLARIDA SODIR ETILGAN JINOYATLAR IZLARINI ANIQLASH, YIG‘ISH VA TADQIQ ETISH USULLARI

Ramazonova M.S., Odilov O.R., Mamatov S.Z.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabalari

Annotatsiya. Tezisda kompyuter tarmoqlarida sodir etilgan jinoyatlarning izlari tasniflanadi hamda ularni aniqlash, yig‘ish va tadqiq etish usullari tahlil qilinadi. Paketlar nusxasi, oqim yozuvlari va turli jurnal manbalarining isbot qiymati, yashash muddati va saqlash xarajatlari qiyoslanib, to‘liq nusxa olish bilan oqim darajasidagi nazorat o‘rtasidagi muvozanat masalasi baholanadi. Izlarni vaqt bo‘yicha bog‘lash shartlari formal ko‘rinishda keltirilib, soatlarni sinxronlash xatoligi voqealar ketma-ketligini aniqlashga qo‘yadigan chegara asoslanadi. Manzil tarjimasi sharoitida atribusiya muammosi, shifrlangan trafikni metama’lumotlar asosida tahlil qilish imkoniyatlari hamda izlarni yashirishga qarshi choralar ko‘rib chiqiladi. Tarmoq izlarining yaxlitligini va huquqiy jihatdan qabul qilinishini ta’minlash bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: tarmoq kriminalistikasi, raqamli iz, oqim yozuvlari, paketlar nusxasi, vaqt sinxronizatsiyasi, manzil tarjimasi, atribusiya, shifrlangan trafik tahlili.

Аннотация. В тезисе классифицируются следы преступлений, совершённых в компьютерных сетях, и анализируются методы их выявления, сбора и исследования. Сравниваются доказательственная ценность, срок жизни и стоимость хранения пакетных захватов, потоковых записей и журналов различных источников. Формально записаны условия временной корреляции следов и обоснован предел, который погрешность синхронизации часов накладывает на установление последовательности событий. Рассматриваются проблема атрибуции в условиях трансляции адресов, возможности анализа зашифрованного трафика по метаданным и меры противодействия сокрытию следов. Даны рекомендации по обеспечению целостности и юридической допустимости сетевых доказательств.

Ключевые слова: сетевая криминалистика, цифровой след, потоковые записи, пакетный захват, синхронизация времени, трансляция адресов, атрибуция, анализ зашифрованного трафика.

Kirish

Kompyuter tarmoqlari orqali sodir etiladigan jinoyatlar - axborot tizimlariga noqonuniy kirish, ma’lumotlarni o‘g‘irlash va shifrlab talab qilish, firibgarlik, bot tarmoqlarini boshqarish va xizmat ko‘rsatishdan voz kechtirish hujumlari - moddiy iz qoldirmaydi. Ularning yagona isbot manbai tarmoq uskunalari, xizmat ko‘rsatuvchi serverlar va himoya vositalari tomonidan qayd etilgan raqamli izlardir.

Bunday izlarning uchta o‘ziga xos xususiyati tergov taktikasini belgilaydi. Birinchidan, ular o‘ta tez yo‘qoladi: paketlar buferda soniyalar, oqim yozuvlari esa cheklangan muddat saqlanadi, shu sababli izlarni qayd etish ko‘pincha hodisa aniqlangunga qadar yo‘lga qo‘yilgan bo‘lishi shart. Ikkinchidan, iz bitta joyda emas, balki o‘nlab mustaqil tugunlarda tarqoq holda shakllanadi va faqat ularni o‘zaro bog‘lash orqali ma’noga ega bo‘ladi. Uchinchidan, izning asosiy qismi bugungi kunda shifrlangan, bu esa tahlil markazini mazmundan metama’lumot tomon siljitadi.

Tezisning maqsadi - tarmoq izlari manbalarini isbot qiymati va saqlash xarajatlari bo‘yicha qiyoslash, izlarni vaqt bo‘yicha bog‘lash shartlarini formal ifodalash hamda atribusiya va shifrlangan trafik sharoitidagi cheklovlarni baholashdan iborat.

Izlar manbalari va ularning tasnifi

Tarmoq izlari qayd etilish darajasiga ko‘ra uch guruhga ajratiladi: to‘liq paketlar nusxasi, umumlashtirilgan oqim yozuvlari va amaliy darajadagi jurnallar. Ularning asosiy tavsiflari 1-jadvalda keltirilgan.

1-jadval

Tarmoq izlarining asosiy manbalari

Iz manbai	Qayd etiladigan ma’lumot	Odatdagi yashash muddati
Paketlar nusxasi (PCAP)	Sarlavhalar va to‘liq foydali yuk	Soatlar – kunlar
Oqim yozuvlari (NetFlow/IPFIX)	Besh element, bayt va paketlar soni, vaqt oralig‘i	Haftalar – oylar
Tarmoqlararo ekran jurnali	Ruxsat etilgan va rad etilgan ulanishlar	Haftalar – oylar
DNS so‘rovlari jurnali	So‘ralgan domen nomlari va javoblar	Kunlar – haftalar
Proksi va veb-server jurnali	URL manzillar, foydalanuvchi agenti, javob kodlari	Oylar
DHCP va NAT jurnallari	IP manzilning qurilma va portga biriktirilishi	Kunlar – haftalar
Autentifikatsiya jurnallari	Kirish urinishlari, hisob yozuvi, manba manzili	Oylar – yillar

Qayd etish usulini tanlash

To‘liq nusxa olish eng boy dalil beradi, ammo saqlash hajmi o‘tkazuvchanlikka to‘g‘ri proporsional o‘sadi. O‘rtacha yuklama R bit/s va saqlash chuqurligi T soniya bo‘lganda zarur xotira hajmi:

$$S_{pcap} = R \cdot T / 8 \qquad (1)$$

Masalan, 1 Gbit/s kanalda o‘rtacha 30 foiz yuklama bilan bir sutkalik nusxa taxminan 3,2 TB joy talab qiladi, bu esa uzoq muddatli saqlashni amalda imkonsiz qiladi. Oqim yozuvlari esa butun ulanishni bir necha o‘nlab baytli yozuvga siqadi:

$$S_{flow} = N_f \cdot s_f \qquad (2)$$

Bu yerda N bilan belgilangan kattalik oqimlar soni, s esa bitta yozuv hajmi. Natijada oqim darajasidagi nazorat bir necha tartibga kam xotira talab qilib, oylar davomida saqlanishi mumkin, biroq foydali yukni tiklash imkonini bermaydi. Shu sababli amaliyotda ikki sathli yondashuv maqbul deb topiladi: doimiy ravishda oqim yozuvlari yig‘iladi, to‘liq nusxa olish esa faqat shubhali manzillar va vaqt oraliqlari uchun tanlab yoqiladi.

Izlarni vaqt bo‘yicha bog‘lash

Turli tugunlardan olingan izlarni yagona voqealar zanjiriga birlashtirish ularning vaqt belgilariga tayanadi. Agar A va B tugunlar soatlarining aniq vaqtdan chetlanishi mos ravishda ε miqdorlar bilan chegaralangan bo‘lsa, A dagi voqea B dagisidan oldin sodir bo‘lgani faqat quyidagi shart bajarilgandagina qat’iy tasdiqlanadi:

$$t_B - t_A > \varepsilon_A + \varepsilon_B \quad (3)$$

Sinxronlash tartibga solinmagan tarmoqlarda chetlanish bir necha daqiqaga yetishi mumkin, bu esa hujum bosqichlarining ketma-ketligi haqidagi xulosani bekor qiladi. Shuning uchun tarmoq uskunalari va serverlarni yagona vaqt xizmatiga ulash, vaqtni muvofiqlashtirilgan umumjahon vaqtida va vaqt mintaqasini ko‘rsatgan holda qayd etish hamda ekspertiza boshlanishida har bir manbaning chetlanishini o‘lchab, hisobotda aks ettirish zarur. Qayd etilgan chetlanish keyinchalik barcha vaqt belgilariga tuzatma sifatida qo‘llaniladi.

Manzil tarjimasi va atribusiya muammosi

Ko‘plab foydalanuvchini bitta tashqi manzil ostida birlashtiruvchi manzil tarjimasi texnologiyalari sharoitida IP manzilning o‘zi aniq qurilmani ko‘rsatmaydi. Konkret abonentni aniqlash uchun kamida to‘rt element birgalikda talab qilinadi: tashqi manzil, tashqi port raqami, aniq vaqt belgisi va transport protokoli. Agar jabrlanuvchi tomonning serveri manba portini qayd etmagan bo‘lsa, operatordagi tarjima jurnali bilan solishtirish imkonsiz bo‘lib qoladi va iz uziladi. Shu bois internetga yo‘naltirilgan xizmatlarda manba portini va aniq vaqtni jurnalga yozish, operatorlarda esa tarjima jurnallarini belgilangan muddat davomida saqlash amaliyoti tavsiya etiladi. Qo‘shimcha murakkablik sifatida manzillarning dinamik taqsimlanishi qayd etilishi lozim: xuddi shu manzil bir necha soatdan keyin boshqa abonentga tegishli bo‘lishi mumkin, shuning uchun vaqt oralig‘i aniq ko‘rsatilmagan so‘rov noto‘g‘ri shaxsga ishora qilishi ehtimoldan xoli emas.

Shifrlangan trafik sharoitidagi tahlil

Transport sathidagi zamonaviy shifrlash protokollari qo‘l siqish bosqichining katta qismini ham yopadi, server nomini yashirish kengaytmalari esa so‘ralgan resursni aniqlash imkonini cheklaydi. Bunday sharoitda tahlil mazmunga emas, kuzatiladigan metama’lumotlarga tayanadi: ulanish yo‘nalishi va davomiyligi, uzatilgan baytlar va paketlar soni, paketlar o‘lchamlari taqsimoti va kelish oraliqlari, qo‘l siqish parametrlari asosida quriladigan mijoz barmoq izlari, nom xizmatiga yuborilgan so‘rovlar va sertifikat ma’lumotlari. Ushbu belgilar to‘plami ko‘pincha foydalanilgan dasturiy vositani, boshqaruv serveri bilan muntazam aloqa shaklidagi xatti-harakatni yoki katta hajmdagi ma’lumotni tashqariga chiqarish faktini aniqlash uchun yetarli bo‘ladi. Shu bilan birga, bunday xulosalar ehtimollik tabiatiga ega bo‘lgani sababli, ular boshqa manbalardagi izlar bilan tasdiqlanishi shart.

Izlarni yashirishga qarshi choralar

Jinoyatchilar tomonidan qo‘llaniladigan yashirish usullari va ularga qarshi choralar 2-jadvalda umumlashtirilgan.

2-jadval

Izlarni yashirish usullari va qarshi choralar

Yashirish usuli	Izga ta’siri	Qarshi chora
VPN va proksi zanjiri	Haqiqiy manba manzilini berkitadi	Xizmat ko‘rsatuvchi jurnallari, vaqt bo‘yicha korrelyatsiya
Anonim tarmoqlar	Marshrutni ko‘p sathli shifrlaydi	Chiqish tugunlari ro‘yxati, xulq-atvor tahlili
Trafikni shifrlash	Foydali yukni o‘qib bo‘lmaydi	Metama’lumot, oqim va qo‘l siqish tahlili

Yashirish usuli	Izga ta’siri	Qarshi chora
Jurnallarni tozalash	Mahalliy izlarni yo‘qotadi	Jurnallarni markaziy, faqat qo‘shib yoziladigan omborga uzatish
Domen nomini tez almashtirish	Infratuzilmani kuzatishni qiyinlashtiradi	Passiv DNS ma’lumotlar bazasi

Izlarning yaxlitligi va huquqiy qabul qilinishi

Tarmoq izining isbot kuchi uning o‘zgartirilmaganini ko‘rsatish imkoniyatiga bog‘liq. Buning uchun nusxa olish tugagach fayl uchun kriptografik xesh qiymati hisoblanadi va raqamli imzo hamda ishonchli vaqt tamg‘asi bilan mustahkamlanadi; MD5 va SHA-1 algoritmlariga nisbatan to‘qnashuv hujumlari amalda namoyish etilgani sababli SHA-256 oilasidan foydalanish tavsiya etiladi. Jurnallar manbadan markaziy, faqat qo‘shib yoziladigan omborga uzatilishi kerak - bu ularning hujumga uchragan tugunda tozalanishiga yo‘l qo‘ymaydi. Bundan tashqari, nusxa olish qaysi nuqtada va qanday filtr bilan amalga oshirilgani, uskuna paketlarni tashlab yuborgan yoki yo‘qligi hujjatlashtirilishi lozim: to‘liq bo‘lmagan nusxa noto‘g‘ri xulosaga olib kelishi mumkin. Nihoyat, yig‘ish hajmi tergov maqsadi bilan mutanosib bo‘lishi va yozishmalar maxfiyligiga doir talablarga rioya etilishi zarur.

Xulosa

Kompyuter tarmoqlarida sodir etilgan jinoyatlarni ochish izlarning tez yo‘qolishi, tarqoqligi va shifrlanganligi bilan bog‘liq uchta asosiy to‘siqni yengishni talab qiladi. Tahlil shuni ko‘rsatadiki, doimiy to‘liq nusxa olish iqtisodiy jihatdan oqlanmaydi; maqbul yechim - oqim darajasidagi uzluksiz nazoratni shubhali yo‘nalishlar bo‘yicha tanlab to‘liq nusxa olish bilan birlashtirish. Izlarni bog‘lashning asosiy sharti soatlarni sinxronlash bo‘lib, chetlanish qiymati voqealar ketma-ketligi haqidagi xulosaning aniqlik chegarasini belgilaydi.

Atribusiya masalasida hal qiluvchi omil manba portini va aniq vaqtni qayd etish hamda manzil tarjimasi jurnallarini saqlash amaliyoti hisoblanadi. Shifrlangan trafik sharoitida esa tadqiqot markazi metama’lumotlar tahliliga siljiydi. Keyingi ishlarda ushbu yondashuvlarni milliy operatorlar infratuzilmasi sharoitida sinovdan o‘tkazish va izlarni avtomatik korrelyatsiyalash vositasini ishlab chiqish rejalashtirilgan.

Foydalanilgan adabiyotlar

1. RFC 3227. Guidelines for Evidence Collection and Archiving.
2. RFC 7011. Specification of the IP Flow Information Export (IPFIX) Protocol.
3. RFC 5905. Network Time Protocol Version 4: Protocol and Algorithms Specification.
4. RFC 6302. Logging Recommendations for Internet-Facing Servers.
5. RFC 6888. Common Requirements for Carrier-Grade NATs (CGNs).
6. RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3.
7. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence.
8. ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence.
9. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response.
10. Davidoff S., Ham J. Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall.
11. Casey E. Digital Evidence and Computer Crime. Academic Press.
12. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi 2022-yil 15-apreldagi O‘RQ-764-sonli Qonuni.

RAQAMLI TASVIRLARDA RUXSATSIZ O‘ZGARISHLARNI ANIQLASH

Ganiyev A.A., Sadirova X.X.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada raqamli tasvirlarni autentifikatsiya qilishda ruxsat etilgan texnik qayta ishlashni mazmuniy o‘zgartirishlardan ajratish muammosi o‘rganiladi. Yarim mo‘rt autentifikatsiya belgisi, qayta ishlash holatini baholash va sun’iy intellektning hududiy tahlilini birlashtiruvchi konseptual yondashuv taklif qilinadi. Qaror qoidalari, tahdid modeli hamda mustaqil sinov protokoli bayon etiladi. Taklifning samaradorligi tajribada tekshirilishi lozim bo‘lgan gipoteza sifatida qo‘yiladi.

Kalit so‘zlar: raqamli tasvir, autentifikatsiya, yaxlitlik, yarim mo‘rt watermark, mazmuniy tahrir, sun’iy intellekt, noaniqlik.

Аннотация. Рассматривается задача разграничения допустимой технической обработки и содержательных изменений цифровых изображений при проверке подлинности. Предлагается концептуальный подход, объединяющий полухрупкий водяной знак, оценку условий обработки и локальный анализ средствами искусственного интеллекта. Описаны модель угроз, правила принятия решений и протокол независимых испытаний. Эффективность подхода сформулирована как гипотеза, требующая экспериментальной проверки.

Ключевые слова: цифровое изображение, аутентификация, целостность, полухрупкий водяной знак, содержательное изменение, искусственный интеллект, неопределённость.

Kirish

Raqamli tasvirlarni tashkilot sayti, elektron arxiv va ijtimoiy tarmoqlarda tarqatishda ularning fayl ko‘rinishi tez-tez o‘zgaradi. Platforma fotosuratni siqishi yoki kichraytirishi mumkin. Shu bilan birga, tasvirga obyekt qo‘shish, yuzni almashtirish yoki yozuvni olib tashlash axborot mazmunini o‘zgartiradi. Har ikkala jarayon piksellarga ta’sir qilgani sababli, har qanday farqni soxtalashtirish deb baholash ortiqcha ogohlantirishlarga olib keladi.

Maqolaning maqsadi oldindan autentifikatsiya qilingan fotosuratlarda ruxsat etilgan qayta ishlash va mazmuniy o‘zgartirishlarni farqlash uchun qaror chiqarish yondashuvini shakllantirishdir. Asosiy e’tibor belgi buzilishining sababini baholashga qaratiladi. Tadqiqot faylni tahrirlashni jismonan taqiqlashni emas, tahrirlangan nusxani tasdiqlangan asl tasvir sifatida qabul qilish xavfini kamaytirishni ko‘zlaydi.

Mavjud usullar va muammoning qo‘yilishi

Kriptografik imzo ma’lumotlarning yaxlitligi va imzolovchi bilan bog‘liqligini tekshirishga xizmat qiladi [1]. Fayl xeshi asosidagi tekshiruvda hatto odatiy JPEG siqish ham nomuvofiqlik keltirib chiqaradi. Bu mexanizm aynan bir xil fayl uchun kuchli dalil beradi, lekin mazmun saqlanganini yoki qaysi hudud tahrirlanganini o‘z-o‘zidan baholamaydi. Shuning uchun baytlar yaxlitligi va mazmuniy haqiqiylik alohida ko‘rilishi kerak.

FaceSigns yarim mo‘rt neyron watermark yordamida odatiy transformatsiyalarga bardoshlilik va zararli manipulyatsiyalarga sezgirlikni birlashtirishni o‘rganadi [2]. EditGuard autentifikatsiya belgilariga yaqin watermark mexanizmlari orqali tahrir hududlarini aniqlash va mualliflikni himoyalashni ko‘zlaydi [3]. OmniGuard esa gibrid lokalizatsiya va buzilish holatlarini

hisobga oladigan tahlilga asoslanadi [4]. Bu ishlar mavjudligi sababli, belgi va AI ni birlashtirishning o‘zi yangi ilmiy natija deb olinmaydi.

TruFor oldindan watermark joylashtirish shartisiz tasvirning vizual va forensik izlarini tahlil qiladi hamda lokalizatsiya ishonchliligini baholaydi [5]. Bunday tahlil qo‘shimcha dalil bo‘lishi mumkin, ammo neyron model xulosasi raqamli imzoning kriptografik kafolatini almashtirmaydi. Mazkur maqolada o‘rganiladigan savol - qayta ishlash holatiga qarab dalillarni qanday baholash va qachon xulosa berishdan tiyilish zarurligidir.

Tahdid modeli va autentifikatsiya siyosati

Tasvir egasi autentifikatsiya belgisini joylashtirib, yakuniy faylni reyestrda qayd etadi. Tahdidchi e’lon qilingan nusxani olishi va undan hosila fayl yaratishi mumkin, ammo imzolash kaliti va himoya belgisining maxfiy kalitiga ega emas. Ishonchli reyestr yoki kalitning buzilishi ushbu model doirasidan tashqarida qoladi. Begona tasvirdan belgini ko‘chirish va tasvirdagi belgini olib tashlash esa tekshiriladigan tahdidlar qatoriga kiritiladi.

“Ruxsat etilgan” o‘zgarish faqat texnik nomiga qarab belgilanmaydi. Masalan, kuchli kichraytirish mayda yozuvni o‘qib bo‘lmaydigan holatga keltirishi mumkin. Shuning uchun siyosat JPEG sifatining minimal darajasi, o‘lchamning minimal nisbati va muhim hududlar saqlanishini belgilaydi. Hujjat fotosurati bilan oddiy tadbir fotosurati uchun bir xil siyosat qo‘llanishi shart emas. Kesib tashlash muhim obyektni yo‘qotsa, u ruxsat etilgan texnik amal deb olinmaydi.

Dastlabki tajriba siyosatida JPEG siqish va butun tasvirni proporsional kichraytirish chegaralangan holda ruxsat etiladi. Obyekt qo‘shish, olib tashlash, almashtirish va tasvir qismini ko‘chirib joylashtirish mazmuniy tahrirlar sifatida belgilanadi. Chegaradan tashqaridagi transformatsiya avtomatik “soxta” emas, tekshirish shartlari buzilgan holat sifatida ajratiladi. Maqsad niyatni aniqlash emas: tasvirning siyosatga muvofiqligi tekshiriladi.

Taklif etilayotgan qaror mexanizmi

Ro‘yxatga olish bosqichida tasvir identifikatori, himoyalangan fayl xeshi, algoritm versiyasi va qayta ishlash siyosati bir yozuvga jamlanadi. Ushbu yozuv imzolanadi. Belgi identifikator bilan birga mazmunga bog‘langan autentifikatsiya ma’lumotini tashishi ko‘zda tutiladi. Mazmunga bog‘lash usuli ruxsat etilgan transformatsiyalarga barqarorlik bilan boshqa tasvirga ko‘chirishga qarshi sezgirlik o‘rtasidagi muvozanatni talab qiladi; bu alohida tajriba bilan tekshiriladi.

Tekshirishda avval reyestr yozuvining imzosi va fayl xeshi solishtiriladi. Moslik aynan ro‘yxatga olingan faylni tasdiqlaydi. Moslik bo‘lmaganda qayta ishlash moduli holat vektorini baholaydi, belgi dekoderi hududiy nomuvofiqlik xaritasini chiqaradi, AI segmentatsiya modeli esa tahrir alomatlari xaritasini hosil qiladi. O‘lcham o‘zgargan bo‘lsa, xaritalar umumiy koordinata tizimiga keltiriladi. Moslashtirish xatosi ham ishonchlilik bahosiga kiritilishi lozim.

Qayta ishlash natijasidagi global belgi xatolari bilan mazmuniy tahrirdan kelib chiqadigan lokal xatolarni birgalikda baholash taklif etiladi. Biroq barcha siqish xatolari bir tekis, barcha tahrirlar esa faqat lokal bo‘ladi degan taxmin qabul qilinmaydi. Teksturali hududlar turlicha buzilishi va keng tahrirlar butun tasvirni qamrashi mumkin. Shu sababli, qaror mexanizmi haqiqiy va tahrirlangan misollarda kalibrlanishi kerak.

Hududiy dalillarni birlashtirishning ishchi ifodasi quyidagicha:

$$S(x,y) = \alpha(q,r)W(x,y) + [1 - \alpha(q,r)]F(x,y).$$

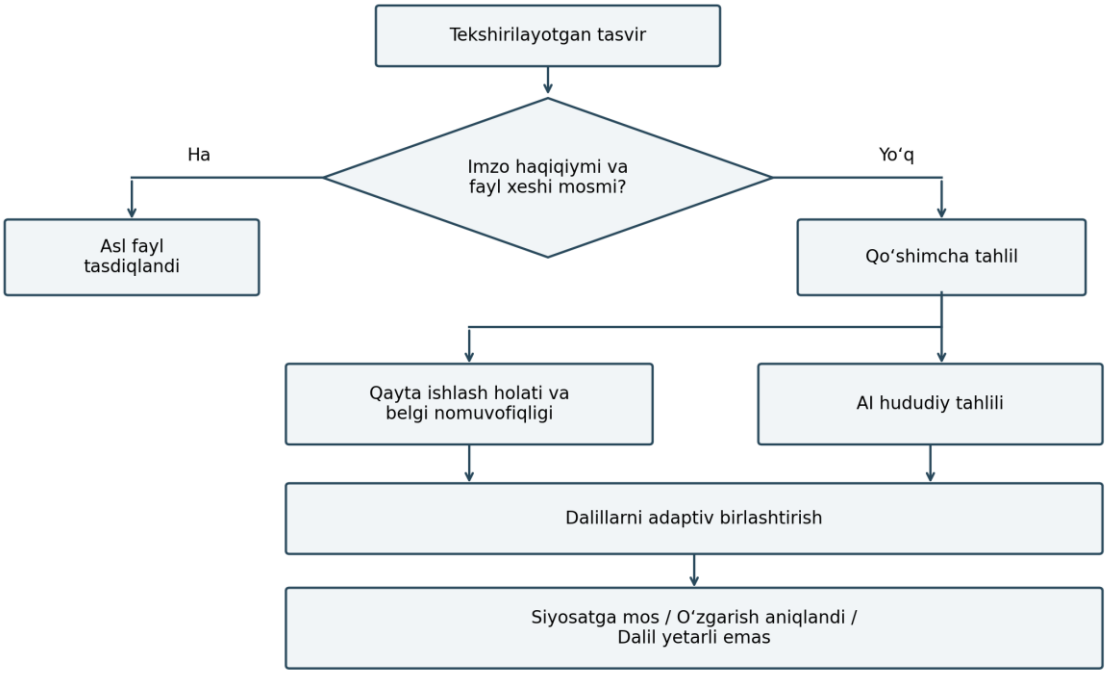
Bu yerda W - belgi nomuvofiqligi balli, F - forensik model balli, q - qayta ishlash holati, r - dekoder va moslashtirish ishonchliligi, α - validatsiyada tanlanadigan og‘irlik. Ballar bir xil

oraliqqa normallashtiriladi. Mazkur ifoda yangi algoritmning isbotlangan samaradorligi emas, tekshiriladigan modelidir. Uni ehtimol sifatida talqin qilish uchun alohida kalibrlash va mustaqil test zarur.

Past va yuqori qaror chegaralari validatsiya to‘plamida belgilanadi. Kuchli hududiy dalil mavjud bo‘lsa tahrir xaritasi chiqariladi; siyosatga mos qayta ishlash va yetarli dalil bo‘lsa mazmuniy moslik haqida ehtiyotkor xulosa beriladi. Oraliq ball, belgining yo‘qolishi yoki tanish bo‘lmagan qayta ishlash “dalil yetarli emas” holatiga olib keladi. Belgining saqlanishi ham o‘z-o‘zidan mazmun mutlaqo o‘zgarmaganini kafolatlamaydi.

Tajriba protokoli

Fotosuratlar manba tasvir darajasida o‘qitish, validatsiya va test guruhlariga ajratiladi. Bitta fotosuratning barcha siqilgan va tahrirlangan hosilalari bitta guruhda qoladi. Zarur hollarda kamera, tadbir yoki manba tashkilot bo‘yicha ham ajratish amalga oshiriladi. Shunday qilib, model bir xil sahna va tasvirlarni turli guruhlarda ko‘rib qolishidan keladigan natija oshishi cheklanadi. Guruhlar hajmi va tarkibi tajriba hisobotida berilishi kerak.



1-rasm. Tasvir autentifikatsiyasi bo‘yicha qaror chiqarish blok-sxemasi

Nazorat amallari sifatida JPEG sifat koeffitsiyentlari 95, 85, 70 va 50 hamda o‘lcham nisbatlari 0,75 va 0,5 tekshirilishi rejalashtiriladi. Bu qiymatlar avtomatik ruxsat chegaralari emas, barqarorlikni tekshirish nuqtalaridir. Mazmuniy tahrirlar kichik va katta hududlarda, siqishdan oldin va keyin bajariladi. Har bir tahrir uchun haqiqiy maska saqlanadi. Belgi ko‘chirish, takroriy siqish va kuchli qayta ishlash holatlari alohida test qilinadi.

Taqqoslashda faqat belgi, faqat AI, doimiy og‘irlikli birlashtirish va taklif etilgan adaptiv variant ishlatiladi. EditGuard va OmniGuard mos ish sharoitida, bir xil ma’lumot va transformatsiyalarda baholanadi. AI uchun foydalanilgan o‘qitish ma’lumotlari hamda hisoblash budjeti ko‘rsatiladi. Qaror chegaralari test natijasiga qarab qayta tanlanmaydi. Qayta ishlash modulini olib tashlash sinovi uning mustaqil hissasini tekshiradi.

Baholash mezonlari va muhokama

Tasvir darajasida yolg‘on ogohlantirishlar va o‘tkazib yuborilgan tahrirlar alohida hisoblanadi. Hudud darajasida F1 va IoU ishlatiladi. IoU aniqlangan hudud bilan haqiqiy hudud

kesishmasining ularning birlashmasiga nisbatidir. Bo‘sh maskali haqiqiy tasvirlar uchun kelishilgan hisoblash qoidasi qo‘llanadi. PSNR va SSIM himoya belgisi qo‘shilgandagi vizual o‘zgarishni baholaydi; ular autentifikatsiya ishonchliligining o‘rnini bosmaydi.

Noaniq xulosalar ulushi va avtomatik qaror berilgan tasvirlar ulushi birga taqdim etiladi. Tizim qiyin misollarning barchasini rad etib, qolganlarida yuqori aniqlik ko‘rsatishi mumkinligi sababli, aniqlikni qamrovdan ajratib baholash noto‘g‘ri bo‘ladi. Natijalar siqish darajasi, tahrir turi va tahrir hajmi bo‘yicha ajratiladi. Mustaqil manba tasvirlar asosidagi ishonch oralig‘i natija barqarorligini baholashga yordam beradi.

Amaliy qo‘llanish uchun tasdiqlangan asl fayl, qayta ishlangan nusxa va noaniq fayl holatlari foydalanuvchiga farqli ko‘rsatilishi kerak. Tasvirda yozuv yoki shaxs olib tashlanganini aniqlash bilan tahrirning huquqiy ruxsatini aniqlash bir vazifa emas. Ruxsat egasi tasdiqlagan tahrir yangi imzolangan versiya sifatida ro‘yxatdan o‘tkazilishi mumkin. Yondashuvning cheklovlari kalitlar xavfsizligi, belgi ko‘chirishga qarshilik va yangi tahrir turlariga umumlashishga bog‘liq.

Xulosa

Raqamli tasvir autentifikatsiyasida baytlar yaxlitligi, mazmuniy moslik va qayta ishlash siyosati ajratildi. Belgi, qayta ishlash bahosi va AI dalillarini adaptiv birlashtirishga asoslangan konseptual mexanizm hamda uning sinov protokoli taklif qilindi. Ushbu maqolada empirik tajriba natijalari berilmaydi. Ilmiy hissa adaptiv baholash va noaniqlikni boshqarishning mavjud usullarga nisbatan foydasini mustaqil tajribada tekshirish bilan aniqlanadi.

Foydalanilgan adabiyotlar

1. NIST. Digital Signature Standard (DSS). FIPS 186-5. 2023. https://doi.org/10.6028/NIST.FIPS.186-5

2. FaceSigns: Semi-fragile Watermarks for Media Authentication. ACM Transactions on Multimedia Computing, Communications, and Applications. 2024. https://doi.org/10.1145/3640466

3. Zhang X. et al. EditGuard: Versatile Image Watermarking for Tamper Localization and Copyright Protection. IEEE/CVF CVPR. 2024. P. 11964–11974. https://arxiv.org/abs/2312.08883

4. Zhang X. et al. OmniGuard: Hybrid Manipulation Localization via Augmented Versatile Deep Image Watermarking. IEEE/CVF CVPR. 2025. P. 3008–3018. https://arxiv.org/abs/2412.01615

5. Guillaro F., Cozzolino D., Sud A., Dufour N., Verdoliva L. TruFor: Leveraging All-Round Clues for Trustworthy Image Forgery Detection and Localization. IEEE/CVF CVPR. 2023. P. 20606–20615. https://arxiv.org/abs/2212.10957

RAQAMLI KRIMINALISTIKADA SUN'IY INTELLEKT ASOSIDAGI PREDIKTIV TAHLIL: KIBERINTSIDENTLARNI REAL VAQTDA ANIQLASH VA DALILLARNI AVTOMATLASHTIRILGAN TAHLIL QILISH

Nasrullayev N.B., Maxmudov A.N.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya: Ushbu maqolada raqamli kriminalistika jarayonlarida sun'iy intellekt (SI) asosidagi prediktiv tahlilni qo'llash masalasi ko'rib chiqilgan. Kiberintsidentlarni real vaqt rejimida aniqlash, xavf darajasini prognozlash va raqamli dalillarni avtomatlashtirilgan tahlil qilishni birlashtiruvchi yetti bosqichli tizim arxitekturasi taklif etilgan. Tasniflash uchun tasodifiy o'rmon, gradiyentli kuchaytirish va ko'p qatlamli neyron tarmoqdan iborat ansambl modeli qo'llanilgan. Eksperimental sinovda taklif etilgan ansambl 94,8 % aniqlik (precision) va 0,41 % yolg'on signallar ulushini ko'rsatgan. Maqolada an'anaviy va SI asosidagi yondashuvlar jadval ko'rinishida solishtirilgan.

Kalit so'zlar: raqamli kriminalistika, sun'iy intellekt, prediktiv tahlil, kiberintsident, mashinali o'qitish, ansambl modeli, real vaqt monitoringi, raqamli dalil, SIEM.

Аннотация: В статье рассматривается применение предиктивного анализа на основе искусственного интеллекта (ИИ) в процессах цифровой криминалистики. Предложена семиэтапная архитектура системы, объединяющая выявление киберинцидентов в реальном времени, прогнозирование уровня риска и автоматизированный анализ цифровых доказательств. Для классификации используется ансамблевая модель из случайного леса, градиентного бустинга и многослойной нейронной сети. В экспериментальной проверке предложенный ансамбль показал точность (precision) 94,8 % и долю ложных срабатываний 0,41 %. Традиционный подход и подход на основе ИИ сопоставлены в табличной форме.

Ключевые слова: цифровая криминалистика, искусственный интеллект, предиктивный анализ, киберинцидент, машинное обучение, ансамблевая модель, мониторинг в реальном времени, цифровое доказательство, SIEM.

Bugungi kunda davlat boshqaruvi, bank-moliya, ta'lim va sog'liqni saqlash tizimlari faoliyati to'liq raqamli infratuzilmaga tayanmoqda. Bu jarayon bilan birga kiberjinoyatlar soni va murakkabligi ham ortib bormoqda. Xalqaro tashkilotlarning yillik hisobotlarida to'lov talab qiluvchi zararli dasturlar, ijtimoiy muhandislik va ma'lumotlarni o'g'irlashga qaratilgan hujumlar eng keng tarqalgan tahdidlar sifatida qayd etilmoqda [1]. Tashkilot tarmog'ida sutkasiga millionlab log yozuvlari hosil bo'ladi va ularni mutaxassis tomonidan qo'lda ko'rib chiqish amalda imkonsizdir.

O'zbekiston Respublikasida 2022-yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun axborot tizimlarini himoya qilish va kiberintsidentlarga javob choralarining huquqiy asosini belgilab berdi [2]. Biroq intsidentni aniqlash va uning dalillarini sudda qo'llash mumkin bo'lgan holatda to'plash hali ham ko'p vaqt talab qiladigan jarayon bo'lib qolmoqda. Ushbu maqolaning maqsadi - sun'iy intellekt yordamida kiberintsidentlarni real vaqtda aniqlash, ularning rivojlanishini prognozlash hamda dalillarni avtomatlashtirilgan tahlil qilish usulini ishlab chiqish va uning samaradorligini eksperimental baholashdan iborat.

Raqamli kriminalistika va sun'iy intellekt. Raqamli kriminalistika - raqamli qurilmalar va tarmoqlardagi ma'lumotlarni dalil sifatida aniqlash, to'plash, saqlash, tahlil qilish va taqdim etish jarayonidir [3]. ISO/IEC 27037 standarti dalillarning yaxlitligini va "dalillar saqlanish zanjiri"ni (chain of custody) ta'minlashni asosiy talab sifatida belgilaydi [4]. An'anaviy kriminalistik tahlil

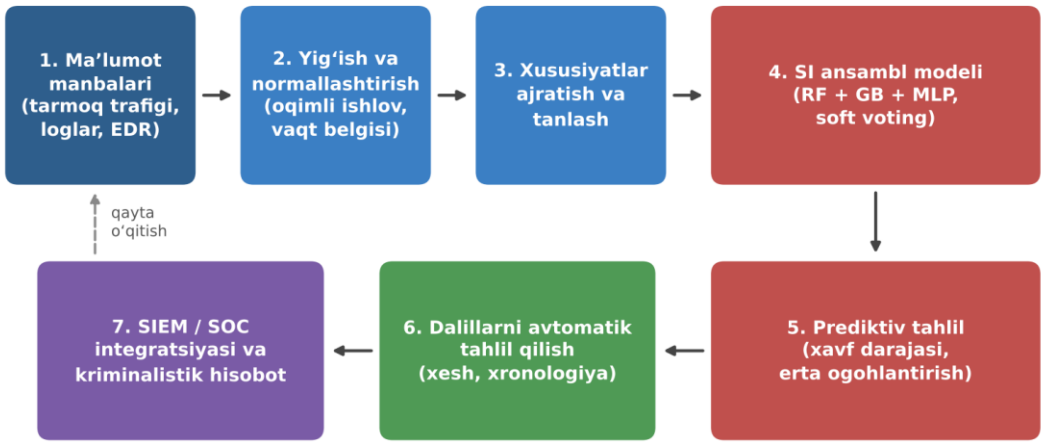
hodisa sodir bo‘lgandan keyin boshlanadi, ya’ni reaktiv xarakterga ega. Sun’iy intellekt esa bu jarayonni prediktiv, ya’ni hodisani uning dastlabki belgilari asosida oldindan aniqlaydigan jarayonga aylantirish imkonini beradi [5]. Ikki yondashuvning asosiy farqlari 1-jadvalda keltirilgan.

1-jadval.

An’anaviy va SI asosidagi raqamli kriminalistik yondashuvlarning qiyosiy tahlili

Mezon	An’anaviy yondashuv	SI asosidagi prediktiv yondashuv
Aniqlash vaqti	Soatlar va kunlar (hodisadan keyin)	Soniyalar (real vaqt rejimida)
Ma’lumotlar hajmi	Tanlab olingan loglar qo‘lda ko‘riladi	Barcha oqim va loglar avtomatik tahlil qilinadi
Noma’lum hujumlar	Imzo (signatura) bazasiga bog‘liq, yangi hujumlar o‘tkazib yuboriladi	Xatti-harakat anomaliyalari orqali aniqlanadi
Dalillar tahlili	Qo‘lda, xronologiya mutaxassis tomonidan tiklanadi	Avtomatik: xeshlash, xronologiya tiklash, hisobot shakllantirish
Prognozlash	Mavjud emas	Xavf darajasi bo‘yicha erta ogohlantirish
Mutaxassis roli	Barcha bosqichlarni bajaradi	Model xulosalarini tekshiradi va tasdiqlaydi

Taklif etilgan usul. Taklif etilgan tizim arxitekturasi 1-rasmda keltirilgan. Birinchi bosqichda tarmoq trafigi, operatsion tizim va ilovalar loglari hamda EDR vositalaridan ma’lumotlar yig‘iladi. Ikkinchi bosqichda turli formatdagi yozuvlar yagona sxemaga keltiriladi va vaqt belgilari sinxronlashtiriladi. Uchinchi bosqichda har bir tarmoq oqimi yoki sessiya uchun statistik xususiyatlar (paketlar soni va o‘lchami, oqim davomiyligi, ulanishlar chastotasi, muvaffaqiyatsiz autentifikatsiyalar soni va boshqalar) hisoblanadi hamda o‘zaro bog‘liqligi yuqori xususiyatlar chiqarib tashlanadi.



1-rasm. SI asosidagi prediktiv raqamli kriminalistika tizimining arxitekturasi

To‘rtinchi bosqichda tasodifiy o‘rmon (RF) [6], gradiyentli kuchaytirish (GB) va ko‘p qatlamli perseptron (MLP) modellaridan tashkil topgan ansambl qo‘llaniladi. Ansambl har bir model bergan sinf ehtimolliklarini o‘rtachalash (soft voting) orqali yakuniy qaror qabul qiladi. Beshinchi bosqichda har bir obyekt (xost yoki foydalanuvchi) uchun t vaqtdagi xavf darajasi quyidagicha hisoblanadi:

$$R(t) = \Sigma_k\, w_k \cdot p_k(x_t), \quad S(t) = \alpha \cdot R(t) + (1 - \alpha) \cdot S(t - 1) \qquad (1)$$

bu yerda $p_k(x_t)$ - k-hujum sinfiga tegishlilik ehtimoli, w_k - sinfning xavflilik vazni, S(t) - eksponensial silliqlangan xavf ko‘rsatkichi, $\alpha \in (0;\ 1)$ - silliqlash koeffitsiyenti. S(t) belgilangan

θ chegaradan oshganda tizim erta ogohlantirish signalini shakllantiradi. Silliqlash bitta tasodifiy yozuv sababli yuzaga keladigan yolg‘on signallarni kamaytiradi, ketma-ket kuzatiladigan shubhali faollik esa xavf darajasini tez oshiradi.

Dalillarni avtomatlashtirilgan tahlil qilish. Oltinchi bosqichda har bir ogohlantirish bilan bog‘liq log fragmentlari va tarmoq paketlari avtomatik ravishda ajratib olinadi, ularning SHA-256 xesh qiymati hisoblanadi va o‘zgartirib bo‘lmaydigan omborga yoziladi. Bu dalillar yaxlitligini va saqlanish zanjirini ta’minlaydi [4, 7]. Shundan so‘ng hodisalar vaqt bo‘yicha tartiblanib, hujumning xronologiyasi tiklanadi. Yettinchi bosqichda natijalar SIEM tizimi va xavfsizlik operatsiyalari markaziga (SOC) uzatiladi hamda kriminalistik hisobot shakllantiriladi. Tahlilchi tomonidan tasdiqlangan yoki rad etilgan ogohlantirishlar modelni qayta o‘qitish uchun ishlatiladi.

Eksperimental baholash. Usulni baholash uchun tarmoq oqimlari va tizim loglari xususiyatlarini imitatsiya qiluvchi 60 000 ta yozuvdan iborat sintetik ma’lumotlar to‘plami shakllantirildi. Har bir yozuv 40 ta xususiyat bilan tavsiflanadi va beshta sinfdan biriga tegishli: normal faollik, DoS hujumi, tarmoqni skanerlash, parolni tanlash (brute-force) va ma’lumotlarni tashqariga chiqarish. Real loglardagi nomutanosiblikni aks ettirish uchun sinflar ulushi mos ravishda 62, 14, 11, 8 va 5 % qilib belgilandi. Ma’lumotlar 70/30 nisbatda o‘qitish va test qismlariga stratifikatsiyalangan holda ajratildi. Modellar Python tilida scikit-learn kutubxonasi [8] yordamida amalga oshirildi.

Natijalarni baholashda quyidagi ko‘rsatkichlardan foydalanildi (sinflar bo‘yicha makro-o‘rtacha qiymatlar):

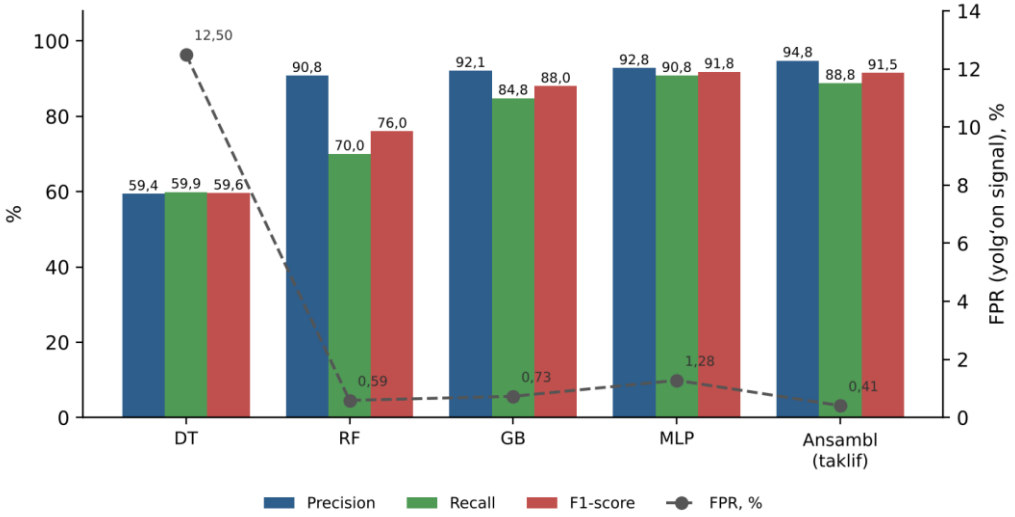
$$Precision = TP / (TP + FP), \quad Recall = TP / (TP + FN), \quad F1 = 2 \cdot P \cdot R / (P + R) \qquad (2)$$

bu yerda TP - to‘g‘ri aniqlangan hujumlar, FP - yolg‘on signallar, FN - o‘tkazib yuborilgan hujumlar. Shuningdek, normal yozuvlarning hujum deb noto‘g‘ri baholangan ulushi (FPR) va bitta yozuvni tasniflash vaqti o‘lchandi. Olingan natijalar 2-jadvalda va 2-rasmda keltirilgan.

2-jadval

Modellarning test to‘plamidagi natijalari

Model	Accuracy, %	Precision, %	Recall, %	F1, %	FPR, %	Vaqt, ms/yozuv
Qaror daraxti (DT)	75,59	59,37	59,89	59,60	12,52	< 0,001
Tasodifiy o‘rmon (RF)	87,98	90,77	69,99	76,02	0,59	0,016
Gradiyentli kuchaytirish (GB)	93,54	92,10	84,82	88,00	0,73	0,029
Neyron tarmoq (MLP)	95,52	92,79	90,80	91,75	1,28	0,008
Taklif etilgan ansambl (ENS)	95,34	94,77	88,78	91,48	0,41	0,048



2-rasm. Modellarning aniqlash ko‘rsatkichlari va yolg‘on signallar ulushi

Natijalar tahlili. Natijalardan ko‘rinadiki, eng yuqori F1 (91,75 %) va to‘liqlik (90,80 %) ko‘rsatkichlariga MLP modeli erishgan. Taklif etilgan ansambl F1 bo‘yicha undan atigi 0,27 foiz punktga past bo‘lsa-da, eng yuqori aniqlik (94,77 %) va eng past yolg‘on signallar ulushini (0,41 %) ta’minladi: bu ko‘rsatkich MLP modelinikidan qariyb 3 marta past. Raqamli kriminalistika uchun bu muhim afzallikdir, chunki har bir yolg‘on signal tahlilchi vaqtini sarflaydi va haqiqiy intsidentlarni ko‘rib chiqishni kechiktiradi. Ansamblda bitta yozuvni tasniflash vaqti 0,048 ms ni tashkil etdi, ya’ni bitta hisoblash oqimida soniyasiga 20 000 dan ortiq yozuvni qayta ishlash mumkin. Bu tizimni real vaqt rejimida qo‘llash uchun yetarli. Shuni ta’kidlash lozimki, natijalar sintetik ma’lumotlarda olingan bo‘lib, keyingi bosqichda ular CICIDS2017 [9] kabi ochiq ma’lumotlar to‘plamlarida va real tarmoq loglarida tekshirilishi rejalashtirilgan.

Xulosa

Maqolada raqamli kriminalistikada sun’iy intellekt asosidagi prediktiv tahlil usuli taklif etildi. Usul ma’lumotlarni yig‘ishdan tortib kriminalistik hisobot shakllantirishgacha bo‘lgan yetti bosqichni yagona tizimga birlashtiradi. Ansambl modeli va eksponensial silliqlangan xavf ko‘rsatkichi intsidentlarni real vaqtda aniqlash hamda ularning rivojlanishini oldindan baholash imkonini beradi, dalillarni avtomatik xeshlash va xronologiyani tiklash esa ISO/IEC 27037 talablariga mos ravishda dalillar yaxlitligini ta’minlaydi. Eksperimental sinov taklif etilgan ansamblning yolg‘on signallarni sezilarli darajada kamaytirishini ko‘rsatdi. Keyingi ishlarda modelni real ma’lumotlar to‘plamlarida sinash, shifrlangan trafik uchun xususiyatlarni kengaytirish va tizimni SIEM platformalariga integratsiya qilish rejalashtirilgan.

Foydalanilgan adabiyotlar

1. ENISA Threat Landscape 2024. - European Union Agency for Cybersecurity, 2024.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. O‘RQ-764-son, 2022-yil 15-aprel.
3. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. - Academic Press, 2011. - 840 p.
4. ISO/IEC 27037:2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.
5. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. - 2016. - Vol. 18, No. 2. - P. 1153–1176.
6. Breiman L. Random Forests // Machine Learning. - 2001. - Vol. 45, No. 1. - P. 5–32.
7. Kent K., Chevalier S., Grance T., Dang H. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. - NIST, 2006.
8. Pedregosa F. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. - 2011. - Vol. 12. - P. 2825–2830.
9. Sharafaldin I., Habibi Lashkari A., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // Proc. of the 4th Int. Conf. on Information Systems Security and Privacy (ICISSP). - 2018. - P. 108–116.

LLM DAVRIDA IJTIMOIY TARMOQLARDAGI SOXTA PROFIL VA BOTLARNI ANIQLASH: USULLAR, CHEKLOVLAR VA GIBRID YONDASHUV

Qudratov U.I., Eshmurodov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada ijtimoiy tarmoqlarda soxta profil va bot akkauntlarning tarqalish ko‘lami, ularning tasnifi hamda aniqlash usullari tahlil qilingan. Thales (Imperva) 2026 yil hisoboti, Meta shaffoflik hisobotlari va DataReportal ma’lumotlari asosida muammoning hajmi baholangan; evristik, mashinaviy o‘qitish, graf va kontent tahliliga asoslangan usullar qiyoslangan. Katta til modellari (LLM) asosidagi yangi avlod botlari an’anaviy detektorlar uchun jiddiy qiyinchilik tug‘dirishi ko‘rsatilgan. Natijalar O‘zbekiston foydalanuvchilari va tashkilotlari uchun amaliy tavsiyalar bilan yakunlangan.

Kalit so‘zlar: soxta profil, bot akkaunt, ijtimoiy bot, botnet, Botometer, graf tahlili, LLM, axborot xavfsizligi auditi.

Аннотация. В статье проанализированы масштабы распространения фейковых профилей и бот-аккаунтов в социальных сетях, их классификация и методы выявления. На основе отчёта Thales (Imperva) за 2026 год, отчётов Meta о прозрачности и данных DataReportal оценён масштаб проблемы; сопоставлены эвристические методы, методы машинного обучения, графового анализа и анализа контента. Показано, что боты нового поколения на основе больших языковых моделей (LLM) создают серьёзные трудности для традиционных детекторов. Даны практические рекомендации для пользователей и организаций Узбекистана.

Ключевые слова: фейковый профиль, бот-аккаунт, социальный бот, ботнет, Botometer, графовый анализ, LLM, аудит информационной безопасности.

Ijtimoiy tarmoqlar axborot almashinuvi, savdo, ishga yollash va ommaviy kommunikatsiyaning asosiy maydoniga aylandi. O‘zbekistonda 2025 yil oktyabr holatiga ijtimoiy tarmoqlarda 14,1 million foydalanuvchi identifikatori qayd etilgan: bu aholining 37,9 foizi bo‘lib, bir yil avvalgidan 41,7 foizga ko‘pdir; internet foydalanuvchilari esa 33,1 millionga (89 foiz) yetgan [1]. Auditoriya shiddat bilan o‘sgan joyda firibgarlar va ta’sir o‘tkazuvchilar uchun ham imkoniyat kengayadi: soxta profil orqali shaxs, mansabdor yoki brend nomidan aldash, bot tarmoqlari yordamida soxta obunachi va sun’iy «jamoatchilik fikri» yaratish mumkin.

Masalan, 2026 yil yanvarida Toshkent shahar hokimligi shahar hokimining nomi va fotosuratidan foydalanib ochilgan soxta akkauntlar orqali fuqarolarga xabar yuborilayotgani haqida ogohlantirdi; shu xabarda so‘nggi besh yilda O‘zbekistonda kiberjinoyatlar soni 68 barobar oshgani va 2025 yilda 46 mingdan ortiq kiberjinoyat aniqlangani qayd etilgan [2]. Demak, soxta akkauntlarni aniqlash nafaqat texnik masala, balki axborot xavfsizligi auditining ham dolzarb vazifasidir. Maqolaning maqsadi - muammo ko‘lamini baholash, aniqlash usullarini tizimlashtirish va ularning samaradorligi hamda cheklovlarini qiyoslashdir.

Tushunchalar, tasnif va muammo ko‘lami.

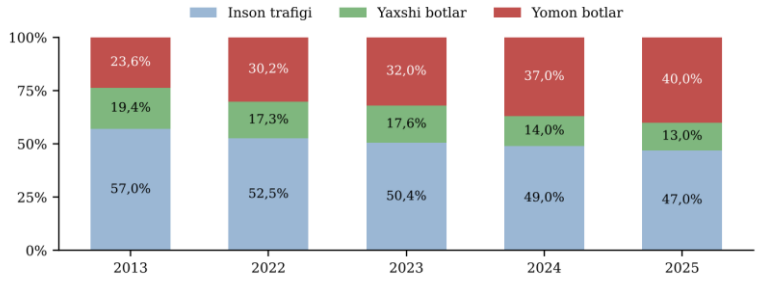
Soxta profil - haqiqiy yoki o‘ylab topilgan shaxs, tashkilot nomidan yaratilgan va foydalanuvchini chalg‘itishga mo‘ljallangan akkaunt. Bot akkaunt - faoliyati to‘liq yoki qisman dastur tomonidan boshqariladigan akkaunt; ijtimoiy bot esa inson xulq-atvorini taqlid qiladigan bot hisoblanadi [3]. Bu tushunchalar kesishadi: aksariyat botlar soxta profil sifatida ro‘yxatdan

o‘tadi, lekin odam boshqaradigan «troll» yoki ikkilamchi akkaunt ham soxta profil bo‘lishi mumkin. Amaliyotda quyidagi turlar ajratiladi: spam va reklama botlari; soxta obunachi va layk «fermalari»; firibgarlik uchun yaratilgan akkauntlar (impersonatsiya, romantik va investitsion firibgarlik); koordinatsiyalangan ta’sir kampaniyalari (botnetlar); ma’lumot yig‘uvchi skreyperlar.

Muammo ko‘lami

Thales (Imperva) hisobotiga ko‘ra, 2025 yilda veb-trafikning 53 foizi avtomatlashtirilgan manbalardan kelgan, 40 foizi zararli botlarga to‘g‘ri kelgan; sun’iy intellektga asoslangan bot hujumlari 2024 yilga nisbatan 12,5 barobar oshgan, bot hujumlarining 27 foizi to‘g‘ridan-to‘g‘ri API’larga, moliya sohasi esa hujumlarning 24 foiziga va akkauntni egallab olish holatlarining 46 foiziga duchor bo‘lgan [4]. 1-rasmda ko‘rinadiki, yomon botlar ulushi 2013 yildagi 23,6 foizdan 2025 yilda 40 foizgacha o‘sgan [4–7]. Hisobot bot-himoya vositalarini sotuvchi kompaniya tomonidan tayyorlangani uchun, uning raqamlarini mustaqil manbalar bilan solishtirish maqsadga muvofiq.

Platformalar ma’lumotlari ham shu manzarani tasdiqlaydi. Meta 2026 yil may oyida Buyuk Britaniya parlamenti qo‘mitasiga yuborgan javobida 2025 yil to‘rtinchi choragida faqat Facebook’da taxminan 1,1 milliard soxta akkaunt bo‘yicha chora ko‘rilganini bildirgan [8]; 2022 yil oxirida esa soxta akkauntlar Facebook oylik faol auditoriyasining taxminan 4–5 foizi deb baholangan edi [9]. 2025 yilda kompaniya Janubi-Sharqiy Osiyo va Yaqin Sharqdagi firibgarlik markazlari bilan bog‘liq 10,9 million akkauntni o‘chirgan va 159 milliondan ortiq firibgarlik reklamasini olib tashlagan, ularning 92 foizi shikoyatdan oldin aniqlangan [10]. Ro‘yxatdan o‘tishga urinishlarning millionlab holati bloklanadi, biroq hisobotga kiritilmaydi [11], ya’ni hujumning haqiqiy hajmi e’lon qilingandan katta.



1-rasm. Veb-trafikda inson, yaxshi va yomon botlar ulushi, 2013–2025 yillar (%)

O‘zbekiston uchun ham statistikani ehtiyot bilan talqin qilish zarur: reklama platformalari API’lariga tayangan NapoleonCat 2026 yil may oyida Facebook’da 17,35 million (aholining 49,3%), Instagram’da 17,06 million (48,5%) foydalanuvchini ko‘rsatgan [12], DataReportal esa takrorlanishlarni chiqarib, 14,1 million identifikatorni keltiradi [1]. Farq metodikaga bog‘liq, shu bois bu raqamlarni «haqiqiy odamlar soni» deb bo‘lmaydi.

Aniqlash usullari

Tadqiqotlarda aniqlash usullari dastlab uch sinfga bo‘lingan: ijtimoiy tarmoq tuzilishiga asoslangan, odam izohlovchilar (crowdsourcing) ishtirokidagi va yuqori bashoratli belgilarga tayanuvchi mashinaviy o‘qitish usullari [13]. Bugungi amaliyotda ularga evristik qoidalar, kontent tahlili va platforma darajasidagi texnik choralar qo‘shiladi (1-jadval).

1-jadval

Soxta profil va botlarni aniqlash usullarining qiyosiy tavsifi

Usul	Asosiy belgilar	Afzalligi	Cheklovi
Evristik qoidalar	Akkaunt yoshi, nom shabloni, rasm, obuna nisbati, post vaqti	Sodda, tushunarli, real vaqtda ishlaydi	Osongina aylanib o‘tiladi; yolg‘on musbat natija ko‘p
Mashinaviy o‘qitish (Botometer)	Profil, kontent, vaqt va tarmoq belgilari bo‘yicha bot balli	Ochiq vosita; katta hajmda ishlaydi	Yangi botlarda umumlashtirish; belgilangan ma’lumot yetishmasligi
Graf tahlili	Obuna, retvit, izoh aloqalari; sinxron harakat	Botnet va koordinatsiyani topadi	Haqiqiy odamlarga bog‘lanib yashiringan botlar
Kontent / LLM-aniqlash	Matn semantikasi, AIGC belgilari, xulq-atvor	LLM botlarga qarshi istiqbolli (98,46%)	Inson va sun’iy matnni ajratish qiyin; ma’lumot tez eskiradi
Platforma va gibrid choralar	Ro‘yxatdan o‘tishni nazorat, xulq-atvor signallari, shikoyatlar	Yaratish bosqichida to‘sadi	Rezident proksi orqali aylanib o‘tiladi; shaffoflik cheklangan

1. Evristik usullar. Eng sodda yondashuv akkaunt metama’lumotlari va xulq-atvoridagi shubhali belgilarni qoidalar bilan baholashdir. Odatiy indikatorlar: yaqinda yaratilgan akkauntning keskin yuqori faolligi; shablon nom (ism va uzun raqamlar qatori); bo‘sh yoki o‘g‘irlangan profil rasmi; obuna va obunachilar nisbatining nomutanosibligi; uzilishsiz yoki qat’iy vaqt oralig‘ida joylanadigan postlar; takrorlanuvchi matn va havolalar. Usul tez va tushunarli, biroq belgilarni biladigan hujumchi uni oson aylanib o‘tadi, haqiqiy yangi foydalanuvchilar ham shu belgilarga ega bo‘lishi mumkinligi sababli yolg‘on musbat natijalar ko‘payadi.

2. Mashinaviy o‘qitish. Nazoratli modellar akkaunt, kontent, vaqt va tarmoq belgilari asosida «bot ehtimoli» balini hisoblaydi. Eng mashhur misol - Indiana universitetida yaratilgan Botometer: past ball inson, yuqori ball bot ekanini bildiradi; vosita veb-interfeys va API orqali ochiq berilgan hamda yetti yildan ortiq vaqt davomida takomillashtirilgan [3, 14]. Nazoratli usullarning kuchsiz tomoni - o‘qitish ma’lumotlarining sifati va yetarliligiga bog‘liqligi hamda yangi turdagi botlarda umumlashtirishning pasayishi [15]; botlar bilan detektorlar o‘rtasidagi doimiy «poyga» tufayli modellarni muntazam qayta o‘qitish kerak [3].

3. Graf (tarmoq) tahlili. Bu yondashuvda foydalanuvchilar tugun, obuna, retvit va izoh kabi aloqalar qirra sifatida modellashtiriladi. U birgalikda harakat qiladigan botnetlarni, ayniqsa siyosat va yangiliklar mavzusidagi sinxron kampaniyalarni topishda matnga asoslangan usullardan ustun turadi [16]. Ammo haqiqiy foydalanuvchilar bilan aloqa o‘rnatib, o‘zini yashiruvchi botlar graf usullarini chalg‘itadi; bunga qarshi HOFA kabi gomofiliyaga yo‘naltirilgan graf boyitish modellari taklif qilingan [16]. Nazoratsiz usullar (masalan, CATCHSYN) faqat topologik belgilarga tayanadi, graf hajmiga nisbatan chiziqli murakkablikka ega va belgilangan ma’lumotni talab qilmaydi [15].

4. Kontent tahlili va LLM davri. Til modellari paydo bo‘lgach, matn bo‘yicha aniqlash qiyinlashdi. Yang va Menczer ChatGPT yordamida inson tilida kontent yaratgan 1140 ta akkauntdan iborat botnetni aniqladi: akkauntlar o‘g‘irlangan rasmlardan foydalangan, bir-biriga javob va retvit orqali zich klaster hosil qilgan; botnetni koordinatsiya belgilari orqali topish mumkin bo‘lgan, biroq o‘sha davrdagi ilg‘or LLM-kontent klassifikatorlari akkauntlarni

odamlardan ajrata olmagan [17]. Shundan so‘ng yangi yondashuvlar paydo bo‘ldi: 2026 yilda taklif etilgan TRACE-Bot semantik tasvirlarni va sun’iy kontentga xos xulq-atvor belgilarini ikki kanalli arxitekturada birlashtirib, LLM botlarni aniqlashda eng yuqori 98,46% aniqlikka erishgan [18]; boshqa ishda esa hujumchi botni taqlid qiluvchi «raqib» ma’lumotlar bilan o‘qitish real hayotdagi, o‘qitishda ko‘rilmagan ma’lumotlarda ham yaxshi natija berishi ko‘rsatilgan [19]. Thales hisobotiga ko‘ra, sun’iy intellekt faoliyatining katta qismi tasdiqlanmagan yoki qonuniy trafikdan farqlanmaydi [4].

5. Platforma va gibrid choralar. Meta ma’lumotiga ko‘ra, aniqlash texnologiyasi har kuni millionlab soxta akkaunt yaratishga urinishni bloklaydi va yana millionlab akkauntni yaratilgan zahoti, ko‘pincha bir necha daqiqada topadi [11]. Biroq IP-manzillarga tayanish samarasi pasaymoqda: 2023 yilda yomon bot trafikining 25,8 foizi uy provayderlari (rezident) tarmoqlaridan kelgan, ya’ni odatiy foydalanuvchidan farqlanmagan [6]. Shu bois samarali tizimlar bir nechta signalni (qurilma va xulq-atvor, graf, kontent, foydalanuvchi shikoyatlari) birlashtiradi va yakuniy qarorni shubhali holatlarda mutaxassis qabul qiladi.

6. Baholash ko‘rsatkichlari. Detektorlarni baholashda faqat umumiy aniqlik (accuracy) yetarli emas: haqiqiy akkauntlar botlardan ancha ko‘p bo‘lgani uchun sinflar nomutanosib bo‘ladi, shu sababli aniqlik (precision), to‘liqlik (recall) va F1 ko‘rsatkichlari birga keltiriladi. Yolg‘on musbat natija haqiqiy foydalanuvchining bloklanishiga, yolg‘on manfiy natija esa botning o‘tkazib yuborilishiga olib keladi; qaysi xato qimmatroq ekani muhitga bog‘liq: masalan, moliya sohasida akkauntni egallab olish xavfi yuqori [4]. TRACE-Bot’ning 98,46% natijasi muayyan tajriba sharoitidagi eng yuqori ko‘rsatkich [18], shuning uchun detektorni real, o‘qitishda ko‘rilmagan ma’lumotlarda alohida sinash zarur [19].

Aniqlash jarayonining sxemasi.

Amaliy tizimni yagona usulga emas, ketma-ket bosqichlardan iborat jarayonga qurish maqsadga muvofiq:

1) Ma’lumot yig‘ish: ochiq profil metama’lumotlari, post vaqtlari va aloqalar (qonuniy asosda, API shartlariga muvofiq).

2) Belgilarni ajratish: profil, xulq-atvor (vaqt ritmi, tezlik), kontent (takrorlar, havolalar, til) va tarmoq (aloqa zichligi, sinxronlik) belgilari.

3) Dastlabki saralash: evristik qoidalar va ML bali yordamida nomzod akkauntlarni ajratish.

4) Koordinatsiyani tekshirish: graf tahlili va klasterlash orqali o‘xshash matn, rasm yoki vaqt izli akkauntlar guruhini topish.

5) Inson tekshiruvi va javob: tasdiqlangan holatda shikoyat berish yoki cheklash, natijani hujjatlash va detektorni qayta o‘qitish.

Xulosa

Tahlil shuni ko‘rsatdiki, avtomatlashtirilgan trafik veb-trafikning yarmidan ko‘pini tashkil etadi, yomon botlar ulushi esa 2013 yildan buyon taxminan 1,7 baravar oshgan; Meta faqat 2025 yil to‘rtinchi choragida Facebook’da 1,1 milliardga yaqin soxta akkauntga chora ko‘rgan. Hech bir aniqlash usuli yagona yechim emas: evristika tez, lekin yuzaki; ML kengaytiriladigan, lekin ma’lumotga bog‘liq; graf tahlili botnetlarni ochadi, lekin yashiringan botlarga zaif; kontent tahlili LLM davrida qiyinlashmoqda. Eng samarali yo‘l - bu usullarni gibrid tizimda birlashtirish, detektorlarni muntazam yangilash va inson nazoratini saqlash. O‘zbekiston uchun asosiy yo‘nalishlar - rasmiy kanallarni tasdiqlash, foydalanuvchilar savodxonligini oshirish va mahalliy tilda (o‘zbek lotin va kirill yozuvida) belgilangan ma’lumotlar to‘plamlarini yaratishdir.

Foydalanilgan adabiyotlar

1. DataReportal. Digital 2026: Uzbekistan.
2. Toshkent shahar hokimligining soxta akkauntlar haqidagi ogohlantirishi.
3. Yang K.-C. va b. Arming the public with artificial intelligence to counter social bots.
4. Thales. 2026 Bad Bot Report: Bad Bots in the Agentic Age.
5. Thales. 2025 Imperva Bad Bot Report.
6. Thales. 2024 Imperva Bad Bot Report.
7. Daily Hive. Imperva Bad Bot Report 2023.
8. Meta. Response to the UK Parliament Science, Innovation & Technology Committee.
9. Social Media Today. Meta Community Standards Enforcement Report, Q4 2022.
10. Meta. Integrity Reports, H1 2026.
11. Meta. Community Standards Enforcement Report: Fake Accounts.
12. NapoleonCat. Social media users in Uzbekistan, 2026.
13. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots. Communications of the ACM, 2016.
14. Social Bots: Detection and Challenges.
15. A comparative study of bot detection techniques with an application related to Covid-19 discourse on Twitter.
16. Social Media Bot Detection Research: Review of Literature.
17. Yang K.-C., Menczer F. Anatomy of an AI-powered malicious social botnet. Journal of Quantitative Description: Digital Media, 2024, vol. 4.
18. TRACE-Bot: Detecting Emerging LLM-Driven Social Bots via Implicit Semantic Representations and AIGC-Enhanced Behavioral Patterns.
19. Adversarial Creation and Detection of AI-Generated Social Bot Content.

SOXTA PROFIL VA BOT AKKAUNTLARNI ANIQLASH ALGORITMLARINING TWIBOT-22 BENCHMARKI ASOSIDA QIYOSIY TAHLILI

Qudratov U.I., Eshmurodov A.A.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Maqolada ijtimoiy tarmoqlarda soxta profil va bot akkauntlarni aniqlovchi algoritmlar tizimlashtirilgan: belgilarga asoslangan nazoratli modellar (Botometer v4), matnga asoslangan chuqur modellar, graf neyron tarmoqlari (BotRGCN), nazoratsiz klasterlash va katta til modellari (LLM). TwiBot-22 benchmarki natijalari asosida algoritmlarning aniqligi va F1 ko‘rsatkichlari qiyoslangan, ularning umumlashtirish, yolg‘on musbat natija va manipulyatsiyaga chidamlilik bo‘yicha cheklovlari tahlil qilingan. Tadqiqot natijalariga tayanib, o‘zbek tili va O‘zbekiston sharoiti uchun gibrid aniqlash sxemasi taklif etilgan.

Kalit so‘zlar: bot aniqlash algoritmi, soxta profil, graf neyron tarmog‘i, Botometer, TwiBot-22, LLM, F1-ko‘rsatkich.

Аннотация. В статье систематизированы алгоритмы выявления фейковых профилей и бот-аккаунтов в социальных сетях: контролируемые модели на основе признаков (Botometer v4), глубокие текстовые модели, графовые нейронные сети (BotRGCN), неконтролируемая кластеризация и большие языковые модели (LLM). По результатам бенчмарка TwiBot-22 сопоставлены точность и F1-мера алгоритмов, проанализированы их ограничения: обобщающая способность, ложноположительные срабатывания и устойчивость к манипуляциям. На основе полученных результатов предложена гибридная схема выявления для узбекоязычной среды и условий Узбекистана.

Ключевые слова: алгоритм выявления ботов, фейковый профиль, графовая нейронная сеть, Botometer, TwiBot-22, LLM, F1-мера.

Thales (Imperva) hisobotiga ko‘ra, 2025 yilda veb-trafikning 53 foizi avtomatlashtirilgan manbalardan kelgan, 40 foizi zararli botlarga to‘g‘ri kelgan, sun’iy intellektga asoslangan bot hujumlari esa 2024 yilga nisbatan 12,5 barobar oshgan [1]. Meta 2025 yil to‘rtinchi choragida faqat Facebook’da taxminan 1,1 milliard soxta akkaunt bo‘yicha chora ko‘rgan [2], bunda ro‘yxatdan o‘tishga urinishlarning millionlab holati bloklanadi, ammo statistikaga kiritilmaydi [3]. Bu ko‘lamda akkauntlarni qo‘lda tekshirish mumkin emas, shu bois ularni aniqlash algoritmik masalaga aylangan.

O‘zbekistonda 2025 yil oktyabrida 14,1 million ijtimoiy tarmoq foydalanuvchi identifikatori qayd etilgan, bu aholining 37,9 foizi [4]. Ichki ishlar vazirligi ma’lumotiga ko‘ra, kiberjinoyatlarning ulushi 2023 yildagi 6,2 foizdan 2024 yilda 44,4 foizga o‘sgan, onlayn savdo platformalaridagi firibgarlik esa kiberjinoyatlarning 11 foizini tashkil etgan [5]; 2026 yil iyunida esa sotuvchi yoki xaridor nomidan aldash usuli 18 foiz ulush bilan alohida ko‘rsatilgan [6]. Soxta profil bu sxemalarning asosiy quroli: 2024 yil oktyabrida Toshkent shahar IIBB tashkilot rahbarlari nomidan ochilgan soxta Telegram akkauntlari orqali xodimlardan ma’lumot olib, bank kartalaridan pul yechib olingani haqida ogohlantirgan [7], 2026 yil yanvarida hokimlik ham shunday akkauntlar haqida xabar bergan [8]. Maqolaning maqsadi - mavjud aniqlash algoritmlarini tizimlashtirish, ularning samaradorligi va cheklovlarini ochiq benchmark natijalari asosida qiyoslash hamda gibrid sxema taklif etish.

Masalaning qo‘yilishi va benchmark ma’lumotlari.

Aniqlash - ikkilik klassifikatsiya masalasi: har bir akkaunt u uchun profil, kontent va xulq-atvor belgilari vektori x(u) hamda aloqalar grafi G = (V, E) berilgan; f(u) ∈ [0, 1] funksiya «bot ehtimoli»ni baholaydi va f(u) ≥ τ bo‘lganda akkaunt bot deb belgilanadi. Tadqiqotlarda usullar odatda uch sinfga ajratiladi: ijtimoiy tarmoq tuzilishiga asoslangan, odam izohlovchilar ishtirokidagi va belgilarga tayanuvchi mashinaviy o‘qitish usullari [9]. Sinflar nomutanosib: eng yirik ochiq benchmark TwiBot-22 da 1 000 000 foydalanuvchining 139 943 tasi bot, 860 057 tasi inson (taxminan 14% bot); ma’lumotlar 88,2 million tvit, 92,9 million tugun va 170,2 million qirradan iborat graf bo‘lib, 4 ob’ekt turi va 14 aloqa turini o‘z ichiga oladi, yorliqlar 1000 ta ekspert izohi asosida zaif nazorat orqali berilgan (yorliq aniqligi 90,5%) [10]. Algoritmlar kirishida ishlatiladigan belgilar 1-jadvalda guruhlangan.

1-jadval

Aniqlash algoritmlarida ishlatiladigan belgilar guruhlari (muallif tasnifi)

Belgilar guruhi	Misollar	Shubhali signal	Kim foydalanadi
Profil	Akkaunt yoshi, nom shabloni, rasm, bio to‘liqligi	Yangi akkaunt, raqamli shablon nom, bo‘sh yoki takrorlangan profil	Evristika, Random Forest/ESC
Vaqt va xulq-atvor	Post vaqti ritmi, faollik tezligi, kunlik tsikl	Sutka davomida uzilishsiz yoki aniq ritmli faollik	Evristika, Random Forest/ESC
Kontent	Matn takrori, havola ulushi, til, mavzu	Shablon matn, spam havolalar	Random Forest, RoBERTa/T5, LLM
Tarmoq (graf)	Obuna/obunachi nisbati, aloqa zichligi, o‘zaro javoblar	Zich klasterlar, sinxron obuna va retvit	GCN, GAT, BotRGCN
Koordinatsiya	Bir vaqtda bir xil matn yoki rasm tarqatish	Guruh bo‘lib harakat qiluvchi akkauntlar	Klasterlash (CATCHSYN)

Sinflar nomutanosibligi sababli faqat aniqlik (accuracy) emas, precision, recall va F1 ko‘rsatkichlari birga keltiriladi va quyidagicha hisoblanadi: precision = TP / (TP + FP), recall = TP / (TP + FN), F1 = 2 · precision · recall / (precision + recall); bu yerda TP - to‘g‘ri topilgan bot, FP - bot deb belgilangan haqiqiy foydalanuvchi, FN - o‘tkazib yuborilgan bot.

Aniqlash algoritmlari tahlili.

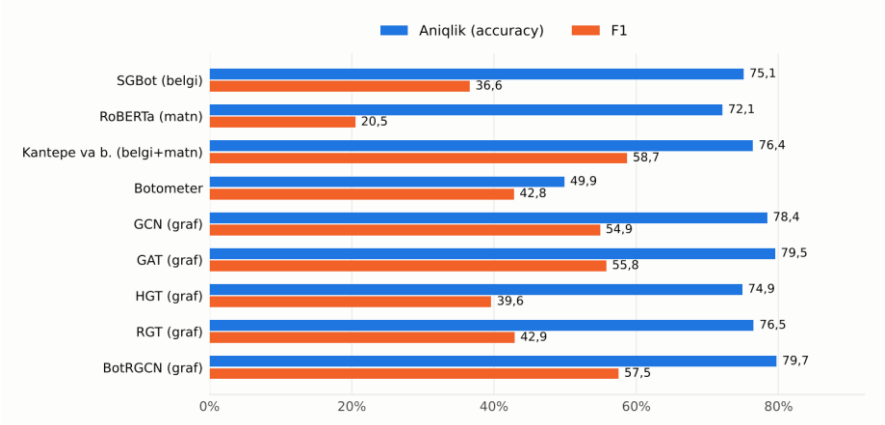
1. Belgilarga asoslangan nazoratli algoritmlar. Klassik yondashuvda akkauntdan yuzlab belgi ajratiladi va Random Forest yoki gradient boosting kabi klassifikator o‘qitiladi. Eng keng tarqalgan misol - Botometer v4: u ixtisoslashgan klassifikatorlar ansambli (ESC) arxitekturasiga o‘tgan, bunda umumiy «inson» klassifikatori bilan birga har bir bot sinfi (astroturf, soxta obunachi, moliyaviy, o‘zini e’lon qilgan, spammer, boshqa) uchun alohida klassifikator o‘qitiladi [11, 12]. Har biri 100 daraxtli Random Forest bo‘lib, yakuniy ball $1 - s_0$ va sinf ballaridan eng kattasi sifatida tanlanadi va Platt kalibrlashidan o‘tkaziladi; 1200 dan ortiq belgi olti toifaga bo‘lingan [11]. Botometer mualliflarining sinovlarida ESC yangi (o‘qitishda ko‘rilmagan) ma’lumotlarda recall’ni 42% dan 84% gacha, F1 ni 47% dan 73% gacha oshirgan; joriy versiyaning o‘zaro tekshiruvdagi AUC qiymati 0,99, javob vaqti 100 ms dan kam, kuniga yarim milliondan ortiq so‘rovga xizmat qiladi [11].

2. Matnga asoslangan chuqur modellar. RoBERTa, T5 kabi til modellari tvit va bio matnini vektorga aylantirib, bot ehtimolini bashorat qiladi va qo‘lda belgi tanlashni talab qilmaydi.

Biroq TwiBot-22 da faqat matnga tayangan RoBERTa 72,1% aniqlikka, lekin atigi 20,5% F1 ga erishgan (1-rasm) [10]: matnning o‘zi nomutanosib sinfda botlarni yetarli to‘liqlik bilan ajrata olmaydi, ayniqsa botlar inson matnini taqlid qilganda.

3. Graf algoritmlari. Graf yondashuvida foydalanuvchilar tugun, obuna, retvit, izoh kabi munosabatlar qirra bo‘lib, GCN, GAT yoki relyatsion R-GCN kabi neyron tarmoqlar qo‘shnilar signalini yig‘adi. BotRGCN obuna munosabatlaridan geterogen graf quradi va R-GCN’ni ko‘p modalli foydalanuvchi ma’lumotiga (semantik va xossa belgilari) qo‘llaydi, bu qo‘lda belgi tanlashni kamaytiradi va turlicha niqoblangan botlarni ushlashga yordam beradi [13]. TwiBot-22 da BotRGCN eng yuqori aniqlikka (79,7%), GAT 79,5% ga, GCN 78,4% ga erishgan; F1 bo‘yicha esa belgi va matnni qo‘shgan Kantepe va b. modeli (58,7%) BotRGCN (57,5%) dan sal oldinda [10]. Mualliflar graf komponenti olib tashlanganda sifat pasayishini va BotRGCN’ning jamoalararo umumlashtirishi eng yaxshi ekanini qayd etgan [10]. Bu metrika tanlovi reytingni o‘zgartirishi mumkinligini ko‘rsatadi.

4. Nazoratsiz algoritmlar va koordinatsiyani aniqlash. Belgilangan ma’lumot yetishmaganda nazoratsiz usullar qo‘l keladi: masalan, CATCHSYN faqat graf topologiyasidan foydalanadi va graf hajmiga nisbatan chiziqli murakkablikka ega [14]. Bunday usullar yakka bot emas, birgalikda harakat qiluvchi guruhni topadi: Yang va Menczer o‘rganilgan ChatGPT-botnetdagi 1140 ta akkauntni aynan o‘xshash xulq-atvor va o‘zaro javoblardan hosil bo‘lgan zich klaster orqali aniqlagan [15]. Shu bilan birga haqiqiy foydalanuvchilarga bog‘lanib yashiringan botlar graf usullarining zaif joyi bo‘lib qolmoqda [16].



1-rasm. TwiBot-22 benchmarkida tanlab olingan 9 algoritmning aniqligi (accuracy) va F1 ko‘rsatkichi, %.

5. LLM asosidagi algoritmlar. Instruksiya bilan sozlangan til modellari atigi 1000 ta belgilangan misolda ilg‘or usullardan ustun kelgan: ChatGPT ansambli F1 bo‘yicha TwiBot-20 da 2,6%, TwiBot-22 da 9,1% yaxshiroq natija bergan [17]. Ammo xuddi shu tadqiqotda LLM yordamida matn va obuna tarmog‘ini manipulyatsiya qilish mavjud detektorlar samaradorligini 29,6% gacha tushirgan, ishonch bahosining kalibrlash xatosi esa o‘rtacha 28,4% ga oshgan [17]. BotSim (AAAI-25) ham an’anaviy ma’lumotlarda yaxshi ishlagan usullar LLM-botlardan iborat BotSim-24 to‘plamida yomonlashishini ko‘rsatgan [18]. TRACE-Bot semantik tasvir va sun’iy kontentga xos xulq-atvor belgilarini ikki kanalda birlashtirib, o‘z tajribalarida 98,46% gacha aniqlikka erishgan [19].

6. Masshtablanish. Amaliy tizimda algoritm tezligi aniqlik kabi muhim: TwiBot-22 da bir qator baseline usullar katta hajm tufayli umuman ishlay olmagan [10], ESC esa bitta so‘rovga 100 millisekunddan kam vaqt sarflaydi [11]. Shu bois onlayn rejimda yengil algoritmlar (evristika, Random Forest) qo‘llanib, og‘ir graf va LLM modellari faqat shubhali akkauntlar uchun ishga

tushirilishi maqsadga muvofiq; aynan shu g‘oya «Taklif etiladigan gibrid sxema» bo‘limidagi sxemaga asos qilingan.

2-jadval

Soxta profil va botlarni aniqlash algoritmlari oilalarining qiyosiy tavsifi

Algoritm oilasi	Kirish	Vakili	Kuchli tomoni	Cheklovi
Belgilarga asoslangan nazoratli (Random Forest)	Profil, kontent, vaqt belgilari	Botometer v4 (ESC) [11, 12]	Tez (<100 ms), natijani izohlash mumkin	Belgilarni qo‘lda tanlash; yangi botlarda umumlashtirish zaif
Matnga asoslangan chuqur modellar	Tvit va bio matni	RoBERTa, T5 [10]	Belgi muhandisligi talab qilinmaydi	Yolg‘iz matn yetarli emas (F1 20,5%); LLM-botlarga zaif
Graf neyron tarmoqlari	Aloqalar grafi + profil belgilari	GCN, GAT, BotRGCN [10, 13]	Eng yuqori aniqlik (79,7%); koordinatsiyani ko‘radi	Katta graf kerak; haqiqiy foydalanuvchilarga bog‘langan botlar
Nazoratsiz usullar va klasterlash	Topologiya, o‘xshashlik izlari	CATCHSYN [14]	Belgilangan ma’lumot shart emas; chiziqli murakkablik	Faqat guruhlarni topadi, yakka botni emas
Til modellari (LLM)	Profil va matn «prompt» ko‘rinishida	Instruksiya bilan sozlangan LLM [17]	1000 misol bilan ilg‘or usullardan ustun	Manipulyatsiyaga ta’sirchan; ishonch bahosi buziladi

Baholash muammolari va cheklovlari.

Umumlashtirish. TwiBot-22 dagi baseline algoritmlar o‘rtacha TwiBot-20 ga nisbatan 2,7% past natija bergan [10]; tayyor Botometer bu benchmarkda 49,9% aniqlik va 42,8% F1 ko‘rsatgan (1-rasm). Demak, bir ma’lumotlar to‘plamida yaxshi ishlagan vosita boshqasida shunday natija berishi kafolatlanmagan. Yolg‘on musbat natija. Rauchfleisch va Kaiser ingliz va nemis tilidagi 4134 ta akkaunt ustida Botometer ballari chegaralari vaqt o‘tishi bilan o‘zgarishini, buning natijasida inson ham bot deb, bot ham inson deb baholanishini ko‘rsatgan [20]. Qarama-qarshi manipulyatsiya. LLM yordamida matn va obunalarni o‘zgartirish detektor ishonchini pasaytiradi [17]. Shu sababli LLM-detektor natijasi dastlabki saralash sifatida qaralib, yakuniy qaror inson tekshiruvida qoldirilishi tavsiya etiladi [17].

Baholash protokoli. Algoritmlarni adolatli qiyoslash uchun: (1) sinflar nomutanosibligida aniqlik bilan birga precision, recall va F1 keltirilsin; (2) model o‘qitishda ko‘rilmagan jamoada yoki boshqa ma’lumotlar to‘plamida sinalsin [10]; (3) ishonch bahosining kalibrlanganligi tekshirilsin [17]; (4) joriy etishdan oldin yolg‘on musbat natijalar qo‘lda audit qilinsin [20].

O‘zbekiston uchun xulosa va tavsiyalar

Tahlil shuni ko‘rsatdiki, graf neyron tarmoqlari eng yuqori aniqlikni bersa-da, F1 bo‘yicha belgi va matnni birlashtirgan modellar ham raqobatbardosh; LLM-detektorlar kuchli, ammo manipulyatsiyaga ta’sirchan. Shu bois amaliy tizim yagona algoritmga emas, gibrid va inson nazorati ostidagi sxemaga tayanishi lozim. O‘zbekiston uchun: (1) Botometer v4 ingliz tiliga mo‘ljallangan lingvistik belgilar o‘rniga tilga bog‘liq bo‘lmagan ballni ham beradi [12], shuning uchun o‘zbek matnlarida dastlab tilga bog‘liq bo‘lmagan belgilarga (akkaunt yoshi, faollik tezligi,

graf) tayanish maqsadga muvofiq; (2) o‘zbek tilida (lotin va kirill yozuvida) belgilangan ma’lumotlar to‘plamini yaratish va detektorlarni muntazam qayta o‘qitish zarur; (3) Telegram va Instagram’dagi rahbarlar nomidan ochiladigan akkauntlar uchun rasmiy kanallar ro‘yxatini e’lon qilish va shubhali murojaatni mustaqil kanal orqali tekshirish tartibini joriy etish kerak [7, 8]; (4) tizim samaradorligini aniqlik bilan birga precision, recall va F1 bo‘yicha o‘lchab borish lozim.

Foydalanilgan adabiyotlar

1. Thales. 2026 Bad Bot Report: Bad Bots in the Agentic Age.
2. Meta. Response to the UK Parliament Science, Innovation & Technology Committee.
3. Meta. Community Standards Enforcement Report: Fake Accounts.
4. DataReportal. Digital 2026: Uzbekistan.
5. O‘zbekiston Respublikasi IIV Kiberxavfsizlik markazi axboroti.
6. IIV Kiberjinoyatlarga qarshi kurashish departamenti boshlig‘ining Senat majlisidagi ma’ruzasi.
7. Scammers target employees via fake Telegram accounts of high-ranking officials.
8. Toshkent shahar hokimligining soxta akkauntlar haqidagi ogohlantirishi.
9. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The rise of social bots. Communications of the ACM, 2016.
10. Feng S. va b. TwiBot-22: Towards Graph-Based Twitter Bot Detection. NeurIPS 2022, Datasets and Benchmarks.
11. Sayyadiharikandeh M., Varol O., Yang K.-C., Flammini A., Menczer F. Detection of Novel Social Bots by Ensembles of Specialized Classifiers. CIKM 2020.
12. Indiana University CNetS. Botometer V4.
13. Feng S., Wan H., Wang N., Luo M. BotRGCN: Twitter Bot Detection with Relational Graph Convolutional Networks.
14. A comparative study of bot detection techniques with an application related to Covid-19 discourse on Twitter.
15. Yang K.-C., Menczer F. Anatomy of an AI-powered malicious social botnet. Journal of Quantitative Description: Digital Media, 2024, vol. 4.
16. Social Media Bot Detection Research: Review of Literature. arXiv:2503.22838, 2025.
17. Feng S., Wan H., Wang N., Luo M., Tan Z., Tsvetkov Y. What Does the Bot Say? Opportunities and Risks of Large Language Models in Social Media Bot Detection.
18. Qiao B. va b. BotSim: LLM-Powered Malicious Social Botnet Simulation. AAAI-25, vol. 39, no. 13, 2025, pp. 14377–14385.
19. TRACE-Bot: Detecting Emerging LLM-Driven Social Bots via Implicit Semantic Representations and AIGC-Enhanced Behavioral Patterns.
20. Rauchfleisch A., Kaiser J. The false positive problem of automatic bot detection in social science research. PLOS ONE, 2020.

МЕТОДЫ ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ НА ОСНОВЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Хамидов Ш.Ж.
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Аннотация. В работе рассматриваются методы предотвращения, обнаружения и расследования утечек конфиденциальной информации с использованием технологии цифровых водяных знаков (Digital Watermarking). Проведён сравнительный анализ методов пространственного и частотного встраивания, цифровых отпечатков пользователей (Digital Fingerprinting), а также современных подходов к маркированию документов и цифрового контента. Предложена концептуальная модель защиты корпоративной информации, основанная на персонализированном внедрении цифровых водяных знаков, криптографической идентификации и анализе устойчивости маркировки к модификациям. Рассмотрены математические модели встраивания и извлечения водяных знаков, критерии оценки надёжности и возможности интеграции технологии с системами предотвращения утечек данных (DLP).

Ключевые слова: информационная безопасность, утечка данных, цифровые водяные знаки, Digital Watermarking, DLP, Digital Fingerprinting, защита документов, DCT, DWT, идентификация источника утечки.

Annotatsiya. Ushbu ishda raqamli suv belgilari (Digital Watermarking) texnologiyasidan foydalangan holda maxfiy axborot sizib chiqishining oldini olish, ularni aniqlash va axborot sizib chiqishi bilan bog‘liq hodisalarni tekshirish usullari ko‘rib chiqilgan. Raqamli suv belgilarini fazoviy va chastotaviy sohalarda joylashtirish usullari, foydalanuvchilarning raqamli barmoq izlari (Digital Fingerprinting), shuningdek, elektron hujjatlar va raqamli kontentni markirovkalashning zamonaviy yondashuvlari qiyosiy tahlil qilingan. Raqamli suv belgilarini individuallashtirilgan tarzda joylashtirish, kriptografik identifikatsiya va markirovkaning turli o‘zgartirishlarga nisbatan bardoshliligini tahlil qilishga asoslangan korporativ axborotni himoyalashning konseptual modeli taklif etilgan. Raqamli suv belgilarini joylashtirish va ajratib olishning matematik modellari, ishonchlilikni baholash mezonlari hamda ushbu texnologiyani axborot sizib chiqishining oldini olish tizimlari (DLP) bilan integratsiyalash imkoniyatlari ko‘rib chiqilgan.

Kalit so‘zlar: axborot xavfsizligi, axborot sizib chiqishi, raqamli suv belgilari, Digital Watermarking, DLP, Digital Fingerprinting, hujjatlarni himoyalash, DCT, DWT, axborot sizib chiqish manbasini aniqlash.

Введение

В условиях цифровой трансформации организаций защита конфиденциальной информации становится одной из ключевых задач информационной безопасности. Расширение использования облачных сервисов, корпоративных информационных систем, электронного документооборота и удалённого доступа увеличивает количество потенциальных каналов несанкционированного распространения данных.

Традиционные механизмы защиты, включая шифрование, разграничение прав доступа и системы Data Loss Prevention (DLP), направлены преимущественно на ограничение несанкционированного доступа и передачи информации. Однако после

получения пользователем легитимного доступа к документу полностью исключить его дальнейшее распространение затруднительно.

Одним из перспективных дополнительных механизмов защиты является технология цифровых водяных знаков, позволяющая внедрять идентификационные сведения непосредственно в структуру цифрового объекта. В отличие от обычных метаданных, водяной знак может сохраняться после определённых преобразований содержимого, что позволяет использовать его для установления происхождения обнаруженной копии.

Анализ существующих методов цифрового маркирования

Цифровой водяной знак представляет собой специальную последовательность данных, внедряемую в цифровой объект для подтверждения его происхождения, проверки целостности или идентификации получателя.

Методы маркирования включают пространственные (LSB), частотные (DCT, DWT), матричные (SVD) и обучаемые алгоритмы. Персонализированное цифровое отпечатывание (fingerprinting) представляет отдельный механизм идентификации получателя и может применяться совместно с перечисленными алгоритмами.

Таблица 1

Методы цифрового маркирования

Метод	Принцип работы	Преимущества	Ограничения
LSB	Изменение младших битов цифрового представления	Простота, высокая ёмкость	Низкая устойчивость к преобразованиям
DCT	Встраивание в коэффициенты дискретного косинусного преобразования	Устойчивость к некоторым видам сжатия	Чувствительность к сильным изменениям изображения
DWT	Маркирование коэффициентов вейвлет-преобразования	Многоуровневое представление сигнала	Повышенная вычислительная сложность
SVD	Модификация сингулярных значений матрицы	Возможность устойчивого встраивания	Риск ложного подтверждения в отдельных схемах
Fingerprinting	Уникальная маркировка экземпляра для каждого пользователя	Идентификация источника распространения	Требует устойчивого кодирования и учёта сговора
Нейросетевые методы	Обучаемое встраивание и обнаружение	Адаптация к определённым искажениям	Зависимость от обучающих данных и модели угроз

Для защиты корпоративных документов особенно важна персонализация каждой выдаваемой копии. При этом обнаружение маркировки указывает на происхождение экземпляра, но само по себе не является достаточным доказательством виновности пользователя: необходимы журналы доступа и проверка возможной компрометации учётной записи.

Математическая модель внедрения цифрового водяного знака

Общая модель внедрения цифрового водяного знака может быть представлена следующим выражением:

$$Y = E(X, W, K, \alpha)$$

где X - исходный цифровой объект; W - идентификационная последовательность; K - секретный ключ; α - параметр интенсивности внедрения; E - функция маркирования; Y - защищённый цифровой объект.

Для частотного метода на основе DCT может применяться аддитивная модель изменения выбранных коэффициентов:

$$C_i' = C_i + \alpha W_i$$

где C_i и C_i'- коэффициенты до и после внедрения; $W_i \in \{-1, +1\}$ - элемент водяного знака.

Извлечение маркировки выполняется функцией:

$$\widehat{W} = D(Y', K)$$

где Y' - исследуемая копия, которая могла подвергнуться модификациям, а D - алгоритм обнаружения или извлечения.

В частном случае обнаружения с известным исходным объектом оценка маркировки может быть получена как:

$$\widehat{W}_i = \frac{C_i' - C_i}{\alpha}$$

Следует учитывать, что последнее выражение справедливо для указанной аддитивной модели при наличии исходных коэффициентов и отсутствии существенных искажений. Для практических DLP-систем предпочтительны схемы, допускающие проверку без хранения и непосредственного сравнения каждой исходной копии.

2.3. Персонализированная маркировка и идентификация источника утечки

Для повышения эффективности расследования утечек предлагается формировать индивидуальный цифровой отпечаток для каждого пользователя:

$$W_u = \mathrm{PRF}_K(ID_u \parallel ID_d \parallel V)$$

где ID_u - идентификатор пользователя, ID_d - идентификатор документа, V - версия документа, PRF_K - криптографическая псевдослучайная функция с секретным ключом K.

Полученная последовательность используется как основа персонализированного водяного знака. При обнаружении несанкционированно распространённого документа выполняется извлечение маркировки и сопоставление с зарегистрированными идентификаторами.

Для оценки совпадения может применяться нормализованная корреляция:

$$\rho(W_u, \widehat{W}) = \frac{\sum_{i=1}^{n}(W_{u,i} - \bar{W}_u)\left(\widehat{W}_i - \overline{\widehat{W}}\right)}{\sqrt{\sum_{i=1}^{n}(W_{u,i} - \bar{W}_u)^2}\sqrt{\sum_{i=1}^{n}\left(\widehat{W}_i - \overline{\widehat{W}}\right)^2}}$$

Если ρ превышает установленный порог τ, система фиксирует вероятное совпадение с маркировкой соответствующего пользователя. Порог должен определяться экспериментально с учётом допустимой вероятности ложного обвинения.

При возможном сговоре нескольких пользователей целесообразно использовать специальные коды цифровых отпечатков. В работе G. Tardos показано, что для вероятностных кодов, устойчивых к сговору до с участников, длина кода может иметь асимптотический порядок:

$$L = O\left(c^2 \log \frac{N}{\varepsilon}\right)$$

где N - количество пользователей, c - максимальное число участников сговора, ε - допустимая вероятность ошибки в соответствующей модели.

Это делает коды Тардоша теоретически обоснованным инструментом для систем отслеживания распространения конфиденциальных копий документов.

Для реализации предлагается следующий алгоритм: (1) проверить права доступа; (2) сформировать идентификатор экземпляра на основе идентификаторов пользователя, документа и версии; (3) закодировать последовательность с коррекцией ошибок и внедрить её в выбранное представление документа; (4) зарегистрировать выдачу, ключевую версию и контрольный хеш; (5) при обнаружении копии извлечь маркировку; (6) сопоставить её с реестром и вычислить статистику совпадения; (7) провести независимую проверку журналов событий. Порог совпадения необходимо выбирать на контрольной выборке для ограничения частоты ложных обвинений.

Предлагаемая модель является проектной: выбор алгоритма встраивания зависит от формата носителя (например, растровая страница PDF, изображение или текст). Для текстовых документов нельзя автоматически переносить показатели устойчивости DCT/DWT, полученные для изображений.

Предлагаемая архитектура системы защиты от утечек

Предлагается интегрировать персонализированное цифровое маркирование в корпоративную систему документооборота с последующим подключением механизмов DLP-мониторинга.

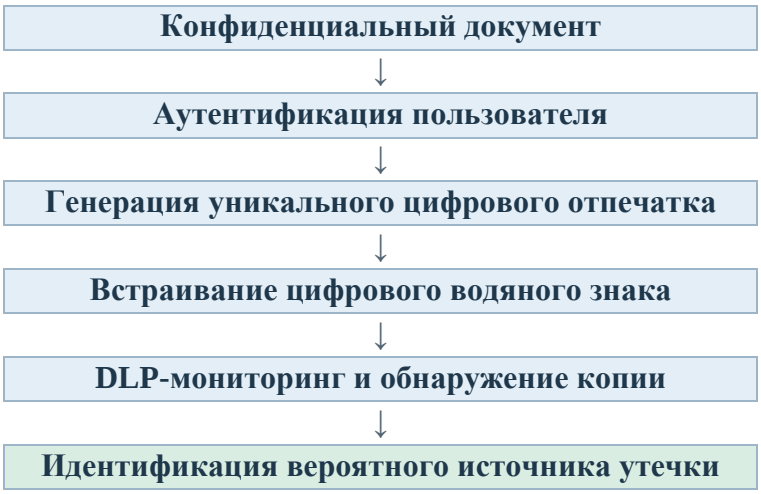


Рис. 1. Концептуальная схема маркирования и последующей идентификации источника утечки

Алгоритм функционирования системы включает аутентификацию пользователя, формирование индивидуального идентификатора, внедрение маркировки в документ, регистрацию параметров выдачи и последующий анализ обнаруженных копий.

При этом цифровые водяные знаки не заменяют механизмы контроля доступа и предотвращения передачи информации. Они дополняют DLP-системы возможностью атрибуции источника после факта распространения данных.

Заключение

В работе рассмотрены основные методы защиты информации от утечек на основе цифровых водяных знаков и проанализированы их функциональные возможности, преимущества и ограничения.

Установлено, что методы пространственного маркирования отличаются простотой реализации, тогда как частотные методы DCT и DWT предоставляют дополнительные

возможности для повышения устойчивости маркировки к отдельным видам преобразований. Применение персонализированных цифровых отпечатков позволяет расширить функциональность системы защиты за счёт идентификации вероятного источника несанкционированного распространения данных.

Предложена концептуальная модель интеграции цифрового маркирования с корпоративными DLP-системами, предусматривающая генерацию индивидуальных отпечатков, встраивание маркировки, регистрацию выдаваемых документов и последующую проверку обнаруженных копий.

Основной вывод исследования заключается в том, что цифровые водяные знаки следует рассматривать не как самостоятельное средство предотвращения всех утечек, а как дополнительный механизм прослеживаемости и расследования инцидентов информационной безопасности. Дальнейшие исследования целесообразно направить на экспериментальное сравнение устойчивости алгоритмов, снижение вероятности ложной идентификации и разработку гибридных методов маркирования электронных документов.

Список использованной литературы

1. Cox I. J., Kilian J., Leighton F. T., Shamoon T. Secure Spread Spectrum Watermarking for Multimedia // IEEE Transactions on Image Processing. - 1997. - Vol. 6, No. 12. - P. 1673–1687. DOI: 10.1109/83.650120.

2. Boneh D., Shaw J. Collusion-Secure Fingerprinting for Digital Data // IEEE Transactions on Information Theory. - 1998. - Vol. 44, No. 5. - P. 1897–1905. DOI: 10.1109/18.705568.

3. Tardos G. Optimal Probabilistic Fingerprint Codes // Journal of the ACM. - 2008. - Vol. 55, No. 2. - Article 10. DOI: 10.1145/1346330.1346335.

4. Barni M., Bartolini F., Furon T. A General Framework for Robust Watermarking Security // Signal Processing. - 2003. DOI: 10.1016/S0165-1684(03)00168-3.

5. Song C.-L., Yang L., Wang X. Secure and Robust Digital Watermarking: A Survey // Journal of Electronic Science and Technology. - 2016. - Vol. 14, No. 4. - P. 343–354. DOI: 10.11989/JEST.1674-862X.506081.

6. Kadian P., Arora S. M., Arora N. Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey // Wireless Personal Communications. - 2021. DOI: 10.1007/s11277-021-08177-w.

7. Uchida Y., Nagai Y., Sakazawa S., Satoh S. Embedding Watermarks into Deep Neural Networks // Proceedings of the ACM International Conference on Multimedia Retrieval. - 2017. - P. 269–277. DOI: 10.1145/3078971.3078974.

8. Kirchenbauer J., Geiping J., Wen Y., Katz J., Miers I., Goldstein T. A Watermark for Large Language Models // Proceedings of the 40th International Conference on Machine Learning. - 2023. - Vol. 202. - P. 17061–17084. URL: https://proceedings.mlr.press/v202/kirchenbauer23a.html.

9. Digital Watermarking - A Meta-Survey and Techniques for Fake News Detection // IEEE Access. - 2024. DOI: 10.1109/ACCESS.2024.3374201.

RAQAMLI KRIMINALISTIKADAGI ZAMONAVIY YUTUQLAR: SUN'IY INTELLEKT VA BULUTLI MUHITDAN RAQAMLI DALILLARNI OLISH ISTIQBOLLARI

Rahmonov N.S.
Farg'ona davlat texnika universiteti

Annotatsiya. Maqolada raqamli kriminalistika sohasidagi zamonaviy yutuqlar, xususan sun'iy intellekt vositalarining raqamli dalillarni qayta ishlashdagi o'rni hamda bulutli muhitdan dalillarni yig'ish bilan bog'liq muammolar tahlil qilingan. Raqamli kriminalistikaning asosiy yo'nalishlari (kompyuter, mobil qurilma, tarmoq va bulutli kriminalistika) qiyosiy ko'rib chiqilgan, dalillarning yaxlitligi va qonuniy kuchini ta'minlashga qaratilgan tavsiyalar berilgan. Tadqiqot natijalari zamonaviy avtomatlashtirilgan vositalar tergov jarayonini tezlashtirishini, biroq ekspert nazoratini va xalqaro standartlarga rioya qilishni bekor qilmasligini ko'rsatdi.

Kalit so'zlar: raqamli kriminalistika, raqamli dalil, sun'iy intellekt, bulutli kriminalistika, dalillar yaxlitligi, xesh-qiymat.

Аннотация. В статье проанализированы современные достижения цифровой криминалистики, в частности роль средств искусственного интеллекта в обработке цифровых доказательств, а также проблемы сбора доказательств из облачной среды. Сравнительно рассмотрены основные направления цифровой криминалистики (компьютерная, мобильная, сетевая и облачная), даны рекомендации по обеспечению целостности и юридической силы доказательств. Результаты исследования показали, что современные автоматизированные средства ускоряют расследование, однако не отменяют необходимости экспертного контроля и соблюдения международных стандартов.

Ключевые слова: цифровая криминалистика, цифровое доказательство, искусственный интеллект, облачная криминалистика, целостность доказательств, хеш-значение.

Kirish

Raqamli texnologiyalarning jadal rivojlanishi jinoyatchilikning shakli va usullarini tubdan o'zgartirmoqda. Bugungi kunda deyarli har bir jinoyat ishida kompyuter, smartfon, ijtimoiy tarmoq, bulutli xizmat yoki boshqa raqamli izlar mavjud bo'ladi. Shu sababli raqamli kriminalistika - raqamli qurilmalardan olingan ma'lumotlarni aniqlash, saqlash, tahlil qilish va sudda taqdim etish bilan shug'ullanuvchi fan va amaliyot sohasi - huquqni muhofaza qilish organlari va kiberxavfsizlik mutaxassislari uchun eng muhim yo'nalishlardan biriga aylandi.

Soha oldida turgan asosiy muammolardan biri - tahlil qilinishi kerak bo'lgan ma'lumotlar hajmining keskin o'sishidir. Bitta tergov doirasida yuzlab gigabayt, ba'zan terabaytlab ma'lumot ko'rib chiqilishi zarur bo'ladi. Bundan tashqari, ma'lumotlarni shifrlash, bulutli infratuzilmalarda saqlash va turli yurisdiksiyalarda joylashgan serverlarga murojaat qilish zarurati dalillarni qonuniy va texnik jihatdan to'plashni murakkablashtirmoqda. Bu esa yangi usullar va avtomatlashtirilgan vositalarni joriy etishni taqozo etadi.

Maqolaning maqsadi - raqamli kriminalistikadagi zamonaviy yutuqlarni tahlil qilish, sun'iy intellekt va bulutli muhit bilan bog'liq imkoniyat va cheklovlarni ochib berish hamda raqamli dalillar yaxlitligini ta'minlash bo'yicha amaliy tavsiyalar shakllantirishdan iborat. Vazifalar:

raqamli kriminalistikaning asosiy yo‘nalishlarini tasniflash; zamonaviy vositalarning afzallik va kamchiliklarini aniqlash; dalillarni qayta ishlash jarayonining umumiy tartibini asoslash.

Tadqiqot uslubi

Tadqiqotda ilmiy va me’yoriy manbalarni tahlil qilish, qiyosiy tahlil hamda tizimli yondashuv usullaridan foydalanildi. Asosiy me’yoriy-uslubiy asos sifatida raqamli dalillarni aniqlash, yig‘ish va saqlash bo‘yicha xalqaro standart va ko‘rsatmalar (ISO/IEC 27037, NIST SP 800-86, RFC 3227) hamda O‘zbekiston Respublikasining kiberxavfsizlik sohasidagi qonunchiligi ko‘rib chiqildi.

Raqamli kriminalistika jarayoni odatda to‘rt bosqichdan iborat deb qaraladi: (1) dalilni aniqlash va muhofaza qilish; (2) uni to‘plash va nusxalash (imaging); (3) tahlil qilish; (4) natijalarni hujjatlashtirish va taqdim etish. Tadqiqotda har bir bosqich uchun zamonaviy vositalarning imkoniyatlari va xavf omillari alohida baholandi. Dalillar yaxlitligini tekshirish uchun kriptografik xesh-funksiyalar (masalan, SHA-256) orqali asl nusxa va ishchi nusxaning mosligini tasdiqlash tamoyili asos qilib olindi.

Natijalar va muhokama

Tahlil natijalari raqamli kriminalistikaning to‘rtta asosiy yo‘nalishida ham sezilarli yutuqlar mavjudligini, ayni paytda har birida o‘ziga xos qiyinchiliklar saqlanib qolayotganini ko‘rsatdi. Ushbu yo‘nalishlarning qiyosiy tavsifi quyidagi jadvalda keltirilgan:

1-jadval

Tahlil natijalari

Yo‘nalish	Asosiy yutuqlar	Asosiy qiyinchiliklar
Kompyuter (disk) kriminalistikasi	Disk nusxasini olish, o‘chirilgan fayllarni tiklash, avtomatlashtirilgan indekslash	Shifrlangan disklar, ma’lumotlar hajmining kattaligi
Mobil qurilma kriminalistikasi	Ilovalar ma’lumotlari, geolokatsiya va aloqa tarixini ajratib olish	Qurilma va operatsion tizimlarning xilma-xilligi, kuchli himoya mexanizmlari
Tarmoq kriminalistikasi	Trafikni tahlil qilish, hodisalar xronologiyasini tiklash	Shifrlangan trafik, jurnallarning qisqa muddat saqlanishi
Bulutli kriminalistika	Bulutli xizmat jurnallari va API orqali ma’lumot olish	Ma’lumotlarning turli yurisdiksiyalarda joylashishi, provayderga bog‘liqlik

Sun’iy intellekt vositalari zamonaviy yutuqlar orasida alohida o‘rin tutadi. Mashinali o‘qitish asosida ishlaydigan tizimlar katta hajmdagi matn, tasvir va jurnal yozuvlarini avtomatik tasniflash, shubhali faoliyatni ajratib ko‘rsatish va qidiruv jarayonini tezlashtirish imkonini beradi. Masalan, tasvirlarni tasniflash, matnlardan mavzu va shaxs nomlarini ajratib olish, hodisalar jurnalidagi anomal yozuvlarni aniqlash kabi vazifalar ilgari ekspert tomonidan qo‘lda bajarilgan bo‘lsa, endi katta qismi avtomatlashtirilishi mumkin.

Shu bilan birga, sun'iy intellektdan foydalanish bir qator muammolarni ham yuzaga keltiradi. Birinchidan, model natijalarining izohlanuvchanligi cheklangan bo‘lishi mumkin, sudda esa dalil qanday olingani asoslab berilishi shart. Ikkinchidan, modelning xatosi (yolg‘on ijobiy yoki yolg‘on salbiy natijalar) tergovga salbiy ta’sir ko‘rsatishi mumkin. Uchinchidan, sun'iy intellekt yordamida yaratilgan soxta materiallar (deepfake) dalillarning haqiqiyligini tekshirishni yanada murakkablashtirmoqda. Shu sababli avtomatlashtirilgan tahlil natijalari faqat yordamchi vosita sifatida qaralishi, yakuniy xulosa esa malakali ekspert tomonidan tasdiqlanishi lozim.

Bulutli muhitdan dalillarni yig‘ish alohida e’tiborga loyiq. An’anaviy yondashuvda jismoniy qurilma tortib olinib, undan nusxa olinadi. Bulutli xizmatlarda esa ma’lumotlar fizik jihatdan bir necha serverda, ba’zan turli mamlakatlarda joylashgan bo‘lishi mumkin. Bu holda dalilni olish provayder bilan hamkorlikka, xalqaro huquqiy yordam mexanizmlariga va xizmat ko‘rsatish shartlariga bog‘liq bo‘lib qoladi. Shuning uchun tashkilotlarga jurnal yuritish (logging) siyosatini oldindan belgilab qo‘yish va muhim hodisalar yozuvlarini yetarli muddat saqlashni yo‘lga qo‘yish tavsiya etiladi.

Raqamli dalillarning qonuniy kuchini ta’minlash uchun uzluksiz saqlash zanjiri (chain of custody) yuritilishi zarur: har bir dalil kim tomonidan, qachon va qanday holatda olingani, kimga topshirilgani hujjatlashtiriladi. Asl ma’lumot ustida bevosita ishlamaslik, faqat tasdiqlangan nusxa bilan ishlash, nusxaning xesh-qiymatini asl nusxaniki bilan taqqoslash va yozishdan himoya qiluvchi (write-blocker) vositalardan foydalanish xalqaro amaliyotda qabul qilingan asosiy tamoyillar hisoblanadi.

Zamonaviy yutuqlar qatoriga tezkor xotira (RAM) kriminalistikasini ham kiritish mumkin. Ko‘plab zararli dasturlar va hujumlar izlari faqat operativ xotirada mavjud bo‘ladi va qurilma o‘chirilganda yo‘qoladi. Shuning uchun ishlayotgan tizimdan xotira nusxasini olish (memory dump) va uni tahlil qilish orqali ishga tushirilgan jarayonlar, tarmoq ulanishlari hamda shifrlash kalitlarini aniqlash imkoniyati paydo bo‘ladi. Biroq bunday nusxa olish tizim holatiga ta’sir qilishi mumkinligi sababli, har bir amal batafsil hujjatlashtirilishi va uning asoslanishi ko‘rsatilishi shart.

Shuningdek, Internet buyumlari (IoT) qurilmalari, aqlli soatlar, transport vositalarining bort tizimlari kabi yangi manbalar tergov uchun qo‘shimcha ma’lumot beradi, ammo ularning yopiq dasturiy ta’minoti va nostandart ma’lumot formatlari tahlilni qiyinlashtiradi. Bu holat sohada yangi maxsus vositalarni ishlab chiqish va mutaxassislarni muntazam qayta tayyorlash zaruratini ko‘rsatadi.

Tahlil natijalarini hujjatlashtirish ham alohida ahamiyatga ega. Ekspert xulosasida qo‘llanilgan vositalar nomi va versiyasi, bajarilgan amallar ketma-ketligi, olingan xesh-qiymatlar va topilmalarning tushunarli bayoni keltirilishi kerak. Bu boshqa mutaxassis tomonidan jarayonni takrorlash va natijani mustaqil tekshirish imkonini beradi, ya’ni ilmiy metodning takrorlanuvchanlik tamoyiliga mos keladi. Bunday shaffoflik dalilning sudda qabul qilinish ehtimolini oshiradi.

Xulosa

Tadqiqot shuni ko‘rsatdiki, raqamli kriminalistika sohasidagi zamonaviy yutuqlar tergov jarayonining tezligi va aniqligini oshirishga xizmat qilmoqda, ayniqsa sun'iy intellekt vositalari katta hajmdagi ma’lumotlarni qayta ishlashda muhim yordam beradi. Biroq bu vositalarni qo‘llash dalillarning yaxlitligi, izohlanuvchanlik va qonuniylik talablariga qat’iy rioya qilishni talab etadi.

Amaliyot uchun asosiy tavsiyalar: xalqaro standartlarga muvofiq jarayonlarni joriy etish; avtomatlashtirilgan natijalarni ekspert tomonidan tekshirish; bulutli muhit uchun jurnal yuritish va ma’lumot olish tartiblarini oldindan belgilash; mutaxassislar malakasini muntazam oshirib borish. Kelgusi tadqiqotlarda deepfake materiallarni aniqlash usullari hamda bulutli muhitda dalillarni transchegaraviy olish mexanizmlarini takomillashtirish masalalariga e’tibor qaratish maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
2. ISO/IEC 27037:2012, “Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence”.
3. NIST Special Publication 800-86, “Guide to Integrating Forensic Techniques into Incident Response”, National Institute of Standards and Technology.
4. RFC 3227, “Guidelines for Evidence Collection and Archiving”, Internet Engineering Task Force.
5. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. - Academic Press.

KORPORATIV TARMOQLARDAGI ZARARKUNANDA DASTURLARNI ANIQLASH USULLARI VA ALGORITMLARI

Haydarov E.D.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Tezisda korporativ tarmoqlarda zararkunanda dasturlarni aniqlashning signaturaga va evristik qoidalarga asoslangan an’anaviy usullari tahlil qilinib, ularning noma’lum, polimorf va metamorf tahdidlar oldidagi cheklovlari ko‘rsatib beriladi. Ushbu muammolarni hal etish vositasi sifatida mashinali o‘rganish usullari, xususan, konvolyutsion neyron tarmoqlar (CNN) va rekurrent neyron tarmoqlar (RNN) qo‘llanilishining afzalliklari asoslanadi. CNN ning bajariluvchi fayllar tuzilmasidan, RNN ning esa API chaqiruvlari va tarmoq trafigi ketma-ketliklaridan belgilarni avtomatik ajratish imkoniyati hamda ularni birlashtirgan gibrid yondashuvning samaradorligi yoritiladi.

Kalit so‘zlar: zararkunanda dasturlar, korporativ tarmoq, signatura tahlili, mashinali o‘rganish, chuqur o‘rganish, konvolyutsion neyron tarmoq, rekurrent neyron tarmoq, LSTM.

Аннотация. В тезисе анализируются традиционные методы обнаружения вредоносных программ в корпоративных сетях, основанные на сигнатурах и эвристических правилах, и показываются их ограничения в отношении неизвестных, полиморфных и метаморфных угроз. В качестве средства решения данных проблем обосновываются преимущества методов машинного обучения, в частности сверточных (CNN) и рекуррентных (RNN) нейронных сетей. Освещаются возможности CNN по автоматическому извлечению признаков из структуры исполняемых файлов, RNN — из последовательностей API-вызовов и сетевого трафика, а также эффективность гибридного подхода, объединяющего обе архитектуры.

Ключевые слова: вредоносные программы, корпоративная сеть, сигнатурный анализ, машинное обучение, глубокое обучение, сверточная нейронная сеть, рекуррентная нейронная сеть, LSTM.

Kirish

Bugungi kunda korporativ tarmoqlar tashkilotning moliyaviy, kadrlar va texnologik ma’lumotlarini saqlovchi hamda biznes jarayonlarini uzluksiz ta’minlovchi asosiy infratuzilmaga aylangan. Bunday tarmoqlarga qaratilgan hujumlarning katta qismi zararkunanda dasturlar – viruslar, troyanlar, to‘lov talab qiluvchi dasturlar (ransomware), josuslik dasturlari va botnet agentlari orqali amalga oshiriladi. Ayniqsa, uzoq muddat yashirin faoliyat yurituvchi maqsadli hujumlar va shifrlovchi dasturlar tashkilot faoliyatini to‘xtatib qo‘yish, maxfiy ma’lumotlarni o‘g‘irlash va katta moddiy zarar yetkazishga qodir.

Zararkunanda dasturlar soni va xilma-xilligi yildan-yilga ortib bormoqda, ularning mualliflari esa obfuskatsiya, shifrlash, paketlash va kodni avtomatik o‘zgartirish texnikalaridan faol foydalanmoqda. Natijada uzoq yillar davomida asosiy himoya vositasi bo‘lib kelgan an’anaviy aniqlash usullarining samaradorligi sezilarli darajada pasaymoqda. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni hamda kriptologiya va axborot xavfsizligi sohasini rivojlantirishga oid qarorlar ham muhim axborot infratuzilmasi obyektlarini zamonaviy tahdidlardan himoya qilish vazifasini qo‘yadi. Shu sababli zararkunanda dasturlarni aniqlashning intellektual usullarini tadqiq etish dolzarb hisoblanadi[1].

Asosiy qism

1. An’anaviy aniqlash usullari va ularning kamchiliklari. Korporativ tarmoqlarda keng qo‘llaniladigan an’anaviy yondashuvlarni uch guruhga ajratish mumkin: signaturaga asoslangan aniqlash, evristik (qoidalarga asoslangan) tahlil va anomaliyalarni statistik aniqlash.

Signaturaga asoslangan usulda fayl yoki tarmoq paketining tarkibi oldindan ma’lum zararkunanda namunalaridan olingan bayt ketma-ketliklari, xesh-qiymatlar bazasi bilan solishtiriladi. Bu usul ma’lum tahdidlarni tez va kam yolg‘on signal bilan aniqlaydi, biroq quyidagi jiddiy kamchiliklarga ega:

– birinchidan, u faqat bazada mavjud bo‘lgan tahdidlarni aniqlaydi, ya’ni nol kunlik (zero-day) hujumlar va yangi oilalar oldida ojiz qoladi;

– ikkinchidan, polimorf va metamorf dasturlar har bir nusxada kodini o‘zgartiradi, natijada bitta oilaga mansub minglab namunalar turlicha signaturaga ega bo‘ladi;

– uchinchidan, signatura bazasini yangilash yangi namunani qo‘lga kiritish, tahlil qilish va tarqatishni talab etadi, bu jarayon soatlab va kunlab davom etishi mumkin, aynan shu oraliqda tarmoq himoyasiz qoladi;

– to‘rtinchidan, bazaning hajmi uzluksiz o‘sib boradi, bu esa oxirgi qurilmalar va tarmoq shlyuzlarida hisoblash yuklamasini oshiradi.

Evristik tahlil fayldagi shubhali instruksiyalar, import qilinadigan funksiyalar yoki xatti-harakatlarni ekspertlar tomonidan tuzilgan qoidalar asosida baholaydi. Bu usul ayrim noma’lum namunalarni aniqlay olsa-da, qoidalarni qo‘lda yozish ko‘p mehnat talab qiladi, qoidalar osonlikcha chetlab o‘tiladi va qonuniy dasturlarni zararkunanda deb belgilash (yolg‘on ijobiy natija) holatlari ko‘p uchraydi. Statik tahlilning o‘zi esa obfuskatsiya va paketlash qo‘llanilganda kodning asl mazmunini ochib bera olmaydi[2,3].

Statistik anomaliya aniqlash usullari tarmoq trafigining odatiy profilidan chetlanishlarni qayd etadi. Biroq korporativ muhitdagi trafikning yuqori dinamikasi ostonaviy qiymatlarni tanlashni qiyinlashtiradi, hujumchilar esa o‘z faoliyatini odatiy trafikka o‘xshatib niqoblaydi. Umuman olganda, an’anaviy usullarning asosiy cheklovi shundaki, ular “ma’lum narsani qidiradi” va belgilarni ajratish uchun inson ekspertiga bog‘liq bo‘ladi.

2. Mashinali o‘rganish usullarining afzalliklari. Mashinali o‘rganish usullari zararkunanda va xavfsiz dasturlar namunalaridan iborat katta hajmdagi ma’lumotlar asosida umumlashgan qonuniyatlarni o‘rganadi va ilgari uchramagan namunalarni ham sinflashtira oladi. Klassik algoritmlar (tasodifiy o‘rmon, tayanch vektorlar usuli, gradiyent bustingi) bu yo‘nalishda yaxshi natija bergan bo‘lsa-da, ular ham ekspert tomonidan qo‘lda ajratilgan belgilarga (n-gramlar, PE sarlavha maydonlari, import jadvali) tayanadi. Chuqur o‘rganish modellari esa belgilarni bevosita xom ma’lumotlardan avtomatik ajratadi, bu ularni obfuskatsiyaga nisbatan barqarorroq qiladi. Ushbu tezisda shu jihatdan eng istiqbolli deb hisoblangan CNN va RNN arxitekturalari ko‘rib chiqiladi.

3. Konvolyutsion neyron tarmoqlar (CNN). CNN dastlab tasvirlarni tanib olish uchun ishlab chiqilgan bo‘lib, kirish ma’lumotlaridagi mahalliy naqshlarni konvolyutsiya filtrlari orqali aniqlaydi. Zararkunanda dasturlarni aniqlashda CNN ikki asosiy yo‘nalishda qo‘llaniladi. Birinchi yo‘nalishda bajariluvchi faylning baytlari kul rangli tasvirga aylantiriladi: har bir bayt 0–255 oralig‘idagi piksel yorqinligiga mos keladi. Bitta oilaga mansub namunalar kod o‘zgartirilgan bo‘lsa ham o‘xshash vizual tuzilmaga ega bo‘lishi aniqlangan, CNN esa bu tuzilmalarni samarali ajratadi. Ikkinchi yo‘nalishda (masalan, MalConv modeli) xom bayt ketma-ketligiga bevosita bir o‘lchamli konvolyutsiya qo‘llaniladi va hech qanday dastlabki tahlil talab etilmaydi.

CNN ning afzalliklari quyidagilardan iborat: belgilar avtomatik ajratiladi; birlashtirish (pooling) qatlamlari tufayli naqshning fayldagi o‘rni o‘zgarsa ham u aniqlanadi; parametrlarning qayta ishlatilishi hisobiga model nisbatan yengil bo‘ladi va grafik protsessorlarda tez ishlaydi. Bu xususiyatlar CNN ni korporativ tarmoqdagi elektron pochta shlyuzlari va fayl serverlarida statik tekshiruv uchun qulay qiladi[4,5].

4. Rekurrent neyron tarmoqlar (RNN). Zararkunanda dasturning haqiqiy maqsadi ko‘pincha uning bajarilish jarayonida – tizim chaqiruvlari, API funksiyalari va tarmoq ulanishlarining ketma-ketligida namoyon bo‘ladi. RNN aynan ketma-ket ma’lumotlarni qayta ishlashga mo‘ljallangan bo‘lib, har bir qadamdagi holatni oldingi qadamlar ma’lumoti bilan bog‘laydi. Oddiy RNN dagi gradiyentning so‘nishi muammosini bartaraf etish uchun LSTM va GRU kabi takomillashgan arxitekturalar qo‘llaniladi, ular uzoq masofali bog‘liqliklarni saqlay oladi.

Amaliyotda dastur izolyatsiyalangan muhitda (sandbox) ishga tushiriladi, uning API chaqiruvlari ketma-ketligi yozib olinadi va LSTM modeliga beriladi. Model, masalan, “faylni ochish – shifrlash – asl faylni o‘chirish – tarmoqqa ulanish” kabi xatti-harakatlar zanjirini ransomware uchun xos deb o‘rganadi. Shuningdek, RNN korporativ tarmoq trafigidagi oqimlar ketma-ketligini tahlil qilib, botnet boshqaruv serveri bilan davriy aloqa yoki ma’lumotlarni sekin-asta tashqariga chiqarish holatlarini aniqlay oladi. RNN ning asosiy afzalligi – u statik obfuskatsiyaga bog‘liq bo‘lmagan, dasturning haqiqiy xulq-atvoriga asoslangan tahlilni ta’minlaydi.

5. Gibrid CNN–RNN yondashuvi. Eng yuqori samaradorlikka ikki arxitekturani birlashtirish orqali erishiladi. Bunda CNN qatlamlari ketma-ketlikdagi mahalliy naqshlarni (qisqa API kombinatsiyalari, bayt bloklari) ajratadi va o‘lchamni qisqartiradi, so‘ngra LSTM qatlami bu naqshlar orasidagi vaqtli bog‘liqliklarni o‘rganadi. Ilmiy adabiyotlarda tizim chaqiruvlari ketma-ketligini sinflashtirishda bunday gibrid modellar alohida modellarga nisbatan yuqoriroq aniqlik ko‘rsatgani qayd etilgan. Korporativ tarmoq uchun taklif etiladigan tizim quyidagi bosqichlardan iborat bo‘lishi mumkin: ma’lumotlarni yig‘ish (oxirgi qurilmalar, pochta shlyuzi, trafik sensorlari), statik bosqichda CNN orqali fayllarni tez saralash, shubhali fayllarni sandboxda bajarib RNN orqali xulq-atvorini baholash va natijalarni SIEM tizimiga uzatish[6,7].

An’anaviy va taklif etilayotgan usullarning qiyosiy tavsifi 1-jadvalda keltirilgan.

1-jadval

An’anaviy va chuqur o‘rganishga asoslangan usullarning qiyosiy tahlili

Mezon	**An’anaviy usullar (signatura, evristika)**	**CNN va RNN asosidagi usullar**
Noma’lum (0-day) namunalar	Deyarli aniqlanmaydi	Umumlashgan belgilar orqali aniqlanadi
Polimorf va metamorf kod	Signatura tez eskiradi	Tuzilmaviy va ketma-ketlik naqshlari saqlanadi
Belgilarni ajratish	Ekspert tomonidan qo‘lda	Model tomonidan avtomatik
Bazani yangilash	Doimiy va kechikish bilan	Davriy qayta o‘qitish
Xulq-atvor tahlili	Qoidalar bilan cheklangan	RNN (LSTM/GRU) vaqtli bog‘liqlikni o‘rganadi
Yolg‘on signallar	Evristikada yuqori	Sozlangan modelda kamayadi

Shu bilan birga, chuqur o‘rganish modellarini joriy etishda ayrim masalalarni hisobga olish zarur: sifatli belgilangan o‘quv ma’lumotlar to‘plamini shakllantirish, modelni hujumchilar tomonidan tayyorlangan raqobatli (adversarial) namunalarga chidamli qilish, natijalarni tushuntirib berish imkoniyatini ta’minlash hamda yangi tahdidlar paydo bo‘lishi bilan modelni muntazam qayta o‘qitish. Amaliyotda eng maqbul yechim chuqur o‘rganish modellarini signatura tahlili bilan birga qo‘llashdir: ma’lum tahdidlar signatura orqali tez filtrlanadi, noma’lum va murakkab namunalar esa CNN va RNN modellariga yo‘naltiriladi[8].

Xulosa. Signatura va evristik qoidalarga asoslangan an’anaviy usullar ma’lum tahdidlarga qarshi samarali bo‘lsa-da, nol kunlik, polimorf va metamorf zararkunanda dasturlarni aniqlashda yetarli emas hamda ekspert mehnatiga va bazani doimiy yangilashga bog‘liq. Mashinali o‘rganish, xususan chuqur o‘rganish usullari belgilarni avtomatik ajratish va umumlashtirish orqali bu kamchiliklarni bartaraf etadi. CNN bajariluvchi fayllarning tuzilmaviy naqshlarini statik tahlil qilishda, RNN (LSTM, GRU) esa API chaqiruvlari va tarmoq trafigi ketma-ketliklari orqali dastur xulq-atvorini baholashda afzallikka ega. Ularni birlashtirgan gibrid CNN–RNN modeli korporativ tarmoqlarda zararkunanda dasturlarni aniqlash tizimlarining aniqligi va moslashuvchanligini oshirishning istiqbolli yo‘nalishi hisoblanadi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 2022-yil 15-aprel, O‘RQ-764-son.

2. Moser A., Kruegel C., Kirda E. Limits of Static Analysis for Malware Detection // Proc. ACSAC, 2007. – P. 421–430.

3. Nataraj L., Karthikeyan S., Jacob G., Manjunath B.S. Malware Images: Visualization and Automatic Classification // Proc. VizSec, 2011.

4. Pascanu R., Stokes J.W., Sanossian H., Marinescu M., Thomas A. Malware Classification with Recurrent Networks // Proc. IEEE ICASSP, 2015. – P. 1916–1920.

5. Kolosnjaji B., Zarras A., Webster G., Eckert C. Deep Learning for Classification of Malware System Call Sequences // AI 2016: Advances in Artificial Intelligence. – Springer, 2016. – P. 137–149.

6. Raff E., Barker J., Sylvester J., Brandon R., Catanzaro B., Nicholas C. Malware Detection by Eating a Whole EXE // AAAI Workshops, 2018.

7. Ucci D., Aniello L., Baldoni R. Survey of Machine Learning Techniques for Malware Analysis // Computers & Security. – 2019. – Vol. 81. – P. 123–147.

8. Vinayakumar R., Alazab M., Soman K.P., Poornachandran P., Venkatraman S. Robust Intelligent Malware Detection Using Deep Learning // IEEE Access. – 2019. – Vol. 7. – P. 46717–46738.

MUNDARIJA

1-SHO‘BA. KIBERXAVFSIZLIKNING ZAMONAVIY MUAMMOLARI

Esanov O.O., ***Sobirova Sh.E.***	MASHINALI O‘QITISH ALGORITMLARI ASOSIDA FISHING HUJUMLARINI ANIQLASH USULINI ISHLAB CHIQISH VA TAHLIL QILISH	**4**
Tashev S.N.	TARMOQ XAVFSIZLIGINI TA’MINLASH UCHUN TRAFIKDAGI PAKETLARNI FILTRLASH USULLARI	**9**
Gafurov Sh.R.	AXBOROT XAVFSIZLIGI MONITORINGI TIZIMIDA XABARLARNI KO‘P DARAJALI SAQLASH VA KORRELYATSIYALASH MEXANIZMI	**14**
Gafurov Sh.R.	ELEKTRON HUKUMAT TIZIMINI MONITORING QILISH DASTURIY VOSITASINI AMALDAGI ANALOGLAR BILAN QIYOSIY SINASH NATIJALARI	**18**
Gafurov A.A.	“.UZ” DOMENIDAGI TAHDIDLARNI QAROR QABUL QILISH DARAXTIGA ASOSLANGAN TAYANCH VEKTORLAR USULI YORDAMIDA ANIQLASH	**22**
Gafurov A.A.	MILLIY SEGMENTDA TAHDID VA HUJUMLAR HAQIDAGI OGOHLANTIRISHLARNI KORRELYATSIYALASH JARAYONINING KONSEPTUAL MODELI	**26**
Xudoykulov Z.T., ***Imamaliyev A.T.***	MUHIM AXBOROT INFRATUZILMALARI OBYEKTLARINING KIBER-FIZIK TIZIM SIFATIDAGI ARXITEKTURAVIY XUSUSIYATLARI VA KIBERXAVFSIZLIK TAHDIDLARINING TASNIFI	**30**
Xudoykulov Z.T., ***Imamaliyev A.T.***	RAQAMLASHGAN QO‘RIQLASH TIZIMLARINING KIBERBARDOSHLIGINI TA’MINLASH MUAMMOLARI	**35**
Xudoykulov Z.T., ***Imamaliyev A.T.***	AN’ANAVIY VA ATRIBUTLARGA ASOSLANGAN FOYDALANISHNI BOSHQARISH MODELLARI	**39**
Bozorov S.M.	AI MODELLARIGA UYUSHTIRILADIGAN HUJUMLAR VA ULARNI OLDINI OLISH CHORALARI	**44**
Bozorov S.M.	KIBERXAVFSIZLIK TIZIMLARINI AI BILAN INTEGRATSIYALASH MUAMMOLARI VA YECHIMLARI	**49**
Мурадова А.А., ***Шарапова Н.А.***	КИБЕРБЕЗОПАСНОСТЬ И НАДЁЖНОСТЬ IoT-ИНФРАСТРУКТУРЫ СИСТЕМЫ «УМНЫЙ ГОРОД»: СОВРЕМЕННЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ	**54**
Raximov B.N., ***Yusupov B.K.***	SUN’IY INTELLEKT VOSITASIDA SHAKLLANUVCHI SINTETIK TAHDIDLARNI FILTRLASH VA RAQAMLI SHAXS XAVFSIZLIGINI TA’MINLASH USULLARI	**60**
Irgasheva D.Y., ***Shakarov A.A.***	KIBERXAVFSIZLIKNI TA’MINLASHDA SUN’IY INTELLEKTNING O‘RNI VA ISTIQBOLDAGI RIVOJLANISH YO‘NALISHLARI	**66**
Sodiqova D.J.	FAYL METAMA’LUMOTLARINI RAQAMLI KRIMINALISTIK TAHLIL QILISH VA ULARNING SOXTALASHTIRILGANLIGINI ANIQLASH USULLARI	**70**
Sodiqova D.J., ***Sodikov U.B.***	MODERN PROBLEMS OF CYBERSECURITY AND METHODS OF SOLVING THEM	**75**
Barotova Z., ***Abduvoxidov D.***	ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: APPROACHES, CHALLENGES, AND FUTURE DIRECTIONS	**78**
Shanning Fu, ***Bekmuratov D.K.***	AI-NATIVE CYBERSECURITY COVERAGE GAPS IN INDUSTRIAL AI SYSTEMS: A REPRODUCIBLE CROSSWALK OF MITRE ATLAS AND ATT&CK FOR ICS	**83**

Fayziyeva D.S., ***Yakubova D.M.***	ZARARLI DASTURIY TA’MINOTNI MASHINALI O‘QITISH USULLARI ASOSIDA ANIQLASHNING ZAMONAVIY MUAMMOLARI	**87**
Samarov X.K., ***Nizomov A.O.***	SIEM TIZIMLARIDA MASHINALI O‘QITISH ALGORITMLARI: XAVFSIZLIK HODISALARINI ANIQLASH VA BOSHQARISHNI KUCHAYTIRISH	**92**
Irgasheva D.Y.	MA’LUMOTLAR BAZALARIDA SHAFFOF SHIFRLASH (TDE) VA USTUN DARAJASIDAGI SHIFRLASH USULLARINING QIYOSIY TAHLILI	**96**
Хакимбеков Д.Т.	АЛГОРИТМЫ И МОДЕЛИ ДЛЯ ОБНАРУЖЕНИЯ ИСКУССТВЕННО СОЗДАННЫХ ВИЗУАЛЬНЫХ ОБЪЕКТОВ	**100**
Sapayev Sh.R.	LOKAL BULUTLI TIZIMLARDA AXBOROT XAVFSIZLIGI TAHDIDLARI MODELINI QURISH VA HIMOYA TALABLARINI SHAKLLANTIRISH	**105**
Jaxongirov M.S.	SUN’IY INTELLEKT YORDAMIDA TARMOQ KIBERHUJUMLARINI ANIQLASH: CIC-IDS2017 TO‘PLAMIDA RANDOM FOREST MODELINI BAHOLASH	**112**
Usmanbayev D.Sh.	AXBOROT TIZIMLARI ANOMALIYALARINI SUN’IY IMMUN TIZIMLAR ASOSIDA ANIQLASH ALGORITMI	**116**
G‘ulomov Sh.R., ***Mirzoyev A.A.***	SANOAT TARMOQLARIDA KIBERXAVFSIZLIK XAVFLARINI MINIMALLASHTIRISH MODELI VA ALGORITMI	**121**
Xolimtayeva I.U., ***Xamdamov D.B.***	ZERO TRUST ARXITEKTURASI: PERIMETR HIMOYASIDAN UZLUKSIZ TEKSHIRUVGA O‘TISHNING DOLZARB MUAMMOLARI	**126**
Toshpulatov Sh.	WEB APPLICATION VULNERABILITY DETECTION METHODS: A COMPARATIVE ANALYSIS OF SAST, DAST, IAST AND MANUAL TESTING	**132**
Abduraufova M.S.	SUN’IY INTELLEKT ASOSIDA FISHING HUJUMLARINI ANIQLASH: GIBRID DATASET, REST API VA TELEGRAM BOT INTEGRATSIYASI	**136**
Olimov I.S., ***Tursunov O.O.,*** ***Bo‘riyev Y.A.***	BUYUMLAR INTERNETI TIZIMLARIDA XAVFSIZLIK MUAMMOLARI VA AUTENTIFIKATSIYALASH USULLARI	**141**
Olimov I.S., ***Karimov A.A.,*** ***Daminov A.A.***	BUYUMLAR INTERNETI TIZIMLARIDA FOYDALANUVCHILARNI AUTENTIFIKATSIYALASH USULLARINING TASNIFI VA QIYOSIY TAHLILI	**147**
Oripov P.X.	DPDK ASOSIDA ZARARLI DOMEN SO‘ROVLARINI INLINE FILTRLASH TIZIMI	**152**
Oripov P.X.	TLS ULANISHIGA QARATILGAN DDoS HUJUMLARINI SHIFRNI OCHMASDAN ANIQLASH VA BARTARAF ETISH USULLARI	**156**
Oripov P.X.	SOC AVLODLARI: RIVOJLANISH TARIXI VA ASOSIY TEXNOLOGIYALAR	**160**
Oripov P.X.	KERNEL, XDP VA DPDK TEXNOLOGIYALARI ASOSIDA PAKETLARNI QAYTA ISHLASH USULLARINING QIYOSIY TAHLILI	**164**
Yusupov B.K., ***Sapayev Sh.R.***	BIOMETRIK AUTENTIFIKATSIYA TIZIMLARINI BAHOLASH METODIKASI: XATOLIK KO‘RSATKICHLARI, TAJRIBA PROTOKOLI VA OCHIQ MA’LUMOTLAR BAZALARIDAN FOYDALANISH	**168**
Samarov X. K., ***Ummatova N. B***	WINDOWS OPERATSION TIZIMIDA NTFS RUXSATLARINING RANSOMWARE HUJUMLARINI BOSHQARISHNING TAKOMILLASHTIRILGAN MODELI	**173**

Samarov X. K., ***Yakubova D.M.***	ZAMONAVIY KIBERXAVFSIZLIK TIZIMLARIDA MASHINALI O‘QITISH ALGORITMLARI ASOSIDA ZARARLI DASTURLARNI ANIQLASH VA TASNIFLASH	**178**
Xolimtayeva I.U. ***Yuldashev B.T.***	KUBERNETES TARMOQ ARXITEKTURASI VA KONTEYNERLASHTIRILGAN MUHITDAGI TRAFIK OQIMI	**183**
Jabbarov N.A., ***Yuldashev B.T.***	SDN TARMOQLARINING TUSHUNCHASI, ARXITEKTURASI VA BOSHQARUV TAMOYILLARI	**188**
Allanov O.M., ***Xalilov N.N.***	KATTA TIL MODELLARINING PROMPT INJECTION HUJUMLARIGA BARQARORLIGI	**193**
Muminova S.Sh., ***Tursunova M.A.***	TELEMEDITSINA PLATFORMALARIDA BEMOR MA’LUMOTLARI XAVFSIZLIGIGA TAHDIDLAR VA RISKLARNI INTEGRAL BAHOLASH MEZONLARI	**198**
Muminova S.Sh., ***Sayfiddinova B.B.***	KAFT VENA TOMIRLARI ASOSIDAGI BIOMETRIK AUTENTIFIKATSIYA TIZIMLARIDA AXBOROT XAVFSIZLIGI TAHDIDLARINI MODELLASHTIRISH	**204**
Tojimatov D.X., ***Ganiyev A.A.***	BILIMLAR GRAFI ASOSIDA KIBERTAHDIDLARNI PROAKTIV ANIQLASH MODELINI QIYOSIY TAHLILI	**208**
Axmedova N.F.	MOBIL OPERATORLARNING BIG DATA PLATFORMALARIDA FIRIBGARLIK VA KIBERHUJUMLARNI INTELLEKTUAL ANIQLASH USULLARI TAHLILI	**213**
Axmedova N.F.	MOBIL OPERATORLARNING BIG DATA INFRATUZILMASIGA QARATILGAN KIBERHUJUMLAR TASNIFI VA QATLAMLI TAHDID MODELI	**218**
Qurbonaliyeva D.V.	HONEYPOT TIZIMLARIDA TARMOQ TRAFIGINI QAYTA ISHLASH VA FINGERPRINTINGGA CHIDAMLILIK	**223**
Qurbonaliyeva D.V.	FISHING HUJUMLARINI ANIQLASHNING ZAMONAVIY TEXNOLOGIYALARI VA VOSITALARI TAHLILI	**227**
Бекмирзаев Ж.О.	СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ ВРЕДОНОСНОГО КОНТЕНТА В ВЕБ-БРАУЗЕРЕ	**232**
Vasiyev N.	AXBOROT XAVFSIZLIGI SIYOSATINI VA TAHDIDLARNI BAHOLASH USULLARI: NAZARIY TAHLIL	**236**
Karimov A.A., ***Olimov I.S.,*** ***Daminov A.A.***	BULUTLI HISOBLASH TIZIMLARIDA AXBOROT XAVFSIZLIGI MUAMMOLARI VA ULARNING TAHLILI	**239**
Yuldasheva N.S., ***Salimov S.A.,*** ***Habibjonova G.M.***	AQLLI UY IoT QURILMALARIDA MA’LUMOTLAR XAVFSIZLIGI MUAMMOLARI VA ULARNI KRIPTOGRAFIK HIMOYALASH YONDASHUVLARI	**242**
Xusenov Sh.S.	DIPFEYK VA SUN’IY INTELLEKT YORDAMIDAGI FISHING HUJUMLARI TAHLILI VA KO‘P QATLAMLI HIMOYA MODELI	**247**
Bozorov O.N.	GENERATIV SUN’IY INTELLEKT MUHITIDA MAXFIY AXBOROTNI SIZIB CHIQISHDAN HIMOYALASH	**250**
Raxmonaliyev S.M.	KORPORATIV TARMOQLARDA ANOMALIYALARGA ASOSLANGAN HUJUMLARNI ANIQLASH TIZIMLARIDA YOLG‘ON SIGNALLAR MUAMMOSI VA BAHOLASH METODIKASINING DOLZARB MASALALARI	**253**
Fayziyeva D.S., ***Abdumuminova Sh.D.***	MASOFAVIY TA’LIM TIZIMLARIDA SUN’IY INTELLEKT ASOSIDA AUTENTIFIKATSIYA QILISH USULLARI	**256**
Yaqubova M.R.	COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR DETECTING FRAUDULENT TRANSACTIONS	**260**

Bafoyeva Sh.A.	MASHINALI O‘RGANISH ASOSIDA REST API LARGA QILINADIGAN HUJUMLARNI ANIQLASH TIZIMI	**263**
Nabiyeva S.S.	KIBERSAVODXONLIKNI OSHIRISH MUAMMOLARINI HAL QILISH YO‘LLARI	**267**
Istamova Sh.Sh.	RAQAMLI TRANSFORMATSIYA SHAROITIDA TIJORAT BANKLARINING MIJOZLAR BILAN ISHLASHIDA KIBERXAVFSIZLIKKA ASOSLANGAN YANGI YONDASHUVLAR	**270**
Fayziyeva D.S., ***Ergasheva F. Y.***	SUN’IY INTELLEKT ASOSIDA MASOFAVIY TA’LIM TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA’MINLASH	**273**
Chunayev N.E., ***Azimbekov S.D.***	ZAMONAVIY AXBOROT TIZIMLARIDA MA’LUMOTLAR BAZASI XAVFSIZLIGI VA ANOMAL SO‘ROVLARNI ANIQLASHNING DOLZARB MASALALARI	**277**
Ганиев С.К., ***Абдуллаев Д.Г.***	ОРГАНИЗАЦИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК	**281**
Mamatqulova M.K., Alishev Sh.A.	ZERO-DAY KIBERHUJUMLARNI ANIQLASHDA FEDERATIV O‘QITISH VA ANOMALIYALARNI ANIQLASHGA ASOSLANGAN TAQSIMLANGAN IDS MODELI	**286**
Ibrohimov S.Sh.	WEB ILOVALARNI HUJUMLARDAN HIMOYALASH DASTURIY VOSITASI XUSUSIYATLARI	**291**
Boqiyev A.A., ***Haydarov E.D.***	TO‘LIQ BO‘LMAGAN TRAFIK BELGILARIDA SUN’IY IMMUN DETEKTORI QARORINING BARQARORLIGINI BAHOLASH	**295**
Xabibullayev J.D.	AXBOROT TIZIMLARIDA LOG-FAYLLARNI SAQLASHNING USULLARI VA ULARNING XAVFSIZLIK KAMCHILIKLARI	**299**
Nasrullayev N.B., ***Xamidov Sh.J.,*** ***Mirzayeva A.B.***	ZARARLI APK FAYLLARNI ANIQLASH MUAMMOLARI VA MODELI	**305**
Qaxramonov E.Q., ***Ismatov N.N.***	ZARARLI DASTURLARNI ANIQLASH VA AXBOROTNI HIMOYALASHDA ZAMONAVIY KIBERXAVFSIZLIK USULLARIDAN FOYDALANISH	**310**
Tashev K.A., ***Yoqubjonov O.N.***	ZAIFLIKLARNI MAXSUS STANDARTLAR ORQALI ANIQLASH HAMDA NMAP VULSCAN MODULI NATIJALARI BILAN INTEGRATSIYALASH: RISKKA ASOSLANGAN MODEL	**315**
Rajabboyeva S., ***Xaitbayev A.***	MATHEMATICAL MODEL OF STREAMING NETWORK TRAFFIC AND THE INFORMATION SECURITY MONITORING PROCESS	**319**
Xabibullayev J.D., ***Xamidov Sh.J.***	QUORUM-SIGNED PERMISSIONED BLOCKCHAIN WITNESS FOR SECURITY LOG INTEGRITY: PROTOTYPE AND FAULT-TOLERANCE EVALUATION	**323**
Xudoykulov Z.T., ***Xayrullayeva E.S.***	BIOMETRIK AUTENTIFIKATSIYANI JORIY ETISH ASOSIDA AXBOROT TIZIMLARIDA XAVFSIZLIK DARAJASINI OSHIRISH MODELI VA ALGORITMI	**327**
Norboboyeva G.Z.	SUN’IY INTELLEKT YORDAMIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH	**329**
Sayfullayev Sh.B.	KORPORATIV TARMOQLARDA KOMPYUTER XAVFSIZLIGI MUAMMOSI VA ZAMONAVIY HIMOYA YONDASHUVLARI	**332**
Seidullayev M.K., ***Jumatashov A.B.***	YURAK-QON TOMIR KASALLIKLARINI TASHXISLASHDA FEDERATIV O‘QITISH VA KRIPTOGRAFIK HIMOYA ASOSIDA BEMOR MA’LUMOTLARI XAVFSIZLIGINI TA’MINLASH	**335**
Kadirov M.M., ***Karimova N.O.,*** ***Zokirova F.R.***	RAQAMLI INFRATUZILMALARGA QARATILGAN TARMOQ HUJUMLARINI MASHINALI O‘QITISH USULLARI YORDAMIDA TASNIFLASH	**340**

G‘ulomov Sh.R., ***Nasriddinova P.F.***	SUN’IY INTELLEKT ASOSIDA TARMOQ HUJUMLARINI ERTA ANIQLASHNING DOLZARB MUAMMOLARI VA RIVOJLANISH ISTIQBOLLARI	**345**
Barotova Z., ***Abduvoxidov D.***	THE IMPORTANCE OF EARLY ATTACK DETECTION IN ENSURING NETWORK SECURITY	**348**
Polvanov R.B., ***Muxamedaliyeva N.M.***	UCH POG‘ONALI RAQAMLI OGOHLANTIRUVCHI SIGNAL MODELINING QAROR QOIDALARI VA XAVFSIZLIK TAMOYILLARI	**353**
Xabibullayev J.D., ***Xamidov Sh.J.***	LOG-FAYLLARNI SAQLASH KAMCHILIKLARINI BARTARAF ETISH USULLARI VA ULAR ORASIDA BLOKCHEYN TEXNOLOGIYASINING O‘RNI	**357**
Maxkamova D.B.	TARMOQ OQIMINI TAHLIL QILISH ASOSIDA HUJUMLARNI ANIQLASHNING MA’LUMOT SIZISHIGA CHIDAMLI USUL VA ALGORITMLARI	**361**
Nasrullayev N.B., ***Xamidov Sh.J.,*** ***Mirzayeva A.B.***	ELEKTRON POCHTA TIZIMLARIDA XABARLARINI VEKTORLASH USULLARI	**366**
Nasrullayev N.B., ***Xamidov Sh.J.,*** ***Mirzayeva A.B.***	BANK-MOLIYA TIZIMIDA XAVFSIZLIKNI TA’MINLASH MUAMMOLARI VA MODELI	**370**
Махмудова М.М.	ВЛИЯНИЕ ПАРАМЕТРОВ ARGON2ID НА ПРАКТИЧЕСКУЮ БЕЗОПАСНОСТЬ ПАРОЛЕЙ: АНАЛИЗ ВЫЧИСЛИТЕЛЬНЫХ ЗАТРАТ И КОМПРОМИССОВ ПО ПАМЯТИ	**375**
Tashev K.A., ***Yoqubjonov O.N.***	FISHING HUJUMLARINI CHUQUR TAHLIL QILISH VA KO‘P QATLAMLI HIMOYA MODELI	**379**
Ahmadov U.S., ***Murodov M.M.***	KORPORATIV TARMOQLARNI KIBERHUJUMLARDAN HIMOYALASH USULLARI	**382**
2-SHO‘BA. KRIPTOLOGIYA SOHASI ISTIQBOLLARI		
Валиулин А.Ш.	МЕТОД ПОСТКВАНТОВОЙ МОДЕРНИЗАЦИИ СИСТЕМЫ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ КОРПОРАТИВНОГО МЕССЕНДЖЕРА	**387**
Haydarov E.D., ***Salimov S.,*** ***Janxojaev A.A.***	KRIPTOGRAFIK O‘LCHAMDAGI TUB SONLARNING TAQSIMOTI VA ULARNI GENERATSIYA QILISHNING NAZARIY ASOSLARI	**392**
Nurullayev M.M.	AGENTLI SUN’IY INTELLEKT TIZIMLARIDA AXBOROT OQIMI XAVFSIZLIGINI TA’MINLASHNING PANJARA MODELIGA ASOSLANGAN YONDASHUVI	**396**
Haydarov E.D., ***Murodov M.,*** ***Janxojaev A.A.***	OCHIQ KALITLI KRIPTOTIZIMLARDA TUB SONLAR: FAKTORIZATSIYA VA DISKRET LOGARIFM MUAMMOLARI	**400**
Xudoykulov Z.T., ***Jabbarov N.A.***	GRAIN V1 OQIMLI SIMMETRIK SHIFRLASH ALGORITMINING TUZILISHI, ISHLASH PRINSIPI VA KRIPTOGRAFIK XUSUSIYATLARI TAHLILI	**404**
Abdullaev T.R., ***Juraev G.U.***	A COMPACT ARITHMETIC PARAMETERIZATION OF PRIMES: FROM 48 LINEAR FUNCTIONS TO A VERIFIED PERIOD-56 FORMULA	**409**
Jurayev G.U., ***Anvarov Sh.S.***	MA’LUMOT ALMASHINUVI TIZIMLARIDA SHIFRLANGAN PAKETLARNI UZATISH USULLARINI TAKOMILLASHTIRISH	**413**
Allanov O.M., ***Shakarov A.A.,*** ***Mavlonov O.N.***	KVANT KOMPYUTERLARINING KRIPTOGRAFIK ALGORITMLARGA TAHDIDI VA POST-KVANT KRIPTOGRAFIYAGA O‘TISH ZARURIYATI	**416**

Daminov A.A., ***Karimov A.A.,*** ***Olimov I.S.***	KRIPTOGRAFIK KALITLARNI HOSIL QILISHDA HKDF ALGORITMINING SAMARADORLIGI VA XAVFSIZLIK XUSUSIYATLARINI TADQIQ ETISH	**420**
Janxojaev A.A., ***Aralbaev I.A.***	KONSORSIUM BLOKCHEYN TEXNOLOGIYASINING QATLAMLI ARXITEKTURASI, KONSENSUS MEXANIZMLARI VA RIVOJLANISH ISTIQBOLLARI	**424**
Mardiyev U.R., ***Turobov A.***	ZKP (ZERO-KNOWLEDGE PROOF) TIZIMLARINI AUTENTIFIKATSIYA VA FOYDALANISHNI BOSHQARISH VAZIFALARIDA QO‘LLASH	**428**
Xursandova Z.S.	POST-KVANT KRIPTOGRAFIYADA ML-KEM ALGORITMLARINING XAVFSIZLIK XUSUSIYATLARI VA ISHLASH SAMARADORLIGI: TAHLIL VA AMALIY TAJRIBA	**433**
Xudoynazarov U.U.	KALITLARNI HOSIL QILISH MEXANIZMLARINING KRIPTOGRAFIK ASOSLARI	**438**
Qozoqova T.Q.	VIDEOKUZATUV TIZIMLARI UCHUN YENGIL OQIMLI SHIFRLAR VA KICHIK HOLATLI KALIT OQIMI GENERATORLARINING QIYOSIY KRIPTOTAHLILI	**443**
Xudoykulov Z.T., ***Qutlimurotov A.H.***	TLS 1.2 VA TLS 1.3 DA KALIT HOSIL QILISH FUNKSIYALARI: MILLIY ALGORITMLAR ASOSIDA QO‘LLASH TAJRIBASI VA O‘ZBEKISTON UCHUN IMKONIYATLAR	**447**
Ortiqboyev A.M.	KRIPTOLOGIYA SOHASIDA KADRLAR TAYYORLASH VA DOLZARB YO‘NALISHLAR	**453**
Axadova O.Ch.	YARIM TUB SONLARNI FAKTORLASHNING GEOMETRIK QIDIRUV USULI VA UNING SAMARADORLIK TAHLILI	**457**
Mardiyev U.R., ***Arabboyev B.B.***	POSTKVANT KRIPTOGRAFIYA VA ML-KEM (FIPS 203) KALIT INKAPSULYATSIYALASH MEXANIZMINING TUZILISHI, XAVFSIZLIK ASOSLARI VA AMALIY JORIY ETISH MUAMMOLARI TAHLILI	**461**
Abduxalilov X.	MOBIL ILOVALARDA SHAXSIY MA’LUMOTLARNI KRIPTOGRAFIK HIMOYALASH TALABLARIGA MUVOFIQLIGINI BAHOLASH USULLARI	**465**
Xudoynazarov U.U.	OCHIQ KALITLI QIDIRISH IMKONIYATLI SHIFRLASH ALGORITMLARIGA PARAMETRLI ALGEBRANI TATBIQ ETISH YONDASHUVLARI	**468**
Turdibekov B.B.	BLOKCHEYN TEXNOLOGIYASINING PAYDO BO‘LISHI VA RAQAMLI FAYLLAR YAXLITLIGINI TA’MINLASHDAGI O‘RNI	**473**
Chunayev N.E.	KVANT KRIPTOGRAFIYASI VA UNING AXBOROT XAVFSIZLIGINI TA’MINLASHDAGI AHAMIYATI	**478**
Imomov E.M., ***Salohiddinov H.F.***	SHIFRLASH ALGORITMLARINING NEYRON TARMOQLAR YORDAMIDA KRIPTOTAHLILI	**481**
Baxtiyorov U.B., ***Sattorov Sh.I.***	TLS PROTOKOLI UCHUN SEANS KALITLARNI GENERATSIYALASH YANGI ALGORITMNI ISHLAB CHIQISH	**485**
Sattarov A.B., ***Abdurashidov B.K.***	GOST 28147-89 BO‘YICHA DIFFERENSIAL NATIJALARNING PARAM-Z S-BLOKLI “MAGMA” SHIFRIGA TATBIQ ETILISH SHARTLARI	**493**
Baxtiyorov U.B., ***Tolmasov J.J.***	TARMOQNING TRANSPORT BOSQICHIDA XAVFSIZ ULANISHNI O‘RNATUVCHI XORIJIY TLS 1.3 PROTOKOLLARI TAHLILI	**498**
Sattarov A.B., ***Normurodov T.B.***	NOL-BILIM USULLARIGA ASOSLANGAN AUTENTIFIKATSIYA PROTOKOLLARINING ISHLASH MEXANIZMLARI VA XAVFSIZLIK XUSUSIYATLARINI BAHOLASH	**503**
Allayorov Y.Sh.	KVANT TEXNOLOGIYALARI VA UNI RIVOJLANTIRISHDA XORIJ TAJRIBALARI	**508**

Kuryazov D.M., Jumaboyev I.N.	BULUTLI HISOBLASH TIZIMLARI TAHLILI VA O‘ZBEKISTON SHAROITIDA QO‘LLASH ISTIQBOLLARI	**513**
Kuryazov D.M., Mingyasharov N.B.	NIST POSTKVANT STANDART ALGORITMLARINI DASTUR VA QURILMALARDA QO‘LLASHDA YON-KANAL HUJUMLARI VA CONSTANT-TIME HIMOYASI	**518**
Karimov A.A., Olimov I.S., Berdiyev H.S.	BULUTLI HISOBLASH TIZIMLARIDA VIRTUAL MASHINA OBRAZLARINI ZERO TRUST VA KRIPTOGRAFIK USULLAR ASOSIDA HIMOYALASH	**523**
Tashev K.A., Maxmudov A.N.	SHIFRLANGAN TARMOQ TRAFIGIDA ZARARLI FAOLLIKNI DESHIFRLASHSIZ ANIQLASHDA SUN’IY INTELLEKT ALGORITMLARINI QO‘LLASH	**526**
Jurayev G.U., Saidmurodov M.A.	IOT MUHITIDA VLC TEXNOLOGIYASINI QO‘LLASH VA EDGE COMPUTING ASOSIDA XAVFSIZLIKNI TA’MINLASH	**531**
Salayev A.K.	CAMELLIA SIMMETRIK BLOKLI SHIFRLASH ALGORITMINING SAMARADORLIGI VA ZAMONAVIY KRIPTOTIZIMLARDA QO‘LLASH ISTIQBOLLARI	**535**
Allanov O.M.	KRIPTOGRAFIK XESH FUNKSIYALARNI TAKOMILLASHTIRISH YONDASHUVLARI	**539**
Ortiqboyev A.M.	PARAMETRLI ALGEBRAGA ASOSLANGAN JAMOAVIY ELEKTRON RAQAMLI IMZO BARDOSHLIGINI OSHIRISH USULI VA ALGORITMI	**542**
Salayev A.K.	PINN YORDAMIDA KIBERFIZIK TIZIMLARDA SENSOR MA’LUMOTLARI YAXLITLIGINI NAZORAT QILISH	**547**
Mahmanazarova Z.N.	RSA VA ML-KEM ALGORITMLARINING KVANT TAHDIDLARIGA CHIDAMLILIGI HAMDA AMALIY CHEKLOVLARINING QIYOSIY TAHLILI	**552**
Xaydarov T.S.	SHA-256 VA SHA-512 HESH FUNKSIYALARINING IKKINCHI PROOBRAZGA BARDOSHLILIGIGA XABAR UZUNLIGINING TA’SIRI	**557**
Xudoykulov Z.T., Qutlimurotov A.H.	O‘zMSt 285:2024 STANDARTIDAGI XESHLASH ALGORITMLARI: ARXITEKTURASI, MATEMATIK ASOSLARI VA DASTURIY AMALGA OSHIRISH SAMARADORLIGI	**560**
Axmedova O.P., Akbarova S.A.	ML-DSA VA SLH-DSA RAQAMLI IMZO ALGORITMLARINING AMALIY SAMARADORLIGINI QIYOSIY TADQIQ QILISH	**565**
Allanov O.M.	TLS 1.2 VA TLS 1.3 PROTOKOLLARIDA PRF/KDF MEXANIZMLARINING KRIPTOGRAFIK XAVFSIZLIGINING QIYOSIY TAHLIL QILISH	**568**
Урозова С.Г.	РОЛЬ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ОБЕСПЕЧЕНИИ ЦЕЛОСТНОСТИ И НЕОТРЕКАЕМОСТИ ДАННЫХ В ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ	**571**
Mamatqulova H.S., Abduganiyev B.	SMART KONTRAKTLARDAGI REENTRANCY ZAIFLIGINI ANIQLASH VA BARTARAF ETISH USULLARINI TAHLIL QILISH	**576**
Haydarov E.D.	KRIPTOGRAFIK TIZIMLARDA PSEVDOTASODIFIY FUNKSIYALAR VA KALIT HOSIL QILISH FUNKSIYALARINING O‘RNI	**581**
Abdurazzoqov J.R.	ZAMONAVIY PSEVDOTASODIFIY FUNKSIYALAR VA KALIT HOSIL QILISH SXEMALARINING QIYOSIY TAHLILI	**585**
Ortikov J.K.	XFA-256 XESH FUNKSIYA ALGORITMINI ISHLAB CHIQISH VA KRIPTOBARDOSHLILIGINI ASOSLASH	**590**
Fozilov Sh.N.	IOT ALOQA PROTOKOLLARINI HIMOYA QILISH UCHUN ELLIPTIK KRIPTOGRAFIYA ASOSIDA SAMARALI KALIT YARATISH USULLARI	**598**

Fozilov Sh.N.	RESURSLARI CHEKLANGAN IOT QURILMALARIDA KRIPTOGRAFIK KALITLAR UCHUN ENTROPIYA MANBALARIGA ASOSLANGAN TASODIFIY SONLAR GENERATSIYALASH ALGORITMI	**602**
Axtamov A.H.	RESURSLARI CHEKLANGAN QURILMALARDA ASCON ASOSIDAGI AEAD, XESH VA XOF FUNKSIYALARINI SAMARALI AMALGA OSHIRISH VA BAHOLASH	**607**
Xamrayev A.Q.	IOT TIZIMLARIDA DASTURIY AMALGA OSHIRISHGA YO‘NALTIRILGAN OQIMLI SHIFRLASH ALGORITMLARINING QIYOSIY TAHLILI	**610**
Mahmanazarova Z.N.	GALUA MAYDONLARI ARIFMETIKASI VA UNING ZAMONAVIY KRIPTOGRAFIK ALGORITMLARDA QO‘LLANILISHI	**614**
Xamrayev A.Q.	IOT QURILMALARI UCHUN APPARAT RESURSLARI CHEKLANGAN SHAROITDA OQIMLI SHIFRLASH ALGORITMLARINI TAHLIL QILISH	**617**
Daminov A.A.	KRIPTOGRAFIK KALITLARNI GENERATSIYALASHDA ENTROPIYA MANBALARINING SIFATINI BAHOLASH USULLARI	**621**
Suyunov S.N.	KVANT HISOBLASH TEXNOLOGIYALARINING VPN TIZIMLARINING KRIPTOGRAFIK XAVFSIZLIGIGA TA’SIRI	**624**
Xudoykulov Z.T., Baxodirov D.U.	KLASSIK OCHIQ KALITLI KRIPTOTIZIMLAR (RSA, ECC, DIFFIE–HELLMAN) VA ULARNING KVANT KOMPYUTERLARIGA NISBATAN ZAIFLIGINI BAHOLASH	**627**
Байпакбаева С.Т.	АЛГЕБРАИЧЕСКАЯ ДИАГНОСТИКА БИТОВЫХ ИСКАЖЕНИЙ СИМВОЛЬНОЙ ИНФОРМАЦИИ В ПОЛЕ GF(31)	**631**
Tursunov O.O., Olimov I.S.	TLS PROTOKOLINING ISHLASH PRINSIPI VA XABARLAR ALMASHINUVI JARAYONI	**634**
Qozoqova T.Q	VIDEOKUZATUV TIZIMLARIDA VIDEO OQIMINI TANLAB SHIFRLASH SXEMALARI: HUJUMLAR TAHLILI VA KALIT BOSHQARUVIGA QO‘YILADIGAN TALABLAR	**642**
Xaydarov T.S.	MERKLE–DAMGÅRD VA WIDE-PIPE KONSTRUKSIYALARINING XAVFSIZLIK JIHATIDAN QIYOSIY TAHLILI	**646**
Xudoykulov Z.T., Qutlimurotov A.H.	TLS 1.3 PROTOKOLI VA MILLIY KRIPTOGRAFIK PROFILLAR: ROSSIYA, BELARUS, XITOY TAJRIBASI HAMDA O‘ZBEKISTON UCHUN IMKONIYATLAR	**650**
Suyunov S.N.	POST-KVANT KRIPTOGRAFIK ALGORITMLAR VA ULARNING VPN TIZIMLARI XAVFSIZLIGINI TA’MINLASHDAGI O‘RNI	**656**
Maxamatjonov I.D.	RESURS JIHATDAN CHEKLANGAN IOT QURILMALARI UCHUN YENGIL KIRISHNI ANIQLASH TIZIMLARI: RESURS BYUDJETIGA ASOSLANGAN QAROR QABUL QILISH MODELI	**659**
Xudoykulov Z.T., Baxodirov D.U.	KVANT KALITLARNI TAQSIMLASH VA POSTKVANT KEM ALGORITMLARINING QIYOSIY TAHLILI	**664**
3-SHO‘BA. RAQAMLI KRIMINALISTIKA YUTUQLARI		
Nematilloyev B.V.	KIBERJINOYATLARNI TERGOV QILISHDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISHNING METODIK ASOSLARI	**670**
Xo‘jamqulova D.N.	MA’LUMOTLARNI YASHIRISHNING STEGANOGRAFIK YECHIMINI TADQIQ ETISH VA TAKOMILLASHTIRISH	**674**
Эргашбеков Н.А.	МЕТОДЫ АНАЛИЗА ЗАШИФРОВАННЫХ ТОМОВ В ПРОЦЕССАХ ЦИФРОВОЙ КРИМИНАЛИСТИКИ	**679**

Xasanov K.A., ***Ganiyev A.A.,*** ***Tairova D.A.***	MATNGA AXBOROT YASHIRISHNING IMKONIYATLARI VA CHEKLOVLARI HAMDA MAVJUD USULLARNING O‘ZBEK TILI SHAROITIDAGI ZAIF NUQTALARI TAHLILI	**683**
Fayzullayev O.X.	O‘ZBEKISTONDAGI ELEKTRON PUL TIZIMLARIDA SUN’IY INTELLEKT VA IJTIMOIY MUHANDISLIK TAHDIDLARI HAMDA ULARGA QARSHI HIMOYA CHORALARI	**688**
Madjitov K. M., ***Sayidmurotov Sh. Sh.***	ZAMONAVIY KIBERXAVFSIZLIK TAHDIDLARI SHAROITIDA AXBOROTLASHTIRISH OBYEKTLARINI ATTESTATSIYADAN O‘TKAZISHNING METODOLOGIK ASOSLARI	**693**
Alimov A.A., ***Botiraliyev N.X.***	OVOZ YOZIB OLISH QURILMALARINI BLOKIROVKA QILISHNING YUQORI CHASTOTALI GIBRID TIZIMLARI: NAZARIY MODELLAR VA AMALIY TAHLIL	**698**
Djurayev N.T.	VIRTUALLASHTIRISH TEXNOLOGIYALARI ASOSIDA IP-TELEFONIYA TARMOQLARI XAVFSIZLIGINI BAHOLASHGA MO‘LJALLANGAN KIBERPOLIGON TIZIMINI ISHLAB CHIQISH	**702**
Muratov O.A., ***Ergashov B.B.***	DASTURIY TA’MINOT XAVFSIZLIGINI TA’MINLASH YO‘LLARI TAHLILI	**707**
Asliddinov Sh.A., ***Amirov A.D.***	KIBERPOLIGON INFRATUZILMASI UCHUN OCHIQ KODLI TEXNOLOGIYALARNI AMALIY SINOV NATIJALARI ASOSIDA TANLASH	**711**
Azizov D.A., ***Xatamov S.Q.***	SUN’IY INTELLEKT AGENTLARINI ISHLAB CHIQISHDA XAVFSIZLIK TAMOYILLARI VA HIMOYA MEXANIZMLARI	**717**
Ubaydullayev Q.X., ***G‘afurov Z.V.***	RAQAMLI KRIMINALISTIK EKSPERTIZADA APPARAT-DASTURIY VOSITALARNING FUNKSIONAL IMKONIYATLARI VA ISHONCHLILIGINI BAHOLASH	**722**
Halimov Sh.G‘.	MOBIL QURILMALARDA RAQAMLI KRIMINALISTIK EKSPERTIZA O‘TKAZISHNING O‘ZIGA XOS XUSUSIYATLARI	**727**
Xalilov H.I.	DEEPFAKELARNI ANIQLASHNING KRIMINALISTIK USULLARI VA ULARNING SUDDA DALIL SIFATIDA QABUL QILINISHI	**730**
Xayinov R.Sh., ***Sheraliyev M.Sh.***	KIBERXAVFSIZLIK VA VIDEOMONITORING TIZIMLARIDA OB’YEKTLARNI INTELLEKTUAL ANIQLASHNING ZAMONAVIY MODELLARI (YOLOv8 VA YOLOv12) TAHLILI	**735**
Шамшиева Б.М.	МЕТОД КЛАССИФИКАЦИИ ЦИФРОВЫХ АУДИОСИГНАЛОВ НА ОСНОВЕ СПЕКТРАЛЬНЫХ И ВЕЙВЛЕТ-ПРИЗНАКОВ ДЛЯ ЗАДАЧ ЦИФРОВОЙ КРИМИНАЛИСТИКИ	**740**
Юлдашева Н.С., ***Салимов С.А.,*** ***Сайжанов И.А.***	РАЗРАБОТКА МОДЕЛИ ОБНАРУЖЕНИЯ ПОДДЕЛЬНЫХ ИЗОБРАЖЕНИЙ И ВИДЕОМАТЕРИАЛОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ	**745**
Юлдашева Н.С., ***Салимов С.А.,*** ***Сайжанов И.А.***	ПРИМЕНЕНИЕ МЕТОДОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ ДЛЯ ВЫЯВЛЕНИЯ ПРИЗНАКОВ DEEPFAKE В ВИДЕОМАТЕРИАЛАХ	**749**
Allanov O., Safoev N., Salimov S.	FINGERPRINT BIOMETRICS: TECHNOLOGIES, SECURITY CHALLENGES, AND FUTURE DEVELOPMENTS	**753**
Ramazonova M.S., ***Odilov O.R.,*** ***Mamatov S.Z.***	KOMPYUTER TARMOQLARIDA SODIR ETILGAN JINOYATLAR IZLARINI ANIQLASH, YIG‘ISH VA TADQIQ ETISH USULLARI	**756**
Ganiyev A.A., ***Sadirova X.X.***	RAQAMLI TASVIRLARDA RUXSATSIZ O‘ZGARISHLARNI ANIQLASH	**760**
Nasrullayev N.B., ***Maxmudov A.N.***	RAQAMLI KRIMINALISTIKADA SUN’IY INTELLEKT ASOSIDAGI PREDIKTIV TAHLIL: KIBERINTSIDENTLARNI REAL VAQTDA ANIQLASH VA DALILLARNI AVTOMATLASHTIRILGAN TAHLIL QILISH	**764**

Qudratov U.I., ***Eshmurodov A.A.***	LLM DAVRIDA IJTIMOIY TARMOQLARDAGI SOXTA PROFIL VA BOTLARNI ANIQLASH: USULLAR, CHEKLOVLAR VA GIBRID YONDASHUV	**768**
Qudratov U.I., ***Eshmurodov A.A.***	SOXTA PROFIL VA BOT AKKAUNTLARNI ANIQLASH ALGORITMLARINING TWIBOT-22 BENCHMARKI ASOSIDA QIYOSIY TAHLILI	**773**
Хамидов Ш.Ж.	МЕТОДЫ ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ НА ОСНОВЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ	**778**
Rahmonov N.S.	RAQAMLI KRIMINALISTIKADAGI ZAMONAVIY YUTUQLAR: SUN'IY INTELLEKT VA BULUTLI MUHITDAN RAQAMLI DALILLARNI OLISH ISTIQBOLLARI	**783**
Haydarov E.D.	KORPORATIV TARMOQLARDAGI ZARARKUNANDA DASTURLARNI ANIQLASH USULLARI VA ALGORITMLARI	**786**