O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Ro‘yxatga olindi:
№ 8/9/750/751
2025-yil “29” 04

“TASDIQLAYMAN”
O‘quv ishlari bo‘yicha prorektor
D.Jalilov
“29” 04 2025-yil

KIBERXAVFSIZLIK ASOSLARI

FANINING O‘QUV DASTURI

Bilim sohasi:	600 000	– Axborot-kommunikatsiya texnologiyalari
	300 000	– Ijtimoiy fanlar, jurnalistika va axborot
Ta’lim sohasi:	610 000	– Axborot-kommunikatsiya texnologiyalari
	320 000	– Jurnalistika va axborot
Ta’lim yo‘nalishlari:	60611000	– Simsiz aloqa va teleradioeshittirish injiniringi
	60610600	- Telekommunikatsiya texnologiyalari
	60611100	- Infokommunikatsiya injiniringi
	60610900	- Radioelektron qurilmalar va tizimlar
	60610200	– Axborot xavfsizligi
	60610400	– Dasturiy injiniring
	60610100	– Axborot tizimlari va texnologiyalari
	60611200	– Kiberxavfsizlik injiniringi
	60610300	– Kompyuter injiniringi
	60320400	– Kutubxona-axborot faoliyati
	60610800	– Pochta aloqa texnologiyasi
	60610500	– Sun’iy intellekt
	60610700	– Televizion texnologiyalar

Toshkent 2025

Fan/modul kodi	O‘quv yili	Semestr	ESCTS kreditlar
KIA1406	2025-2026	3, 4	6
Fan/modul turi	**Ta’lim tili**		**Haftadagi dars soatlari**
majburiy	O‘zbek/rus		4/6

	Fanning nomi	Auditoriya mashg‘ulotlari (soat)	Mustaqil ta’lim (soat)	Jami yuklama (soat)
1.	**Kiberxavfsizlik asoslari**	72	108	180

2. **1. Fanning mazmuni**

Fanni o‘qitishdan maqsad – talabalar kasbiy faoliyatida axborot tizimlari va axborot resurslarining kiberxavfsizligini ta’minlash bo‘yicha masalalarni yechishda bilim, ko‘nikma va malaka shakllantirishdan iborat.

Fanning vazifasi – talabalarni kiberxavfsizlikning asosiy tushunchalari bilan tanishtirish, kriptografiya asoslari, foydalanishni nazoratlash, tarmoq, bulutli hisoblash, buyumlar interneti va kompyuter xavfsizligini ta’minlashning hamda axborot xavfsizligiga tahdidlar va ularga qarshi kurashishni samarali usul va vositalarini o‘rgatishdan iborat.

2. Asosiy nazariy qism (ma’ruza mashg‘ulotlari)

I. Fan tarkibiga quyidagi mavzular kiradi:

1-bo‘lim. Xavfsizlik konsepsiyasi

1-mavzu. Kiberxavfsizlikning asosiy tushunchalari: Axborot xavfsizligining hayotdagi timsollari, kiberxavfsizlik, axborot xavfsizligi, konfidensiallik, yaxlitlik, foydalanuvchanlik, risk, hujumchi kabi fikrlash, tizimli fikrlash, aktiv, tahdid, zaiflik, boshqarish vositasi, kiberxavfsizlikning bilim sohalari.

2-mavzu. Risklarni boshqarish: Risk darajasi, chastotasi va matritsasi, risklarni boshqarish, muhim ko‘rsatkichlari, bosqichlari, tashkilotda risklarni boshqarishning freymvorki va axborot tizimlari (Risk Management Information Systems, RMIS).

3-mavzu. Kiberjinoyatchilik, kiberqonunlar, kiberetika va kriminalistika: ichki kiberjinoyatlar, tashqi kiberjinoyatlar, kiberqonunlar, milliy qonunlar, xalqaro kiberqonunlar, kiberetika, raqamli kriminalistika va mobil kriminalistika.

2-bo‘lim. Kiberxavfsizlik arxitekturasi, strategiyasi va siyosati

4-mavzu. Kiberxavfsizlik arxitekturasi, strategiyasi va siyosati: Kiberxavfsizlik arxitekturasi, strategiyasi, kiberxavfsizlik siyosati va uni amalga oshirish: xavfsizlik siyosatining zaruriyati, xavfsizlik siyosatining afzalliklari, xavfsizlik siyosatining iyerarxiyasi, xavfsizlik siyosati xususiyatlari, axborot xavfsizligi siyosatining turlari.

3-bo‘lim. Axborotning kriptografik himoyasi

5-mavzu. Kriptografiyaning asosiy tushunchalari: asosiy terminlar, kriptografiya bo‘limlari, kriptotizim, Kerkxofs prinsipi, kriptografiya tarixi, kriptografik akslantirishlar, bir martali bloknot.

6-mavzu. Simmetrik kriptografik algoritmlar: oqimli simmetrik shifrlash algoritmlari, A5/1 oqimli shifrlash algoritmi, blokli simmetrik shifrlash algoritmlari, simmetrik kriptotizimlardagi muammolar va afzalliklari, simmetrik kriptotizimlarda kalit uzunligi.

7-mavzu. Ochiq kalitli kriptotizimlar: bir tomonlama funksiya, faktorlash muammosi, modul arifmetikasi, RSA algoritmi, ochiq kalitli kriptotizimlardan foydalanish, ochiq kalitli kriptotizimlarda kalit uzunligi, afzalliklari va muammolar.

8-mavzu. Ma’lumotlar yaxlitligini ta’minlash usullari: xesh funksiya, xabarlarni autentifikatsiyalash kodi, elektron raqamli imzo tizimlari, ochiq kalitlar infrastrukturasi, X.509 raqamli sertifikat formati.

9-mavzu. Kriptografik ilovalar. Apparat-dasturiy shifrlash, apparat shifrlash, dasturiy shifrlash, disk va fayl tizim sathida shifrlash, kriptografik protokollar: SSH, SSL/TLS, IPSec, blockchain ilovalari, e-hukumat va elektron to‘lov ilovalari, elektron pochta ilovalari.

4-bo‘lim. Foydalanishni nazoratlash

10-mavzu. Identifikatsiya va autentifikatsiya vositalari: identifikatsiya, autentifikatsiya va avtorizatsiya, bir tomonlama va ikki tomonlama autentifikatsiya, ko‘p omilli autentifikatsiya, parol tizimlari, elektron qurilmalar, biometrik tizimlar.

11-mavzu. Ma’lumotlardan foydalanishni mantiqiy boshqarish: foydalanishni boshqarish, foydalanishni diskretsion boshqarish usuli (Discretionary access control, DAC), foydalanishni mandatli boshqarish usuli (Mandatory access control, MAC), foydalanishni rollarga asoslangan boshqarish usuli (Role-based access control, RBAC), foydalanishni attributlarga asoslangan boshqarish usuli (Attribute-based access control, ABAC), foydalanishni boshqarish matritsasi, ACL yoki C-list.

12-mavzu. Ko‘p sathli xavfsizlik modellari: Bell-LaPadula modeli, Biba modeli, mantiqiy va fizik foydalanishlarni boshqarish.

13-mavzu. Ma’lumotlarning fizik xavfsizligi: Fizik xavfsizlik, uning zaruriyati, fizik xavfsizlikka ta’sir qiluvchi omillar, tab’iy tahdidlar, sun’iy tahdidlar, fizik xavfsizlikni nazoratlash, boshqa fizik xavfsizlik choralari, ogohlik / o‘qitish, ma’lumotlarni xavfsiz yo‘q qilish: qog‘oz va elektron ma’lumotlarni yo‘q qilish usullari.

5-bo‘lim. Tarmoq xavfsizligi

14-mavzu. Kompyuter tarmoqlari va tarmoq xavfsizligi muammolari. Tarmoq turlari, tarmoq topologiyalari, OSI modeli, tarmoqqa qo‘yiladigan talablar, TCP/IP modeli, tarmoq vositalari. Zaiflik, tahdid, hujum, ichki tahdid, tashqi tahdid, razvedka hujumlari, kirish hujumlari, zararli hujumlar, xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari.

15-mavzu. Tarmoq xavfsizligini ta’minlovchi vositalar: tarmoqlararo

ekranlash, virtual xususiy tarmoqlar, suqilib kirishlarni aniqlash tizimlari (Intrusion Detection System, IDS), ma'lumotlarning sirqib chiqishini oldini olish tizimlari (Data Leakage Prevention, DLP), yolg'on nishonlar yoki tuzoqlar (honeypot).

16-mavzu. Simsiz tarmoq xavfsizligi: simsiz tarmoq turlari, simsiz tarmoqlardagi mavjud xavfsizlik muammolari, simsiz tarmoqlarda xavfsizlikni ta'minlash: WEP, WPA, WPA2 protokollari.

17-mavzu. Bulutli hisoblash tizimlari va IoT (Internet of Things - Buyumlar interneti) xavfsizligi: bulutli hisoblash tizimlari, modellari, xavfsizligi, maxfiylik va shaxsiylik masalalari hamda tahdid turlari, IoT tizimlari, arxitekturasi, tarmoq va apparat xavfsizligi, hamda tahdidlar turlari.

6-bo'lim. Foydalanuvchanlikni ta'minlash usullari

18-mavzu. Foydalanuvchanlik tushunchasi: zaxira nusxalash, ma'lumotlarni qayta tiklash va hodisalarni qaydlash: foydalanuvchanlik, zaxira nusxalash, zaxira nusxalash vositalari. RAID texnologiyasi, afzalliklari va kamchiliklari, zaxira nusxalash usullari, zaxiralash turlari. Ma'lumotlarni qayta tiklash, ma'lumotni yo'qolish sabablari, ma'lumotlarni qayta tiklash vositalari, hodisalarni qaydlash, Windows OTda hodisa turlari.

7-bo'lim. Dasturiy vositalar xavfsizligi va zararli dasturlardan himoyalanish

19-mavzu. Dasturiy vositalardagi xavfsizligi: veb saytlar bilan bog'liq xavfsizlik muammolari, keng tarqalgan veb zaifliklar, xavfsiz va xavfsiz bo'lmagan dasturlar tillari, kukini mos sozlash, brauzerlarda shaxsiy ma'lumotlarni himoyalash, Windows, Linux, Mobil OT lar xavfsizligi.

20-mavzu. Zararli dasturlardan himoyalanish: zararli dasturlar va ularning turlari, viruslar va ularning klassifikatsiyasi, viruslarni amalga oshiruvchi vazifalari, zararli dasturiy vositalarni aniqlash usullari va vositalari, ularning kamchiliklari.

8-bo'lim. Maxsus bo'lim

21-mavzu. Qayd yozuvini himoyalash va ijtimoiy injineriyaga qarshi himoya: qayd yozuviga aloqador ma'lumotlarni himoyalash, siz bilan aloqada bo'lgan tomon va aloqada bo'lmagan tomonlarda ma'lumotlarni himoyalash, parollar: parollarni generatsiyalash, boshqarish, saqlash va uzatish, parolga alternativ usullarni aniqlash. Kiberxavfsizlikda inson omili, ijtimoiy injineriya turlari, ijtimoiy injineriya mutaxassislari foydalanadilan prinsiplar, ijtimoiy tarmoqlarda ma'lumotlarni bo'lishmaslik, qalbaki ijtimoiy media ulanishlarini aniqlash, xavfsiz dasturiy vositalardan foydalanish.

3. Amaliy mashg'ulotlar

Amaliy mashg'ulotlar uchun quyidagi mavzular tavsiya etiladi:

1. Kiberxavfsizlikda risklarni baholashni o'rganish.
2-3. Klassik shifrlash algoritmlarini ishlash tartibini o'rganish.
4. TrueCrypt dasturi yordamida ma'lumotlarni shifrlashni o'rganish.
5. Operatsion tizimda (Windows OT) parolga asoslangan autentifikatsiya mexanizmini o'rnatish va sozlashni o'rganish.

6-7. Razvedka hujumini amalga oshirishni o‘rganish.
8-9. Tarmoqlararo ekran vositasi yordamida tarmoq himoyasini qurish.
10. Xavfsiz Wi-Fi simsiz tarmog‘ini qurish.
11. Maxsus dasturiy vositalar yordamida ma’lumotlarni qayta tiklashni o‘rganish.
12. Shaxsiy kompyuterlarda viruslarga qarshi himoyani o‘rnatish.
13. Parollardan foydalanishni boshqarishni o‘rganish.
14-15. Ijtimoiy tarmoqlardan ma’lumotlarni to‘plashni o‘rganish.

Amaliy mashg‘ulotlar multimediya qurilmalari bilan jihozlangan auditoriyada bir akademik guruhga bir professor-o‘qituvchi tomonidan o‘tkazilishi zarur. Mashg‘ulotlar faol va interaktiv usullar yordamida o‘tilishi, mos ravishda munosib pedagogik va axborot texnologiyalar qo‘llanilishi muqsadga muvofiq.

4. Mustaqil ta’lim va mustaqil ishlar

Talabaga berilgan mustaqil ishning asosiy maqsadi – o‘qituvchi rahbarligi va nazoratida muayyan o‘quv ishlarini mustaqil ravishda bajarish uchun bilim, ko‘nikmalarni shakllantirish va rivojlantirish.

Mustaqil ta’lim uchun tavsiya etiladigan mavzular:

1. Kiberxavfsizlikga oid milliy va xorijiy meyoriy-huquqiy hujjatlar tahlili.
2. Axborotni ximoyalashning kriptografik usullari.
3. Enigma shifrlash mashinasi va uning bardoshligi.
4. Axborotni foydalanuvchanligini ta’minlashda antivirus, IDS, IPS, TE vositalarining o‘rni.
5. Zararli dasturiy vositalarni klassifikatsiyasi va himoya usullari.
6. Axborot-kommunikatsiya texnologiyalari xavfsizligiga bo‘ladigan tahdidlar.
7. Zararkunanda dasturlarning turlari.
8. Kompyuter viruslari va virusdan himoyalanish usullari.
9. Xorijiy davlatlarning elektron raqamli imzo algoritmlari tahlili.
10. Identifikatsiya va autentifikatsiya tushunchasi va vazifalari.
11. Axborot tizimlari va resurslaridan ruxsatsiz foydalanishlarni aniqlash uslubiyati.
12. Simsiz aloqa tizimlarida axborot resurslarini himoyalash.
13. Axborotni ruxsatsiz foydalanishlardan himoyalash.
14. Ijtimoiy injeneriyada hujumlar tahlili.
15. Zamonaviy antivirus dasturiy vositalari va ularning imkoniyatlari.
16. Kiberjinoyat va kiberhuquq.
17. Tarmoqda uzatiluvchi axborotni himoyalashda kriptografiyaning o‘rni.
18. Zararkunanda dasturlar va ulardan himoyalanish (masalan, Malwarebytes misolida).
19. Kiberjinoyatchilik va uni keng tarqalishining sabablari.
20. Yuz tasviriga asoslangan autentifikatsiya usuli va uning xususiyatlari.
21. Barmoq iziga asoslangan autentifikatsiya usuli va uning xususiyatlari.
22. Elektron raqamli imzo va uni resublikamizda tadbiq etilish holati.
23. Kiberxavfsizlik sohasi bo‘yicha mutaxassis toifalari.

	24. Kiberxavfsizlik sohasida karyera yo‘llarini o‘rganish. 25. Axborot xavfsizligi sohasida ish boshlash. 26. Kiberxavfsizlik sohasida mashhur sertifikatlar. 27. Parollarni boshqarish tizimlari (masalan, LastPass) va ulardan foydalanish. 28. Virtual himoyalangan tarmoq va undan amaliyotda foydalanish (masalan, CyberGhost yoki ExpressVPN misolida). 29. Sotsial injineriya nima va uning zamonaviy usullari. 30. ESET NOD32 antivirus vositasidan foydalanish. 31. Kaspersky antivirus vositasi va undan foydalanish. 32. Biror tarmoklararo ekran vositasini (masalan, ZoneAlarm) o‘rnatish va sozlash. 33. Virtual ximoyalangan tarmok va undan amaliyotda foydalanish (masalan, CyberGhost yoki ExpressVPN misolida). 34. Windows OTda foydalanuvchi qayd yozuvini (xususan, paroldan foydalanish siyosatini) sozlash. 35. Windows OTda zaxira nusxalashni (Backup and Restore) amalga oshirish. 36. Windows OTda imtiyozlar turlari, fayl va kataloglar uchun foydalanishni boshqarish tartibi. 37. Linux OTda imtiyozlar turlari, fayl va kataloglar uchun foydalanishni boshqarish tartibi. 38. Ma’lumotlarni qayta tiklash vositalari (masalan, Recuva yoki EaseUS Data Recovery Wizard Pro) va ular yordamida ma’lumotlarni qayta tiklash. 39. VeraCrypt dasturiy vositasi yordamida ma’lumotlarni himoyalash. Mustaqil o‘zlashtiriladigan mavzular bo‘yicha talabalar tomonidan mustaqil ishlar tayyorlash, uni taqdimot qilish va amalda bajarish tavsiya etiladi.
3.	**Ta’lim natijalari / Kasbiy kompetensiyalar** Fanni o‘zlashtirish natijasida talaba: – kiberxavfsizlikni ta’minlash aspektlarini huquqiy, tashkiliy va texnik sathlari; – kiberxavfsizlik tamoyillari haqida *tasavvurga ega bo‘lishi;* – kiberxavfsizlikning asosiy tushunchalari va ta’riflarini; – kiberxavfsizlikning huquqiy-meyoriy bazasini; – kiberxavfsizlik sohasida xalqaro, milliy va idoraviy meyoriy-huquqiy bazani; – axborotning konfidensialligi, butunliligi va foydalanuvchanligi tushunchalarini *bilishi va ulardan foydalana olishi*; – kiberxavfsizlikka tahdidlarning asosiy turlari hamda ularga qarshi kurashish metod va usullarini tushuntirib berishi; – axborotning maxfiyligi, butunligi va foydanuvchanligining buzilishi usullarini tahlil qilish; – axborotning yo‘qolishi va buzilishi sabablari, turlari, kanallarini tahlil qilish; – axborotni himoyalash usullari va vositalarini qo‘llash; – kriptografiya, foydalanishni boshqarish, tarmoq va kompyuter xavfsizligini

	5. https://www.youtube.com/watch?v=TySFu5_4n8o&list=PLURBKSuWbZEOhFKGsR0fqAk8i7RxtRoV0
7.	Fanning o'quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining 2025-yil 29.04 8/4(tasdiq)-son bayonnomasi bilan tasdiqlangan.
8.	**Fan/modul uchun ma'sullar:** Xudoykulov Zarif Turakulovich – Muhammad al-Xorazmiy nomidagi TATU, "Kriptologiya" kafedrasi mudiri, PhD, dotsent.
9.	**Taqrizchilar:** Allanov O.M. – Muxammad Al-Xorazmiy nomidagi TATU, "Kiberxavfsizlik va kriminalistika" kafedrasi mudiri, PhD, dotsent (turdosh OTM). Axmedova O.P. – Fan texnika va marketing tadqiqotlari markazi – "UNICON.UZ" MCHJ Axborot xavfsizligi va kriptologiya Ilmiy-tadqiqot bo'limi boshlig'i, t.f.n. (turdosh ITM).

	ta'minlash *ko'nikmalariga ega bo'lishi kerak.*
4.	**Ta'lim texnologiyalari va metodlari:** – ma'ruzalar; – interfaol keyslar-stadilar; – seminarlar (mantiqiy fikrlash, tezkor savol javoblar); – guruhlarda ishlash; – taqdimotlarni qilish.
5.	**Kreditlarni olish uchun talablar:** Fanga oid nazariy va uslubiy tushunchalarni to'la o'zlashtirish, tahlil natijalarini to'g'ri aks ettira olish, o'rganilayotgan jarayonlar haqida mustaqil mushohada yuritish, oraliq nazorat shakllarida berilgan vazifa va topshiriqlarni bajarish, yakuniy nazorat bo'yicha yozma ishni topshirish.
6.	**Asosiy adabiyotlar** 1. Robin Sharp, Introduction to Cybersecurity: A Multidisciplinary Challenge, Textbook, - Springer Cham, 2023. – 452 p. 2. S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoykulov. Kiberxafsizlik asoslari: o'quv qo'llanma, -T.: "Nihol print" OK, 2021. – 224 b. 3. С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев. Основы кибербезопасности: учебное пособие, -Т.: «Mahalla va oila nashriyoti», 2021. -240 с. **Qo'shimcha adabiyotlar** 1. Tairakawa Kousho. Securing the Digital Frontier: An Introduction to Cybersecurity for Beginners. Independently published, 2023. — 139 p. 2. В.Ф.Шаньгин, Информационная безопасность компьютерных систем и сетей: учебное пособие - М. : ФОРУМ : ИНФРА-М, 2019. - 416 с. 3. Ian Neil. (2018). CompTIA security+ certification guide: master IT security essentials and exam topics for CompTIA security+ SY0-501 certification, Birmingham: Packt Publishin. (online access from PolyU Library) (No. of words required: 10,000 words). 4. Wu, C. (2021). IoT Network Layer Security. In Internet of Things Security (Advances in Computer Science and Technology, pp. 107-123). Singapore: Springer Singapore, (online access from PolyU Library), ISBN: 9811613710 ISBN: 9789811613715, DOI: 10.1007/978-981-16-1372-2_7. **Internet saytlari** 1. https://csec.uz/uz/ 2. https://unicon.uz/ 3. https://lex.uz/ru/docs/-5960604 - O'zbekiston Respublikasining KIBERXAVFSIZLIK TO'G'RISIDA Qonuni, 15.04.2022 yildagi O'RQ-764-son 4. https://www.youtube.com/watch?v=_HcACxBsBLg