ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

ЎЗБЕКИСТОН РАДИОТЕХНИКА, ЭЛЕКТРОНИКА ВА АЛОҚА ИЛМИЙ-ТЕХНИКА ЖАМИЯТИ

ИҚТИСОДИЁТНИНГ РЕАЛ ТАРМОҚЛАРИНИ ИННОВАЦИОН РИВОЖЛАНИШИДА АХБОРОТ–КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ АҲАМИЯТИ

Республика илмий-техник анжуманининг

МАЪРУЗАЛАР ТЎПЛАМИ

3-ҚИСМ

СБОРНИК ДОКЛАДОВ

Республиканской научно-технический конференции

ЗНАЧЕНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ИННОВАЦИОННОМ РАЗВИТИИ РЕАЛЬНЫХ ОТРАСЛЕЙ Э КОНОМИКИ

ЧАСТЬ 3

6-7 апрел 2017 йил

ТОШКЕНТ – 2017

Конференция ташкилий қўмитасининг

Т А Р К И Б И:

Тешабаев Т.З.	раис, ректор
Усмонов Б.Ш.	раис ўринбосари, ИИ проректори
Мухидинов М.М.	РЭА ИТЖ раиси ўринбосари
Муллабоев К.Ю.	ЎзР Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги бўлим бошлиғи
Назарова М.Х.	ЎзР Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги бўлим бошлиғи
Умаров Х.П.	МАТИ бўйича проректор
Синдаров Ш.Э.	М ва И бўйича проректор
Хамдамов Р.Х.	ДМваАДМЯ маркази директори
Хасанов Х.П.	UNICON.UZ ДУК директори
Иминов Т.К.	“АЛСКОМ” компанияси директори
Давронбеков Д.А.	ЎзР Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги бўлим бошлиғи
Исманов К.	Телекоммуникация факультети декани
Закирова Ф.М.	КТ факультети декани
Нуралиев Ф.М.	ТТ факультети декани
Тураев Ш.Ш.	И ва Б факультети декани
Ташев К.А.	АТ факультети декани
Шакаров К.А.	Магистратура бўлим бошлиғи
Ульянова Н.В.	ИПКТ бўлим бошлиғи
Рахимов Н.О.	Катта илмий ходим - изланувчи
Алламуратова З.Ж.	котиба, ИПКТ бўлимининг катта илмий ходим-изланувчиси

4-Шўъба.

АХБОРОТ-КУТУБХОНА ВА АРХИВЛАР ЖАРАЁНЛАРИНИ БОШҚАРИШ

ЁШЛАРДА КИТОБХОНЛИК КЎНИКМАЛАРИНИ ШАКЛЛАНТИРИШДА ОИЛАНИНГ ТУТГАН ЎРНИ

Б. И. Ганиева
(ТАТУ, кафедра мудири)

Китобнинг инсон ҳаёти, кишилик жамияти маънавий тараққиётидаги беқиёс ўрни қадимдан маълум. У дунёни таниш, билим бериш билан бирга гўзалликка муҳаббат уйғотиш, ундан завқланиш, ёвузликдан нафратланиш туйғусини пайдо қилади. Болалар китобхонлигини ташкил қилишда ахборот-кутубхона муассасаси, умумий ўрта таълим муассасалари ҳамда оила зиммасига ниҳоятда мураккаб ва масъулиятли вазифа юкланади.

Оила китобхонлиги бу - оила аъзоларининг ақл-заковати ва юксак маънавиятини шакллантирувчи, инсон маънавий дунёсини бойитувчи, китобга меҳр-муҳаббат ҳамда уни заруриятга айлантиришнинг маълум тизимидир. Бу тизим ўсмирларнинг ақлий, маънавий, ахлоқий, эстетик ривожланиши тизимидан иборат бўлиб, ўзбек оилаларининг китобхонликка доир бой анъанаси ва ҳозирги даврда тўпланган бой тажрибасига асосланади.

Бугунги кунда китобхонлик сифат жиҳатдан янги босқичга кўтарилмоқда. Ёшлар маънавияти тадрижий ривожланиб борувчи фаол жараён. Шу жиҳатдан оилада китобхонликни шакллантиришда, китоблар воситасида тарбиялашда қуйидаги омилларга эътибор берилиши лозим:

1. Болаларда китоб ўқиш иштиёқини ҳосил қилиш.
2. Китоб танлашда боланинг маънавий даражасини ҳисобга олиш лозим.
3. Китоб танлашга ихтисослашиш.
4. Китобни экспертизадан ўтказиш.
5. Китоб ўқишни кузатиб, назорат қилиб бориш.

Бу масалалар ниҳоятда мураккаб бўлиб, болаларнинг китобхонликка бўлган муносабатини белгилайди. Тан олиш керак, ёшларимизнинг бугунги китобхонлик даражаси юксак даражада эмас. Бу ижтимоий муаммодан чиқишнинг ягона йўли ота-онанинг ёрдамга келишидир. Мактабда ўқитувчи, уйда ота-она болада китоб ўқиш кўникмасини ҳосил қилиши керак. Бунда оддийдан мураккабликка, яъни мураккаблиги жиҳатидан нормал, боланинг камолот даражасига мос бўлган китоблар танлаш қўл келади. Шарқ мутафаккирларининг тажрибасига кўра, китобхон қайси мавзуга қизиқса шу мавзудаги китобни тақдим қилиш, китоб ўқишга кўникма ҳосил қилгач эса аста-секин унга ихтисослашган китоблар тақдим қилиб борилади.

Ота-онанинг болада китоб ўқиш кўникмасини ҳосил қилишдаги илк вазифаси китоб танлаб беришдир. Уларнинг савиясига мос бўлган адабиётларни кенг тарғиб қилиш ёшларни жамиятнинг муносиб фуқароси, мустақил давлатимизнинг етук, баркамол инсонлари бўлиб етишиши учун ва маънавиятининг юксаклиги билан оиласига ва жамиятга фойда келтиришга олиб келади. Китоб танлашда китобхоннинг маънавий даражасини ҳисобга олиш бирмунча мураккаб омилдир. Бунда боланинг маънавий даражасига таяниш, унинг интеллектуал ўсишига олиб келади. Боланинг ёш хусусиятини, психологик имкониятларини ҳисобга олиш унинг рационал ўсишига олиб келса, маънавий даражасини ҳисобга олиш эса интеллектуал ривожлантиради. Бу эса рационалликдан кўра кенг қамровли ва самаралидир. Шунинг учун бутун оилада китобхонлик руҳи бўлиши керак. Бунда оиладаги китобга бўлган муносабат, биринчи навбатда, ота-онанинг китобга бўлган муносабати муҳим омил ҳисобланади. Оилада китобхонлик руҳи бўлса, бу бевосита боланинг руҳиятига ҳам таъсир этади. Юқорида таъкидланганидек, бунда илк тавсияни бадиий адабиётдан бошлаб, кейинчалик маълум бир ихтисослар бўйича китобларни тавсия этиш мумкин.

Бошланғич босқичларданоқ ўсмирнинг маънавий дунёси, тарбия муҳити, қизиқиши, дунёқараши ва психологик хусусиятлари ҳисобга олиниб, ихтисослаштирилиб

борилиши керак. Бу тажриба Америка таълим тизимида ўзини оқлаган. Америка тажрибасига асосан, болани 12 ёшга қадар ихтисослаштиришга ҳаракат қилинади ва шу асосда китоб танлаб берилади. Бу дастлаб мутахассисларни чўчитган эди, лекин Америка таълим тизимининг кейинги 30 йиллик тажрибаси ўсмирларни бошланғич синфлардаёқ ихтисослаштириш самарали эканлигини исботлади. Бунда асосий натижа ўсмирда мустақил фикрлаш ва ҳаракат қилишга интилишнинг пайдо бўлишига эришилди.

Ота-она бола учун китоб танлаётганида китобнинг маъно-мазмуни, услубий жиҳатдан мутахассис тавсиялари асосида танлаши мақсадга мувофиқ. Бу тарбиянинг асосий йўналишидан чалғимасликка, ўсмир маънавий дунёсининг тўғри шаклланишига ва қўйилган мақсадга етишишга олиб келади. Бу ўзбек миллий педагогикаси тажрибасидан ҳам маълум. Улар талабга жавоб бермайдиган китобни ўз фарзандига ўқишни қатъий тақиқлаган. Бугун ҳам бу тарбия жиҳати муҳим саналади. Ота-оналар тарбия жараёнининг натижаси бўлган китобхонлик билан кўпроқ қизиқиши керак. Шу маънода ўсмирлар китобхонлигини мониторинг қилиб бориш мақсадга етишнинг самарали жиҳатларидан биридир.

Мониторинг, ўқилган китоблар юзасидан савол-жавоблар, китобхонлик кечалари, мулоқот, давра суҳбатлари, турли мавзуларда мунозаралар, илмий-амалий анжуманлар, суҳбатлар, социологик-эмпирик тадқиқотлар ва аналитик текширувлар воситасида амалга оширилиши мумкин. Китоб ўқишни мониторинг қилиб боришда хориж тажрибаларига мосланиш янада мақсадга мувофиқдир.

Бугунги кунда ўсмирларда китоб ўқиш кўникмасини ҳосил қилиш учун асосий мақсад тарғиботнинг янгича турли усуллари асосида маданий-тарихий, маънавий-ахлоқий меросни тарғиб қилиш, ўтган буюк мутафаккирлар ижодларини кенг ёйиш, ота-боболаримиз, буюк аждодларимиз қолдирган бой маданий ва маънавий меросга садоқатни тарбиялаш, муқаддас қадриятларимизни сақлаш ва асраб-авайлашдек туйғуларини уйғотиш каби тарғиботни кенг йўлга қўйишимиз керак.

Фақат бу борада биз китоб воситасида тарбиялашнинг янги усул ва механизмларини яратишимиз лозим.

Ота-оналар болаларга китоб танлашда, айниқса боланинг ёши, психологияси, қизиқиши, дидини ҳисобга олиши ёки зарурият пайдо бўлганда мутахассислар билан маслаҳатлашиши керак. Шу билан бирга ҳар бир бадиий юксак асарнинг тарбиявий жиҳатларига ҳам эътибор бериш зарур.

Оилаларда яна бир муҳим муаммо – китобни асраш ва уни ўзидан кейинги оила аъзоларига ёки бошқаларга етказишдир. Кўпинча биз кузатган оилаларда китоб танлаш, уни ўқишга эътибор берилади-ю, лекин авайлаб-асрашга, китобга меҳрни тарбиялашга бефарқ қарайдилар. Кузатишлар натижасида дарсликлар, жуда кўп рангли болаларбоп китоблар йиртилиб, чизилиб, ахлат қутиларига ташланганлигининг гувоҳи бўлдик. Болаларга “Китоб ҳам нондек азиз”лигини тушунтиришда катталарнинг ўзи ибрат бўлиши зарур. Олимларнинг фикрича бир одам бутун умри бўйи 2000 та китоб ўқий олиш имкониятига эга экан. Шунинг учун болалик, кейинчалик ўсмирлик йилларида ўқилган китоб унда бир умрга ёрқин таасуротлар қолдириши муқаррардир.

Боланинг камолоти – бу жамият камолотидир. Камолга етган индивидлар жамият ривожи ва камолотини белгилайди. Бугунги экилган яхшилик уруғи – болалар китобхонлигини тарбиялаш, эртанги кун учун мустаҳкам ва баракали ҳосил. Бугунги китобга меҳр қўйган бола, эртанги вояга етган мустақил Ўзбекистонимизнинг мустакил фикрловчи фуқаросидир. Шунинг учун ҳам кенг жамоатчилик эътиборини болалар ва ўсмирлар китобхонлиги эстетик диди ва маънавий дунёсини шакллантиришга қаратиш зарур. Ўзлигимизни англаётган бугунги кунда инсонларнинг онги ва руҳиятини ҳам тарбиялашдек улкан вазифа қўйилаётган экан - болаликка, ҳусусан унинг китобхонлигига бепарво бўлмайлик.

ЭЛЕКТРОННАЯ БИБЛИОТЕКА ПО ТЕХНИЧЕСКОЙ РЕАБИЛИТАЦИИ

М.А.Рахматуллаев (профессор ТУИТ)

Применение ИКТ в сфере информационно-библиотечного дела привело к существенному прогрессу не только в услугах сугубо библиотечного характера, но и при создании баз данных различного назначения. Принципы и методы, применяемые при разработке электронных библиотек оказались эффективны и в других областях, включая медицину. Значительные успехи медицины последних десятилетий во многом обязаны применению современных средств вычислительной техники.

Проект TechRehab - TECHNOLOGY OF REHABILITATION (ТЕХНОЛОГИЯ РЕАБИЛИТАЦИИ), выполняемый по гранту программы ERASMUS++ имеет следующие цели: создание основ для использования новых методологий и новых технологических инструментов в деятельности по реабилитации посредством (I) реализации магистерской программы по данной области, (II) установки и настройки специализированного оборудования, (III) реализация платформы ИКТ для электронного обучения , распространения знаний, гармонизации и интернационализации.

Проект выполняется в ТУИТ совместно с партнерами

<u>От ЕС:</u>

University of Sannio, (Италия), Университет Пьера и Марии Кюри (Франция), Медицинский университет в городе Пловдив (Болгария), Европейская ассоциация физической и реабилитационной медицины(Эстония), Вильнюсский университет (Литва), PLUX - Wireless Biosignals, S.A. (Португалия)

<u>Узбекистан:</u>

Филиал Ташкентского университета информационных технологий в Карши, Ташкентский педиатрический медицинский институт (ТПМИ), Филиал Ташкентского педиатрического медицинского института в Нукусе, Центр внедрения электронного образования в образовательных учреждениях при МВССО, Республиканский специализированный научно-практический медицинский центр терапии и медицинской реабилитации. Системы технической реабилитации имеют три важных компонента: технически средства (hardware); программные средства (software) и базы данных (database). Технические средства включают весь комплекс средств вычислительной техники, от датчиков до серверов. Программные средства включают компьютерные программы по обработке сигналов, получаемых от датчиков, программы отображения информации на экране, формирования статистической информации и т.д. База данных включает данные о клиентах (пациентах), аналитической информации, статистической информации и т.д.

В данной статье рассмотрены вопросы по формированию баз данных, разрабатываемых в виде электронных библиотек. Электронная библиотека технической реабилитации включает электронный каталог пациентов плюс всю информацию о них с учет ом динамики изменения их состояния.

Система дистанционного контроля реабилитируемых клиентов является одной из подсистем системы технической реабилитации и предназначена для сбора и обработки биосигналов от клиентов (инвалидов), нуждающихся в реабилитации.

Система обработки сигналов – это программно-технический комплекс для сбора биометрических сигналов о состоянии клиента. Причем видов сигналов может быть множество: давление, температура, сердечный пульс(ритм) и др. Для получения сигналов используются датчики.

Система мобильной связи здесь служит для передачи сигналов системе средствами оператора мобильной связи.

Система телеметрической обработки предназначена для аналогово-цифрового преобразования сигналов и включения данных о состоянии клиентов в базы данных по различным показателям.

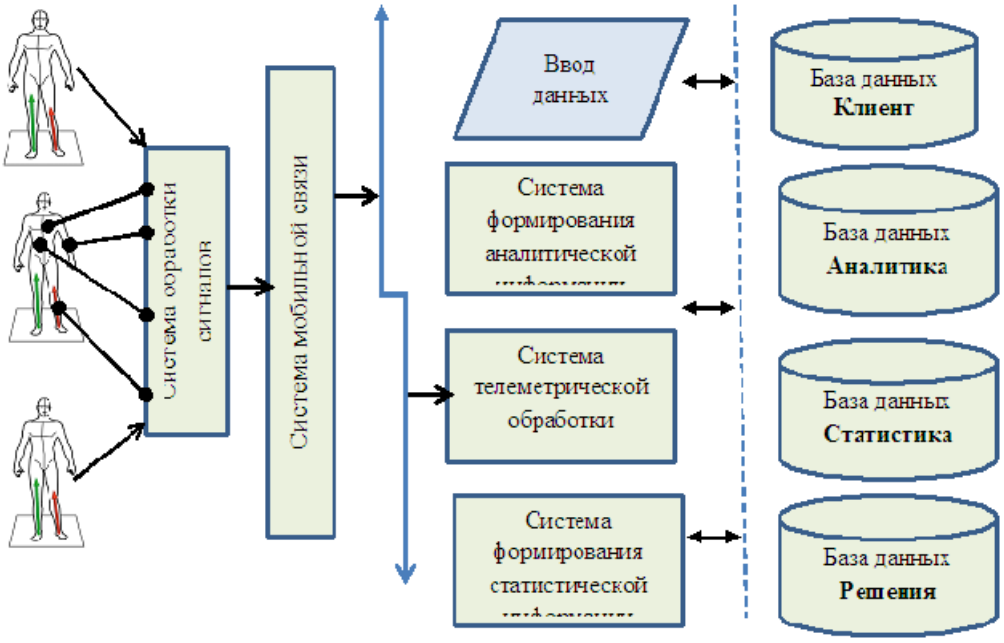


Рис.1. Система дистанционного контроля реабилитируемых клиентов

Функция «Ввод данных» предназначена для формирования базы данных (База данных «Клиент») об инвалидах (клиентах), нуждающихся в реабилитации. Эта база данных включает полную информацию об клиентах, включая его идентификационный номер (ID), фамилию, имя, отчество, диагноз, характеристики болезни, а также критерии оценки состояния, получаемых от датчиков. Кроме того указывается дата измерения состояния.

База данных **Клиент**

ID	ФИО	Адрес	Характеристика заболевания	Критерии оценки состояния					Период
				K_1	K_2	K_3		K_n	
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.

Система формирования аналитической информации предназначена для формирования базы данных о динамике (База данных «Аналитика») изменения состояния клиента в процессе реабилитации. Формируются графики зависимостей проведённых лечебных реабилитационных процедур и значений критериев оценки состояния клиента.

База данных **Аналитика**

ID	Динамика изменения состояния клиента				
1.	2.	3.	4.	5.	6.

Система формирования статистической информации предназначена для расчета статистических данных

База данных **Статистика**

ID	Вид заболеваний		Характеристика заболевания	Ход реабилитации	
1.	2.	3.	4.	5.	6.

Полученная информация о состоянии пациента позволяет принимать решения о методике (тактике) реабилитации, стандартные решения о которых хранятся в базе данных Решения по реабилитации.

База данных **Решения по реабилитации**

№	Вид заболеваний	Характеристика заболевания	Технические решения по реабилитации	Методика реабилитации	Примечание
1.	2.	3.	4.	5.	6.

Применение современных информационных технологий в реабилитации позволяет:

- Существенно снизить риск повторного кризиса заболевания
- Оперативно прослеживать за состоянием больным
- Получать статистическую информацию о динамике состояния больного
- Принимать экстренные меры при ухудшении состояния больного.

СОЗДАНИЕ ИНДЕКСА ЦИТИРОВАНИЯ В УЗБЕКИСТАНЕ. ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Хайруллаев Б. А. (магистрант ТУИТ),
М. А. Рахматуллаев (профессор ТУИТ)

На протяжении нескольких десятилетий, в западных странах оценка качества академических журналов, квалификация исследователей и научных организаций, проводится путем подсчета цитирования в научных статьях. Каждый академический журнал среди остальных обладает своей собственной репутацией, надёжностью, популярностью, а также недостатками. Исходя из этого, оценка статьи происходит по следующему принципу – «Чем качественнее уровень академического журнала, в котором опубликована научная работа, тем выше качественный оценочный уровень статьи». Статья, опубликованная в журнале с высоким рейтингом, влияет на репутацию исследователя, следовательно, значительно повышая влиятельность в научной среде. Уровень академического журнала, определяется наукометрическими параметрами, такими как impact Factor (IF), h-index, eigen factor и другими наукометрическими индексами. Все эти общепринятые наукометрические индексы базируются на индексе цитирования (Citation Index).

Формализация описания научных статей, стандартизация их представления сделало возможным определение данных цитирований в программных комплексах. Описываются возможности моделей таких как: BIBO, Dublin core, FRBR, MARC 21, ORB, PRISM, RDA, SRO, SKOS, SPAR, SWAN.

В данном докладе излагаются подход и алгоритм создания индекса цитирования, которые могут быть использованы для обработки научных журналов в Узбекистане.

Рассмотрим функциональную структуру системы определения индекса цитирования научных журналов, который состоит следующих подсистем:

- Ввод данных – выполняет основную задачу, формирует в базе данных полный текст, метаданные о журналах, номеров, выпусков, статей, организаций.
- Обработка данных (извлечение/разбивка) – формирует в базе данных основной массив информации, который в дальнейшем необходим в процессе анализа и расчета наукометрических параметров. Подсистема выполняет задачу автоматизированного извлечения из:

  - номеров журнала полного текста формата PDF, в XML формат статей;
  - статей, такие метаданные как название, автор и соавторы, аннотация, ключевые слова, цитирования;
  - библиографической базы данных, других систем, а также структурированное размещение выше перечисленной извлеченной информации в базе данных системы.

- Индексирование пристатейных ссылок – подсистема производит поиск цитирований, из статей номера журнала, в базе данных системы. В процессе формирует таблицы сущности цитирований за каждый год, и для поступивших новых статей, ставится значение по цитированию «0». Для поступившей каждой

статьи, ссылающийся на источник, суммирует значение «1» источнику, а если в БД системы не существует библиографического описания источника, то оно переносится в БД пристатейных ссылок и присваивается данное значение.

- Подсчёт цитирования и наукометрических параметров – подсистема формирует итоговое значение суммы каждому библиографическому описанию, номеру и тому журнала.
- Вывод данных – подсистема выводит массив данных запрошенной пользователем системы в запрашиваемой форме.

Реализация индекса цитирования на сегодня предполагает несколько этапов и создание основных разделов, таких как:

- базы данных;
- извлечения (extract and parsing) данных (Процесс – 2);
- присвоение цитирований (Процесс – 3);
- расчёта цитирования и наукометрических индексов (Процесс – 3, 4, 5);
- интерфейсов ввода и вывода информации (Вывод).

Этап I. Извлечение данных. Издательства, выпуская в свет очередной номер журнала, издают в печатной и в электронном формате. Одним из основных требований является выпуск номеров онлайн в доступе. Для подсчета цитирований и других наукометрических индексов, издательства на договорной основе отправляют номера журналов в формате PDF, аналитическим системам. Решаются вопросы по автоматизации процесса извлечения/преобразования в другой формат статей и метаданных. Существует несколько готовых решений подсистем конвертирования, таких как: Apache PDFbox, Pdf2xml, LA-PDFText, Cermine, PDFX. Данные подсистемы конвертируют в полу-структурированный вид документ формата pdf, в формат такие как xml, txt, html и другие, которые можно легко преобразовать и использовать.

Этап II. Обработка полу-структурированных документов. Этап представляет извлечение БС из множеств документов, таких как научных статей, и других научных работ, которые содержат БС в документе. В большинстве научных документах БО представляется в виде сносок или в источнике литературы содержащий БС в конце документа. Общее количество документов в БД, может быть довольно большим от несколько тысяч документов.

Разработанный алгоритм предназначен для присваивания новых ID тегов в тексте, или идентификаторов цитирования для каждого извлечён нового БО. После извлечения новой БО и его значения в тексте (тега), в фигуре I, новый тег сравнивается в II, с существующими тегами в таблице ID тегов, в фигуре III. Данный процесс выполняет сравнение начального имени автора в новом БО, с каждым существующим БО, в фигуре III. Если совпадение найдено в любом из БС, то в фигуре IV, программа сравнивает информацию репортера между новой и найденной ссылкой (БО). Если найдено соответствие между репортером и информацией, в фигуре V, данные репортера совпали с количеством данных цитирования (БС), то два БС считаются идентичными. В этом случае, только извлеченный тег присваивается число уже существующий присвоенный тег, в фигуре VI, и этот номер тега присваивается различным таблицам базы данных. В частности, ID документа из которого было извлечено цитирование, добавляется к существующим ID документам, для присвоения идентификатора тега или идентификатора цитирования (БС), в таблице ID тегов (в таблице идентификатора тега).

Если вновь извлеченный тег еще не существует в таблице ID тегов, из процессов сравнения IV, V присваивается тегу новый номер, данный процесс происходит в фигуре VII, и помещается как новая запись цитирования (БО), в таблицу ID цитирования, а также в другие таблицы в базе данных.

Таким образом, реализация предложенного метода и программной реализации позволит создать электронную библиотеку научных журналов, проиндексировать ее на предмет выявления наиболее цитируемых журналов из базы данных.

АХБОРОТ-КУТУБХОНА, АРХИВ ВА МУЗЕЙ МУАССАСАЛАРИДА ФОЙДАЛАНУВЧИЛАРГА АХБОРОТ ХИЗМАТИ КЎРСАТИШНИНГ УМУМИЙ ВА ЎЗИГА ХОС ТОМОНЛАРИ

М.Х.Махмудов (ТАТУ доценти, педагогика фанлари номзоди)

Кейинги йилларда кутубхоналар, архивлар, музейлар, илмий-ахборот органлари фаолиятини координациялаш ва кооперациялаш зарурияти ҳақида фикрлар кўпайиб бормоқда. Табиийки уларни ўзаро фаолияти қандай асосда бўлиши керак деган масалани ҳал этиш зарур бўлади. Ушбу асосларни аниқлаш ва шакллантиришда юқоридаги муассасаларнинг асосий фаолиятларидан бири бўлган-ахборот хизмати кўрсатишнинг умумий ва ўзига хос томонларини таҳлил қилиш орқали эришиш мумкин деб ўйлаймиз.

ГОСТ 7.0-99 “ Ахборот-кутубхона фаолияти, библиография” га кўра *ахборот хизмати* тушунчаси “ фойдаланувчиларни зарур ахборот билан таъминлаш учун, ахборот органлари ва хизматлари томонидан тавсия этиладиган ахборот хизматларидир”. Бу тушунчани на фақат кутубхоналардан фойдаланувчиларга, балки архив ва музейлардан фойдаланувчилар учун ҳам қўллаш мумкин.

Ахборот хизмати орқали юқоридаги муассасалар ўзларини асосий функцияларидан бирини амалга оширадилар. Бу функция бизнингча ахборотни тўплаш, қайта ишлаш, сақлаш ва уни фойдаланувчиларга етказишдир. Ахборот хизмати кўрсатиш функцияси орқали ижтимоий тажрибалар, маданий бойликлар ҳозирги ва келгуси авлод учун етказилади ҳамда тўпланган ахборот ресурсларидан одамларни ахборот ва маданий талаблари қондирилади.

Юқоридаги ахборот муассасаларни бир қанча ўзига хос функциялари бўлиши билан бирга улар учун умумий бўлган жиҳатлар ҳам мавжуд. Шулардан бири фойдаланувчиларга ахборот хизмати кўрсатишдир.

Кутубхон, архив, музей ва бошқалардаги ахборот хизмати кўрсатиш умумий мазмунга эга бўлиши билан бирга, хизмат кўрсатиш шакллари билан бир-биридан фарқ қилади. Агар кутубхона учун бу - ҳужжатларни вақтинча фойдаланиш учун бериш ёки маълумот бериш бўлса, музейлар учун - бу кўргазмалар хизмати, экскурсиялар ташкил этишдир. Бу дегани кутубхоналар ва архивлар кўргазмалар ташкил этмайди, музейлар, ҳужжатлар ва маълумотномалар бермайди дегани эмас. Гап бу ерда асосий хизмат кўрсатиш шакллари ҳақида кетаяпти. Шунга асосланган ҳолда кутубхоначилик, архив ва музей хизматини фойдаланувчиларни зарур ахборот билан кутубхоначилик ёки архив ёки музей ва бошқа хизмат кўрсатиш билан таъминловчи ахборот хизматини турларидан бири сифатида қарашимиз мумкин.

Янги ахборот технологияларини кенг қўлланилиши натижасида ахборот муассасалари кўрсатадиган хизматлар орасидаги чегаралар сезиларли равишда йўқолиб бормоқда. Уларни кўпчилиги Интернетдан фойдаланмоқдалар, энг муҳим шакллардан бири кўргазмалар бўлмоқда: музейлар ўзларини экспозияларини намойиш этмоқдалар, кутубхоналар китоб бойликларини, архивлар – ноёб ҳужжатларни ва бошқа. Юқоридаги муассасаларда *тақдимот* шаклидан кенг фойдаланилмоқда.

Ҳужжатлардан нусҳа олиш имкониятларининг пайдо бўлиши эса кутубхона ва архив муассасаларида ҳужжатларни вақтинчалик фойдаланиш учун бериш эмас, балки ҳужжатни нусҳасини сотиш имкониятини бермоқда. Хизмат кўрсатишнинг умумийлиги – ўзаро бир-бирига боғлиқ бўлган қизиқишларни ва ахборот муҳитида интеграциялаш тенденциясини вужудга келиши сабабларидан бири бўлиши мумкин. Кейинги йилларда кутубхона, архив ва музейларни ҳамкорликдаги лойиҳаларнинг яратилиши бунга мисол бўлиши мумкин.

Хизмат кўрсатиш-бу фойдаланувчиларни ахборот ресурсларига яқинлаштириш механизми бўлиб, улардан фойдаланиш ҳуқуқини беради. Кутубхоначи китобни сақлаш хоналаридан қидириб топиб ва уни китобхонга бериш орқали китобхонни ундан

фойдаланишини таъминлайди; музей ходими экскурсия воситасида рассом ижодини, уни асарини тушунишни енгиллаштиради; архив ходими фондлар бўйича йўл кўрсатқичлар орқали фойдаланувчиларни фондларга яқинлаштиради. Фойдаланувчиларни ахборотлардан фойдаланишларини таъминлаш-барча ахборот муассасалари амалга оширадиган ахборот хизмати кўрсатишнинг *иккинчи* умумий жиҳати ҳисобланади.

Ахборотга киришни, ундан фойдаланишни таъминлаш орқали ушбу муассасалар интеллектуал эркинликка, жамиятни демократлаштириш, билимни, таълимни тарқатишга ёрдам беради; ахборот ва фойдаланувчи ўртасидаги вақт ва муҳит алоқаларини ташкил этади, улар коммуникацияни амалга оширади; фойдаланувчиларга маданий қадриятларни етказиш орқали, турли маданиятларни кириб келишини, шахсни ижтимоий мослашувини ва бошқаларни таъминлайди.

Ахборотдан барчани фойдаланишини таъминлаш мақсадида кутубхоналарни, архивларни, музейларни шохобчалари, кутубхона пунктлари, кўчма кўргазмалар, архив ҳужжатлари кўргазмалари ташкил этилади. Бундай кўргазмаларда чекланган хизмат кўрсатиш ишлари амалга оширилса ҳам, уларни яшаш жойларида, иш жойларида, ўқиш жойларида, дам олиш масканларида ва бошқаларда ташкил этилиши жамиятни ахборотлаштиришга кўмаклашади.

Хизмат кўрсатиш орқали ахборот ресурсларини фойдаланувчиларга очиқ бўлишини таъминлаш орқали ушбу муассасалар одамларни ахборотга бўлган талабларини қондирадилар. Бу эса ушбу муассасаларни ахборот хизматини амалга оширишдаги *учинчи* умумий жиҳати ҳисобланади.

Шунга қарамасдан улар олдида ахборотни қайта ишлаш ва хизмат кўрсатишни ташкил этиш, ахборот бозоридаги рақобат, шунингдек ахборотни тўплаш, қайта ишлаш ва сақлаш учун катта молиявий харажатларни қоплаш каби муаммолар қолаверади.

Бу эса ахборот хизматини ташкил этишда яна бир механизмни – муассасалар ўртасидаги координация ва кооперацияни ривожлантиришни талаб этади. Янги ахборот технологияларини жорий этилаётганлиги туфайли бу механизм кенг қўлланилмоқда. Кутубхона, архив ва музейлар фаолиятини координация ва кооперациялаш имкониятлари ва мақсадга мувофиқлиги нафақат уларни умумий хусусиятлари мавжудлигидагина эмас, шу билан бирга бир қатор ўзига хосликларига, чунончи уларда сақланаётган ҳужжатларнинг типлари, ўз фойдаланувчилар гуруҳига эга эканлиги ва шу асосда хизмат кўрсатишни ташкил этишидир.

Ушбу муассасалар ўз хизматларини координациялаш ва кооперациялаш орқали фойдаланувчиларга бир жойда ва бир вақтнинг ўзида турли тип ва хилдаги ҳужжатларни, маданий қадриятларни тақдим этиши орқали Ватанимиз ва жаҳон тарихи ва маданияти ҳақида уларда тўлиқ тасаввур ҳосил қилишлари мумкин.

KUTUBXONALARDA INTERAKTIV XIZMATLARNI TASHKIL ETISH

Alimova M. (TATU talabasi),
A.M. Xundibayev A.M. (texnika fanlari nomzodi, TATU o`qituvchisi)

Mamlakatimizda milliy axborot tizimini shakllantirish, davlat va jamiyat hayotining barcha jabhasida zamonaviy axborot-kommunikatsiya texnologiyalari hamda telekommunikatsiya vositalaridan foydalanish ko‘lamini kengaytirish, “elektron hukumat”ni shakllantirish borasida tizimli ishlar amalga oshirilmoqda.

Xususan, axborot-kommunikatsiya texnologiyalari yordamida aholi manfaatlariga xizmat qiluvchi, davlat organlari bilan qulay va samarali munosabatlarni o‘rnatuvchi 2015 yilning 9 dekabrida qabul qilingan O‘zbekiston Respublikasining «Elektron hukumat to‘g‘risida»gi 395-sonli Qonuni asosida “elektron hukumat” tizimi izchil tatbiq etilayapti.

Qonuning 18-moddasida elektron davlat xizmatlarining turlari quyidagicha keltirilgan. Elektron davlat xizmatlari axborot va interaktiv davlat xizmatlari tarzida bo‘lishi mumkin :

• Axborot davlat xizmati ariza beruvchilarning axborotga bo‘lgan ehtiyojlarini qanoatlantirishga qaratilgan, davlat organining faoliyati to‘g‘risidagi axborotni e’lon qilish va boshqacha tarzda tarqatish yo‘li bilan ko‘rsatiladigan elektron davlat xizmatidir.

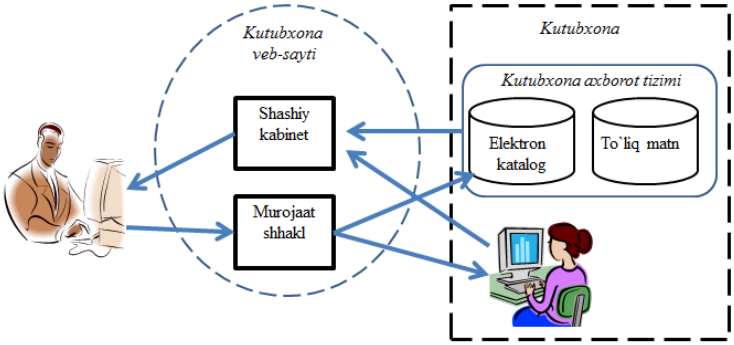
• Interaktiv davlat xizmati ariza beruvchiga ariza beruvchi va elektron davlat xizmati ko‘rsatuvchi davlat organi o‘rtasida ikki tomonlama elektron hamkorlik yo‘li bilan ko‘rsatiladigan elektron davlat xizmatidir.

Kutubxonalardagi davlat xizmatlari Yagona interaktiv davlat xizmatlari portali orqali ko‘rsatilmasada, har bir muassasa o‘z veb saytida bu xizmatlarni tashkil qilmoqda. Bunda foydalanuvchi masofadan turib kutubxona fondi va kataloglari bilan tanishishi hamda buryutmalari berishi mumkin. Bundan tashqari kutubxonalar o‘zaro almashinuvi, yig‘ma kataloglar tayyorlash jarayonida qatnashishi uchun ham bu xizmatdan foydalanadilar.

Interaktiv xizmat olish uchun foydalanuvchi (kitobxon yoki tashkilot nomidan murojaat qiluvchi shaxs) kutubxona veb-saytiga tashrif buyurib, undagi interaktiv xizmat olish shaklini to‘ldiradi (1-rasm). To‘ldirilgan shakldagi murojaat quyidagi ikki yo‘nalishdan biri bo‘ylab yuboriladi.

Birinchisi, kutubxonada joriy etilgan axborot tizimi orqali. Bu tizim avtomatik ravishda murojaatni qabul qilib, ma’lumotlar bazasidan (odatda, elektron katalogdan va u orqali to‘liq matn bazalaridan) murojaatda so`raglan ma’lumotlarni qidiradi. Interaktiv xizmatning bu yo`nalishi o`zining avtomatlashganligi bilan ahamiyatli. Unda murojaatga javob avtomatik ravishda tayyorlanadi va adresatga (murojaat etuvchiga) yuboriladi.

Ikkinchisi, axborot tizimidan olinmaydigan xizmatlar uchun bo‘lib, web-saytdan kelgan murojaatni kutubxona xodimi qabul qilib oladi va qo‘lda bajaradi. Har ikki holatda ham (birinchi holatda avtomatik ravishda, ikkinchi holatda esa qo‘lda) murojaatga tayyorlangan javob web-saytdagi foydalanuvchi kabinetiga yuboriladi. Foydalanuvchi shu kabinetdan o‘zining murojaatiga berilgan javobni oladi.



1-rasm. Interaktiv xizmat ko`rsatish.

Ayrim interaktiv xizmatlar Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi web saytida (www.natlib.uz) keltirilgan.

BASIC CONCEPTS AND ANALYSIS OF THE USE OF ICT IN MEDICAL REHABILITATION

M. Khasanova (TUIT student)

Present time all medicine and rehabilitation researches are based on use information technologies. A worldwide researchers of rehabilitation systems mainly used electromechanical, electrical, optical, thermal, acoustic signal, transducer and sensitive biosensors to develop rehabilitation apparatuses. Rehabilitation technology services are provided for people with severe mobility, learning, emotional, visual, hearing, neurological, neuromuscular, and other

disabilities. Although the fastest advances of medical technology in the globe, people taking rehabilitation systems randomly after major operation, chronic pain, severe accident, orthopedic anarchy, brain injury, Parkinson's disease (neurological disorder), psychological disorder, sports related injury and lastly for older individuals.

Wide varieties of technologies are available to provide tele rehabilitation services. K.K. Tan et al. conducted tele rehabilitation is getting ever more popular, because it is effective in bringing rehabilitation services to rural populations by means of audio visual systems and its initial implementation studies presented encouraging results.

Sanford et al. conducted clinical trials in a study to evaluate the effectiveness of physical therapist/occupational therapist sessions trough tele video technology for follow-up visits. The study reported that potential use of tele video sessions was encouraging for meeting the needs of in-home physical therapist/occupational therapist.

Although there are existing systems for telemedicine purposes, they are not specifically designed to perform well in low bandwidth environments Parmanto et al. developed a versatile tele rehabilitation system, used in some of the just-mentioned studies, which support audiovisual data exchange.

Researchers applied different types of wearable and wireless biosensors for rehabilitation systems. In another literature, some scholars reviewed home-based tele rehabilitation for stroke patients. They focused on some limited biosensors, their application in physical recovery systems and are compared each other. A study conducted by Michael Pramuka et al. the tele rehabilitation technologies distributed seven types of techniques. The techniques are textual based technologies, audio based technologies, and vision based technologies, virtual reality, web-based technologies, wireless technologies, integrated systems. The utilizing newly technologies is benefit in the field of medicine. However, numerous challenges arise when rehabilitation services are provided remotely instead of in traditionally face-to-face contexts. In addition, not all products are designed with end-user mind. Think about asking someone with large hands to use a cell phone with small buttons, or consider need to be physically present at a certain time and day of the week to record your favorite television program. The receiver of remote clinical services may experience issues similar to those that researchers faced with daily technology. Examples of technologies used for remote service delivery include computers, internet connections, and wireless devices (cell phone, monitoring device, and patients design application).

Clinicians who communicate with people with disabilities and participate with them in remote rehabilitation type services will need to become knowledgeable about technology usability and accessibility. If clients are given a role in managing technology during the rehabilitation session, (e.g. measuring, collecting and transmitting data) clinicians may experience difficulties related to the client's understanding and use of technology. Nursing assistants and other clinical personal who assist clients may trained to provide remote rehabilitation services, and may experience similar difficulties with use and installation of technology. Technology difficulties in the various stages of use (connecting, installing, adjusting programming, recording/sending data etc.) can negatively affect the effectiveness of tele rehabilitation.

In conclusion, I would like to notice that now to use new information technologies in medicine is one of the important scientific and practical directions. We should study and develop telemedicine and active use ICT in medical organizations, including policlinics, hospitals and others.

KUTUBXONADA AVTOMATLASHTIRILGAN ISH O'RNINI TASHKIL ETISHNING VIZUAL MODELI

E.A.Eshboyev (Qarshi davlat universiteti katta o'qituvchis),
F. Yu. Shodiyev (Qarshi davlat universiteti o'qituvchisi)

Kutubxonalarda bajariladigan ishlarni avtomatlashtirish, kutubxonachilar va kitobxonlar uchun bir qator qulayliklarni yaratadi. Ayniqsa kitoblar uchun buyurtmalar berishni masofadan turib amalga oshirish va buyurtmalar berish vaqtining chegaralanmasligiga erishish, kutubxonachi va kitobxonlarning vaqtini tejaydi. Bulardan tashqari kutubxona fondidan unumli foydalanish imkoniyati ham yaratiladi. Bu kabi masalalarni hal etish uchun puxta o'ylab tuzilgan model asosida ishlab chiqilgan dasturiy ta'minot talab etiladi.

Bunday modelni ishlab chiqish muhim amaliy ahamiyatga ega bo'lib, uni UML (Unified Modeling Language) notatsiyalari yordamida tuzish mumkin. UML da tuzilgan model 2 ta afzallikka ega bo'ladi.

Birinchidan, turli toifadagi kasb egalari uchun tushunarli bo'lgan vizual modelga ega bo'lish.

Ikkinchidan, tuzilgan modelni Rational Rose dasturi yordamida C++, Java kabi dasturlash tillaridagi kodlarga generatsiyalash.

Yuqorida keltirilgan fikrlarga asoslanib, kutubxona ishini avtomatlashtirishga mo'ljallangan vizual modelni ishlab chiqamiz.

Model qurishni Rational Rose dasturida UML notatsiyalaridan foydalanib, "Ketma–ketliklar" diagrammasini qurishdan boshlaymiz.

Buning uchun Rational Rose dasturi ishga tushirilgach quyidagi qadamlarni bajarish kerak bo'ladi:

1. Dasturning brauzer oynasidagi Logical View buyrug'i ustida sichqonchaning o'ng tugmasi bosiladi.
2. Ochilgan menyudan New → Sequence Diagramm tanlanadi.
3. So'ngra, yangi diagrammaga "Buyurtmani kiritish" deb nom beramiz.
4. Hosil bo'lgan diagrammani ochish uchun uning ustida sichqonchaning chap tugmasi ikki marta bosiladi.

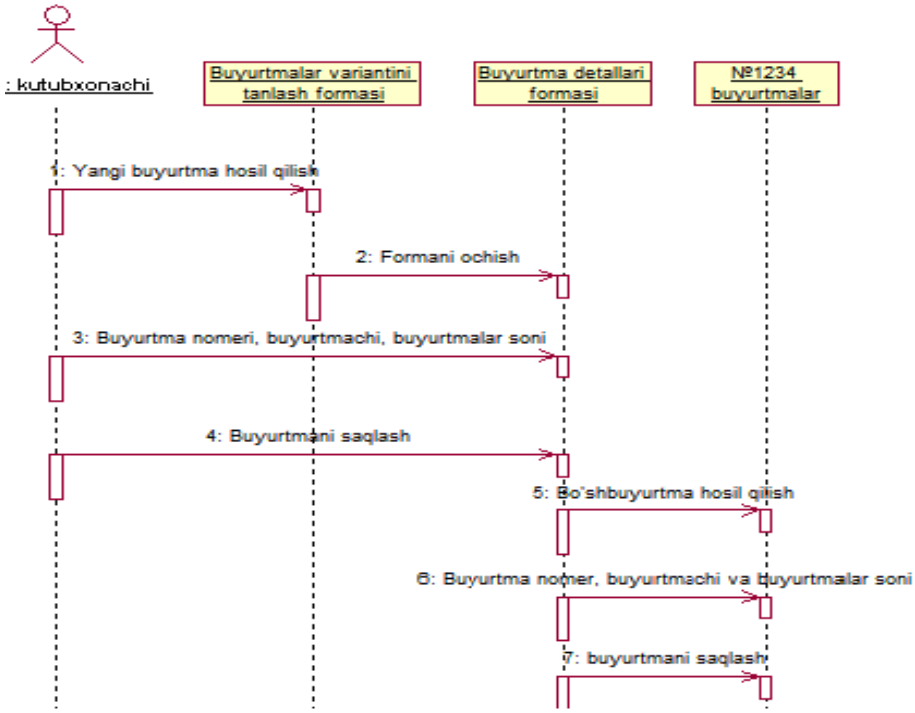
Shundan so'ng, diagrammaga ta'sir etuvchi shaxslar va ob'ektlarni qo'shish quyidagicha amalga oshiriladi:

1. Brauzer oynasidan "kutubxonachi" - ta'sir etuvchi shaxs nomi diagrammaga olib o'tiladi.
2. Instrumentlar panelidan object (ob'ekt) tugmasi bosiladi.
3. Yangi ob'ektni diagrammaning yuqori qismiga joylashtirish uchun u yerda sichqoncha chap tugmasi bosiladi.
4. Hosil bo'lgan ob'ektni "Buyurtmalar variantini tanlash formasi" deb nomlaymiz.
5. "Buyurtma detallari formasi" ham shu tarzda hosil qilinadi.
6. Buyurtmalarni boshqarish uchun esa "№1234 buyurtmalar" ob'ektini hosil qilamiz.

Endi, diagrammaga xabarlar qo'shishni amalga oshiramiz. Buning uchun quyidagi amallarni bajaramiz:

1. Instumentlar panelidan Object Message tugmasi bosiladi.
2. Ijrochi hayotidan ob'ekt hayotiga tomon chiziq o'tkaziladi.
3. Xabarni ajratib, unga " Yangi buyurtma hosil qilish" deb nom beramiz.
4. Diagrammaga navbatdagi xabarlarni joylashtirish va ularni nomlash ham shu tarzda amalga oshiriladi.

Natijada hosil qilingan diagrammaning yakuniy ko'rinishi 1-rasmdagi kabi bo'ladi. Endi boshqaruv ob'ektlari (kutubxonachi va buyurtma beruvchi kitobxonlar) bilan kutubxona fondi ma'lumotlar bazasini bog'lashni amalgam oshirish kerak bo'ladi.



1-rasm. Buyurtmalarni qabul qilishning “Ketma-ketliklar” diagrammasi.

Diagrammadan ko’rinib turganidek “Buyurtmalar detail formasi” bir qancha javobgarliklarni o’z zimmasiga olib, u ob’ektning samarali ishlashi uchun xizmat qiladi. Bulardan tashqari, yangi buyurtmaning o’zi ham biror ma’lumotlar ba’zasida saqlanishi kerak. Shuningdek uning boshqa ob’ektga ham ilova qilinishlik ehtimoli bor.

UML notatsiyalari yordamida tuzilgan vizual model o’zining tushunarliligi bilan barcha foydalanuvchi (kutubxonachi, kitobxon, dasturchi va hokazo) larda kechayotgan jarayonlar haqida aniq va tiniq fikrlarning uyg’onishiga sabab bo’ladi.

Bundan ko’rinadiki, har bir foydalanuvchi tuzilishi lozim bo’lgan dasturiy ta’minot haqida o’z fikrlarini bildira oladi, ya’ni kutubxonachi va kitobxonlar dasturdan foydalanish jarayonida uchraydigan noqulayliklarni dasturchiga osonlik bilan tushuntira olishadi. O’z o’rnida dasturchi ham kutubxona ishidan to’liq xabardor bo’lmasada, mavjud muammoni aniq tasavvur qiladi. Bu xatti-harakatlar tuzilgan dasturiy vositani muntazam takomillashtirib borish imkonini beradi.

ТАЛАБАЛАРДА АХБОРОТ ОЛИШ МАДАНИЯТИНИ ШАКЛЛАНТИРИШНИНГ МУҲИМ ЙЎНАЛИШЛАРИ

Б. И. Ганиева
(ТАТУ, «Ахборот-кутубхона тизимлари» кафедраси мудири)

Ўзбекистон Республикаси Президентининг “Китоб маҳсулотларини чоп этиш ва тарқатиш тизимини ривожлантириш, китоб мутолааси ва китобхонлик маданиятини ошириш ҳамда тарғибот қилиш бўйича Комиссия тузиш тўғрисида”ги 2017 йил 12 январдаги Ф-4789 Фармойишида мамлакатимизда муҳим соҳа ривожи билан боғлиқ аҳоли, хусусан, ёшлар ўртасида китоб мутолааси ва китобхонлик маданиятини оширишда бир қатор муаммолар мавжудлиги қайд этиб ўтилди. Ушбу соҳадаги камчиликларни бартараф этиш, аҳолининг китобхонлик маданиятини юксалтириш бўйича комплекс чора-тадбирларни ишлаб чиқиш бўйича бир қатор вазифалар белгиланди. Бу борада ўқиш маданияти, унинг таркибий қисларига тўхталиб ўтамиз. Бугунги кунда ўқиш маданияти, мутолаа маданияти, китобхонлик маданияти деб юритилаётган тушунчалар, ахборот олиш маданиятининг ажралмас қисмларидир.

Ахборот олиш маданиятини тарбиялаш ўта мураккаб жараён бўлиб, уни илмий жиҳатдан тадқиқ этиш, мазкур жараёндаги турли хил ҳолатларни таҳлил қилиш муҳим аҳамиятга эга бўлади. Негаки, китоб-кутубхона-китобхон тизимидаги ҳар бир бўғин ўзига хос хусусиятлари билан ажралиб туради. Ўқиш маданиятини ўрганишга бағишланган тадқиқотларнинг деярли барчасида мазкур ҳодиса «китоб-китобхон-кутубхона» тизимидан иборат деб қаралади. Мазкур жараён «объект-субъект-объект» йўналишларида тадқиқ этилади. А.Умаров фикрича: Шу анъанавий «объект-субъект-объект» тизимида китоб–китобхон, китобхон–кутубхоначи, тажрибали китобхон–тажрибаси кам китобхон муносабатлари тарзида ўрганишга эътибор қаратилмайди. Олим «объект-субъект-объект» тизими ўрнига «субъект-субъект-объект» тизими назариясини асослаб берди. Бу тизимда тизим ясовчи муҳим белгилар: Ахборот олиш технологияси, ахборот олиш даражаси ҳамда ахборот олиш интенсивлигидир. Ахборот олиш технологиясининг миқдорий жиҳати эса талабанинг тез ёки секин ўқишида намоён бўлади.

Ахборот олиш маданиятининг иккинчи тизим ясовчи хусусияти – ахборот олиш даражаси ҳам мутолаа технологияси билан боғлиқ бўлиб, талаба томонидан маълумотни англаш даражасини билдиради.

Ахборот олиш маданиятининг энг муҳим тизим ясовчи хусусияти – мутолаа интенсивлигидир. Бунда манбалардан фойдаланиш даврий суръати тушунилади. Мутолаа интенсивлигининг юқори бўлишини таъминловчи омиллар сифатида А.Умаров биринчи ўринга мутолаага, яъни ўқишга ва маълумот олишга қизиқиш даражасининг юқори бўлишига эътибор қаратади. Муаллиф: «бу хусусият шахсда ёшлигидан, мактаб партасидан, ҳатто болалар боғчасидан шаклланади. Демак, жамиятда баркамол шахсларни камол топтиришнинг муҳим жиҳатларидан бири - ўқувчи-ёшларда мутолаага қизиқишни шакллантириш лозим» деб ҳисоблайди. Мутолаа интенсивлигининг юқори бўлишини таъминловчи омиллар сифатида:

1) мутолаага ва маълумот олишга қизиқиш даражасининг юқорилиги;
2) мутолаа манбаларининг қизиқарли, мазмунан бой бўлиши;
3) мутолаа манбаларига осон эга бўлишни таъминлаш;
4) бозор иқтисоди талабларига мос равишда турли адабиётлар ва бошқа мутолаа манбаалари рекламасини кенг йўлга қўйиш керак

Дарҳақиқат, ўтказилган тадқиқотлар натижаси ҳам кутубхоналарда ахборот олиш маданиятини тарбиялашда бу омилларнинг асосли эканини тасдиқлади. Ўқишнинг интенсивлиги жамиятда мутолаа маданиятининг даражасига мутаносиб бўлиб, интенсивлик қанчалик юқори бўлса, мутолаа маданияти ҳам шунчалик юқори бўлади. Учинчи омилнинг асосий бўғини иқтисодий омил ҳисобланади. Яъни аҳолининг харид қуввати билан мутолаа манбаларининг баҳоси бир-бирига мутаносиб бўлиши керак.

Ахборот олиш маданиятини шакллантириш – комплекс ҳал қилиниши лозим бўлган кўпқиррали муаммодир. Ахборот маданияти - ахборотга бўлган муносабат, ахборотга нисбатан дунёқарашни шакллантириш методологиясини яратиши, болаларга ахборот жамиятининг фалсафасини тушунтириши, ахборот оқими орасидан керакли, зарур ахборотларни танлаб олиш кўникмаларини шакллантириши жиҳатидан муҳим аҳамиятга эгадир. Бироқ шуни алоҳида таъкидлаш лозимки, шахснинг ахборот олиш малакаларини шакллантириш узоқ ва тизимли йўл тутишни талаб этади. Шунинг учун ҳам мазкур муаммо фақатгина маълум бир давлат чегараларидан чиқиб, глобал характерга эга бўлди. Бу борада чоп этилган бир қатор ҳужжатлар гувоҳлик беради: Халқаро ахборот саммити (Женева, 2003 й.; Тунис, 2005 й.) 2006 йилда Сеулда ИФЛАнинг Бутунжаҳон 72-кутубхоначилик ва ахборотлаштириш конгрессида ЮНЕСКО нинг очиқ форуми бўлиб ўтиб, мазкур форумда бошқа бир қатор муҳим йўналишлар билан бирга ахборот олиш маданиятини шакллантириш масаласи муҳим йўналишлардан бири эканлиги тан олиниб, ривожлантириш, ғоялари илгари сурилди. Бутундунё хамжамияти томонидан ИФЛА ва ЮНЕСКОнинг ахборот маданиятини шакллантириш борасидаги ғоялари тан олиниб, маъқулланган.

Ахборотни танлаш ва ундан унумли, тўғри фойдаланиш эса инсоннинг онг даражаси билан боғлиқ. Онг даражаси билим даражасига, билим даражаси эса ўз навбатида билишга, яъни реаллик ва борлиқдаги воқеа-ҳодисалар мазмун-моҳияти билан мутаносиб бўлиши даркор. Шунинг учун биринчи навбатда ахборот олаётган киши уни мутлақлаштирмасдан, ўз шуури даражасида таҳлил қилиб, сўнг қабул қилиши лозим.

Мамлакатимизда 28-30 ёшдан катта бўлган кишилар интернет тармоғидан қандай ахборот олиш ва уни ўз фикрига эга бўлган ҳолда қабул қилиб, ахборотнинг ҳар қандай ҳуружидан ҳимоялана олади.

Бунинг учун:

- ✓ ёшлар билан мунтазам мулоқотда бўлиш;
- ✓ интернет тармоғини миллий қадрият ва анъаналаримизни ўзида акс эттирувчи веб-сайтлар билан бойитиш;
- ✓ таълим муассасаларини интернет тармоқига улашда одоб-ахлоқ қоидаларига мувофиқ бўлмаган сайтлардан фойдаланишга чекловларни жорий этиш;
- ✓ ёшларда ахборот ресурсларидан фойдаланиш маданиятини шакллантириш вояга етмаган ёшларга оид миллий қонунчилигимизга маънавий таҳдидлар, ахборот хуружларининг олдини олишга қаратилган зарур ўзгартиш ҳамда қўшимчалар киритиш керак.

Ахборот олишга доир билим, кўникма ва малакаларни эгаллаш:

- ✓ инсоннинг ахборотни ўзлаштириш савияси ва ундан фойдаланиш сифати; ахборот олиш фаолиятининг сифат тавсифи (инсон ҳаёт фаолиятининг ахборот олиш, узатиш, сақлаш ва ундан фойдаланиш соҳасидаги сифат тавсифи);
- ✓ ахборот устидаги иш турларида: уни олиш, тўплаш, кодлаштириш ва унга қайта ишлов беришда, шу асосда сифат жиҳатдан янги ахборот яратишда, уни узатишда, ундан амалий фойдаланишда инсон, жамият ёки муайян қисмининг камол топганлик даражаси;
- ✓ ахборот манбаларини онгли равишда танлаш ва уларга қайта ишлов бериш алгоритмини эгаллаш;
- ✓ кутубхоначилик-библиографик саводхонлик, мутолаа (китоб ўқиш) маданияти, ахборотлашув жараёни нима эканлигини ва уни кутубхона жойлашган туманда, ҳудудда амалга ошириш хусусиятларини билиш;
- ✓ ахборотлашув ҳуқуқий майдонида, муаллифлик ҳуқуқи муаммоларида, сўз эркинлигида, шахснинг ахборот жиҳатдан хавфсизлигида ва ҳоказоларда мўлжал ола билиш;
- ✓ “кутубхоначилик-библиографик билимлар”, “китоб ўқиш маданияти”, “кутубхоначилик-библиографик маданият”, “ахборот олиш саводхонлиги”, таълим жараёнида ахборотнинг роли муҳим эканлигини англаб етиш, анъанавий, электрон, тармоқли ва бошқа ахборот ресурсларидан мажмуавий фойдаланиш, ўзини ахборот ташувчиси ва тарқатувчиси деб билиш, фаол ахборот олиш;
- ✓ одамнинг ахборот жамиятидаги хулқ-атвор қоидалари мажмуида намоён бўлади.

АХБОРОТ-КУТУБХОНА СОҲАСИ КАДРЛАРИ МАЛАКАСИНИ ОШИРИШ ВА УЛАРНИ ҚАЙТА ТАЙЁРЛАШ ИСТИҚБОЛЛАРИ

К.М.Ғуломова (ЎМКҲТТКМО ва УҚТ институти “Бошқарувда ахборот технологиялари” кафедраси катта ўқитувчиси)

Ўзбекистоннинг жаҳон ахборот технологиялари оламига тез суръатларда кириб бориши Республикамизнинг барча соҳаларида ўзгаришлар содир бўлишига олиб келди, жумладан кутубхоналарнинг таълим тизимидаги ўрни ва мавқеи, бажарадиган вазифалари, электрон кутубхоналар, уларда замонавий хизмат кўрсатиш усулларини янада такомиллаштириш борасида янги ўзгаришлар содир бўлди.

Аҳолига замонавий ахборот технологиялари асосида ахборот-кутубхона хизматини кўрсатишнинг янги босқичига ўтишни таъминлаш мақсадида Ўзбекистон Республикаси биринчи Президентининг 2006 йил 20 июндаги “Республика аҳолисини ахборот – кутубхона билан таъминлашни ташкил этиш тўғрисида”ги қарори, “Электрон ҳужжатлар айланиши тўғрисида” (2003), “Электрон рақамли ёзувлар тўғрисида”ги (2004) қонунлар, “Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникация технологияларини жорий этиш тўғрисида”ги Ўзбекистон Республикаси биринчи Президентининг Фармони ва “Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникация технологияларини жорий этиш чора – тадбирлари тўғрисида”ги Ўзбекистон Республикаси Вазирлар Маҳкамасининг қарори, Ўзбекистон Республикаси Президентининг "2011-2015 йилларда ахборот-коммуникация технологиялари асосида ахборот-кутубхона ва ахборот-ресурс хизматларини янада сифатли ривожлантириш чоралари тўғрисида" 2011 йил 23 февралдаги Қарори, “Ахборот кутубхона” тўғрисида 2011 йилда қарор ва қонунлар эълон қилинди.

Мазкур қабул қилинган меёрий ҳужжатлар асосида республика миқёсида ахборот-кутубхона соҳасида олиб борилиши керак бўлган ислоҳотлар, мазкур соҳада малакали кадрларни тайёрлаш ва малакасини ошириш каби бош омиллар акс этган.

Албатта кутубхоначилик ишининг, ахборот-кутубхона соҳасининг ривожланиши, кутубхоначи кадрларнинг тайёргарлик даражаси ва сифатига боғлиқдир. Малакали кутубохоначи кадарларни тайёрлаш ва уларнинг малакасини ошириш ахборот-кутубхона соҳасини ривожлантиришнинг муҳим бўғини ҳисобланади. “Кадрлар тайёрлаш миллий дастури” ва “Таълим тўғрисида”ги қонунда ҳам Ўзбекистоннинг келажаги ва тараққиёти учун барча соҳада етук малакали кадрлар тайёрлаш мақсад қилиб қўйилган.

Шунинг учун ҳам мамлакатимизда ва жамиятда ёшларнинг онгида миллий мафкурани шакллантириш, уларнинг дунёда содир бўлаётган янгиликлар, воқеалардан керакли хулосалар чиқаришлари, интернет олмидаги ахборотлардан тўғри фойдаланишга ўргатишда педагоглар ва кутубхоначи кадрларнинг маҳорати муҳим аҳамият касб этади.

Ахборот кутубхона соҳасида ходимларининг малакасини ошириш ва уларни қайта тайёрлаш борасида турли мазмун ва шаклдаги ислоҳатлар олиб борилмоқда. Улар жумласига қуйидагиларни киритиш мумкин:

- Ахборт-кутубхона ва ахборот-ресурс марказлари раҳбарлари ва ходимларини илғор технологиялар асосида жаҳон стандарталри асосида ўқитиш;
- Кутубхоначилик соҳасига замонавий компьютер ва мультимедиа технологиялари жорий этилиши орқали ахборот-кутубхона муассасалари ва ахборот-ресурс марказларида тўлиқ матнли электрон ресурсларини ўз ичига олган электрон каталогларни яратиш, маълумотларни тезкор излаш имкониятини таъминловчи автоматлаштирилган тизим жорий этишга ўргатиш;
- Ахборот-кутубхона соҳасини ислоҳ қилиш ахборот – ресурс ва ахборот – кутубхона фаолиятини белгилаб берувчи ҳуқуқий – меъёрий ҳужжатларни ишлаб чиқиш борасида янгиликлардан ҳабардор қилиш қилиш;
- Кутубхона ҳодимлари ўз малакаси ва имкониятларидан келиб чиққан ҳолда бошқа кутубхоналар билан ҳамкорликда тажриба алмашиш йўли билан турли семинарлар ўтказиш борасида янгиликлардан хабардор қилиш;
- Замон талабларидан келиб чиққан ҳолда фойдаланувчиларга юқори даражадаги замонавий хизмат кўрсатиш усулларини ўргатиш;
- кутубхоначи кадрларни малакасини ошириш ва қайта тайёрлашни янгича таркиб, мазмун асосида ташкил қилиш ҳамда бу тизимни бошқаришни шакллантириш, эътиборни қаратиш;
- Коллеж ва лицейлар ахборот-ресурс марказларига услубий ва амалий ёрдам бериш, улар учун семинарлар, анжуманлар, қисқа курслар ташкил этишни режалаштириш.

Юқорида кўрсатиб ўтилган вазифаларни амалга ошириш ва шу билан бирга кутубхоналарда истеъмолчининг ахборотга бўлган талаб ва эҳтиёжларини қондириш ва

уларга замонавий хизмат кўрсатиш, ахборот- кутубхона ва ахборот-ресурс марказида китобхоналарга китоб танлашда, китобларни тарғиб қилишда уларнинг руҳиятини кўтаришда яқиндан ёрдам берадиган ва ўз ўрнида китобхонларга эстетик завқ бағишлайдиган очиқ кўргазмалар ташкил этиш учун, биринчи ўринда мутахассис кадрларни кутубхона ишига жалб этиш, уларнинг малакасини ошириш ва қайта тайёрлаш, ҳамда ходимлар ўртасида меҳнатни тўғри тақсимлаш зарурдир.

АВТОРИТЕТ МАЪЛУМОТЛАРГА ФУНКЦИОНАЛ ТАЛАБЛАР

Г. Э. Зиёдуллаева (ТАТУ, ассистенти)

Автоматлаштирилган ахборот-кутубхона тизимининг янги имкониятларини очиш, яъни электрон каталоглаштиришда авторитет файлларни яратиш ва ундан фойдаланиш ахборот-кутубхона тизимининг самарали фаолият юритишини таъминлайди. Бизга маълумки, авторитет файлнинг асосий функцияси маълумот кидирув элементларини кенгайтириб, номларнинг турли формасини тартибга солади, ҳужжатлар оқимини ҳисобга олиш сифатини оширади, библиографик маълумотлар базасидан қидирувни тўлиқ ва аниқ таъминлайди. Шундай экан ушбу функциялардан келиб чиқиб авторитет маълумотлар ҳамда улар билан ишлаш уларга қўйиладиган талабларни ишлаб чиқиш зарур ҳисобланади.

Бу борада Халқаро кутубхоналар ассоциацияси ва муассасалари федерацияси - ИФЛА томонидан ишчи гуруҳ шакллантирилиб бунинг асосида авторитет файллар учун турли ечим ва талаблар ишлаб чиқилган.

Улар 3 та ишчи гуруҳ АФ бўйича тадқиқотнинг 3 хил йўналиши бўйича иш олиб борилган. Булар:

1) «Библиографик ёзувларгв функционал талаблар» (“Functional requirements of bibliographic records” – FRBR) лойиҳаси доирасида библиографик тизим учун авторитет ёзувларга функционал талабларни аниқлаш;

2) Авторитет маълумотларга халқаро стандарт рақамни қўйиш ва уни ўрганиш (International Standard Authority Data Number – ISADN), авторитет ёзувлар типларини аниқлаш, фойдаланувчилар имконияти ва фойдланиш имконини яратиш лойиҳаси;

3) АФ тузилиши масаласи билан боғлиқ бўлиб, у Электрон тижорат тизимда маълумотларнинг изоҳи, яъни INDECS (Interoperability of Data in E-Commerce Systems, Халқаро архив кенгаши/стандартлар тавсифи бўйича қўмита-ICA/CDS (International Council on Archives/Committee on Descriptive Standards; ISO/TC46 стандартлар тавсифи ва халқаро рақамлаштириш аспекти- ISO/TC46 for international numbering and descriptive standards, Европа илмий кутубхоналари консорциуми- CERL (Consortium of European Research).

АФ учун функционал талабларнинг мақсади эса кутубхона, архив, музей каталогларида ташкилот ҳақида маълумотлар, тавсифланган ахборот каби маълумотлар жамланган бўлиб, уларга библиографик ишлов берилади ва авторитет ёзув орқали фойдаланувчига тақдим этилади. Авторитет маълумотлар ўзида сарлавҳалар таҳririning турли вариантлари бўйича ташкилот, авлод, шахс аниқлиги бўйича нашрлар жойлашиши учун қўлланиладиган бошқа ахборот ва кириш нуқтасини текширувчи маълумотлардан ташкил топади.

Кириш нуқтаси эса ўзида қайсидир объект идентификацияси учун расмий қабул қилинган ёки номнинг вариант формасини шакллантиради.

Авторитет назорат эса объект идентификациясини билдириб, каталог функциясининг ажралмас қисми сифатида кириш нуқтаси бошқарув жараёнининг узлуксизлигини таъминлайди. Авторитет назорат каталогида турли хилликни аниқлаш учун назорат нуқта сифатида фойдаланилади. Каталогда библиографик ресурсларни

қидиришда сарлавҳа ёки автор номи формаси назоратини таъминлашда, фойдаланувчи учун муҳим элемент бу авторитет назорат ҳисобланади.

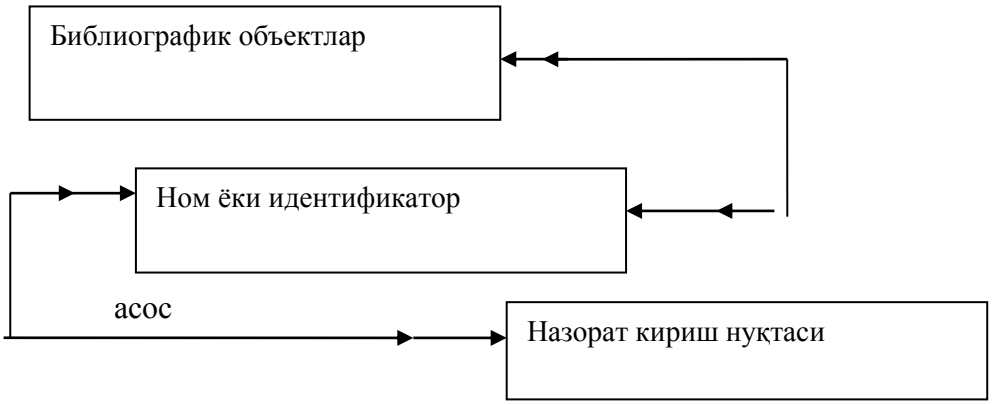
Авторитет маълумотларнинг функционал талаблари ғоявий (концептуал) моделини шакллантириш учун аввало авторитет файл маълумотларига функционал талаблар таҳлили, авторитет файл маълумотларига ишлов бериш қоидалари, библиографик ёзувларни халқаро тақсимлаш ва унинг структурасини аниқлаш талаб этилади. Концептуал моделда авторитет файлларни шакллантириш ҳақида маълумотлар берилади. Моделнинг тизим остилари қилиб объект, атрибут, алоқа каби терминлар қўлланилган. Бу терминлар асосида уларнинг бир-билан алоқаси шакллантирилган. Яъни АФ яратиш учун объект-атрибут, объект-алоқа, тарзида модел яратилган.

Объект – атрибут: концептуал моделни яратишда масаланининг калити бу алоҳида объект ёки қандайдир ттрибут деб олинган. Каталогизатор АФ маълумоти ёрдами билан ташкилот номи ва шахс номи назорати ҳақида анъанавий тарзда фараз юритиш мумкин. Шахс номи ва ташкилотни объект сифатида аниқлаш кўп имкониятлар, номларнинг боғланиш назорати ва керагидан ортиқ меҳнат сарфлашни қисқартиради. Бу номларда библиографик, авторитет ёзувларни бошқаси билан боғлаш ва АЁ да буни объектлар сифатида назорат қилиш мумкин.

Авторитет маълумотларга функционал талабларнинг концептуал модели диаграмма шаклида бўлиб, унда айрим белгилар ишлатилган. Бу тўртта белгидан иборат бўлиб, улар худди алгоритм яратишда қўлланидиган блок схемалар кўринишида тасвирланади:

№	Блок схема шакли	Тавсифи
1		Қандайдир объект мазмунини билдиради
2		Икки ёки ундан ортиқ объект гуруҳини билдиради
3		Объектлар орасида алоқани англатади
4		Аниқ объект мисолида алоқани билдиради

Объект-алоқа диаграммасини аниқ номлар ёки идентификаторларга библиографик ёзувлар содда тарзда шакллантириш мумкин. Каталоглаштириш жараёнида эса бу номлар ва идентификаторлардан назорат қилинадиган кириш нуктасини шакллантиришнинг асоси сифатида фойдаланилади.



1-расм. Концептуал моделнинг фундаментал асоси.

Объектлар: диаграммада объектлар фойдаланувчилар қизиқадиган авторитет маълумотлар сифатида келтирилган.

Объектлар авторитет маълумотлардан ташкил топган бўлиб, улар библиографик ёзувларга функционал талаблар: шахс, ташкилот, асар, ифода , тимсол, физик бирлик, концепция, предмет, воқеа, ва яна битта қўшимча объект –авлод/оила қилиб белгиланган. Булар диаграмманинг юқори қисмида тасвирланган.

БЁ даги кириш нуқталари икки асосий функцияни яъни: библиографик ёзувни топиш ва бир хил характеристикага эга бўлган ёзувларни гуруҳларга ажратишни бажаради. Кириш нуқталари китобхонни библиографик тасвирга олиб боради, библиографик тасвир (БТ) эса топилган ёзувни сўровга мос келишини аниқлашга имкон беради, ҳужжат жойлашган жой тўғрисидаги маълумотлар эса изланаётган ресурсни олиш имконини беради. Авторитет/норматив ёзув электрон каталог маълумотлар базасида “бирга кўп” механизми бўйича библиографик ёзувларга кириш нуқтасини назорат қилади.

КОРПОРАТИВ ТАРМОҚДА ОЧИҚ РЕСУРСЛАР ЭЛЕКТРОН КУТУБХОНАСИ

Ў. У.Каримов (ТАТУ ассистенти)

Одатда *электрон кутубхона* тушунчаси ахборот ресурсларини яратиш, сақлаш ва самарали фойдаланиш имкониятини берувчи ҳамда Интренет/Интранет тармоқлари орқали тақдим қилинадиган *интеграллашган ахборот тизими* сифатида таърифланади. Электрон кутубхона атамаси турли муаллифлар томонидан турлича талқин қилинмоқда ва ҳар бир ҳолда бу таърифларда ўзига хосликлар кўзга ташланмоқда. Ўзбекистон Республикасининг “Ахборот-кутубхона фаолияти тўғрисида”ги Қонунида электрон кутубхонага қуйидагича таъриф берилган: *электрон кутубхона* — ахборот-кутубхона фондининг электрон шакли.

Баъзи бир муаллифлар электрон кутубхона тушунчасини вақт ўтиб бориши билан турлича талқин қилинишини кўрсатсалар [Шрайберг Я. Л.], баъзи бирлари электрон кутубхона ресурслари таркибига қараб электрон кутубхонага таъриф бермоқдалар. Электрон кутубхона тушунчасига берилаётган турли туман таърифлар жамият истеъмоли ва ахборотлашган жамият талаблари ҳамда ахборот ва коммуникация технологиялари ривожи асосида пайдо бўлмоқда.

Электрон кутубхоналар ривожининг замонавий йўналишларидан бири бу *очиқ ресурслар электрон кутубхонасидир*. Очиқ ресурслар – бу фойдаланувчиларга ИНТЕРНЕТ/ИНТРАНЕТ тармоқлари орқали ҳеч бир шартларсиз, бепул тақдим қилинадиган ахборот ресурсларидир. Корпоратив тармоқдаги “очиқ ресурслар” – бу Корпорация аъзолари ихтиёридаги электрон ресурслар ҳисобланади. Бу очиқ ресурсларга бўлган муаллифлик ҳуқуқи қуйидагилардан бирига мос келиши мумкин:

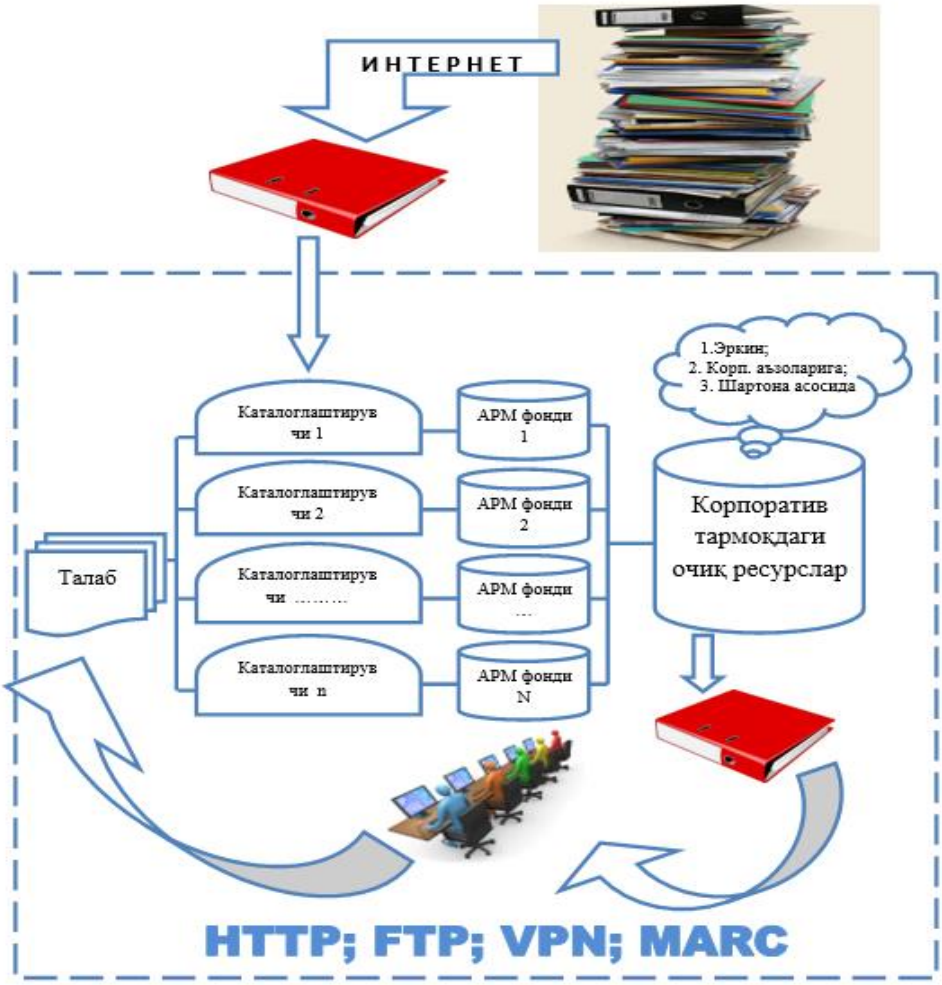
- Очиқ ресурс фақат Корпорация аъзоларга бепул тақдим қилинади;
- Очиқ ресурс барча фойдаланувчиларга тақдим қилинади:
- Очиқ ресурс Корпорацияга аъзо бўлмаган фойдаланувчиларга фақат шартнома асосида тақдим қилинади.

Интеграциялашув ва Корпоративлик очиқ ресурслар электрон кутубхоналарга ҳос бўлган хусусиятлардир. Очиқ ресурслар электрон кутубхоналари интеграциялашуви деганда ягона ахборот тизими доирасида ресурслар ва сервисларнинг бирлашуви тушунилади. Ресурслар ва хизматлар таркиби қўйилган мақсадга қараб танланади.

Очиқ ресурслар электрон кутубхонасининг корпоративлик хусусияти маълум бир мақсадга (масалан, йиғма электрон каталог яратиш, ҳужжатларни электрон шаклга ўтказиш ва бошқалар) эришиш учун ахборот-кутубхона муассасаларининг ихтиёрийлик тамойили асосида бирлашувида кўринади.

Корпоратив тармоқда очиқ электрон кутубхонасини ташкил қилишда ишни дастлаб, Корпорация аъзолари бўлган ахборот-кутубхона муассасаларидан фойдаланувчилар қизиқишларини ўрганишдан бошлаш зарур.

Ахборот-кутубхона муассасалари маълум бир мақсадни кўзлаб ихтиёрийлик асосида бирлашадилар. Корпоратив электрон кутубхона “ҳамкорликда электрон ресурслар яратиш ва улардан биргаликда фойдаланиш” ғояси асосида ташкил қилинади.



Корпоратив тармоқда очиқ ресурслар электрон кутубхонасини ташкил қилиш модели.

Корпоратив тармоқда очиқ ресурслар электрон кутубхонасини яратиш босқичлари:

1. Электрон кутубхона фондини очиқ электрон ресурслар билан комплектлаш.
2. Электрон кутубхона каталогини шакллантириш.
3. Электрон кутубхона орқали хизмат кўрсатиш.
4. Электрон ахборот-кутубхона фонди тўғрисидаги статистик маълумотларни тўплаш, ишлов бериш ва таҳлил қилиш.

Корпоратив ахборот тизимлари соҳасидаги замонавий тенденцияларга мувофиқ очиқ ресурсли электрон кутубхоналар яратишда қуйидагиларга алоҳида эътибор бериш керак:

- Очиқ архитектура – тизим сервис моделлари асосида қурилиб, унда умумий функционаллик аниқланган маълум бир сервислар жамламаси сифатида шаклланади. Сервисларнинг умумий сони чекланмаган.
- Модуллик – тизимни компоновка қилишда алоҳида модуллардан фойдаланганлиги туфайли уни турли ахборот сўровларига мос келиши таъминланади. ЭК ратишдаги мазкур ёндошув модулларнинг функционал ва интерфейс жиҳатдан мос келишини талаб қилади.
- Мантиқий мустақиллик – мантиқий боғланган турли электрон ахборот ресурслар жамламасини фойдаланиш учун шакллантирни таъминлаш. Телекоммуникация муҳитида мантиқий мустақиллик интероперабеллик ва дастурий-техник таъминотнинг ўзгаришидан ва қўрилмаларга боғлиқ бўлмаслигида кўринади;

- Физик мустақиллик – янги электрон ресурслар қўшиш, мавжуд электрон ресурсларни зарур бўлганда ўчириш, физик электрон ресурсларни янги муҳитга кўчириб ўтказиш;
- Тақсимланганлик – электрон ахборот ресурсларни ва сервисларни турли ахборот-кутубхона муассасалари серверларида жойлашттириш. Электрон кутубхонанинг бошқариш ҳуқуқлари ва воситаларини етарли даражада ахборот-кутубхона муассасалари орасида тақсимлаш имконияти.

ДУНЁНИНГ ЙИРИК КУТУБХОНАЛАРИ ТАҲЛИЛИ

Н.Ш.Матқурбонова (ТАТУ талабаси)

Ўзбекистон Республикасининг 2011 йил 13 апрелда қабул қилинган “Ахборот кутубхона фаолияти тўғрисида”ги Қонунига асосан ахборот-кутубхона муассасалари қуйидаги кутубхоналар киритилди:

- Ўзбекистон Миллий кутубхонаси;
- ахборот-кутубхона марказлари;
- ахборот-ресурс марказлари;
- давлат ҳокимияти ва бошқаруви органларининг кутубхоналари;
- бошқа кутубхоналар (фуқаролар ўзини ўзи бошқариш органларининг, нодавлат нотижорат ташкилотларининг, тижорат ташкилотларининг кутубхоналари).

Ахборот-кутубхона муассасалари фаолиятини ривожлантиришда дунёнинг бой фонд ва юқори нуфузга эга кутубхоналарини ўрганган ва уларнинг фаолиятини чуқур тахлил қилган ҳолда стратегиялар ишлаб чиқиш муҳимдир.

Интернет маълумотларига кўра, нуфузли кутубхоналар сони 100 га яқин. Мазкур рўйхатнинг биринчи бешталигида АҚШнинг *Конгресс кутубхонаси*, Буюк Британиянинг *Британия кутубхонаси*, АҚШнинг *Нью-Йорк Оммавий кутубхонаси*, Россиянинг *Россия Давлат кутубхонаси* ва *Россия Миллий кутубхоналари* жой олган. Уларнинг фондида қандай ресурслар тўпланган, улар қандай бошқарилади, фойданувчиларига қай усулда хизмат кўрсатилади, деган саволлар туғилиши табиий ҳол.

Дунёдаги энг йирик кутубхона сифатида эътироф этилаётган Вашингтонда жойлашган Конгресс кутубхонаси 1800 йилда ташкил этилган бўлиб, дастлаб фақат Конгресс аъзоларига хизмат қилган кутубхона кейинчалик аҳолининг барча қатламлари учун ўзининг бой фондини тақдим этган. Унинг дастлабки фондида 700 та китоб жамланган. Ҳозирги кунда фондининг умумий ҳажми 160 млн.дан ортиқ бўлиб, китоблар, кенг тоифали ва юқори характерли (инкунабул жамланмаси китоблари, монография ва серияли китоблар, журналлар, рисолалар, техник ҳисоботлар ва бошқа чоп этилган манбалар), классификация қилинмаган манбалар, хусусан, аудио материаллари, қўлёзмалар, хариталар, микроформалар, тасвирий (филмлар, DVDлар, телевизион-радиоэшиттиришлар), мусиқий ноталар, фотографиялар, афишалар, тасвирий асарлар ташкил этади. Конгресс кутубхонасининг махсус бўлими мавжуд бўлиб, унинг асосий вазифаси муаллифлик ҳуқуқини расмийлаштиридир. Кутубхонадаги мавжуд бой ресурслар билан бир қаторда, мазкур фондни тартибга солиб, фойдаланувчиларга тақдим этувчи ходимлар ва уларнинг малакаси катта аҳамиятга эга. Конгресс кутубхонаси фаолиятининг бир маромда бориши, фондининг тўғри ташкил қилиниши, абономент ва фойдаланувчиларга хизмат кўрсатиш, фондни рақамли кўринишга ўтказиш ва бошқа ишлар билан шуғулланувчи ходимларнинг умумий сони 3138 нафар кишини ташкил этиб, шунинг натижаси ўлароқ, мана қарийб 215 йилдирки, Конгресс кутубхонаси нафақат АҚШ аҳолисига, балки бутун жаҳон аҳолисининг маънавий эҳтиёжларини қондириб келмоқда.

Фонди жиҳатдан Конгресс кутубхонасидан кейинги, иккинчи ўринда турувчи Британия кутубхонаси 1753 йилда ташкил қилинган бўлиб, ҳозирда кутубхона фондида

жами 150 млн.дан ортиқ ресурс сақланмоқда. Бундай катта ҳажмдаги манбаларнинг бут сақланиши учун Британия кутубхонасининг биноси ажабтовур кўриниш: жами 14 қаватдан иборат бинонинг 9 қавати ер устида, 5 қавати эса ер остида жойлашиб, фонд сақланиши учун етарли шароитлар билан таъминланган. Фонд таркибига китоблар, қўлёзмалар, карталар, газета ва журналлар, расмлар, ноталар, патентлар, маркалар ва ёзиб олинган овозлар йиғилган. Британия кутубхонаси ўзининг ноёб фонди ҳамда нодир экспонатлари билан дунёнинг бошқа кутубхоналаридан ажралиб туради. Ноёб фонди қаторида "Беовульф" эпосининг ягона нусхаси, "Гутенберг Инжили"нинг 2 нусхаси, 1215 йилдаги "Буюк ҳартия хурлиги"нинг 2 нусхаси, Леонардо да Винчи асарларининг асл нусхалари, *Pastime with Good Company* шеърлари, Аурелья Стайн тўпламининг Дуньхуан қўлёзмаси кабилар сақланади. Британия кутубхонаси(British library)нинг расмий интернет сайти маълумотига кўра, кутубхонадан кунига 16000 нафар фойдаланувчиларнинг ташрифи таъкидлаб ўтилган. Британия кутубхонасининг ўқув залларидаги фонддан фойдаланиш жараёнида фойдаланувчилар учун қатъий амал қилиниши лозим бўлган талаблардан бири, залда *фақатгина қаламдан* фойдаланишдир. Ручкалардан фойдаланиш таъқиқланганлигининг асосий сабаби, фонднинг яроқлилигини сақлаб туришдир. Бунинг натижаси ўлароқ Британия кутубхонасида сақланаётган барча манбалар, бир неча йиллардан буён фойдаланувчиларнинг маънавий оламига шода-шода дуру-гавхарлар инъом этиб келмоқда.

Юқорида айтиб ўтилган машҳур кутубхоналар бирданига бундай юксакликка чиқиб қолмаганлар. Бир неча юз йиллар давомида фондини бутлаш турли усуллардан фойдаланганлар. Хизмат кўрсатиш даражасини ошириш учун бир қанча усуллар ўзининг самарасини бериб, кутубхоналар фаолияти ҳозирги кунда бир маромда давом этмоқда.

Юртимиз ахборот-кутубхона муассасаларининг фонди электрон кўринишга келтириб, электрон каталог тузилмоқда. Фойдаланувчиларга ҳам анъанавий, ҳам замонавий технологиялар асосида хизмат кўрсатиш йўлга қўйилмоқда. Ахборот-кутубхона муассасаларининг виртуал хизмат кўрсатиш тизимини жорий этишда жаҳон кутубхоналарининг услубларидан фойдаланиш катта аҳамият касб этади.

ЖАМИЯТДА АХБОРОТ АЛМАШИНУВИ МАДАНИЯТИНИ ОШИРИШНИНГ СОЦИАЛ ЖИХАТЛАРИ

Ш.А. Раҳимова (ТАТУ ассистенти)

Замон шиддат билан ривожланиб бормоқда. Бугун фанда яратилган бирор-бир янгилик эртасига бутун дунёга тарқалиб улгурмай, ўша ихтиронинг янада такомиллашган нусхалари пайдо бўлмоқда. Буни шубҳасиз, ахборот алмашинувидаги замонавий коммуникация технологиялари иштироки билан боғлашимиз мумкин. Сабаби, глобал тармоқ ёрдамида бир жойдан иккинчи жойга маълумот жўнатиш учун сонияларнинг ўзи кифоя қилмоқда. Ижтимоий ҳаётда ёшларнинг интеллектуал салоҳияти ижтимоийлашув орқали шаклланса, замонавий дунёда ёшлар ўртасида ахборот алмашинуви жараёнларининг ҳам беқиёс ўрин тутади.

Мамлакатимизда аҳоли ва айниқса ёшларимиз учун ахборот ресурслари, жумладан Интернет глобал тармоғидан фойдаланиш борасида кенг имкониятлар яратилганлигини таъкидлаш билан бирга, жамият ривожланишнинг ахборот босқичига кириши инсон катта ҳажмдаги ахборотни қабул қилиш ва уни қайта ишлаш ҳамда фойдаланишнинг ҳозирги замон воситалари ва усулларини эгаллашга том маънода тайёр эмаслигини ҳам кўрсатиб қўйди.

Ҳозирги кунда ахборот майдони глобаллашувининг авж олиши, замонавий ташвиқот усуллари ва техник воситаларининг такомиллашуви нафақат алоҳида олинган шахснинг онгига, балки бутун бир халқларнинг турмуш тарзига таъсир ўтказиш, давлатларнинг сиёсатини ташқаридан туриб бошқариш учун шароит яратмоқда.

Замонавий ва самарали ечимлар топиш учун кўплаб, структура жиҳатидан мураккаб ахборот тизими яратилмоқда, натижада, ахборотлаштириш жараёнида иштирок этувчилар сони кун сайин ортиб бормоқда. Бу ўз навбатида инсонларни ахборот ресурсларидан рационал фойдаланиш йўлларини қидиришга мажбур қилмоқда. Замонавий шароитда янги ахборот оқими қанчалик тез кўпайса шу билан бирга уларнинг эскириш муддатлари ҳам тезлашмоқда, бу ўз навбатида, ахборотни танлаш, унга эришиш қийинчиликларини келтириб чиқармоқда.

Янги ахборот технологиялари фаолиятининг ижтимоий натижалари бениҳоя ранг-барангдир. Улар инсон меҳнат фаолияти характерини, унинг ижтимоий алоқаларини, социал муносабатларнинг шакл ва мазмунини ўзгартиради. Шу билан боғлиқ равишда тадқиқотчиларнинг диққат-эътибори марказида ахборот технологияларининг инсон руҳиятига таъсири, компьютер воситасидаги мулоқот ва Интернетдаги инсон фаолиятининг ўзига хос жаҳатлари каби масалалар ўрин олди. XX асрнинг 60 йилларида илк бор ахборот олиш ва узатишнинг электрон воситалари ривожи билан боғлиқ усуллари ва ўзгаришлар қайд этилган эди. М.Маклюэн бу жараённи “ахборот алмашинувидаги мавжуд чизиқли фикрлаш ўрнини “мозаикали” фикрлар эгаллай бошлади, тафаккурнинг асосий тузилмавий тамойили сифатида асотир (миф)ларнинг қайта тикланиши бошлангандек, гўё” – деб баҳолайди. Бу билан М.Маклюэн инсондаги фикрлаш усули ва социал муносабатларнинг ўзгаришига “мулоқот воситалари”нинг таъсир жиҳатларига алоҳида эътибор қаратади.

Маълумки, ҳар қандай жамият социал меъёрлар орқали бошқарилади ва тартибга солинади. Социал меъёрлар одамлар ва уларнинг бирлашмалари ўртасидаги “инсон-инсон” муносабатларини тартибга солувчи, умумий ҳулқ-атвор қоидаси ҳисоблаб келинган. “Жамиятда инсон ва шахс фаолияти, ҳатти-ҳаракатлари ва ҳулқ-атворларини социал меъёрлар бошқарар экан, у жамият бошқарувининг ажралмас қисми сифатида, шахс ёки социал гуруҳ ҳулқ-атворини муайян социал муҳитга мослаштирувчи қоидалар мажмуини ташкил этади”. Социологияда социал меъёр мажмуасидан келиб чиқиб, болалик ва ёшликка аниқ тартиб киритилган. Хусусан, ёшликнинг дастлабки, қуйи чегараси 14-16, юқори чегараси эса 25-30 ёш қилиб белгиланган. Илгари сурилган мавзу “ахборот алмашинуви” билан боғлиқ экан, унда табиийки ёш кўрсаткичи муҳим ўрин тутади.

Фан-техника тараққиётининг ҳозирги даражаси қўл меҳнатини камайтириш билан бирга, инсонларда ақлий ва асабий зўриқишни кучайтирмоқда. Бу эса автоматлашув билан ижодиёт ўртасидаги зиддиятни бартараф этиш, инсонга технократик ёндашишнинг салбий оқибатлари олдини олишни талаб қилади. Айниқса, техник тараққиёт информатика, генетика каби янги тармоқларнинг ривожи билан бир қаторда мураккаб фалсафий, аҳлоқий муаммоларни ҳам келтириб чиқарди. Бу эса ўз навбатида тадқиқотчилар олдига инсон интеллекти ва “фикрловчи машиналар”нинг келажаги қандай бўлади? – деган саволни туғдиради.

Ҳаётнинг юқори суръатда тезлашиб кетиши ёшлар ўртасидаги ахборот алмашинуви социал ноаниқликларни кўпайишига ва унинг натижасида уларнинг ўзларини хавфга қўйишлари кучайиб бормоқда. Социологлар “ноаниқлиқ” тушунчасини қуйидагича изоҳлайдилар: “Тизимли ёндашув (Т.Парсонс назарияси)дан келиб чиқиб, ноаниқлик социал тизимда вужудга келадиган ўзаро фаолият элементларидаги муносабатларни акс эттиради”. Ноаниқликни англаш учун аниқлик элементини В.Готт ва А.Урсуллар аниқлик таснифи билан қиёслайдилар: “Агар аниқлик ҳолати шахслар яъни ёшлар орасида бир-бирига нисбатан мустақил, кескин фарқ қилувчи социал, руҳий чегаралар билан ажралиб турса, ноаниқлик мавжуд объект ёки ҳодиса жараёнларида қарамлилик, бўйсунишлик кузатилади”.

Социолог шахснинг, хусусан ёшларнинг жамиятга мослашув жараёнини ижтимоийлашув жараёнлари билан ўрганади. Табиийки, ижтимоийлашув вояга етиб

келаётган ҳар қандай индивидда ижобий ёки салбий хусусиятларни бир вақтда ўзлаштириб бораверади.

Замонавий ёшларнинг социал муҳит шарт шароитларига ижтимоийлашувидаги хусусиятлар трансформациялашган жамият ва унинг оқибатида вужудга келган субъектив вазиятларга боғлиқ бўлиб қолади. Бу жараёнда ёшларнинг ўз олдиларига қўйган вазифалар, ахборотлашган жамиятда ахборот алмашинуви маданиятини шакллантириш масалалари, шарт шароитга мослашув ва истиқболдаги эришилиши кўзланган мақсадлар социологик нуқтаи назардан илмий таҳлил ва башорат қилиниши лозим.

Шундай экан, ахборотлашган жамиятда жамоатчилик фикрини ўрганиш, бунда эса сифатли социологик тадқиқотлар ўтказиш зарурати юзага келади. Табиийки, бу мутаҳассисдан юқори касбий маҳоратни талаб этади. Социологик амалиёт бўйича тегишли билим ва тайёргарликка эга бўлмаган инсон муаммони ўрганиш вақтида кўплаб субъектив нуқсонларга йўл қўйиши мумкин. Шу билан бирга социологик тадқиқотларни ташкил этиш маҳсус билимларни талаб этиши, хусусан, назарий-методологик дастурнинг экспертлар томонидан қанчалик илмий ва асосли ёзилганлиги, мақсад ва вазифаларнинг тўғри қўйилганлиги, илмий гипотезаларнинг тўлиқ асосланганлиги ва репрезентативликнинг таъминланганлигига боғлиқ бўлади.

Ижтимоий ҳаётда жамоатчилик фикри инсонлардаги ўзаро социал муносабатларга киришувнинг муҳим механизмларидан бири ҳисобланади. У маълум даражада бошқарув жараёнларига таъсир кўрсатиши, мавжуд тизимнинг ижтимоий аҳамиятга эга бўлган фикр ва қарорларини шакллантириши ва қўллаб-қувватлаши мумкин.

Хулоса қилиб айтадиган бўлсак, ахборотлашган жамиятда ёшларнинг ахборот алмашинуви масаласи замонавий шароитда социал ва психологик мазмун касб этиб, ижтимоий ҳодисаларни инобатга олган ҳолда изчил тадқиқ этишни талаб этади. Умуман олганда янги ахборот технологиялари ва улардан инсон ҳаётида фойдаланишни такомиллаштириш борасида бир- бирига мутлақо зид бўлган баҳо ва прогнозларни учратиш мумкин. Бир томондан, ижтимоий фикрда компьютерларнинг ёш авлоднинг онгу тафаккурига фақат салбий таъсир ўтказиши ҳақидаги тушунча ўрнашиб қолган. Аммо бу фикрга зид ўлароқ янги ахборот технологияларнинг жамиятга ва жумладан, талим тизимига фақат ижобий, самарали таъсири ҳақидаги ўта кўтаринки қарашлар ҳам кенг тарқалган. Ўзбекистон Республикасида кечаётган социал-иқтисодий ислоҳотлар негизида мазкур кўтарилган масала ахборотлар жамияти кишиси характерини баҳолашда ўзининг илмий аҳамиятига эга бўлиб бораверади.

РЕКЛАМНАЯ ДЕЯТЕЛЬНОСТЬ ИНФОРМАЦИОННО-БИБЛИОТЕЧНЫХ УЧРЕЖДЕНИЙ

У. Э. Моллаходжаев (магистрант ТУИТ)

Реклама становится своеобразной интегрирующей силой человеческой деятельности. В конце XX века в странах с развитой экономикой реклама превратилась в универсальное общественное явление. В рекламе объединились многие ключевые проблемы функционирования сознания общества, взаимодействия материального и идеального факторов, технологии и культуры. Возрастание роли библиотечной рекламы является характеристикой особого типа общества - информационного. В целом можно считать, что мониторинг функционирования библиотечной рекламы как социального феномена - это необходимый и всегда актуальный компонент современной духовной и материальной деятельности в информационно-библиотечной сфере.

В свете требований, выдвинутых Постановлением Президента Республики Узбекистан № ПП - 381 от 20 июня 2006 года «Об организации информационно – библиотечного обеспечения населения республики» к созданию качественно нового уровня информационно-библиотечного обслуживания населения значительную

организационную и содержательную функции приобретает рекламно-информационная деятельность ИБУ. В целях повышения эффективности информационно-библиотечного обслуживания пользователей в удовлетворении их духовных, образовательных, культурных, досуговых, познавательных, производственных и других потребностей необходимо использовать современные технологии и маркетинговые решения, в том числе организацию рекламной деятельности.

Важнейшей формой продвижения библиотечных продуктов и услуг является библиотечная реклама, которая представляет собой информацию об информационно-библиотечном учреждении в целом, его продукции и услугах с целью оповещения о них пользователей и стимулирования спроса на информационные ресурсы библиотеки.

Теоретическое осмысление библиотечной рекламы в информационно-библиотечных учреждениях Узбекистана становится актуальной проблемой в силу специфичности и особенности социального и культурного опыта данного государства. Важная функция рекламы – социальная. Для сферы культуры, в том числе и библиотечного дела, она – определяющая, поскольку реклама способствует интеграции населения, становлению его единства. Реклама унифицирует потребности и вкусы населения, органично связывая материальное и духовное в жизни любого человека. Создавая спрессованный опыт, она аккумулирует чувства и опыт всего общества.

Экономическая функция рекламы сводится в основном к информированию о товаре или услуге, их популяризации, повышению спроса, товарооборота и производства, то есть реклама развивает экономику и влияет на уровень жизни.

Познавательная функция рекламы состоит в том, что она является одним из способов познания, освоения реального мира – мира «вещей», «идей», «услуг», ознакомления со всем универсумом человеческой деятельности. Рекламные акции, участниками которых вольно или невольно становятся люди, рекламные объявления, которые они видят, слышат и воспринимают, являются конечными продуктами целого ряда исследований, стратегических и тактических планов, конкретных решений и действий, составляющих в своей совокупности процесс рекламы.

В последние годы реклама стала необходимым атрибутом деятельности многих учреждений культуры. Отсюда интерес специалистов к рекламе, как средству раскрытия перед населением возможностей тех или иных фирм (в том числе и библиотечно-информационных учреждений), и привлечения к использованию их ресурсов всё новых и новых пользователей. В настоящее время любая библиотека должна найти своё место в рыночных отношениях. Важнейшее место в этой ситуации отводится рекламе. Современный отечественный и зарубежный опыт свидетельствует, сколь значительны её возможности во всех сферах деятельности общества. По мнению английского библиотековеда Б.Ашервуда, реклама позволяет сделать библиотеку «видимой», прозрачной и, на взгляд автора, показать ее в контексте культурной жизни республики во многом конкурентоспособной в сфере учреждений культуры и средств массовой информации.

С 1990-х гг. рекламно-информационная деятельность становится неотъемлемым компонентом библиотечной сферы. Специалисты отрасли активно используют опыт зарубежных ученых, разработанные ими методики. Однако теоретического обоснования необходимости библиотечной рекламы до сих пор нет.

Цель библиотечной рекламы – оповещение потенциальных потребителей о библиотечно-информационных ресурсах, изданиях и услугах, предоставляемых библиотекой. Необходимо заинтересовать их и побудить отдать предпочтение иному или иному «товару» из числа аналогичных информационных ресурсов, продуктов и услуг.

Достижение данной цели возможно при выполнении следующих задач:

- формирование престижного имиджа библиотеки в сознании населения, спонсоров, представителей местных органов власти и управления, общественных организаций и т.д.;

- информирование о новых библиографических услугах, введённых библиотекой, её информационно-библиографическими подразделениями;

- сохранение популярных существующих библиографических услуг, убеждение пользователей не забывать о широких возможностях информационно-библиографических подразделений и обращаться к ним;

- воздействие на потребителя информации с целью его ориентации на приобретение рекламируемого товара; информирование о новых услугах, ресурсах и продукции библиотеки;

- акцентирование внимания потенциальных пользователей на специфических особенностях предлагаемых библиотечных ресурсов, продуктов и услуг;

- выделение сегментов рынка, которые необходимо охватить рекламой.

Основная функция рекламы библиотеки – определить целевую аудиторию, найти своего пользователя библиотечно-информационных ресурсов и услуг.

Основными направлениями рекламы, определяющими её суть, являются следующие:

- информация о библиотечной сети обслуживаемого района в целях ориентации в ней, о возможностях других библиотек сети (например, о получении требуемых изданий по МБА и т.п.);

- информация о библиотеке и (или) ее структурных подразделениях (филиалах, отделах);

- информация о библиотечном фонде, его составе и структуре;

- информация об услугах, предоставляемых библиотекой, и о её интеллектуальной продукции.

К рекламе библиотеки предъявляют ряд требований:

- ✓ делать акцент на новом, неожиданном, иногда даже сенсационном из ресурсов, продуктов и услуг библиотеки;
- ✓ особенно активно продвигать услуги на рынок на стадии их внедрения;
- ✓ подчёркивать отличительные особенности и преимущества предлагаемых ресурсов, продуктов, услуг, которые выделяют их из массы аналогичных товаров на рынке.

Требования к рекламе определяются, в частности тем, что она выступает одним из самых действенных инструментов маркетинга уже на начальном этапе, исследуя ожидания и предпочтения населения. Методы их изучения, формулировки запросов и т.п. выбирают таким образом, чтобы они служили рекламе библиотеки.

В своей рекламной деятельности библиотеки опираются на Закон Республики Узбекистан «О рекламе», принятый 25 декабря 1998 г. № 723-I, а также на Закон Республики Узбекистан «Об информационно-библиотечной деятельности», который был принят 13 апреля 2011 г. Библиотеки должны соблюдать этические стандарты рекламной деятельности. В частности, они должны не допускать недобросовестной, недостоверной, заведомо ложной информации. Речь в данном случае идёт о рекламе не просто как о вывеске над входом, а как о хорошо продуманной и целенаправленной политике. Грамотная рекламная политика библиотеки – это, прежде всего, определённая система приёмов, основанных на знании психологии, которые, вызывая заинтересованность читателя, побуждают его обращаться к библиотеке снова и снова.

АРХИВ ҲУЖЖАТЛАРИ ЙИҒМА ЭЛЕКТРОН КАТАЛОГИНИ ЯРАТИШ ВА ҲУЖЖАТ ҚИДИРИШ МАСАЛАЛАРИ

Ш.М.Мухаммаджонов (ТАТУ ассистенти)

Ҳозирги кунда архив ҳужжатлари ҳажмининг шиддат билан ўсиб бориши фойдаланувчи учун уларни кўриб чиқиш имкониятини қийинлашишига олиб келмоқда. Архив фондларини узоқ муддатли сақланиши, уларни тезда излаб топиш ва улардан унумли фойдаланиш ва долзарб аҳамиятга эга. Шу боис, архивларнинг электрон

каталогини яратиш, кейинчалик эса уларнинг йиғма электрон каталогини яратиш муҳим масала ҳисобланади.

Электрон каталог (ЭК) турли хил қидирув белгилари (калит сўзлар, муаллифлар, китоб номи, йиллар) воситасида ахборотни қидириб топиш, қидирувни муайян муддат оралиғида чегаралаш ва бошқа имкониятлар яратади.

Электрон каталог самарадорлигининг асосий кўрсатгичи қуйидагилар ҳисобланади:

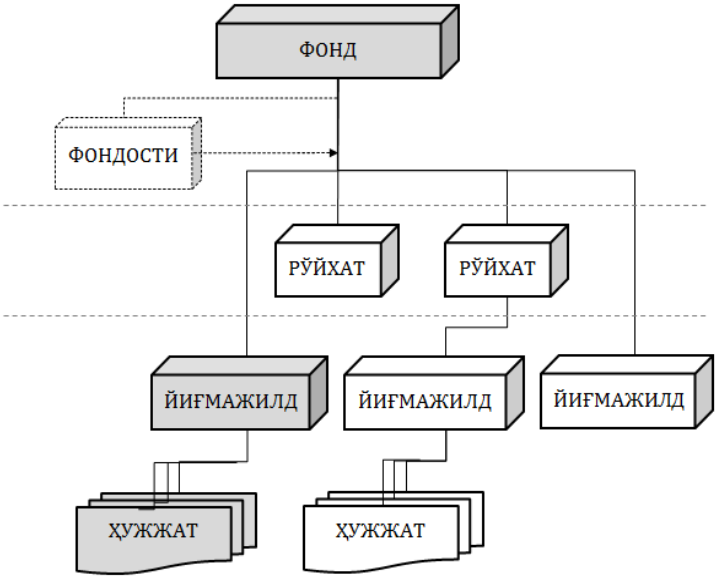
- Карточкали каталогларга нисбатан электрон ёзувларда юқори тезликда қидириш;
- Электрон каталогни тез суръатларда кўпайтириш имкониятининг мавжудлиги, яъни зарурат туғилганда ЭКни керакли нусхада кўпайтириш мумкин;
- ЭКга масофадан туриб кириш;
- ЭК қисқа вақт оралиғида катта ҳажмдаги ахборотларни кўриб чиқиш ва керакли адабиётни танлаб олиш;
- Ҳужжатга турли критериялар бўйича боғланган ҳужжатларни ҳам кўриб чиқишга имкон беради.

Архив ҳужжатлари йиғма электрон каталоги – бу бир нечта архив муассасасаларининг электрон каталоглари мажмуи ҳисобланади. Йиғма электрон каталог ёрдамида ягона интерфейс орқали турли архив фондларидан қидиришни амалга ошириш мумкин.

Электрон каталогдаги архив тавсифларини ISAD(G) халқаро стандарти асосида каталоглаштириш архив фондининг иерархик тузилмасини тўлиқ қамраб олиш имконини беради.

Архив тавсифи иерархик тамойилга асосланади ва *фонд - [фондости] – рўйхат – йиғмажилд – ҳужжат* каби тавсиф даражаларига эга бўлиши мумкин (1-расм).

Архив муассасаларида ҳужжатлари тавсифланадиган фондлар учун асосан *фонд – йиғмажилд - ҳужжат* варианти мос келади.

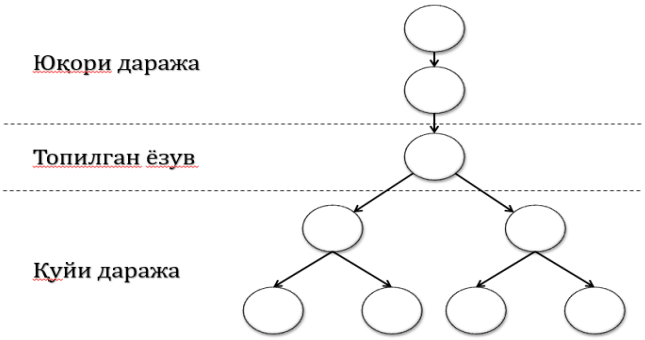


1-расм. Архив фондлари структурасининг иерархик модели

Архив ҳужжатларини қидириш интерфейси юқоридаги даражалардан бирини ёки барчасини танлаш имконини бериши лозим (2-расм).

2-расм. Архив ҳужжатларини қидириш алгоритми.

Қидирув натижаси қуйидаги схемага асосан ҳужжатга боғлиқ равишда барча даражалар бўйича кўриб чиқиш имконини бериши керак (3-расм).



3-расм. Қидирув натижасининг иерархик даражаси.

Электрон архив тизимида архив тавсифи билан бирга бошқа бир неча асосий объект турлари мавжуд: архив тавсифи, авторитет ёзув, архив муассасаси, фаолият, ҳуқуқлар ва белгилар. Қўшимча объектларга архивга қабул қилиш ва жамлаш манбалари ёзувлари киради. Асосий объектлар бир-бирига мантиқан боғланган. Улар орасидаги семантик алоқани қуйидагича тасвирлаш мумкин (4–расм).

4-расм. Электрон архив тизими объектларининг семантик модели.

Қидирув тизими нафақат архив ҳужжатлари, балки шахслар ва ташкилотлар авторитет ёзувлари, мавзули каталог (маълумотномалар), архив муассасалари ва сақлаш жойлари бўйича ҳам қидириш имконини бериши лозим.

АХБОРОТ МАДАНИЯТИНИ ШАКЛЛАНТИРИШ МАСАЛАЛАРИ

З.Ш.Султанова (ТАТУ ассистенти)

Замонавий жамиятнинг фарқли белгиларидан бири бу ўсиб келаётган ёш авлодни теварак атрофда бўлаётган ўзгаришларга доимий мослаштириб бориш ҳисобланади. Цивилизациянинг ривожланишида унинг асл моҳиятини олдин қандай бўлганлиги билан таққослаймиз. Унинг ўзига хослик белгилари узлуксизлик, шиддатлилик, глобал характерлиликдир. Ахборотлаштириш асрида ахборот хуружининг авж олиши айниқса ёшларда ахборот олиш маданияти, ўқиш маданиятини шакллаштиришни тақозо этади. Бу ахборотлаштириш асрида янги иқтисод, янги сиёсат, янги жамият юзага келди. Янги жамиятда инсондан фақат ақл кучи талаб этилади. Бундай жамиятда меҳнат характерининг ўзи ўзгаради: ишлаб чиқаришнинг барча соҳаларида ақлий меҳнат физик меҳнатни сиқиб чиқаради.

Мутахассисларнинг таъкидлашича, бугун ахборот шиддат билан янгиланиб, ҳажми ошиб бормоқда. Натижада билимнинг ўсиши темпи илгарилаб кетмоқда. Ўтган асрда жамииятда ҳаётни иккига бўлиб, ўқиш даври ва иш даври бўлган.

Бугун компьютерлар, компьютер тармоқлари, улкан ҳажмдаги ахборот ресурсларидан оқилона фойдаланишда жамият ва инсон учун ахборот маданияти феноменининг глобал аҳамиятини англаш талаб этилади. Ахборот маданияти феноменининг пайдо бўлишининг асосий факторлари бу ахборотлаштириш асрига ўтишнинг универсал ижтимоий муҳим категориялари, яъни ахборот ҳажмининг ўсиши, жамиятни ахборотлаштириш, техника ва технологиянинг ривожланиши, ахборот жамиятининг шаклланиши кабилар.

Ахборот маданияти - Мутолаа маданиятнинг муҳим белгиларидан бири. Ахборот маданияти инсоннинг мустақил шахс бўлиб шаклланишида муҳим аҳамият касб этади. Доимий мутолаа билан банд бўлган шахс фикр юрита олувчи ўз мустақил фикрига эга бўлган шахсдир. Ахборот оқимининг тезлик билан ривожланиши бугунги кунда ахборотларни тўғри саралашда қийинчилик туғдирмоқда. Техника асрида технологик воситаларнинг ривожланиши бутун дунё бўйича ўқишга бўлган эҳтиёжни камайтирди.

«Ахборот олиш» атамаси илк бор XX-асрнинг 70-йилларида пайдо бўлди; кутубхоначилар ушбу тушунчани ривожлантириш ва оммавийлаштириш бўйича ташаббус кўрсатдилар. Бу атама биринчи бор библиографлар К.М. Войханск ва Б.А. Смирноваларнинг «Кутубхоначилар ва китобхонлар ахборот маданияти хусусида» [«Кутубхона ва ахборот», 1974 й.] ва Э.Л. Шапиронинг «Ахборот сўровларининг ноаниқликларини камайтириш йўллари ҳақида» [“Илмий-техник кутубхоналар» журнали, 1975й.] номли мақолаларида фанга олиб кирилди. Ахборот маданияти қуйидагилардан ташкил топади.

- Кутубхона - библиография саводхонлиги
- Ўқиш маданияти
- Компьютер саводхонлиги

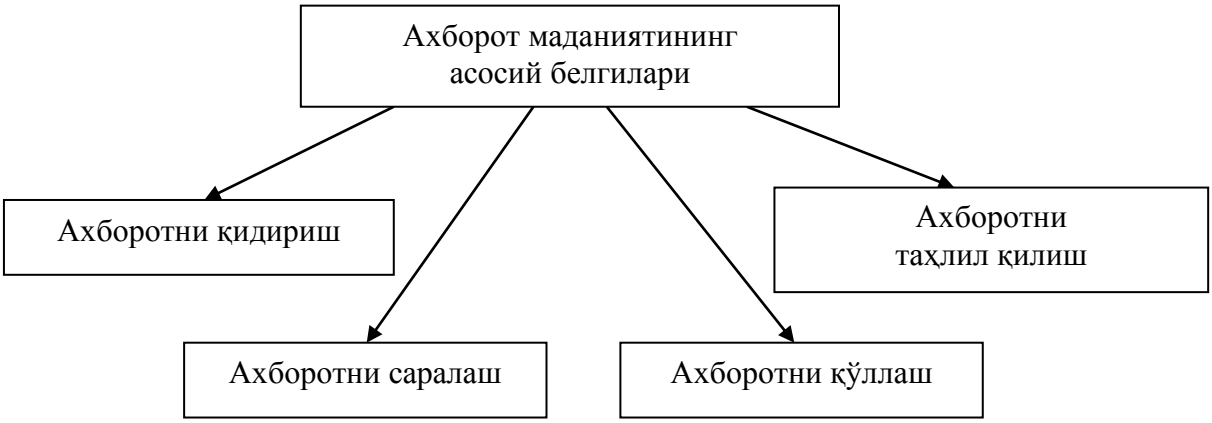
Кутубхона-библиография саводхонлиги–кутубхона ва ахборот ресурс марказининг маълумот-библиография фонди аппаратини осонлик билан йўналтира олиш кўникмасига эга бўлган малакали фойдаланувчини тайёрлаш учун зарур

Мутолаа маданияти – нашр этилган ишларни тўлақонли тушуниш ва қабул этишда фойдаланувчи учун зарур бўлган билим ва кўникма.

Компьютер саводхонлиги - компьютер бўйича кўникмаларга эга бўлиш материални тезкор ва самарали шакллантириш қобилиятини, маълумот қидируви ва маълумотни қайта ишлаш бўйича салоҳиятни ривожлантиради ва талаб этади.

Ахборот маданияти бу - ахборот билан мақсадни кўзлаган холда ишлаш кўникмасига эга бўлиш, шунингдек, ахборотни фойдаланиш учун ола билиш, компьютер

ахборот технологиясини, янги техник восита ва услубларини таҳлил қилиш ва узатиш. Қуйидагилар ахборот олиш маданиятининг асосий белгилари:



Ахборот олиш маданияти инсоннинг турли ижодий қобилиятлари маҳсули бўлиб бу қуйидаги аспектларда намоён бўлади:

- техник воситалардан фойдаланишда маълум бир кўникмаларда (Телефондан тортиб шахсий компьютер ва компьютер тармоқларигача);
- асосини турли дастурий маҳсулотлар ташкил этувчи компьютер ахборот технологияси фаолиятидан фойдалана билиш маҳоратида;
- турли ахборот билан ишлай билиш фаолиятида;
- ўз иш фаолияти соҳасида ахборот оқими хусусиятлари борасида тасаввурга эга бўлишда.

Ахборот олиш маданиятига эга бўлиш - бу ҳар бир инсон ўзлигини англашида ўз ўрни ва вазифасини билишда катта аҳамиятга эга бўлган фазилатларини кенг кўламда очиб беришдаги жараён. Таьлим ахборот олиш маданиятини шакиллантиришда катта аҳамиятга эга бўлиб, таьлим олиш тизимидаги ривожланиш ва ҳар бир кишини самарали тарзда ахборот ва ахборот воситаларидан фойдалана билиши жамият юксалишига сабаб бўлади.

РОЛЬ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ В ФОРМИРОВАНИИ ПРОФЕССИОНАЛЬНЫХ НАВЫКОВ БУДУЩИХ СПЕЦИАЛИСТОВ

Ю.Г.Ануфриева (ассистент ТУИТ)

В процессе изучения терминологии был проведен сопоставительный анализ понятий грамотность, информационная грамотность, компьютерная грамотность, *информационная культура*, эти термины - синонимы, имеющие общее смысловое содержание.

Под информационной культурой понимают совокупность принципов и реальных механизмов, обеспечивающих позитивное взаимодействие этнических и национальных культур, их соединение в общий опыт человечества.

Второе определение информационной культуры это - оптимальные способы обращения со знаками, данными, информацией и представление их заинтересованному потребителю для решения теоретических и практических задач; механизмы совершенствования технических сред производства, хранения и передачи информации; развитие системы обучения, подготовки человека к эффективному использованию информационных средств и информации.

Один из ведущих специалистов в области информатизации Э.П. Семенюк под информационной культурой понимает - информационную компоненту человеческой культуры в целом, объективно характеризующую уровень всех осуществляемых в обществе информационных процессов и существующих информационных отношений.

Вплоть до начала 80-х годов XX в. в словарях русского языка и педагогические справочные издания фиксируют лишь одно значение термина грамотность — определённая степень знания законов и правил родного языка в сочетании с навыками устной и письменной речи. Грамотность главным образом трактуется как умение читать и писать. В одном из самых авторитетных словарей русского языка – словарь С.И.Ожегова в 1987 г. трактует слово «грамотный» следующим образом:

1. Умеющий читать и писать, а также умеющий писать грамматически правильно.
2. Обладающий необходимыми знаниями, сведениями в какой-либо области.
3. Выполненный без ошибок, со знанием дела.

В международной практике вопросы определения понятия грамотности, его статистические характеристики с середины XX. в. рассматривались на международных совещаниях по статистике и программам переписей населения. Генеральная конференция ЮНЕСКО (10-я сессия, Париж, 1958 г.) рекомендовала всем странам при проведении переписей населения считать грамотными лиц, умеющих читать с пониманием прочитанного и написать краткое изложение о своей повседневной жизни. С середины 70-х годов XX в. в международной практике также наблюдается отход от элементарного понимания грамотности, происходит расширение объема понятия «грамотность». Так, на Всемирном конгрессе министров просвещения по ликвидации неграмотности (Тегеран, 1965 г.) был предложен термин «функциональная грамотность», понимаемая не только как способность человека выполнять стандартные, механические операции с текстовой и числовой информацией, но предполагающая обязательное понимание и самостоятельные действия. В соответствии с таким подходом в 1978 г. был пересмотрен текст рекомендации о международной стандартизации статистики в области образования, предложенный ЮНЕСКО; согласно новой редакции этого документа, грамотным считается тот, кто может участвовать во всех видах деятельности, в которых грамотность необходима для эффективного функционирования его группы или общины и которые дают ему также возможность пользоваться чтением, письмом и счётом для своего собственного развития и для развития группы или общины.

Современную трактовку понятия грамотности содержит «Оксфордская иллюстрированная энциклопедия: Народы и культуры»: «Грамотность – (literacy), умение читать и писать. Согласно определению ЮНЕСКО, человек считается грамотным, если «умеет читать и понимать прочитанное и записывать короткие простые утверждения, касающиеся его повседневной жизни», и функционально грамотным, если «может участвовать в любой деятельности, которая требует грамотности для успешной работы его группы или общины». Конкретное содержание понятия грамотность менялось исторически, расширяясь с ростом обществ, требований к развитию индивида - от элементарных умений читать, писать, считать и т. п. к владению минимумом общественно необходимых знаний и навыков (функциональная грамотность).

При изучении данного вопроса социологи отметили, что в любом из толкований информационная культура предполагает овладение ею людьми с целью эффективного преодоления объективно существующих информационных барьеров:

- ✓ языковых (овладение языками межнационального общения);
- ✓ пространственных (нахождение нужных данных в избыточном массиве информации);
- ✓ географических (нивелирование значительной взаимной удаленности источника и потребителя информации);
- ✓ количественные (определение достаточного количества источников информации).

Информационная культура включает в себя получение знаний и умений в процессе обучения на всех этапах, необходимость подготовки человека к жизни в информационном обществе побудило к проведению комплекс исследований и разработок по следующим основным направлениям:

- изучение и обобщение отечественного опыта образовательных и библиотечных учреждений по формированию информационных знаний и умений;
- исследование уровня информационных знаний и умений различных категорий потребителей информации, включая, прежде всего, учащуюся молодежь;

Стратегия формирования информационной культуры личности предполагает:

- получение общего образования на всех этапах получения образования человека;
- специальную подготовку при обучении в средних специальных учебных заведениях, высших учебных заведениях;
- обучение различных категорий потребителей информации, в первую очередь специалистов, работающих в информационно-библиотечных учреждениях;
- в процессе обучения будущих специалистов – на практических занятиях во время прохождения практики в информационно-библиотечных учреждениях;
- формирование информационной культуры среди пользователей и читателей информационно-библиотечных учреждений – постоянные процессы, необходимые для формирования навыков получения и обмена информацией, эффективному использованию информационных средств и информации.

ЭЛЕКТРОН КУТУБХОНАЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ДОЛЗАРБЛИГИ

Ш.Норматов (ТАТУ катта илмий ходим-изланувчиси)

Кейинги вақтларда электрон жамоат кутубхоналаридан фойдаланиш борасида катта ўсиш кузатилди ва бу истеъмолчиларга уларнинг географик жойлашувидан қатъий назар, онлайн ўқиш ва изланиш имкониятларини яратди. Ташриф буюрувчилар қачонлардир анъанавий кутубхоналардан олиш қийин бўлган ахборотларга кириш имкониятига эга бўлдилар ҳамда электрон кутубхона енгилликлари ва хизматларига кўникиб бўлишди.

Аммо кутубхоначилар уларнинг тизим ва тармоқларига таъсир кўрсатувчи хавфсизлик муаммосига унчалик ҳам эътибор бераверишмайди. Электрон кутубхоналар ва уларнинг интернет иловалари ишончли хавфсизлик тизимини талаб қилади. Чунки бутун дунёдан миллионлаб иштирокчилар ушбу сайт хизматлардан фойдаланиш учун ташриф буюришади. Мустаҳкам хавфсизлик тизими ушбу иловалар нархи ва фойдалилигини оширувчи ҳамда онлайн-хизматлар ёрдамида истеъмолчилар ишончи даражасини кўрсатувчи муҳим омиллардан бири ҳисобланади . Агар кутубхона хатарга дучор бўлиб, у матбуотда эълон қилинса, фойдаланувчилар ишончига путур етади. Шунинг учун ҳам кутубхона тизим хавфсизлигини ишончли таъминлаш жиддий аҳамиятга эга.

Шу вақтга қадар нафақат Ўзбекистонда, балки бошқа мамллакатларда ҳам электрон кутубхона хавфсизлиги соҳасидаги салмоқли адабиётлар ва тадқиқотлар кузга ташанмайди.

Ахборот ресурсларига онлайн кириш имкониятининг яратилиши электрон кутубхоналар сингари хизмат кўрсатишлар сонининг ошишига олиб келди. Жамоат кутубхоналарининг зудлик билан глобал миқёсда маҳаллий жамоат билимларини сақлаш ва ёйишда Web 2.0 каби янги технологиялардан фойдаланиб билимларга мурожаат этишга имкон берадиган платформага ўтиши кутилмоқда. Шу нуқтаи назардан, консорциум ва кутубхоналар гуруҳи хамкорликда бошқарувда электрон нашрлар ва ҳужжатларни тайёрлаш ҳамда хизматларни кўрсатишда биргаликда ишлашлари катта аҳамиятга эгадир.

Ҳозирда Буюк Британия жамоат кутубхоналари реестри рўйхатида 219 та кутубхона мавжуд. LibWeb каталоги ғарбий Европа электрон жамоат кутубхоналаридан танлаб олинган рўйхатда эса Францияга 93, Италияга 80 ва Германияга 133 та кутубхонани ҳисоблайди . Электрон контентни таъминлаб берувчи кутубхоналар сонининг ошиши билан ушбу хизматлардан фойдаланишга рухсат берилган ташриф буюрувчиларнинг кўлами ҳам кенгайиб боради. Аммо ижобий ўзгаришларга муаммосиз эришиб бўлмайди. Кутубхоначилар ўз ташриф буюрувчилари ва тизимларининг ҳимоясига катта эътибор қаратишлари керак.

Хакерлик ҳужумлари ва шахсий ахборотларнинг йўқотилиши ҳақидаги кўплаб янгиликлар истеъмолчилар ишончининг потенциал йўқолишига олиб келади. Айрим фирмалар ўз соҳаларида хавфсизликни таъминлашни мустақил бошқара олишмайди. Шунинг учун ҳукумат истеъмолчилар шахсий ахборотларини муносиб ҳимоялаш ва ҳимояланган тизимлар учун минимал талабларни таъминлаш бўйича қонунларни қабул қабул қилади.

Буюк Британияда Маълумотлар ҳимояси тўғрисидаги қонун 1998 йилдан буён компанияларнинг шахсий ахборотларини ҳимоялаш соҳасидаги ҳуқуқий мажбуриятларини аниқлайди ва маълумотларни сақлаш бўйича техник мажбуриятларни регламентлайди. 2008 йилда хатар ҳақида оголантиришга талаблар ва Давлат ҳукумати органларининг текширувларни ўтказиш бўйича бошқа қонун киритилди .

Франциянинг Маълумотлар хавфсизлиги тўғрисидаги директиваси 2004 йилда кучга кирди ва у шахсий ахборотларни қайта ишлашни тартибга солади.

Италиянинг Маълумотлар хавфсизлиги кодекси 2003 йил июнда қабул қилинган бўлиб, ташкилотлардан конкрет техник, мантиқий ва ташкилий минимал хавфсизлик чораларини ишлаб чиқишни талаб қилади.

Испаниянинг Маълумотлар хавфсизлиги тўғрисидаги директиваси 2003 йил апрелда кучга кирган ва шахсий маълумотларни ҳимоялашда, шунингдек ташкилот бузилиш содир этилганида истеъмолчиларни огоҳлантиришда фойдаланиш шарт бўлган конкрет хавфсизлик мажбуриятларини кўяди. Испания фирмаларига маълумотлар ҳимояси ва хавфсизлиги тўғрисидаги қонунларни бузганлик учун юридик санкция киритилди.

Ўзбекистон Республикасида 1997 йилда “Ахборот олиш кафолатлари ва эркинлиги тўғрисида”, 2004 йилда “Ахборотлаштириш тўғрисида”ги Давлат қонунлари қабул қилинди. 2013 йилда Республика Ахборот хавфсизлигини таъминлаш маркази ташкил этилди. Ушбу марказнинг асосий маркази “Электрон ҳукумат” ахборот тизимлари, ресурслари ва маълумотлар базаси тизими комплексларининг ахборот хавфсизлигини таъминлашга қаратилган.

Бошқа соҳалар билан қиёслаганда кутубхона маъмурларида бошқалардан фарқ қилувчи муаммолар мавжуд. Улар ходимлар, шунингдек кутубхона компьютерларидан фойдаланувчилар ва уларнинг веб сайтларига ташриф буюрувчилар каби кенг жамоатчилик учун хавфсиз тизимини таъминлаши шарт. Кутубхоначилар онлайн электрон тижорат транзакциялари билан персоналлашган хизматларни йўлга қўяди ҳамда шахсий маълумотлар ва тўловларни амалга ошириш имкониятини ўз ичига олган аккаунтларни яратади. Ушбу жараёнда кўпгина кутубхона хизматларидан фойдаланишга рухсат олиш учун ташриф буюрувчилар ўзларининг манзил ёки телефон рақами каби шахсий маълумотларини тизимга киритади. Баъзи хусусий кутубхона маълумотлар

базасининг обуна бўлиш нархи қимматлиги сабабли бу ресурслар хакерларнинг алоҳида қизишини уйғотиши мумкин. 2002 йилнинг ёзида ва 2004 йилнинг май ойида АҚШнинг Индиана Университетида хакерларнинг ҳужуми оқибатида иккита хавфсизлик қоидаларининг бузулиши кузатилган. Натижада янги ҳимоя воситаларини қўшиб тизимни тиклаш ва модернизациялаш учун кўп вақт ва куч сарф этилган.

Шундай қилиб, электрон кутубхоналар хавфсизлигини таъминлаш долзарблигининг кучайишига сабаб бўлаётган қуйидаги омилларни ажратиб кўрсатиш мумкин:

- Электрон кутубхоналар тизимларида ва тармоқларида сақланаётган ахборотлар ҳажми ҳамда кутубхона фойдаланувчилари сонининг кескин ошиб бориши;
- Ахборот хавфсизлигини ишончли таъминлаш воситалари нархининг нисбатан қимматлилиги;
- Электрон кутубхоналар хавфсизлигини таъминлаш усуллари, моделлари ва ёндашувларининг тўлиқ шаклланмаганлиги;
- Илмий техниканинг сўнгги ютуқларидан хавфсизлик тизимларини бузишда ҳам фойдаланишнинг мумкинлиги.

RFID (RADIO FREQUENCY IDENTIFICATION) TEHNOLOGIYASINI AXBOROT-KUTUBXONA TIZIMLARIDA JORIY QILISH

I.A. Holboyev (TATU talabasi)

Axborot-kutubxona boshqaruvi kitob tarqatish, sistemalashtirish, materiallarni kataloglashtirish hamda shtrix-kodlarni biriktirish kabi jarayonlarni o’z ichiga mujassamlashtiradi. Ko’plab jarayonlar, yuqoridagilarni hisobga olgan holda, to’g’ridan-to’g’ri foydalanuvchilarni qoniqtirish ta’siriga egadir. Masalan, hatto kichik kutubxonalarda ham, kitoblar ko’p hollarda o’z joyida bo’lmasligi mumkin, bu esa o’z navbatida foydalanuvchilarning noroziligiga olib kelishi mumkin.

Birinchi RFID tehnologiyalariga asoslangan ilovalar 1980 – yilning oxirlariga to’g’ri keladi. RFID tehnologiyasining rivojlanishi bilan uning narxi ham tusha boshladi, bu esa o’z navbatida uni keng qo’llanilishiga olib keldi. Masalan, RFID-belgilar arzonlashgani sari, uning kutubxonalarda joriy qilish ham ortib bordi.

RFIDning eng sodda tizimi uch moduldan tashkil topgan: RFID-belgi, RFID-o’quvchi va antennadan tashkil topgan. RFID-belgi chip va bog’lovchi elementdan tashkil topgan; har bir belgi ob’yektga qo’shilgan unikal elektron kodga ega va ularni aniqlash maqsadida ishlatiladi. RFID-o’quvchilar RFID-belgidagi axborotlarni o’qish va ularga axborot yozish uchun mo’ljallangan qurilmalardir. RFID-o’quvchilar portativ yoki stantsionar bo’lishi mumkin.

RFID tehnologiyasi axborot-kutubxona muassasalarida turli xil modullarida ishtirok etadi. Masalan, axborot-kutubxona muassasasining har bir materialiga RFID-belgilarini biriktirish; o’z-o’ziga hizmat ko’rsatish tizimi orqali foydalanuvchilar kitoblarni olish; maxsus qurilmalar orqali kitoblarni qabul qilish; RFID-belgilarni biriktirish orqali maxsus eshiklar orqali kitoblarning o’g’irlanishini oldini olish; va nihoyat RFID portativ o’quvchilar bilan kutubxonachi qidirish jarayoni orqali noto’g’ri qo’yilgan kitobni o’z joyiga joylashtirish.

Axborot-kutubxona muassasalari RFID texnologiyasini o’z-o’ziga hizmat ko’rsatish tizimini axborot-kutubxona muassasalarida rivojlantirish maqsadida joriy qilishmoqda. Foydalanuvchilar axborot-kutubxona resurslarini maxsus qurilmalar orqali buyurtma berishi va ularni qaytarishi mumkin. Buning uchun axborot-kutubxona muassasasining kartochkasi va PIN kod zarur bo’ladi. Bu texnologiya yordamida o’z-o’ziga hizmat ko’rsatish soddalashadi, ya’ni bu jarayon kutubxonachining bu jarayonlarda ishtirok etishi shart emasligini ko’rsatadi.

Bundan tashqari, qaytarilgan kitoblarni saralashda ham kutubxona ishchilarining qo'l ishida qiladigan jarayonlarini qisqartiradi. RFID belgining o'g'irlashga qarshi himoya funksiyasi borligi, o'g'irlashga qarshi qo'shimcha choralarni ko'rish vazifalaridan ozod etadi va bu bir kompleksda mujassam bo'ladi, ya'ni kitob buyurtma berish, ularni qaytarib olish va ularni o'g'irlashdan himoya qilish.

RFID axborot-kutubxona boshqaruvi sohasida oddiy bar-kod yoki magnit belgilarga nisbatan sezilarli qulaylikalarni beradi. U intellektual axborotlar va kutubxonani boshqarishni ta'minlaydi, bu esa o'z navbatida foydalanuvchilarga yuqori sifatli hizmat ko'rsatishni anglatadi. Texnologiyani rivojlantirish kerakligiga qaramasdan bozor iqtisodiyotini jadal rivojlanishi, RFID texnologiyani porloq kelajagidir, darhaqiqat, u kelajakda O'zbekistonda axborotlarni taqdim etish va axborot-kutubxona muassasalarini boshqarishda asosiy rol o'ynaydi.

Xulosa qilib ayatdigan bo'lsak, RFID texnologiyasi O'zbekistonda qo'llanilayotgan, tez rivojlanayotgan va qulay texnologiyalardan biridir. RFID texnologiyasini qo'llash katta va kichik axborot-kutubxona muassasalarida o'z-o'ziga hizmat ko'rsatishning samaradorligini oshiradi hamda kutubxonachining qolgan bo'sh vaqti boshqa axborot-kutubxona ishlarida qo'llanilishiga sarf etiladi.

КУТУБХОНА РЕСУРСЛАРИ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ҲУҚУҚИЙ ЖИҲАТЛАРИ

Ш.Б.Норматов (ТАТУ катта илмий ходим-изланувчиси)

Охирги бир неча ўн йиллик ичида бутун дунё жамияти ахборот технологияларига боғлиқ ҳолда ривожланмоқда. Бугунги ахборот асрида миллионлаб фойдаланувчилар тижорат, таълим, соғлиқни сақлаш каби мураккаб жараёнларда кўплаб ахборот контенти объектларига мурожаат қилмоқда ва уларни ўзгартимоқда. Глобал тармоқ инфратузилмаси ва интернет технологиялари ёрдамида маълумотларни алмашиш анча арзон ва осон амалга оширилмоқда. Натижада ахборот кутубхона тизимлари ва тармоқларида ҳам ахборотларни сақлаш ва уларнинг конфеденциаллигини таъминлаш муаммоси вужудга келди. Бундан ташқари тизимнинг бутунлиги ҳам таҳдид остида қолди. Бундай тизимлар учун бутунлик ва ахборотнинг эркин олиниш хусусиятига бўладиган таҳдидлардан ҳимояланиш катта аҳамият касб этади.

Ҳар қандай ислоҳот уни амалга оширишнинг ҳуқуқий асосларига таянади. Ахборот кутубхона тармоқларида хавфсизлигини таъминлаш соҳасида ҳам бу борада қатор ишлар амалга оширилган. Шундай қилиб, қуйида кутубхона ресурслари хавфсизлигини таъминлашнинг ҳуқуқий жиҳатлари халқаро ва миллий қонунчилик ҳужжатлари асосида кўрсатиб берилади.

Халқаро ҳуқуқий ҳужжатлар. Ахборот хавфсизлигига доир бир нечта стандарт ва қоидадалар мавжуд. Энг аввало ISO стандартлари бу соҳада анча устунликка эга.

ISO / IEC 27002: 2005 (ахборот хавфсизлигини таъминлаш бўйича қоидалар тўплами) стандарти BS 7799 асосида яратилган бўлиб, 1990 йилларнинг ўрталарида босилиб чиққан. Британия стандарти ISO / IEC га мувофиқ ISO / IEC 17799: 2000 сифатида қабул қилинган. 2005 йилда бошқа ISO / IEC 27000 серияли стандартлар билан мувофиқлаштириш учун қайта кўриб чиқилган ва 2007 йилда қайта рақамланган (шундан сўнг ўзгармаган).

Бу стандарт ушбу соҳанинг қуйидаги 10 та йўналиши бўйича бошқариш тамойиллари ва амалий тавсиялардан ташкил топган: хавфсизлик сиёсати; ахборот хавфсизлигини ташкил қилиш; активларни бошқариш; инсон ресурслари хавфсизлиги; атроф муҳит (environmental) ва физик хавфсизлик; алоқа воситалари ва операцияларни бошқариш; киришни назорат қилиш; ахборот тизимларини йиғиш, яратиш ва кузатиб бориш; ахборот хавфсизлиги ходисаларини бошқариш; бандлик узлуксизлигини бошқариш, амал қилиш.

ISO / IEC 27001 ISO: 2005 (Ахборот хавфсизлигини бошқариш тизими – талаблар) стандартb ҳам BS 7799 дан келиб чиққан. Биринчи қисм ахборот хавфсизлигини бошқариш бўйича тавсиялардан иборат бўлиб, 1998 йилда кўриб чиқилган, халқаро стандарт ташкилотларининг узоқ давом этган муҳокамасидан сўнг 2000 йилда ISO га ISO / IEC 17799 "Ахборот технологиялари - ахборот хавфсизлигини бошқариш учун қоидалар тўплами" стандарти сифатида қабул қилинди. ISO / IEC 17799 2005 йилда қайта кўриб чиқилди ва ниҳоят 2007 йил июлда ISO / IEC 27002 сифатида ISO 27000 серияли стандартлар қаторига киритилди. У ташкилот доирасида ахборот хавфсизлигини бошқариш тизимини (АХБТ) ҳужжатлаштиришда яратиш, қўллаш, эксплуатация қилиш, мониторинг, рецензиялаш, сақлаш ва такомилллаштиришга талабларни аниқлайди.

ISO/IEC 27002:2005 – "Ахборот технологияси. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари. Ушбу стандартда ахборот хавфсизлигини бошқариш бўйича келтирилган ахборот хавфсизлигининг зарурати, ахборот хавфсизлиги талабларини аниқлаш, ахборот хавфсизлиги хавфларини баҳолаш, ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш ва ахборот хавфсизлигини жорий қилиш учун таянч нуқтани танлаш каби тадбирлар ахборот хавфсизлигини бошқариш учун амал қилинадиган принциплар сифатида қабул қилиниши ва кўпгина ташкилотлар учун қўлланиши мумкин.

Буюк Британияда Маълумотлар ҳимояси тўғрисидаги қонун 1998 йилдан буён компанияларнинг шахсий ахборотларини ҳимоялаш соҳасидаги ҳуқуқий мажбуриятларини аниқлайди ва маълумотларни сақлаш бўйича техник мажбуриятларни регламентлайди. 2008 йилда хатар ҳақида оголантиришга талаблар ва давлат ҳукумати органларининг текширувларни ўтказиш бўйича бошқа қонун киритилди.

Францияниг Маълумотлар хавфсизлиги тўғрисидаги директиваси (Қонун №. 2004-801) 2004 йилда кучга кирди ва у шахсий ахборотларни қайта ишлашни тартибга солади.

Испаниянинг Маълумотлар хавфсизлиги тўғрисидаги директиваси 2003 йил апрелда кучга кирган ва шахсий маълумотларни ҳимоялашда, шунингдек ташкилотда бузилиш содир этилганда истеъмолчиларни огоҳлантиришда фойдаланиш шарт бўлган конкрет хавфсизлик мажбуриятларини қўяди.

Миллий ҳуқуқий ҳужжатлар. *RH 45-215:2009 - Раҳбарий ҳужжат. Маълумотлар узатиш тармоғида ахборот хавфсизлигини таъминлаш тўғрисида Низом.* Ушбу ҳужжат N 100:2002 «Маълумотлар узатиш миллий тармоғида ахборот хавфсизлигини таъминлаш тўғрисида низом» ўрнига амалга киритилган бўлиб, маълумотлар узатиш тармоғида (МУТ) ахборот хавфсизлигини таъминлаш бўйича асосий мақсадлар, вазифалар, функциялар ва ташкилий-техник тадбирларни белгилайди.

RH 45-024:2009 - Раҳбарий ҳужжат. Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлигини таъминлаш тизими тўғрисида Низом. Ушбу норматив ҳужжат Алоқа ва ахборотлаштириш соасида ахборот хавфсизлигини таъминлаш тизимининг асосий мақсадлар, вазифалар, функциялар ва ташкилий структурасини белгилайди.

Ҳужжат мулкчилик шаклидан қатъий назар алоқа ва ахборотлаштириш соҳасининг барча ташкилотлари ва хўжалик юритувчи субъектлари (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожантириш вазирлигининг ҳудудий бошқармалари, Вазирлик қошидаги ташкилотлар, муассасалар, ўқув юртлари ...) томонидан қўллаш учун мўлжалланган.

Ўзбекистон Респуликасининг "Ахборотлаштириш тўғрисида"ги қонуни. Ушбу қонуннинг 19 ва 20-моддаларида ахборот ресурслари ва ахборот тизимларини ҳимоя қилишнинг асосий мақсадлари ва тартиби келтириб ўтилган:

"19-модда. Ахборот ресурслари ва ахборот тизимларини муҳофаза қилиш қуйидаги мақсадларда амалга оширилади:

шахс, жамият ва давлатнинг ахборот хавфсизлигини таъминлаш;

ахборот ресурсларининг тарқалиб кетиши, ўғирланиши, йўқотилиши, бузиб талқин этилиши, тўсиб қўйилиши, қалбакилаштирилиши ва улардан бошқача тарзда рухсатсиз эркин фойдаланилишининг олдини олиш;

ахборотни йўқ қилиш, тўсиб қўйиш, ундан нусха олиш, уни бузиб талқин этишга доир рухсатсиз ҳаракатларнинг ҳамда ахборот ресурслари ва ахборот тизимларига бошқа шаклдаги аралашишларнинг олдини олиш;

20-модда. Ахборот ресурслари ва ахборот тизимлари муҳофаза қилинишини ташкил этиш.

Ахборот ресурслари ва ахборот тизимлари, агар улар билан ғайриқонуний муносабатда бўлиш натижасида ахборот ресурсларининг ёки ахборот тизимларининг мулкдорларига, эгаларига ёхуд бошқа юридик ҳамда жисмоний шахсларга зарар етказилиши мумкин бўлса, муҳофаза қилиниши керак”.

Юқорида келтирилганлардан мамлакатимизда ҳам ахборот хавфсизлиги соҳасидаги қонунчиликнинг сезиларли ривожланганлигини ва ахборот ресурслари хавфсизлигини таъминлашнинг долзарблигини кўриш мумкин.

АХБОРОТ МАДАНИЯТИНИ ШАКЛЛАНТИРИШ ОРҚАЛИ ЎҚУВЧИНИ КИТОБХОНГА АЙЛАНТИРАМИЗ

К.Н. Юсупова (ЎМКҲТТКМО ва УҚТИ катта ўқитувчиси)

Бугунги кунда ахборот олиш маданиятини шакллантириш энг долзарб бўлган масалалардан бири ҳисобланади, чунки, ахборот оқимининг тезликда ўсиб бориши, тақдим этилаётган ахборотлар орасидан керакли, зарурий ва фойдалиларини ажратиб олиш мураккаб жараёндир. Бунинг учун ҳар бир шахс мустақил фикрга эга, дунёқараши кенг ахборотлар уюмидан ўзи учун кераклилигини ажратиб олиш салоҳиятига эга бўлиши лозим. Ахборот олиш маданиятини шакллантиришнинг бир нечта босқичлари мавжуд бўлиб улар орасида энг муҳими бу кишилар орасида ўқиш маданиятини юксалтиришдир. Аҳолиси мунтазам равишда ўқиш, мутолаа қилиш билан машғул бўлган жамият пойдевори мустаҳкам бўлишига жаҳон мамлакатлари орасида ўқиш маданияти даражасини таҳлил қилиш чоғида яна бир бор амин бўлдим. Бир неча йиллар инсонлар орасида ўқишга бўлган эътиборнинг пасайганлигини ва бу ривожланган давлатларни ҳам четлаб ўтмаганлигини билдим. Ўқиш маданиятини шакллантириш одамлар орасида жиноятчиликни, бепарволикни олдини олади. Замонавий технологияларнинг ривожланиши ўқишга бўлган этиборни бир мунча пасайтириб юборди. Давр талабини инобатга олган ҳолда ахборот олиш маданиятининг бир бўлаги бўлган ўқиш маданиятини ҳам замонавий кўринишда тарғиб этиш мақсадга мувофиқ. Бунинг энг самарали усули бу мультимедиа воситаларидир. Мультимедиали дастурлар, воситалар бугунги кунда бутун дунё миқёсида жадал ривожланмоқда ва уларга бўлган талаб ҳам ортиб бораяпти. Бунинг асосий сабаби бу мультимедиали воситаларнинг эътиборни жалб қилувчи жиҳатларидир.

Ахборот олиш маданиятини шакллантиришда мультимедияли дастурлардан фойдаланишнг самараси юқори. Унда тингловчи бир вақтнинг ўзида ҳам эшитиши, кўзи билан кўриши, ўзи хам дарс давомида бевосита иштирокчига айланиб бирон бир янгиликлар киритиши мумкин. Ахборот олиш маданиятини шакллантириш ишини кичик ёшдаги болалар билан бошлаш кутилган натижани беради деб ҳисоблайман. Чунки болалар онги хали тоза ва унга қайси тарафдан тарбия берсанг шу тарафдан ривожланиб камолга етади. Биз уларга кичикликларидан ахборот билан ишлашни ўргатиб борсак, уларда ахборот олиш маданиятини шакллантирсак, келажакда уларда турли зарарли ахборотларга қарши имунитет пайдо бўлади. Бу эса энг зарурий масалалардан биридир.

Мультимедиали дастурлар тайёрлаш жараёни қийин жараён, мультимедиали дастурлар эса қиммат бўлиши билан бирга таълим сифатини оширишда катта таъсир кучига эга. Ахборот олиш маданиятини шакллантиришда мультимедиали воситаларнинг

роли юқори. Улар қабул қилиш тезлигини оширади, мустақил фикр юритишга ўргатади ва фойдаланувчида интерфаол қобилятни шакллантиради. Мультимедиали мутолаа орқали билим олиш сифати тезликда шаклланади ва ўқувчиларда олинаётган ахборотга нисбатан қизиқиш самараси кескин ортади. Мультимедиали дарсликлардан фойдаланувчи ўқитувчиларнинг дарс ўтказишлари учун осонликлар ва қулайликлар мавжуд. Анъанавий таълим воситаларидан фарқли ўлароқ медиа технологиялари сезиларли равишда эрта ривожланишдаги имкониятларини кенгайтиради, боланинг ақлий ва ижодий қобилиятларини мувафаққиятли тарзда амалга оширишда ўз ҳиссасини қўшади. Нафақат уларга тайёр керакли маълумотларни беради, балки керакли маълумотни ўзлари қидириб топишларига ундайди. Медиа ресурслардан фойдаланиш буйича керакли вазифа ва маълумотларни кўпгина сайтлардан топиш мумкин. Шу тарзда ўрганиш жараёни фаоллашади. Медиа таълим ушбу максадга эришишнинг энг самарали услубларидан бири. Медиа таълим педагогик фаолиятнинг идеологияси сифатида ушбу вазиятда умумтаълим билим кўникмаларини эгаллашнинг шаклланишида эришиладиган самаранинг кафолати сифатида аҳамият касб этади, шунингдек, таълим берувчи ва таълим олувчининг ахборот маданияти кўникмаларини шакллантиришида ҳам. Шу ўринда мактаб кутубхоналарининг ҳам ўқиш маданиятини шакллантиришда ва ривожлантиришда тасири катта ҳисобланади. Кутубхоначининг ташаббуси ва эътибори билан кутубхонадан фойдаланувчини ўқувчидан китобхонга айлантириш мумкин. Кутубхоналарга жалб этишнинг бир қанча замонавий усулларидан, масалан, виртуаль китоб кўргазмалари, китобхонлар марофонлари, китоб аукционлари, кутубхонадан ташқаридаги ўқишлардан фойдалниш ижобий натижани беради. Ахборот маданиятини шакллантиришнинг энг самарали усулларидан яна бири бу ёшлар порталини яратиш ҳисобланади. Бунинг бир қанча сабаблари мавжуд яни, портал яратилганда:

- ✓ Ёшларга бағишланган манбаларни бир жойга тўплаш имконияти яратилади;
- ✓ Ёшлар ўртасида ахборот қидирувини амалга ошириш кўникмаси шаклланади;
- ✓ Турли манбалардан керакли ахборотларни топиш ва улардан фойдаланиш билими ошади;
- ✓ Ота оналар учун бехавотир манба ҳисобланади.

KUTUBXONA FOYDALANUVCHILARI O’RTASIDA NOYOB ADABIYOT MANBALARINI TARG’IB QILISH

R. Jumanazarova (TATU magistranti)

Xotirasiz barkamol kishi bo`lmaganidek, o`z tarixini bilmagan xalqning kelajagi ham bo`lmaydi. ***I.A. Karimov.***

Yurtimizda noyob nashrlarni saqlash va ularni kelajak avlodga yetkazib berish borasida ko’plab ishlar amalga oshirilayotgani sir emas, albatta. Hususan, O‘zbekiston Respublikasi Vazirlar Mahkamasining 2012-yil 9 iyuldagi “Nodir, alohida qimmatli va noyob nashrlar saqlanishini ta’minlash, ularning fondini tizimli ko‘paytirish va boyitish chora-tadbirlari to‘g‘risida”gi qarorining qabul qilinganligi ham ushbu borada muhim dasturilamal bo’lib xizmat qilmoqda.

Barchamizga ma’lumki, o’zbek xalqi juda ham boy tarixiy o’tmishga ega. Buni biz ajdodlarimizdan bizga qoldirilgan ma’naviy meroslarda ham ko’rishimiz mumkin. Zero, Prezidentimiz ta’kidlaganlaridek, Navoiy, Ulug`bek, Bobur, Mashrab, Furqat, Qodiriy va xalqimizning boshqa buyuk farzandlari va ularning merosi O`zbekiston xalqlari umuminsoniy qadriyatlarining ravnaqi va boyishiga xizmat qilib kelgan edi va bundan buyon ham xizmat qiladi. Shunday ekan, biz avlodlar ajdodlarimiz qoldirgan ulkan merosni ko’z qorachig’imizdek asrashimiz darkor. Yurtimizda faoliyat yuritayotgan Axborot Kutubxona Markazlarida tashkil qilingan noyob nashrlar fondlarida bu borada ko’plab ishlar amalga oshirilmoqda.

Hususan, bunday xayrli ishlar O'zbekiston Milliy kutubxonasi Axborot-kutubxona fondlarini konservatsiya va restavratsiya qilish bo'limida amalga oshirilmoqda bu jarayonda bo'lim xodimlari axborot kutubxona fondlarini konsevratsiya va restavratsiya qilish xizmatida qo'lyozmalarni saqlash rejimiga qat'iy amal qilmoqdalar, yani bu jarayonda ular muqovani restavrsiya qilish, qog'ozlarni restavratsiya qilish, juz bo'laklariga bo'lish va ajratish, tikib jamlab chiqish, qo'lyozmani muqovaga qayta joylashtirish kabi ishlarni sitqidildan amalga oshirmoqdalar. Ushbu bo'limning rahbari Marif Salimov ta'kidlaganlaridek: "Bizning asosiy maqsadimiz qo'lyozma kitoblarni saqlash va asrashga qaratilgandir. O'z faoliyatimizda bu sohani murakkabligi va mas'uliyatliligi, hamda qo'yilgan har bir kichik xatoning oqibatini hisobga oladigan bo'lsak, soha mutaxassislarining doimiy aloqada va hamkorlikda ish olib borishlari zarur deb bilamiz. O'z yechimini kutayotgan turli muammolarni birgalikda hal qilish uchun hamkorlikda tayyormiz" deydilar. Undan tashqari yurtimizda ajdodlarimiz tomonidan yaratilgan qadimiy hujjatli meroslarni saqlash, ularni keng jamoatchilik e'tiboriga ma'lum qilish borasida ham kutubxonaning kitob muzeyida "Qo'lyozmalar, nodir va alohida qimmatga ega nashrlar" xizmati fondidagi qadimiy noyob kitoblardan tez-tez ko'rgazmalar tashkil qilinmoqda.

Kutubxona foydalanuvchilari orasida noyob adabiyot manbalarini targ'ib qilish borasida Xorazm Ma'mun akademiyasi ham o'z xizmatlari bilan muhim ahamiyat kasb etmoqda. Xorazm Ma'mun akademiyasida zamonaviy axborot resurs markazi tashkil qilingan. ARM dagi Noyob kitoblar fondida 150 nusxaga yaqin noyob qo'lyozma va toshbosma asarlar saqlanadi. Ularning katalogi yaratilib, bir necha ilmiy maqolalar chop etilgan. Fondda saqlanayotgan "Daqoiq ul-axbor" toshbosmasining Abullays Samarqandiy qalamiga mansubligi aniqlangan. "Tariqa Muhammadiya" asari esa chet el katologlari bilan qiyoslanib uning yurtimizdagi yagona nodir qo'lyozma ekanligi ma'lum qilingan. Shuningdek, noyob kitoblar fondidan ma'naviy, huquqiy, didaktik mazmundagi bir qancha nodir qo'lyozmalar joy olgan. Xorazm Ma'mun akademiyasining qo'lyozma va nodir kitoblar fondi 20 ming nusxani tashkil etadi. Ulardan 4000 tasi elektron nashrga o'tkazilgan.

Xorazm viloyati axborot kutubxona markazida ham 2000 dan ziyod nodir adabiyotlar mavjud bo'lib, ularning 600 dan ortig'i noyob kitoblar, qo'lyozmalar hisoblanadi. Ularning ayrimlari XVIII va XIX asrlarga oid toshbosma kitoblardir. Nodir kitoblar orasida arab, qozoq, tatar, ingiliz, nemis, rus tillarida chop etilgan asarlar ham mavjud. Bugungi kunda ARM da jahon adabiyotining nodir asarlaridan bo'lgan Alisher Navoiyning "Xamsa" si va Firdavsiyning "Shoxnoma" asarining elektron nusxalari yaratilgan. ARM da bunday elektron nusxalarini yaratilishi uning erishayotgan yutuqlaridan biri hisoblanadi. Elektron katolokka o'zbek va rus tillarida barcha nodir adabiyotlarining bibliografik yozuvlari kiritilgan bo'lib, ulardan noyob va nodir asarlar 582 nomda, arab tilida 140 nomda, rus tilida 553 nomdagilar tashkil qiladi. AKM ning ilmiy-uslubiy bo'limi mudiri Mavluda Qurbanbaevaning aytishlaricha: "Bizning oldimizdagi maqsadimiz Xorazmning tarixi, madaniy merosi, urf odatlari, san'atiga qiziquvchi sayyohlarni, ayniqsa, xorijlik sayyohlarni, axborot kutubxona markazimizga ko'proq jalb qilish, uning fondlarida mavjud nodir kitoblar, qo'lyozmalar bilan tanishtirish uchun kutubxonamizga sayohatlar uyishtirish va ularga tobora manzur xizmatlar ko'rsatishdir".

Qolaversa, so'nggi paytlarda elektron manbalarning keng tarqalishi ham ma'lumot manbalarini kutubxona foydalanuvchilari orasida targ'ib qilishning ahamiyatini yuksaltirdi.

Biz foydalanuvchilar nafaqat yurtimiz miqyosida chegaralanib qolmasdan, balki, chet mamlakatlar miqyosida ham noyob adabiyotlar va ulardan qanday foydalanish kerakligi haqida bilimlarga ega bo'lishimiz lozim. Ushbu egallagan tajribamiz orqali, biz chet mamlakatlarda mavjud saytlar orqali u yerga tashrif buyurishimiz mumkin. Masalan, Amerika Qo'shma Shtatlari milliy davlat katalogi Kongress kutubxonasining kartali katalogi sifatida yaratilgan. Mazkur katalog ham bosma, ham mikrofilm ko'rinishida chop qilingan. Bugungi kunda milliy davlat katalogidan Kongress kutubxonasi saytida **catalog.loc.gov** manzilida bepul foydalanish imkoniyati mavjud. Shuningdek milliy davlat katalogidan pulli ravishda OCLC nomli bibliografik tarmoq orqali ham foydalanish mumkin bo'lib uning fondiga kitoblar, xaritalar, musiqa asarlari, ko'p seriyali filmlar, noyob adabiyotlar, qo'lyozmalar, vizual materiallar

hamda ko'plab boshqa manbalar kiritilgan. Kongress kutubxonasining kolleksiyasi 139 million dona adabiyotlarni tashkil qilib, shundan 21 million donasi kitoblar, 61 million donasi qo'lyozmalar va noyob nashrlar, 13 million donasi fotosur'atlar, 5 million donasi xarita, 5,5 million donasi musiqa notalari va 1,2 million donasi harakatlanuvchi sur'atlardan yani kinofilmlardan iborat.

The American Book Trade Directory (Amerika kitob savdosi ma'lumotnomasi) nashriga AQSHda 25 mingdan ziyod chakana va noyob kitob sotuvchilari, kitoblarning ulgurji savdosi bilan shug'ullanuvchi kompaniyalar ro'yxati kiritilgan. Foydalanuvchilar mazkur nashrdan muayyan mavzuga ixtisoslashgan noyob kitoblarni va shu bilan birga boshqa tildagi kitoblar chakana savdosi bilan shug'ullanuvchi do'konlar va kutubxona kolleksiyasi haqidagi ma'lumotlarni topishlari mumkin.

Shuni aytishimiz mumkinki, noyob nashrlar qatorida ensiklopediyalar ham foydalanuvchilarning ma'naviy bilim olish jarayonida muhim ahamiyat kasb etadi. Ensklopediya har qanday kutubxonanaing axborot negizini tashkil etadi, chunki har qanday savol uchun eng tez javob aynan ensklopediyadan topilishi mumkin. Internet tarmog'ining ko'lamida so'nggi yillar davomida ensklopediyalardan foydalanish imkoniyati tobora kengayib borayotganini hisobga oladigan bo'lsak buning ko'rsatkichi yuqori darajalarda ekanligini ko'rsatadi.

Shuni alohida ta'kidlab o'tishimiz lozimki, agar ensklopediyalar, noyob nashrlar va qo'lyozmalar bo'lmaganida yoki bizgacha etib kelmaganida oldingi zamonlarda inson faoliyatining har bir jabhasi jihatlarini qamrab olgan ma'lumot manbalari ham mavjud bo'lmas edi.

Aytingchi, dunyoda bu qadar boy merosga ega boshqa xalqlar ham bormi? Tomirimizda Navoiy, Ulug`bek, Bobur, Amir Temur va xalqimizning ana shunday buyuk insonlarining qoni oqar ekan, biz farovon va go'zal turmush yaratish uchun beqiyos imkonimiz bor, desak adashmagan bo'lamiz albatta. Bu kuch bizni vatanimiz oldida turgan buyuk maqsadlarni ado etishga chorlaydi.

АХБОРОТ КУТУБХОНА МУАССАСАЛАРИДА ЗАМОНАВИЙ АХБОРОТ-КУТУБХОНА ХИЗМАТЛАРИ

М.Файзиев (ТАТУ магистранти)

Ёшларнинг интелектуал салоҳиятини оширишда ахборот-кутубхона муассасаларининг ўрни беқиёсдир. Қадимдан кутубхоналар илм тарқатувчи маскан ҳисобланиб келинган. Асосий вазифа албатта кутубхоначи зиммасига тушар эди. Бугунги кунга келиб бу вазифа янада масъулиятли тус олмоқда.

Ахборот-кутубхона муассасаларининг бош мақсади барча тоифадаги фойдаланувчиларнинг ахборотга бўлган талабини қондиришдан иборат. Ушбу мақсад йўлида ҳар бир ахборот-кутубхона муассасаси ўзи учун стратегия ишлаб чиқиши ва турли тоифадаги фойдаланувчиларга кўрсатиш мумкин бўлган ахборот-кутубхона хизматлари сонини кўпайтириб бориши мақсадга мувофиқдир.

Фойдаланувчиларнинг қизиқишларини ўрганиш, фойдаланувчиларга ижод эркинлигини яратиб бериш, жамиятнинг бошқа уюшмалари билан ҳамкорликда изланишлар олиб бориш ва ўзаро ҳамкорликни рағбатлантириш ахборот-кутубхона муассасалари олдида турган долзарб масалалардан ҳисобланади.

Ушбу мақоладан кўзланган мақсад жахондаги етакчи ахборот-кутубхона муассасаларида фойдаланувчиларга кўрсатиладиган хизматларни ўрганиб, шу аснода Ўзбекистондаги ахборот-кутубхона муассасаларида фойдаланувчиларга хизмат кўрсатишдаги камчиликларни аниқлаш ва уларни бартараф этиш чораларини таклиф қилишдан иборат.

Мазкур тадқиқот дунёдаги етакчи ахборот-кутубхона муассасаларида фойдаланувчиларга кўрсатилаётган хизмат турларини тахлил қилишдан бошланди. Бугунги кунга қадар АҚШ нинг Флорида штатидаги Майами университети кутубхонаси, АҚШ нинг Масачусетс штатидаги Бостон оммавий кутубхонаси, АҚШ нинг Конгресс кутубхонаси, Австралия Миллий кутубхонаси, Ирландиянинг Дублин Тринити коллеж кутубхонаси, Ўзбекистон Миллий кутубхонаси ва бошқа йирик кутубхоналар тахлил қилинди. Мисол тариқасида қуйидаги 3 та йирик ахборот-кутубхона муассасалари танлаб олинди.

1. Дублин шаҳрида жойлашган Тринити-коллеж кутубхонаси Ирландиянинг энг йирик кутубхонаси саналади. Мазкур кутубхона 1592-йилда ташкил топган бўлиб, 1801-йилдан буён Буюк Британия ва Ирландия мамлакатларида чоп этилаётган нашрларнинг мажбурий нусхасини ўзида сақлаб келмоқда. Кутубхонанинг фонди 6 миллиондан ортиқни ташкил қилади.

2. Америка қўшма штатларининг Масачусетс штатидаги Бостон оммавий кутубхонасига 1848-йилда асос солинган бўлиб, фонди 24 миллиондан ортиқни ташкил қилади.

3. Алишер Навоий номидаги Ўзбекистон Миллий кутубхонасига 1870-йилда асос солинган. Ўзбекистондаги энг йирик ва мажбурий нусхаларни сақловчи кутубхона саналади, фонди 7 миллиондан ортиқни ташкил қилади.

Мазкур Кутубхоналарнинг мақсади кенг оммага кўрсатиладиган хизматлар сонини ошириш натижасида фойдаланувчиларнинг ахборотга бўлган эҳтиёжини қондиришдан иборат.

№	Кўрсатиладиган хизмат турлари	Ташкилот номи		
		Тринити-коллеж кутубхонаси	Бостон оммавий кутубхонаси	Ўзбекистон Миллий кутубхонаси
1	Интернет, wi-fi	+	+	+
2	Принтер, сканер ва нусха олиш хизмати	+	+	+
3	Хужжатни уйга бериш хизмати	+	+	-
4	Йиғма электрон каталог хизматидан фойдаланиш	+	+	+
5	Жамоа бўлиб укув хона брон қилиш	+	-	-
6	Кутубхоналараро китоб етказиб бериш	+	+	-
7	Кўчма кутубхоналар ташкил қилиш	-	+	-
8	Махсус мутахассислар хизмати ()	+	+	-
9	Маълумот-ахборот хизмати	+	+	+
10	Ногиронлар учун махсус хизматлар	+	+	+
11	Библиография хизматлари	+	-	+
12	Экскурсия хизмати	-	+	+
13	Компьютерни ижарага бериш	-	+	+
14	Болалар хонаси	-	+	-
15	Турли хил қўшимча курслар	+	+	-
16	Хорижий тилларни ўргатиш курслари	+	+	+
17	Онлайн тўловларни амалга ошириш	+	-	-
18	Илмий-маълумот базаларига аъзолик	350 дан ортиқ	100 дан ортиқ	5 та
19	Электрон кутубхона яратиш	+	+	-

Йирик кутубхоналарда кўрсатиладиган хизматлар таҳлили

Ахборот-кутубхона хизматларини асосан икки турга бўлиш мумкин: анъанавий ва ноанъанавий хизматлар. Анъанавий хизматлар бу китоб бериш, каталоглаштириш, библиография, фондни сақлаш каби хизматлар саналса, ноанъанавий хизматлар сафига замонавий ахборот технологияларидан фойдаланган ҳолда хизмат кўрсатиш киради. Бугунги кунда ноанъанавий ахборот-кутубхона хизматларидан фойдаланувчилар сони ошиб бораётганлигини гувоҳи бўлишимиз мумкин.

Таҳлил натижаларига кўра фойдаланувчилар эътиборини онлайн тарзда амалга оширилаётган хизматлар жалб қилаётгани маълум бўлди. Асосан электрон кутубхона яратиш хизматларига, айнан кутубхоначилик ишидаги тўловларни онлайн амалга ошириш хизматига ва илмий-таълимий маълумотлар базаларидан узлуксиз фойдаланишни жорий этиш каби хизматларга бўлган талаб ортиб бормоқда.

Ўзбекистон жаҳон миқиёсига чиқиши, дунёдаги илм-фан соҳасидаги илғор янгиликлардан жуда тез хабардор бўлиши ва Ўзбекистон олимларини дунё таниши учун ҳам халқаро ташкилотлар билан маълумот алмашиши муҳим саналади. Шу мақсадда Ўзбекистон бир неча йирик илмий-таълимий маълумотлар базаларга аъзо бўлиб, улар жумласига Ebsco, Emerald, Springer, ProQuest, Thomson Reuterslар киради. Лекин жаҳондаги бошқа йирик кутубхоналарнинг илмий-таълимий маълумотлар базаларидан фойдаланиш суръати бизникига нисбатан 20 баравардан 100 бараваргача юқори эканлигини кўришимиз мумкин.

Ўзбекистон ривожланган мамлакатлар қаторига кириши учун илмий-таълимий маълумотлар базаларидан узлуксиз фойдаланишни йўлга қўйиши, илмий-таълимий маълумотлар базаларини шакллантириши, муаллифлар билан масофадан туриб ҳар қандай масалаларни ҳал қила олиш методикасини ва мавжуд илмий-таълимий ресурслар тарғиботини мунтазам амалга ошириш механизмларини ишлаб чиқиши ҳамда уларни тадбиқ этиши лозим.

ОСОБЕННОСТИ РЕКЛАМЫ В ДЕЯТЕЛЬНОСТИ ИНФОРМАЦИОННО - БИБЛИОТЕЧНЫХ УЧРЕЖДЕНИЙ

У.Моллаходжаев (магистр ТУИТ)

Реклама играет важную роль в жизни любой библиотеки, так как выступает инструментом оповещения реальных и потенциальных пользователей о предоставляемых ею услугах и продуктах, создает привлекательный образ библиотеки, увеличивает степень доступности ее ресурсов. Чтобы привлечь интерес к конкретным изданиям и помочь пользователям ориентироваться в фонде библиотеки, необходимо его рекламировать. Это касается и различных библиотечных мероприятий, и прочих услуг. Применение рекламных средств делает библиотечное обслуживание более эффективным, способствует повышению активности пользователей, помогая в удовлетворении их потребностей. Напомним, что библиотечная реклама широко применялась в процессе обслуживания читателей в постсоветском пространстве. В книге Л. Б. Хавкиной «Руководство для небольших и средних библиотек» есть подраздел «Реклама», где рассмотрены ее основные виды (печатные, рукописные оповещения, объявления, световая реклама в общественных местах, по радио, в кино). В настоящее время по этой теме опубликованы работы таких известных специалистов в этой области, как М.В. Гончаров, М. Я. Дворкина, С. Г. Матлина, Е.А. Песоцкий, Е.Р. Силеманова, Г.Л. Цесарская и др.

Одно из направлений профессиональной деятельности информационно-библиотечных учреждений — реклама собственного учреждения. Есть два пути создания рекламной продукции библиотек. Первый — библиотеки самостоятельно изготавливают рекламную продукцию (объявления, афиши, программы, листовки и др.). Второй — ее делают сторонние исполнители на основе заказа, сформулированного специалистами этих учреждений. Важным требованием к библиотекарям, участвующим в рекламной

деятельности является компетентность. Она подразумевает знание истории вопроса, ориентацию в достижениях коллег, умение оценить представленный исполнителем проект, наличие навыков составления текстов рекламных сообщений и графического исполнения.

Источниковедческой и практической основой подобных знаний служат публикации по вопросам рекламы и собственно рекламная продукция библиотек, которую — вплоть до настоящего времени — не собирают, не сохраняют и не делают достоянием всех желающих. Но чтобы заниматься рекламой, необходимо знание — истории, традиций, опыта коллег, лучших достижений и т. п. Все это должно найти свое воплощение в экспозициях «Библиотека в рекламе» создаваемых в этих учреждениях. По мнению некоторых специалистов в данное время, в информационном пространстве Узбекистана, Интернет или другие медиа средства не могут составить конкуренцию традиционным средствам получения информации.

Первоначальная задача рекламы - это донесение информации. А информировать общественность есть о чем. Ведь роль библиотеки не утилитарна, это не только предложение книг или периодических изданий. Эта традиционная роль библиотеки, к сожалению, но очень вероятно, будет вытеснена Интернетом. Потенциал современной библиотеки лежит в ее статусе - важного социального института, в тех социально необходимых программах, информационной базой которых она может стать. И это не в далеком будущем. Всем известно, какое значение уделяется библиотекам государством в программе идеологического воспитания молодежи. Известны и многочисленные проекты и гранты, выигранные библиотеками Узбекистана, в частности и Национальной библиотекой Узбекистана им. Алишера Навои. За последние 10 лет были осуществлены проекты «Библиотека и социальные проблемы читателей», «Дебатный центр» и т.п. К сожалению, плохо информированы об этих достижениях библиотек широкие слои населения. Знают об этом в основном читатели, которые регулярно пользуются услугами библиотеки ,это главным образом студенты и научные работники. Тут же всплывает и другая проблема - эго имидж. Не обо всех библиотеках читатели отзываются хорошо. Тому существует множество причин: плохое обслуживание, дискомфортный интерьер, но чаще всего незнание о возможностях предоставляемых существующей сферой услуг библиотеки. Однако в библиотеках развитых и процветающих стран перечисленные проблемы не стоят так остро - они пользуются заслуженным уважением в обществе. И это не без помощи хорошей рекламы.

Очевидно, что в стратегии развития любой библиотеки проблеме рекламы должно отводиться особое место.

Каковы же пути ее реализации?

В структуре многих библиотек Узбекистана появился отдел маркетинговых исследований или просто маркетинговый отдел, в деятельность которого входит такой аспект, как PublicRelations , т.е «связи с общественностью. Я думаю, что и рекламную деятельность никто не может осуществлять лучше.

Определенный опыт в этой области наработан сотрудниками Национальной библиотеки Узбекистана. Реклама была задействована в проекте «Библиотека и социальные проблемы читателей». Рабочей группой разрабатывались и реализовывались некоторые идеи рекламной деятельности. В частности, был подготовлен краткий курс-презентация, знакомящий с принципами проведения рекламной кампании в библиотеке, который хранится и доступен в Отделе научных и маркетинговых исследований. Курс был проведен для работников 6 районных библиотек города Ташкента, принявших участие в проекте. Результатом курса стала инициативность в подготовке рекламных материалов и определенные успехи в этой области. Образцы рекламных проспектов, листовок хранятся в Национальной библиотеке Узбекистана,

Рекламная деятельность в ее современном виде, наследующая многовековые традиции, - это массово-коммуникационная деятельность, создающая и распространяющая

лаконичные, экспрессивно-суггестивные, информативно-образные тексты, адресованные группам людей, с целью побудить их к нужному выбору, действию, поступку. На основе изучения и анализа литературы и библиотечной практики, опыт, накопленный библиотеками, еще незначителен.

Предлагаемые рекомендации:

1. Эффективность рекламной деятельности информационно- библиотечных учреждений зависит от того, есть ли в ее структуре специализированного подразделения, в круг задач которого входят формирование единой политики в этой области, т.е. разработка и методическое обеспечение наиболее общих вопросов стратегии и тактики рекламы. В настоящее время большинство этих учреждений хотели бы заниматься рекламой, но не знают, как это делать. Целесообразно было бы готовить специалистов по библиотечному дизайну, менеджеров библиотечных социально-культурных программ, библиотекарей-маркетологов и пр.

2. В целях совершенствования рекламной деятельности информационно-библиотечным учреждениям нужно активно искать контакты со спонсорами, предпринимателями; заключать договоры с предприятиями; налаживать постоянные и не требующие высокой оплаты отношения с прессой, радио, местным телевидением и городским транспортом.

3. Разумно и эффективно использовать внешнее пространство библиотеки (создание яркой, привлекающей внимание вывески– своеобразной визитной карточки библиотеки; раздача листовок с рекламной информацией в около библиотечной зоне; размещение информации на площади витрин и стен библиотеки; человек-плакат и пр.).

4. Необходимо повышать уровень внутри библиотечной рекламы. Для этого можно использовать логотип – эмблему или знак библиотеки обычно в виде рисунка с аббревиатурой. Они вызывают у пользователей позитивные ассоциации между деятельностью библиотеки и конкретной программой.

5. Привлечь внимание пользователей именно к библиотечной рекламной информации довольно сложно, что обязывает делать ее такой, чтобы она представляла для пользователя особую значимость, предлагала эффективные формы удовлетворения информационных потребностей.

6. Рекламная деятельность во многом сориентирована на фактических пользователей библиотеки и мало направлена на потенциальных пользователей, в частности, на молодежь, что снижает ее эффективность. Необходимо распространять информацию о библиотеке (режим работы, маршруты транспорта, предстоящие мероприятия и т.д.) через объявления на информационных стендах в учебных заведениях, на рекламных досках подъездов жилых домов, в местных газетах, на городском транспорте, в метро, на радио и т.д.

Приведенный опыт в этой статье охарактеризовал особенности рекламы в информационно-библиотечных учреждениях, как проблема реклама ставит своей целью формирование нового взгляда на рекламную деятельность, как на необходимую составляющую инновационных процессов происходящих в современных информационно-библиотечных учреждениях и предлагает свои взгляды по улучшение эффективности их деятельности.

5-Шўъба.

АХБОРОТ ХАВФСИЗЛИГИНИНГ ЗАМОНАВИЙ МУАММОЛАРИ ВА РИВОЖЛАНИШ ИСТИҚБОЛЛАРИ

К ВОПРОСУ ФУНКЦИОНИРОВАНИЯ МЕЖСЕТЕВОГО ЭКРАНА В СПЕЦИАЛЬНОЙ ФИЛЬТРАЦИИ ТРАФИКА

С.К. Ганиев (ТУИТ, д.т.н., профессор)
Ш.Р. Гуломов (ТУИТ, старший преподаватель)

Для оценки функционирования межсетевого экрана в специальной фильтрации трафика рассмотрим множество атак на компьютерную сеть $A = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9\}$:

A_1. Маскирование.

A_2. Dos/DDOS атака.

A_3. Атака с использованием троянских программ.

A_4. Атаки с использованием коммуникационных протоколов.

A_5. Флуд атак.

A_6. Несанкционированный доступ к файлам.

A_7. Спуфинг атак.

A_8. Фишинг атак.

A_9. Сканирование портов.

Предполагается, что P — вероятность появления любой из девяти атак из заданного множества A равновероятны.

$$P_A = \frac{1}{A} = \frac{1}{9} = 0{,}11$$

Применение режима фильтрации пакетов в специальной фильтрации трафика позволяет защитить компьютерную сеть от атаки маскированием и DOS/DDOS, то есть вероятность обнаружения атак в режиме фильтрации пакетов равна:

$$P_{\text{фильтрации пакетов}} = \frac{2}{9} = 0{,}22$$

Применение режима контроля сессии в специальной фильтрации трафика позволяет защитить компьютерную сеть от таких атак, как троянские программы, коммуникационные протоколы, Флуд и несанкционированный доступ к файлам. При этом вероятность обнаружения атак равна:

$$P_{\text{контроль сессии}} = \frac{4}{9} = 0{,}44$$

Применение режима трансляции сетевых адресов в специальной фильтрации трафика позволяет защитить компьютерную сеть от Спуфинг атак, Фишинг атак и сканирования портов. При этом вероятность обнаружения атак в режиме трансляции сетевых адресов равна:

$$P_{\text{Трансляция сетевых адресов}} = \frac{3}{9} = 0{,}33$$

Предполагается, что в компьютерную сеть поступают данные, каждое из которых состоит из последовательности пакетов. Все данные независимо друг от друга с вероятностью P_A могут представлять угрозу в виде атаки из заданного множества A. Поскольку входящие данные фильтруются элементами межсетевого экрана, то определяется вероятность того, что атака будет обнаружена. Пусть событие A — данные блокировано, а событие $\bar{A}$ — данные не блокировано. Событие $\bar{A}$ определяется как сумма

двух несовместных вариантов, то есть:

$$\bar{A} = \bar{A}_1 + \bar{A}_2,$$

где $\bar{A}_1 -$ данные не содержит атаку, $\bar{A}_2 -$ данные содержит атаку, но не обнаружены со стороны специальной фильтрации трафика.

$$P(\bar{A}_1) = 1 - P_A = 0{,}89$$

Чтобы определить $P(\bar{A}_2)$ надо умножить вероятность того, что данные содержат атаку на вероятность того, что эта атака не будет обнаружена со стороны специальной фильтрации трафика. Вероятность того, что атака не будет обнаружена, равна:

$$(1 - P_{\text{фильтрации пакетов}}) \times (1 - P_{\text{контроль сессии}}) \times (1 - P_{\text{трансляция сетевых адресов}})$$

При этом можно определить, что

$$P(\bar{A}_2) = P_A\left[(1 - P_{\text{фильтрации пакетов}}) \times (1 - P_{\text{контроль сессии}}) \times (1 - P_{\text{трансляция сетевых адресов}})\right] = 0{,}11[(1 - 0{,}22) \times (1 - 0{,}44) \times (1 - 0{,}33)] = 0{,}032$$

$$P(\bar{A}) = P(\bar{A}_1) + P(\bar{A}_2) = 0{,}89 + 0{,}03 = 0{,}92$$

Вероятность обнаружения атак в специальной фильтрации трафика:

$$P(A) = 1 - P(\bar{A}) = 1 - 0{,}92 = 0{,}08$$

Ниже на таблице приведен сравнительный анализ оценки функционирования межсетевого экрана в разных фильтрациях трафика.

Таблица

Оценки функционирования межсетевого экрана в разных фильтрациях трафика

Вероятность / Названия фильтрации трафика	Вероятности появления атак P_A	Вероятность того, что данные не содержит атаку $P(\bar{A}_1)$	Вероятность того, что данные содержит атаку $P(\bar{A}_2)$	Вероятности обнаружения атак $P(A)$
Межсетевой экран в специальной фильтрации трафика	0,11	0,89	0,032	0,08
Межсетевой экран с высоким уровнем безопасности (система обнаружения атак)	0,09	0,91	0,031	0,06
Межсетевой экран с динамической фильтрации пакетов	0,11	0,89	0,073	0,04

В заключении следует отметить, что сравнительный анализ функционирования межсетевого экрана в разных фильтрациях трафика показывает, что вероятность обнаружения сетевых атак в специальной фильтрации трафика выше, чем в других фильтрациях трафика.

ИЕРАРХИЯ ПРОЦЕССОВ ИЗМЕРЕНИЯ СЕТЕВОГО ТРАФИКА

М.М. Каримов (МВССО, заместитель министра)
Ш.Р. Гуломов (ТУИТ, старший преподаватель)

Идентифицировать сетевой процесс, проходящий через межсетевой экран (МЭ), возможно по доступным характеристикам трафика несвязанным с процессом его фильтрации. Другими словами, доступными для измерений будут характеристики тех

виртуальных соединений, не запрещенные правилами фильтрации трафика или механизмом контроля потоковых сессий МЭ. Временные характеристики не рассматриваются, поскольку для них характерны большие разбросы значений и сильная изменчивость. В качестве характеристик можно использовать статистические моменты: математическое ожидание и дисперсию:

$$M = \frac{1}{n}\sum_{i=1}^{n} X_i, D = \frac{1}{n}\sum_{i=1}^{n} X_i^2 - M^2 ,$$

где $n -$ количество интервалов измерения; $X_i -$ количество пакетов, зафиксированных в интервале измерения сетевого трафика.

Измерение сетевого трафика состоит из двух этапов: получение данных и их анализ.

На первом этапе осуществляется процедура непосредственного измерения характеристик трафика, к которым относятся данные о циркулирующих в сети пакетах, порождаемых различными протоколами. Сбор данных осуществляется в какой-либо точке сети при помощи средств, регистрирующих трафик пакетов, с информации о заголовках пакетов и временной метки их регистрации.

На втором этапе осуществляется процедура обработки собранной информации при помощи средств, позволяющих преобразовать данные в соответствии с используемыми моделями и предоставить характеристики трафика в виде числовых значений или исходных данных для построения графиков.

Средства, применяемые в ходе проведения измерений: утилита для захвата IP-пакетов на сетевом интерфейсе - создание дампа трафика, утилита анализа полученного дампа, утилита построения графиков.

В качестве объектов измерения могут быть физические сигналы в канале передачи, отдельные пакеты, виртуальные соединения, состоящие из последовательностей пакетов и агрегированный трафик. При проведении измерений необходимо учитывать следующие важные факторы:

- каждое измерение изменяет состояние пакета. При прохождении пакета через промежуточное сетевое устройство осуществляется уменьшение времени жизни (TTL) на единицу и пересчет контрольной суммы для каждого пакета;
- измерение пакетов «возмущает сеть». Происходит добавление задержек в процесс передачи пакетов, что в свою очередь приводит к проявлению новых свойств.
- измеряемые характеристики трафика можно получить на интервале времени, который связан с минимальным размером пакета и временем жизни виртуального TCP соединения.

На рисунке приведена схема иерархической связанности процессов измерении сетевого трафика.

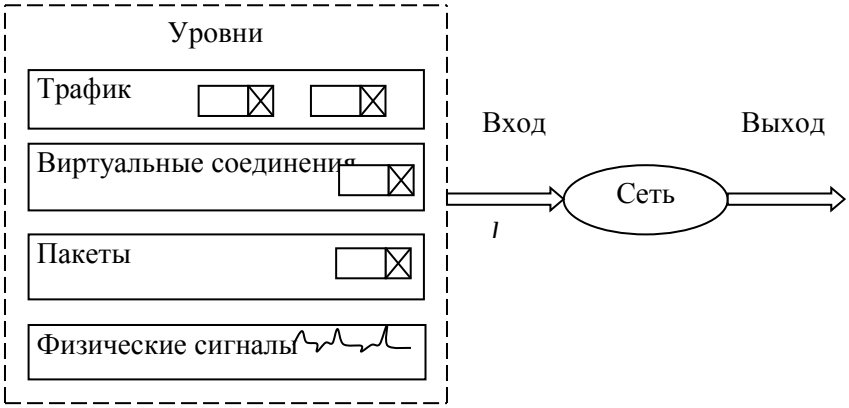


Рис. Иерархическая связанность процессов измерения сетевого трафика

Для оценки измерений сетевого трафика были использованы пропускная способность канала сети Ташкентского университета информационных технологий.

В результаты эксперимента были определены, что пропускная способность канала сети Ташкентского университета информационных технологий равна на 100 Мбит/с.

Оценки измерений сетевого трафика определяется формулой:

$$\Delta t = \frac{l_п}{\lambda},$$

Где $l_п$ — длина пакета; λ —пропускная способность канала.

В таблице приведены результаты оценки измерений сетевого трафика в разных пропускных способностях канала и длинах пакетов.

Таблица

Оценки измерений сетевого трафика в различных пропускных способностях

№	Длина пакета $l_п$ (минимальный)	Длина пакета $l_п$ (длинный)	Длина пакета $l_п$ (выше длинного)	Пропускная способность λ	Оценки измерений сетевого трафика для минимального пакета $\Delta t = \frac{l_п}{\lambda}$	Оценки измерений сетевого трафика для длинного пакета $\Delta t = \frac{l_п}{\lambda}$	Оценки измерений сетевого трафика для выше длинного пакета $\Delta t = \frac{l_п}{\lambda}$
1.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	10 Мбит/с	0,000048= 48×10^{-6} Мбит/с	0,0011= 11×10^{-4} Мбит/с	0,0045= 45×10^{-4} Мбит/с
2.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	50 Мбит/с	0,0000096= 96×10^{-7} Мбит/с	0,00022= 22×10^{-5} Мбит/с	0,0009= 9×10^{-4} Мбит/с
3.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	100 Мбит/с	0,0000048= 48×10^{-7} Мбит/с	0,00011= 11×10^{-5} Мбит/с	0,00045= 45×10^{-5} Мбит/с
4.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	1000 Мбит/с	0,00000048= 48×10^{-8} Мбит/с	0,000011= 11×10^{-6} Мбит/с	0,000045= 45×10^{-6} Мбит/с
5.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	5000 Мбит/с	0,000000096 =96×10^{-9} Мбит/с	0,0000022= 22×10^{-7} Мбит/с	0,000009= 9×10^{-6} Мбит/с
6.	64 байт= 0,00048 Мбит	1500 байт=0,011 Мбит	6000 байт=0,045 Мбит	10000 Мбит/с	0,000000048 =48×10^{-9} Мбит/с	0,0000011= 11×10^{-7} Мбит/с	0,0000045= 45×10^{-7} Мбит/с

В качестве заключения следует отметить, что измерение характеристик сетевого трафика дает возможность собирать информацию о заголовке пакета и предоставить пакет в виде числовых значений, что позволяет обнаружить пакеты и анализировать дампа трафика в любой точке сети.

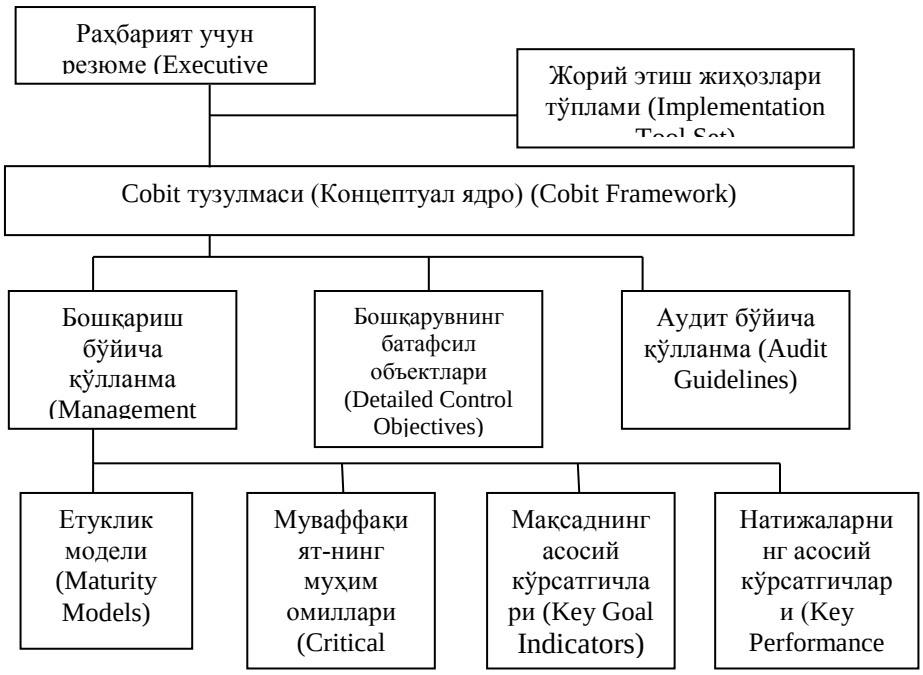
АХБОРОТ ТИЗИМЛАРИ АУДИТИНИНГ COBIT СТАНДАРТИ ХУСУСИДА

А.А. Ганиев (ТАТУ, кафедра мудири)

Ахборот технологиялари соҳасида иқтисодиёт субъектларининг бизнес талабларига мувофиқ сервисларни тақдим этиш ички назоратнинг тегишли тизим ва методологияси мавжудлигини назарда тутади. Cobitга асосланган назорат тизими бу талабларга жавоб беради, чунки:

- иқтисодиёт субъектлари бизнес талаблари билан боғланган;
- IT фаолият турларини тушунарли жараён модели кўринишида ташкил этади;
- таъсир этиш зарур бўлган IT ресурсларининг асосийларини аниқлаб беради;
- назорат мақсадини аниқлайди.

Cobit стандартини иқтисодиёт субъектлари бизнесига йўналтирилиши бизнес мақсадларини ахборот технологиялари билан боғлиқлигидан, эришилган муваффақиятларни баҳолаш кўрсаткичлар ва моделларни аниқлаб олишдан, бизнес ва IT-жараёнлар эгаларининг масъуллик даражасини аниқлашдан иборат.



Расм. Cobit стандарти китоблари таркиби

Бошқача айтганда, Cobit стандарти асосига шундай асосий фикрлар қўйилганки, бу ҳар қандай иқтисодиёт субъект (унинг бошқарув тизимини)ни маълум бизнес мақсадларига эришиши учун зарур бўлган ахборот билан таъминлаш учун, IT жараёнларни табиий гуруҳланган IT-ресурслар ёрдамида бошқариш керак бўлади. Ҳозирги Cobit стандартининг биринчи версияси 1996 йилда, иккинчи версияси 1998 йилда, кейинчалик учинчи версияси ишлаб чиқилган. Стандартнинг учинчи версиясига, асосига “IT бошқариш тизими” (IT Governmence) “Бошқариш бўйича қўлланма” киритилган.

Шундай қилиб, Cobitнинг учинчи таҳририга турли хил истеъмолчиларга йўналтирилган бир нечта китоблар кирган (расм).

“Рахбарият учун резюме” стандартнинг қолган бўлимларига кириш бўлиб,иқтисодиёт субъектининг бошқарув тизимини олий бўғинига Cobit стандартини улар субъектида фойдаланиш ҳақида қарор қабул қилишга мўлжалланган.У Cobit миссиясини ва “АТ бошқарув тизими” тушунчасини аниқлайди. “Концептуал ядро” ёки Cobit структураси стандарт структураси кенгайтирилган тавсифи, назоратни юқори даражадаги мақсадлари ва уларга тушунтиришларни ўз таркибига олади. Cobitни асосий

концепцияси ахборот тизимларида бошқариш механизмларини, хўжалик юритувчи субъект фаолияти мақсадларини мададлаш ва бу фаолият талабларини қондириш учун қандай ахборот зарурлигидан келиб чиқиб, шакллантиришни таклиф этади. Ахборот бу контекстда уни бошқариш IT-жараёнлар доирасида бажарилаётган АТ ресурсларидан фойдаланиш натижалари каби кўрилади.

Cobitнинг концептуал ядроси тўртта доменда (IT жараёнлари гуруҳлари) гуруҳланган:

- режалаш ва ташкил этилиши (planning and organization)- ечимларни жорий этиш йўналишларини аниқлайдиган ва сервисларни таъминлайдиган;
- сотиб олиш ва жорий этиш (acquisition and implementation)- ечимларни жорий этишни ва улар асосида сервислар кўрсатишни таъминлайди;
- эксплуатация ва кузатиб бориш (delivery and support)- ечимларнинг ўзи ва уларни энг сўнгги фойдаланувчилар учун қўллаш мумкинлиги;
- мониторинг (monitoring)- барча жараёнларни тўғри йўналишда илгари сураётганлигига ишонч ҳосил қилиш учун, улар устидан назорат.

Бу доменлар ўзида 34 та юқори даражали бошқариш объектни (ҳар бир IT жараён учун битта вазифа) бирлаштиради.

“Назоратнинг детал объектлари” китобида 34 IT-жараёнларнинг ҳар бири учун назорат объектлари (вазифа)нинг батафсил тавсифини очиб беради. Уларнинг ҳаммаси бўлиб 318 объект саналган. Алоҳида назорат объекти олдида турган ҳар бир вазифа IT-жараён доирасида аниқ бир бошқариш муолажаси эвазига эришиш зарур бўлган кутилаётган натижалар шаклини ўз таркибига олади.

“Бошқариш бўйича қўлланма” хўжалик юритувчи субъектлари раҳбарларига ахборот технологияларини бошқаришнинг энг самарали стратегиясини амалга оширишга, ахборот ресурсларидан ва мос жараёнлардан фойдаланиш устидан назорат ўрнатишга, мониторинг олиб боришга, хўжалик субъектининг ўрнатилган мақсадларига эришишни қиёсий баҳолашга ва ҳар бир IT-жараён доирасида самарадорликни баҳолашга имкон беради.

“Жорий этиш ускуналар тўплами” Cobit стандарти муҳим концептуал қоидаларини аниқлаштиришларни ҳамда ихтиёрий иқтисодиёт субъекти фаолиятига уларни жорий этиш жараёни алгоритмини ўз ичига олади.

Китоб ўз таркибига қуйидаги асосий компонентларни олади:

- обзор қисм (Executive Overview);
- амалий тажриба ва тақдимотлар (Case Studies, Power Point Presentations)билан бир қаторда жорий этиш бўйича қўлланма;
- хўжалик юритувчи субъект ITни бошқариш тузулмасини таҳлил этишга кўмаклашувчи воситаси: субъект раҳбарияти хабардорлигини Диагностикаси (Management Awareness Diagnostic) ва IT бошқарувини Диагностикаси (IT Control Diagnostic).
- тез-тез бериладиган саволлар ва уларга жавоблар (FAQs).

Cobit стандартини иқтисодиёт субъекти бизнесига жорий этиш жараёнининг асосий босқичлари қуйидагилар:

- фаолият мақсадини стандартнинг концептуал ядроси асосида аниқлаш;
- IT жараёнлар ва юқори даражали ва бошқарувнинг батафсил объектлари асосида бошқарув механизмларини танлаш;
- жорий этиш дастурини ишлаб чиқиш ва бизнес режа билан мувофиқлаштириш;
- “Аудит бўйича қўлланма” асосида мавжуд муолажалар ва бошқарув механизмларини жорий этиш натижаларини баҳолаш;
- хўжалик юритувчи субъектнинг жорий статусини, муваффақиятга олиб келувчи муҳим ҳаракатларни идентификациялашни баҳолаш ва “Бошқариш бўйича қўлланма” асосида иқтисодиёт субъектининг бизнес мақсад вазифаларига эришиш самарадорлигини ўлчаш.

Ва ниҳоят, “Аудит бўйича қўлланма”IT-жараёнларини аудитлашга йўналтирилган китоб ҳисобланади. Қўлланмада Cobit концептуал ядроси билан аниқланадиган 34 юқори даражали IT-жараёнлар ва 318 бошқарувнинг детал объектларидан ҳар бирини амалга оширилишини қандай аудитлаш баён этилган. Бу аудиторга хўжалик субъектида ахборот технологияларининг бошқарув тизимини Cobit стандарти ва бу субъект мақсад вазифалари талабларига адекват амалга оширилганлигини баҳолашга ҳамда уни яхшилаш бўйича тегишли бошқарувчи тавсияларни ишлаб беришга имкон беради.

АХБОРОТ ТИЗИМЛАРИ АУДИТИНИ ТАРТИБЛАШ МАСАЛАСИ ҲАҚИДА

А.А. Ганиев (ТАТУ, кафедра мудири)

Ҳозирги шароитда аудит ахборотни ҳар томонлама тадқиқ этишда ва баҳолашда, бошқарув қарорларини қабул қилишда, бутун бир бизнес тизимни, хусусан унинг ахборот тизимини ривожланиш истиқболини белгилашда деярли унинг ўрнини босиб бўлмайдиган ҳамда бу тизимларни бошқаришни мададлаш асбоби бўлиб, унинг долзарблиги кескин ошиб бормоқда. Бу хўжалик юритувчи субъектларни ахборот ва уларни ишловчи ахборот технологияларига боғлиқлигини ошиши билан кузатилади.

Вақт ўтиши билан ахборот тизимлари аудитини ўтказишга ёндошиш тартиблашди ва стандартлашди. Йирик аудиторлик компаниялар шу соҳадаги профессионалларнинг ассоциацияларини ташкил этдилар ва улар IT соҳасида аудиторлик фаолиятига оид стандартларни яратиш ва амалда бўлишини кузатиб борадилар. 1967 йил профессионалларнинг кичик гуруҳи ахборот тизимлари аудити ва назорати ассоциациясини таъсис этдилар (Information Systems Audit and Control Association, ISACA).

Бугун ISACA ахборот технологиялари ва ахборот хавфсизлигини бошқариш, назорати ва аудити ҳамда ахборот хавф-хатарларини бошқариш соҳасида дунёда етакчилик қилиб келмоқда. Ҳозирги вақтда ISACAда 160 дан ортиқ мамлакатлардан 86000 дан ортиқ аъзолари мавжуд. Унинг асосий мақсади- IT маъмурлари ва аудиторлари кундаликда фойдаланишлари учун ахборот технологияларини бошқариш бўйича ҳужжатларнинг стандартлашган тўпламини тадқиқ этиш, ишлаб чиқиш, чоп этиш ва илгари суришдир.

ISACA стандатрлар билан бир қаторда, ахборот тизимлари аудиторининг ахлоқий кодексини ишлаб чиқди ва унинг асосий принциплари:

- ахборот тизимларини қабул қилинган стандартлар ва қўлланмаларга мувофиқ келтиришда кўмаклашиш;
- ахборот тизимлари аудити соҳасида ўз фаолиятини ISACA қабул қилган стандартларга мувофиқ олиб бориш;
- иш берувчилар, ҳиссадорлар, мижозлар ва жамият манфаатларини кўзлаб, садоқат ва адолат билан ҳаракат қилиш;
- ноқонуний ёки адолатсиз фаолиятда атайин қатнашмаслик;
- ўз хизмат вазифаларини бажаришда олинган ахборотлар конфиденциаллигини сақлаш;
- конфиденциал ахборотдан шахсий манфаат йўлида фойдаланмаслик ва ахборот эгасининг рухсатисиз учинчи шахсларга бермаслик;
- хизмат вазифаларини бажаришда мустақил ва объектив бўлиб қолиш;
- аудиторнинг мустақиллигига таҳдид солувчи фаолиятдан қочиш;
- ахборот тизимлари аудитини ўтказиш билан боғлиқ бўлган маҳоратини юқори даражада бўлишини касбий тадбирларда қатнашиб мададлаш;
- ўтказилган аудит натижалари ҳақида барча манфаатдор томонларни хабардор қилиш.

Ҳозирги вақтда ассоциация тадқиқлаш ва тартибга солиш ишлари билан бир

қаторда, юқори малакали мутахассисларга бутун дунёда тан олинадиган халқаро сертификатлар беради:

- ахборот тизимларининг сертификатланган аудитори (Certified Information System Auditor, CISA);
- ахборот хавфсизлигини сертификатланган менеджери (Certified Information Security Manager, CISM);
- АТ корпоратив бошқариш соҳасида сертификатланган мутахассис (Certified in the Governance of Enterprise IT, CGEIT).

ISACA- ўтган давр ичида дунёда тан олинган “Назорат объектлари учун ахборотга алоқадор технологиялар” (Control Objectives for Information and Related Technology, Cobit) ва ITда инвестицияларни бошқариш (Va IIT), халқаро стандартларни ишлаб чиқди ва мунтазам янгилаб бормоқда. Бу стандартларнинг тузилиши ва мазмуни ҳар қандай иқтисодиёт субъектлари ва аудити бошқарув тизимларини барча сайтларда методологик таъминлашга имкон беради.

Ҳозирги вақтда Cobit стандарти ахборот технологиялари ва ахборот хавфсизлиги аудити, назорати ва бошқариш соҳасида қирқта халқаро стандартлар синтези ҳисобланади. Унинг асосий стратегик вазифаси иқтисодиёт субъектлари бошқарув тизимининг раҳбарлик бўғини билан бу субъектлар ва IT департаменти фаолияти йўналиши мақсадларини кўришларидаги фарқларини бартараф этишдан иборат.

Cobit стандарти аудитга қўйиладиган мажбурий талабларни аниқлаб беради ва тартибга солади ва унинг натижалари бўйича шаклланадиган ҳисоботлар шаклини белгилайди.

У қуйидагиларни тақдим этади:

- аудиторларга - касбий ахлоқий кодекснинг касбий талабларига мувофиқ ишларни минимал мақбул даражада бажарилишини;
- ахборот тизимларининг сертификатланган аудиторларига - уларнинг ишларига қўйиладиган мажбурий талабларни;
- менеджерлар ва бошқа манфаатдор шахсларга - IT соҳасида энг яхши амалиётчиларнинг касбий ишларига талаб этиладиган даражалари ҳақида ахборот тақдим этиш.

Стандарт домен (IT жараёнлар гуруҳи) ва алоҳида бизнес жараёнлар даражасида энг яхши амалий тажрибаларни очиб беради ҳамда ҳаракатларни бошқарила оладиган ва изчил тузулма шаклида тартибга солади. Бу тажриба бажаришдан кўра кўпроқ назоратга йўналтирилган. Стандартда очиб берилган меъёрлар ахборот технологияларига инвестицияларни энг яхши ҳолатга келтиришга, тақдим этилаётган сервислар даражасига бўлган ишончни таъминлашга ва вазиятни номаъқул ривожланган ҳолатида йўл кўрсатилиши мумкин бўлган кўрсаткичларни ишлаб бериши мумкин.

ПЕРСПЕКТИВЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

С.Ю. Юсупов (ТУИТ, доцент)

Сегодня одним из наиболее перспективных направлений является разработка и производство продукции на основе биотехнологий, например, интеллектуальные системы безопасности на основе биометрии. Биометрические технологии основаны на интеграции исследований в области электроники, информатики, медицины, собственно биометрии.

Биометрические системы идентификации, доступные в настоящее время или находящиеся в стадии разработки, включают в себя системы доступа по отпечатку пальца, ДНК, форме уха, геометрии лица, температуре кожи, отпечатку ладони, сетчатке, радужной оболочки глаза, подписи и голосу. В последние годы интерес к биометрии возрос в связи с созданием так называемых “биометрических систем безопасности”,

основанных на измерении уникальных биологических, физиологических и поведенческих характеристик, индивидуальных для каждого человека. Задачей системы является проверка схожести параметров неизвестного объекта с параметрами объектов, имеющимися в базе данных и, при достижении определенного критерия схожести, выдача заключения о совпадении объектов. В противном случае – отрицательное заключение. Анализ, основанный на проверке отпечатков пальцев, является самой старой методикой биометрического опознания. Метод прижился в криминалистике и до сих пор широко используется в наши дни. Причиной тому - генетически обусловленная уникальность радужной оболочки глаза, которая различается даже у близнецов. Одним из бурно развивающихся в настоящее время технологических направлений в биометрии является распознавание по геометрии лица. Действительно лицо является одним из наиболее доступных и естественных для идентификации объектов. К преимуществам таких систем можно отнести: дистанционное функционирование (не требуется физический контакт пользователя с системой), естественность предъявления лица для большинства людей, гигиеничность (например, по сравнению со снятием отпечатков пальцев), скрытность (при необходимости) и т.п. Так для системы, обеспечивающей безопасность аэропорта или банка, возможно, достаточно будет ввести в ее базу данных одну фотографию лица разыскиваемого человека или даже его фоторобот. При таких же условиях обеспечить безопасность на базе других биометрических систем невозможно в принципе. Наряду с технологией распознавания по радужной оболочке просмотр сетчатки глаза также является наиболее точной и надежной биометрической технологией. Несмотря на относительную сложность технологии просмотра сетчатки глаза (необходимо наличие специальной инфракрасной аппаратуры для подсветки глазного дна), этот метод давно известен. Принцип регистрации глазного дна не прост, что является одним из недостатков, ограничивающих применение этого метода. Исследования в области биометрических систем безопасности ведутся в настоящее время во многих странах, особенно активно в США, Израиле в силу объективных причин. Например, предлагается следующие технологии:

1. Уникальная технология Vibroimage (Аура), которая позволяет использовать обработку изображений биологических объектов, полученных с помощью обычных видеокамер, для анализа физиологического и нервно-психологического состояния человека.

2. Уникальная технология 3D-pulse (объемный пульс), которая представляет собой возможность с помощью дактилоскопического сенсора получать объемные изменения пульсовой волны для расчета физиологических и нервно-психологических характеристик человека.

На основе этих технологий разрабатываются системы национальной безопасности, которые имеют большое коммерческое применение, особенно с учетом современных тенденций. Установка таких систем может происходить повсеместно: на стратегически важных, секретных, охраняемых объектах для защиты от несанкционированного доступа и нападений, в аэропортах, таможне, пограничных пунктах, местах массового скопления народа для предотвращения возможных общественно опасных действий со стороны агрессивно настроенных субъектов, терактов и т.д. В связи с распространением международного терроризма озабоченность государств состоянием защиты общества будет неуклонно возрастать. Учитывая вышесказанное, можно сделать вывод о том, что наука и техника XXI в. будут работать над проблемой создания систем безопасности на национальном и международном уровнях. Сегодня в различных странах существует несколько тысяч компьютеризированных мест, хранилищ, исследовательских лабораторий, банков крови, банкоматов, военных сооружений, доступ к которым контролируется устройствами, которые сканируют уникальные характеристики человека. Наряду с функцией идентификации, такие системы имеют ряд других функций, например, учет и контроль рабочего времени, пересечение границ и т.д.

В соответствии с ростом числа приложений, где возможно применение биометрических технологий, растет и объем производства биометрических устройств. Биометрия активно развивается, системы контроля доступа – это, по сути, вчерашний день. Огромный потенциал в биометрии представляет развитие систем безопасности на ее основе, представляющих оптимальное решение данной проблемы.

ТАРМОҚДА МАЪЛУМОТЛАРНИ ҲИМОЯЛАШДА МИЛЛИЙ ТАРМОҚЛАРАРО ЭКРАН ДАСТУРИНИ ИШЛАБ ЧИҚИШ МУАММОЛАРИ

С.Ю. Юсупов (ТАТУ, доцент)
У.О. Мамажонов (ТАТУ, магистрант)

Тармоқ орқали бўладиган ҳужумларни бартараф этишда одатда тармоқлараро экран (Firewall) ларнинг аппарат ёки дастурий воситаларидан фойдаланилади. Тармоқлараро экранларнинг ишлаш принсипи OSI моделининг тармоқ сатхида пакетли маълумотларни кириш - чиқишини назорат қилишга асосланган бўлиб, TCP/IP протоколидан фойдаланади ва компютердаги портларни текшириб туради.

Тармоқлараро экран тармоқдан ўтувчи барча пакетларни кўради ва иккала (кириш, чиқиш) йўналиши бўйича пакетларни белгиланган қоидалар асосида текшириб, уларга рухсат бериш ёки бермасликни ҳал қилади. Ҳимоя воситасининг қуйида санаб ўтилган қулайликлари, айниқса, пакетларни филтрлаш функцияси DOS (Denial-of-service) ҳужумига қарши ҳимояланишнинг самарали воситасидир. Пакет филтрлари қуйидагиларни назорат қилади:

- физик интерфейс, пакет қаердан келади;
- манбанинг IP-манзили;
- қабул қилувчининг IP-манзили;
- манба ва қабул қилувчи транспорт портлари.

Тармоқлараро экран баъзи бир камчиликлари туфайли DOS ҳужумидан тўлақонли ҳимояни таъминлаб бера олмайди:

- амалга ошириш камчиликлари — ҳар бир тармоқлараро экран мураккаб дастурий (дастурий-аппарат) мажмуа кўринишида экан, у хатоликларга эга. Бундан ташқари, дастурий амалга ошириш сифатини аниқлаш имконини берадиган ва тармоқлараро экранда барча спецификацияланган хусусиятлар амалга оширилганлигига ишонч ҳосил қиладиган синов ўтказишнинг умумий методологияси мавжуд эмас;
- қўллашдаги (експлуатациядаги) камчиликлар — тармоқлараро экранларни бошқариш, уларни хавфсизлик сиёсати асосида конфигурациялаш жуда мураккаб ҳисобланади ва кўпгина вазиятларда тармоқлараро экранларни нотўғри конфигурациялаш ҳоллари учраб туради.

Портларни текшириш (Port Scanning) ҳужум тури одатда тармоқ хизматини кўрсатувчи компютерларга нисбатан кўп қўлланади. Тармоқ хавфсизлигини таъминлаш учун кўпроқ виртуал портларга эътибор қаратишимиз керак. Чунки портлар маълумотларни канал орқали ташувчи воситадир. Компютерда 65 536 та стандарт портлар мавжуд. Компютер портларини мажозий маънода уйнинг эшиги ёки деразасига ўхшатиш мумкин. Портларни текшириш ҳужуми эса ўғрилар уйга киришдан олдин эшик ва деразаларни очиқ ёки ёпиқлигини билишига ўхшайди. Бир вақтда барча портларни таҳлил қилиш мақсадида хабар юборилади, натижада реал вақт давомида фойдаланувчи компютернинг қайси портини ишлатаётгани аниқланади, бу эса компютернинг нозик нуқтаси ҳисоб-ланади. Айнан маълум бўлган порт рақами орқали фойдаланувчи қандай хизматни ишлатаётганини аниқ айтиш мумкин. Масалан, таҳлил натижасида қуйидаги порт рақамлари аниқланган бўлсин, айнан шу рақамлар орқали фойдаланилаётган хизмат номини аниқлаш мумкин:

- Port #21: FTP (File Transfer Protocol) файл алмашиш протоколи;

- Port #35: Хусусий принтер сервер;
- Port #80: HTTP traffic (Hypertext Transfer [Transport] Protocol) гиперматн алмашиш протоколи;
- Port #110: POP3 (Post Office Protocol 3) E-mail портоколи.

Портларни текшириш ҳужумига қарши самарали ҳимоя ечими тармоқлараро экран технологиясидан унумли фойдаланиш кутилган натижа беради. Барча портларни бир вақтда текшириш ҳақидаги келган сўровларга нисбатан тармоқлараро экранга махсус қоида жорий этиш йўли билан ҳужумни бартараф этиш мумкин.

Аммо, тармоқлараро экранлардан юртимиз фойдаланувчилар қатламининг жуда кам қисми фойдаланади. Бунинг сабаблари сифатида бир қанча омилларни келтириш мумкин.

Биринчидан, тармоқлараро экран тўғрисида фойдаланувчиларда тушунча етарли эмаслиги.

Иккинчидан, тармоқлараро экранларнинг миллий оммабоб кўриниши мавжуд эмаслиги.

Учинчидан, мавжуд тармоқлараро экнарларнинг дастурий таъминоти мураккаб, ва фойдаланишга тушунарли эмаслиги.

Тўртинчидан, тармоқлараро экранларнинг ўрнатиладиган созламалари кўплиги.

Бешинчидан, тармоқлараро экранлар нафақат кириш балки чиқишга ҳам чекловлар ўрнатиши ва яна шу каби бир қанча аспектлардир.

Шу каби муаммоларни ҳал этишга дастурий жихатдан ёндошиш талаб этилади. Ва, биз тармоқлараро экранларнинг миллий кўринишини ишлаб чиқишимиз керак деб хисоблаймиз.

Ҳулоса ўрнида, тармоқлараро экрандан фойдаланувчилар сонини кўпайтиришимиз учун ишлаб чиқилажак дастурий таъминот ўзбек тилида, содда интерфейсга эга бўлиши керак. Дастурий таъминотнинг ўрнатиладиган созламалари имкон қадар соддалаштирилиши, камайтирилиши ва тушунарли ҳолга келтирилиши керак.

Мазкур дастурий воситани ишлаб чиқишимизнинг яна бир зарурий жихати биз фойдаланаётган тармоқлараро экранлар чет мамлакатлар махсулотлари эканлиги ва уларга ишонч йўқлигидир. Ҳимоялаш тизимини ишлаб чиққан дастурчи уни бузиш йўлларини ҳам билади. Шундан келиб чиқиб, тармоқлараро экраннинг миллий оммабоп кўринишини ишлаб чиқишимиз зарур деб хисоблаймиз.

AXBOROT XAVFSIZLIGI INSIDENTLARIGA JAVOB QAYTARISHNI TASHKIL ETISH JARAYONI

Sh.R. Gulomov (TATU, katta o'qituvchi)

XXI-asrga kelib axborot texnologiyalarining turli sohalarga tadbiq etilishi natijasida ish olib borish va ishni tashkil etish jarayonlari o'zgardi. Axborot texnologiyalari olib kirgan o'zgarishlar natijasida funksional jarayonlarni avtomatlashtirishga erishildi.

Lekin axborot texnologiyalaridan foydalanish ilgari ma'lum bo'lmagan xavflarni keltirib chiqardi.Yuqori texnologiyalarning sohaga tadbiqi natijasida har qanday turdagi korxona faoliyatiga kiberjinoyatchilarning aralasha olish imkoniyati yuzaga keldi. Korxona ishiga bu tarzda aralashishning bir necha sabablari bor, odatda buzg'unchilar pullarni o'g'irlashga harakat qiladilar, lekin ba'zi hollarda esa ular korxona obrosiga putur yetkazish maqsadida yoki maxfiy ma'lumotni o'g'irlash uchun bu ishni amalga oshiradilar. Axborot xafsizligi insidentlari oldindan rejalashtirilgan yoki tasodifiy bo'lishi (masalan, xato yoki tabiiy ofat tufayli yuzaga kelgan) bo'lishi hamda texnik yoki fizik omillar ta'sirida ro'y berishi mumkin. Ularning natijasi ma'lumotni ruxsatsiz oshkor qilish, o'zgartirish, yo'q qilish yoki ma'lumotni ishlatib bo'lamydigan holatga keltirish, tashkilot aktivlariga ziyon yetkazish yoki ularni talon-taroj qilish bo'lishi mumkin.

Axborot xavsizligini texnik insidentlari (bo'lishi mumkin bo'lmagan tarmoq faolligi, xizmatning ishdan chiqishiga mo'ljallangan hujumlar, ruxsat etilmagan ma'lumotni qo'lga kiritishga urinish, zararli kodni yuklash va hakozo) avtomatik aniqlanishi mumkin, masalan, nazorat yozuvlari tahlili qurilmalari, tarmoqlararo ekranlar, hujumlarni aniqlash tizimalri, zararli kodlarni aniqlashning instrumental vositalri (antiviruslar) tomonidan yuboriiladigan ogohlantirish signallari bo'lishi mumkin.Bugungi kunda axborot xavfsizligi intsidentlariga javob qaytarish (AXIJQ) dolbzarb muammolardan hisoblanadi. Birinchidan, bu mavzu juda ommabop, boshqa tomondan, u mavhumlik muammosi bilan bog'liq, chunki aynan tekshiruv vaqtida tizimning aniq zaif tomonlari, tahdidlarning izlari aniqlanib, axborot xavfsizligi (AX) xodimlarining malakasi, AX tizimining tuzilish sifati tekshiriladi.

Shuni ta'kidlab o'tish joizki, kompaniya axborot xavfsizligiga bo'lgan hujumlar yashiriladi, sababi hech kim o'z xatolarini tan olishni hohlamaydi va shu bilan raqobatchilarga qo'shimcha asoslar berishni hohlamaydilar. Buning natijasida hujumlarning soni uzluksiz ravishda o'sib boradi, ular to'g'risidagi ma'lumot esa qoida bo'yicha sir saqlanadi va biz OAV da e'lon qilingan kam miqdordagi hujumlar to'grisidagi ma'lumotlargagina ega bo'la olamiz. Boshqa tomondan bunday "aniqlik" kompyuter hujumlarini tavtish etuvchi mutaxassislarni qidirishdagi yoki kompaniyaning hujumlarga javob qaytarish jarayonini tashkil etishdagi qiyinchiliklarni anglatadi. Umuman olganda, aniq sabablarga ko'ra ijrochi o'z mijozlarining bajarilgan ish to'g'risidagi murojatlarga javob qaytara olmaydi.

Shuningdek, bu turdagi ishlarni bajarish ijrochi va buyurtmachi o'rtasidagi ishonchni talab etadi. Bu turdagi mutahassisdan nimalar talab etilishini sanab o'tishga harakat qilamiz:

- xavfsizlik prinsiplarini anglash;
- axborot ob'yektlarining nuqsonlari va zaifliklarini bilish;
- internet qurilmalari haqida tushuncha;
- tarmoq protokollarini bilish;
- tarmoq xavfsizligi muammolarini bilish;
- zararkunanda dasturlar (virus, troyanlar) to'g'risida tushuncha;
- dasturlash malakasiga ega bo'lish.

Axborot xavfsizligi hujumlariga javob qaytarish guruhi.

Axborot xavfsizligi intsidentlariga javob qaytarish guruhi (ing. Information Security Incident Response Team (AXIJQG)) bu tashkilotning ishonchli va malakali a'zolari guruhi bo'lib, axborot tizimlariga tegishli belgilangan javobgarlik doirasida axborot xavfsizligining buzilishiga javob qaytarishni bajaradi, koordinatsiyalaydi va jarayonni ushlab turadi. AXIJQG ni yaratishdan maqsad axborotni yuborish jarayoni va qayta aloqa, boshqarish, kerakli koordinatsiya kabilardan dars olish, bundan tashqari AX insidentlariga javob qaytarish, baholash uchun tashkilotni mos personal bilan ta'minlashdan iborat. AXIJQG a'zolari AX hujumlariga bog'liq bo'lgan jismoniy va moliyaviy zararni shuningdek, korxonaning nomini tiklashdagi zararni kamaytirishda qatnashishlari mumkin. AXIJQG tarkibi miqdor, yo'nalish, tashkiliy-huquqiy tuzilma va boshqa kompaniya boshqaruvining xarakteristikalariga bog'liq. Shuningdek, AXIJQG ning minimal tarkibi: AXIJQG bosharuvchisi, registrator-baholovchi, hujumlar registratsiyasi ma'limotlar bazasi administratori, kompyuter sud ekspertizasi mutahhassisi, yurist, tizim masalalari bo'yicha mutaxassis, tarmoq masalalari bo'yicha mutaxassis va axborot xavfsizligi bo'yicha mutaxassis-ekspert.

AXIJQG ajratilgan guruh bo'lib, personalining asosiy vazifasi hujumlarni tavtish qilish hisoblanmaydi, regitrator-baholovchi va hujumlar registratsiyasi ma'lumotlar bazasi administratori bundan mustasno.

Axborot xavfsizligiga hujumning turiga qarab AXIJQG a'zoligiga shartnoma asosida aniq ixtisoslashgan masalalar bo'yicha mutaxassislar olinishi mumkin. Guruh azolari ichki lavozim vazifalaridan kelib chiqqan holda AXIJQG ichida bir qancha funksiyalarni bajarishi mumkin.

AXIJQG tarkibi.Ushbu personalning miqdor va tarkibi tashkilot faoliyati maqsadi va masshtabiga mos tushishi lozim.

AXIJQG alohida tuzilgan guruh yoki korxonaning turli bo‘limlaridan (masalan, axborot texnologiyalari, buxgalteriya, kadrlar bo‘limi va marketing) jalb etilgan xodimlar jamoasi bo‘lishi mumkin.

AXIJQG boshqaruv a’zolarini xabardor qilish uchun boshqa biznes jarayonlaridan alohida bo‘lgan tizimga ega bo‘lishi kerak.

AXIJQG majburiyatlari.

AXIJQG majburiyatlarini 2 ta asosiy guruhga ajratish mumkin:

- ***Joriy vaqtdagi harakatlar***, asosiy masala bilan bog‘liq – tahdidlarga javob qaytarish;
- ***Profilaktik harakatlat,*** joriy vaqt masshtabida yuzaga kelmaydigan va yordamlashuvchi vazifani bajaradigan harakatlar.

Birinchi guruhga kiruvchi hisobotlarni (hujumlar klassifikatsiyasi) baholash va boshqa tashkilotlar (javob qaytarish kordinatsiyasi), guruhlar va internet xizmatlari ta’minotchilari bilan birgalikda qabul qilingan ma’lumotlar ustida ish olib borish, shuningdek, hujumdan so‘ng tizim xizmatini qayta tiklashda (muammolarni hal qilish) lokal foydalanuvchilarga yordam berishni o‘z ichiga oladi.

Hujumlar klassifikatsiyasi quyidagilarni o‘z ichiga oladi:

- ***hisobotlarni baholash:*** kiruvchi ma’lumot muhimlilik darajasiga qarab tartiblanadi, bunda davom etayotgan hodisalar va aniqlangan tendensiyalarga bog‘liq bo‘ladi.
- ***tekshiruv:*** hujum va uning masshtabi aniqlanadi.

Javob qaytarish kordinatsiyasi o‘z ichiga quyidagilarni oladi:

- ***axborotni kategoriyalash:*** hujumga taalluqli bo‘lgan ma’lumot (ro‘yxatga olish jurnallari, bog‘lanish ma’lumotlari va hk) axborotlarni oshkor qilish siyosatiga asoslangan holda kategoriyalanadi.
- ***kordinatsiya:*** axborotlarni oshkor qilish siyosatiga ko‘ra boshqalar hujum haqida xabardor etiladilar.

Muammolarni bartaraf etishning vazifalari quyidagilar:

- ***texnik ta’minot;***
- ***muammolarni hal etish:*** hujum va uning paydo bo‘lish sabablarini yo‘qotish;
- ***qayta tiklash:*** tizimni normal holatga qaytarishda yordam ko‘rsatish.

Shunday qilib hujum uyushtirilgan, intsident yuzaga kelgan axborot tizimida, intsidentlariga javob qaytarishni tashkil etish korxonaning asosiy axborot xavfsizlik muammolaridan biri hisoblanadi.

Shuning uchun tashkilotda foydalanilayotgan texnik qurilmalar ishi (dasturiy yoki dasturiy – apparat vositalar) axborot xavfsizligi insidentlariga javob qaytarishda zarur va ammo faqat tarmoqqa, tizimga, yoki servislarga mo`ljallangan bo`lishi talab qilinmaydi. Axborot xavfsizligi insidentlariga javob qaytarish texnik qurilmalari butunlay avtonom bolishi ham mumkin. Axborot xavfsizligi insidentlariga tezkor javob qaytarishning asosiy maqsadi insidentning oldini olish yoki ehtimoliy zararni tezlik bilan minimallashtirishdan iboratdir.

ЗАРАРКУНАНДА ДАСТУРЛАРНИНГ СОДДА ДИНАМИК ТАҲЛИЛИ

Б.К. Юсупов (ТАТУ, ассистент)

Ҳозирги кунда компьютер фойдаланувчилари олдида катта муаммо зараркунанда дастурлардан (вируслар) ҳимояланиш муаммоси туради. Айниқса бу муаммо катта корхоналарга зарар келтирмоқда. Чунки компьютер вируслари натижасида маълумотлар ўчирилади ёки рўхсатсиз нусхаланади. Маълумотларни, ҳамда компьютерларни ҳимоялаш учун махсус мутаҳассислар зараркунанда дастурларга (ЗД) қарши ҳимоя тизимларини яратишга жалб қилинган. Аммо шундай бўлсада, бу тизимлар тўлиқ кафолат бера олмайди, сабаби ЗД янги номаълум турларини ҳисобга олиб бўлмайди. Шунинг учун ЗД дастурларни аниқловчи ва даволовчи антивирус дастурларни ўзини ва базасини янгилаб туриш мақсадга мувофиқ.

ЗД таҳлилини амалга оширишда содда таҳлил ҳар доим ҳам мувофаққиятли бўлмайди. Зараркунанда дастурий воситаларнининг содда динамик таҳлили одатда содда статик таҳлил иш бермаган ҳолда фойдаланилиб, таҳлил зараркунанда дастурий восита бевосита юклангандан сўнг амалга оширилади. Бу усул орқали ЗД ларнинг вазифалари тўлиқ аниқланади. Шу сабабли мақолада содда динамик таҳлиллаш технологиялари билан танишиб чиқамиз.

Sandboxes. Ушбу дастурий воситалар содда динамик таҳлиллашда кенг фойдаланилиб, у хост операцион тизим (ОТ) билан ҳимояланган соҳани ҳосил қилади ва ЗД ушбу соҳада юклайди. Бу турдаги воситаларга Norman SandBox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, ва Comodo Instant Malware Analysis **(**open source**)** ларни олиш мумкин. Амалда Norman SandBox ва GFI Sandboxлардан кенг фойдаланилади. Умумий ҳолда барча sandboxes дастурий воситалари бир хил ишлаш алгоритмига эга. Яъни, ЗД ҳимояланган соҳада юкланади ва ОТ белгиланган соҳаларидаги ўзгаришларга асосан таҳлил натижалари шакллантирилади. Қуйида GFI Sandboxда олинган PDF туридаги таҳлил натижаси келтирилган.

Расмда кўрсатилганидек, GFI Sandboxнинг таҳлилари олтита бўлимга кўра олинган:

- ***Analysis Summary бўлими.*** Бу бўлида ЗД статик таҳлил натижаси ва динамик таҳлил натижаларининг юқори даражали маълумотлари келтирилади;
- ***File Activity бўлими.*** Бу бўлимда ЗД томонидан ўчирилган, очилган, яратилган ва фойдаланилган барча файллар рўйхати келтирилади;
- ***Created Mutexes бўлими.*** Бу бўлимда ЗД томонидан яратилган ресурслар рўйхати келтирилади;

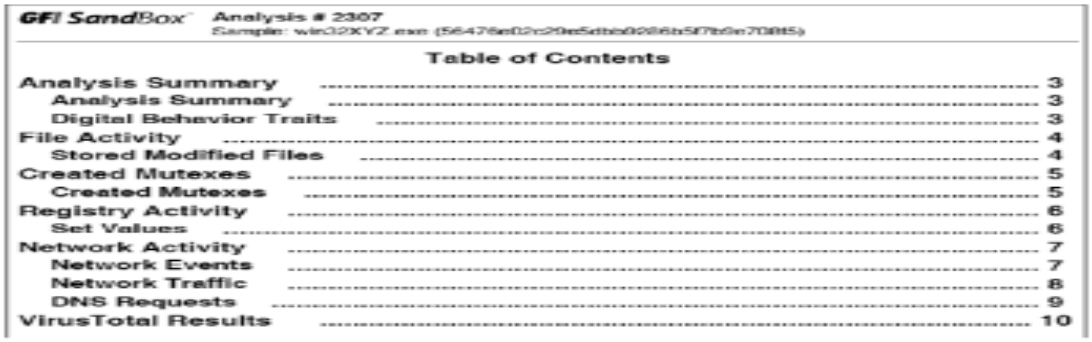

GFI SandBox Analysis # 2307

Table of Contents

Analysis Summary 3
Analysis Summary 3
Digital Behavior Traits 3
File Activity 4
Stored Modified Files 4
Created Mutexes 5
Created Mutexes 5
Registry Activity 6
Set Values 6
Network Activity 7
Network Events 7
Network Traffic 8
DNS Requests 9
VirusTotal Results 10

1-расм. GFI Sandboxнинг win32XYZ.exe ЗД учун содда таҳлил натижаси

- ***Registry Activity бўлими.*** Бу бўлимда регистрда мавжуд бўлган ўзгаришлар келтирилади;
- ***Network Activity бўлими.*** Бу бўлимда ЗД томонидан тармоқдан фойдаланиш даражаси ва ҳолати келтирилади;
- ***VirusTotal Results бўлими.*** Бу бўлимда ЗД VirusTotal орқали сканерлаш натижаси келтирилади.

Sandbox камчиликлари. Кўплаб Sandbox дастурий воситалари бин нечта катта камчиликларга эга. Масалан, Sandboxларда ЗД фақат юклаш орқали таҳлилланади (буйруқлар сатрида буни амалга ошириш имокнияти мавжуд эмас). Агар ЗД буйруқлар сатридан юкланишни сўраса бу ҳолда Sandbox дастурлар бу ЗД юклай олмайди.

Бундан ташқари қуйидаги камчиликлар кузатилади:

- ЗД тез-тез вертуал машина юкланганини аниқлайди ва бу ҳолда ЗД юкланишдан ўзини тўхтатиши ёки ўзини бошқача тутиши мумкин. Бу барча Sandboxлар учун мос эмас;
- Баъзи ЗД юкланишда ОТ махсус файл ва регистр маълумотларини талаб этади. Бу маълумотлар ўз навбатида Sandboxда мавжуд бўлмайди.
- Агар ЗДлар *dll* файл кенгайтмасида бўлса, улар юкланувчи ЗДлар (.exe кенгайтмали) дек тўлиқ Sandboxга юкланмайди.

- Sandbox муҳити ЗД учун мос бўлмаслиги мумкин. Масалан, Windows XP га мос бўлган ЗД, Windows 7 учун мос бўлмаслиги мумкин.
- Sandboxлар ЗД ларни вазифасини аниқласада, аслида нима қилаётганинини айтмайди.

ЗД юклаш (running malware). Содда динамик таҳлиллаш технологиялари ЗД юкланмаган ҳолда уларни таҳлиллай олишмайди. ЗДларнинг аксарияти *.exe* ва *.dll* файл кенгайтмаларида бўлишларини ҳисобга олиб, қуйида бу икки турдаги файлларни юклаш усулларини қараб чиқилади. *.exe* кенгайтмали файл юкланишга осон бўлиб, одатда сичқонча тугмачасини икки марта босиш орқали ёки буйруқлар сатридан фойдаланган ҳолда юкланади.

.dll кенгайтмали файллар нисбатан хийлакор бўлиб, windows ОТ буни қандақй қилиб автоматик юклашни билмайди.

Барча турдаги замонавий Windows ОТлари *rundll32.exe* файлига эга бўлиб, бу файл ўзида *DLL* ларни юклаш имкониятини сақлайди. Ушбу файл орқали ЗД юклаш тартиби қуйидагича:

C:\>rundll32.exe DLLname, Export arguments

Бу ерда *Export* қиймати олинган *DLL* файл ичидан експорт қилиниши керак бўлган функция номи. Статик таҳлиллаш усулида фойдаланилган дастурий воситалар PEview ёки PE Explorer орқали *DLL* файл ичидаги функция номи аниқланади. Масалан, *rip.dll* деб номланувчи файл ўзида *Install* ва *Uninstall* деб номланувчи функцияларни олади. Бу ҳолда юқоридаги тартиб қуйидагича бўлиши мумкин:

C:\>rundll32.exe rip.dll, Install

Баъзи ҳолларда DLL шаклидаги ЗДлар хизмат каби ўрнатилишни талаб этади.

C:\>rundll32 ipr32x.dll,InstallService ServiceName

C:\>net start ServiceName

Бу ердаги *ServiceName* DLL файл таркибидан олинади. net start буйруғи эса хизматни Windows ОТ амалга ошириш учун керак бўлади.

Process Explorer ёрдамида жараёнларни кузатиш. Ушбу дастурий восита Windows томонидан ишлаб чиқилган бўлиб, динамик таҳлиллашда кенг қўлланилади.

Бу дастурий восита орқали актив жараёнлар рўйхатини, жараёнлар орқали юкланган DLL файллар рўйхатини, жараёнларнинг хусусиятларини ва тизим ҳақида умумий маълумотларни олиш мумкин. Бундан ташқари жараёнларни тугатиш, юклаш каби амалларни бажариш мумкин.

Дастур ойнасида жараёнлар шажара шаклида берилади. Ойнада 7 устун бўлиб, Process устида жараён номи, PID устида жараён идентификация номери, CPU устида фойдаланиш кўрсаткичи, Description, Company name, Working set, Private bytes устунларидан иборат.

Шундай қилиб, одатий ҳолда дастур ойнасида хизматлар пушти рангда, жараёнлар кўк рангда, янги жараёнлар яшил рангда, тугатилган жараёнлар қизил рангда тасвирланади. Яшил ва қизил ранглар вақтинчалик саналади. ЗД таҳлиллашда бу дастур орқали янги жараённи ҳосил бўлишини ранглар ўзгариши орқали билиш мумкин. Юқорида келтириб ўтилган дастурлардан самарали фойдаланишни ўрганиш ЗД бажарадиган зарарли жараёнларни тўлиқ тушиниш ва ўлардан ҳимояланиш учун махсус алгоритмларни ишлаб чиқиш имкониятини беради.

БИОМЕТРИК КРИПТОТИЗИМЛАРНИНГ ХАВФСИЗЛИГИ ТАҲЛИЛИ

С.К. Ганиев (ТАТУ, т.ф.д., профессор)
З.Т. Худойқулов (ТАТУ, ассистент)

Ахборотнинг криптографик ҳимояси ҳозирги кунда долзарб усуллардан ҳисобланади ва ахборотнинг конфиденциаллигини, яхлитлигини, аутентификациясини

таъминлашда ва рад этишдан ҳимоялашда фойдаланилади. Криптографик ҳимоя усуллари ўзининг бардошлиги ва ишончлиги билан бошқа ҳимоя усулларидан ажралиб туради.

Криптография соҳаси симметрик шифрлаш тизимлари, очиқ калитли шифрлаш тизимлари, электрон рақамли имзо тизимлари ва криптографик калитларни бошқариш тизимларидан ташкил топган.

Симметрик ва очиқ калитли шифрлаш алгоритмлари маълумотни конфиденциаллигини таъминлашда, электрон рақамли имзо тизимлари ахборот яхлитлигини, аутентификациясини таъминлашда ва рад этишдан ҳимоялашда қўлланилади.

Криптографик калитларни бошқариш тизимлари қолган барча тизимлар учун асос ҳисобланиб, уларнинг бардошлиги ва ишончлигини таъминлашда муҳим рол ўйнайди. *Кирхгоф принципига* биноан криптографик тизимнинг бардошлиги фақат калит ноъмалум бўлган ҳолда аниқланади.

Криптографик калитларни бошқариш тизимида криптографик калитларни генерациялаш жараёни муҳим ҳисобланади. Криптографик алгоритмларда фойдаланилган калитлар сифатида одатда, пароллардан ва токенларда сақланган калитлардан фойдаланилади.

Паролларни калит сифатида фойдаланишда унинг тасодифийлик даражаси қаршилик қилади. Бундан ташқари паролларни инсон хотирасида сақланиши қийин. Токенларни унитилиши ва йўқотилиши жиддий муаммоларга сабаб бўлади.

Ҳозирда юқорида келтирилган муаммоларни олдини олишда турли ёндашувлардан фойдаланилмоқда. Биометрик хусусиятларнинг инсондан ажралмаслиги ва унда унитилаш хавфи мавжуд эмаслиги улардан криптографик калит сифатида фойдаланишга имкон беради. Биометрик параметрларни криптография соҳасида қўлланилиши янги, *биометрик криптография* соҳасини яратилишига асос бўлди. Ҳозирда бу соҳада қуйидаги ёндашувлар кенг фойдаланилмоқда:

- криптографик калитни озод этиш (*key release*);
- криптографик калитни яшириш (*key binding*);
- криптографик калитни генерациялаш (*key generation*).

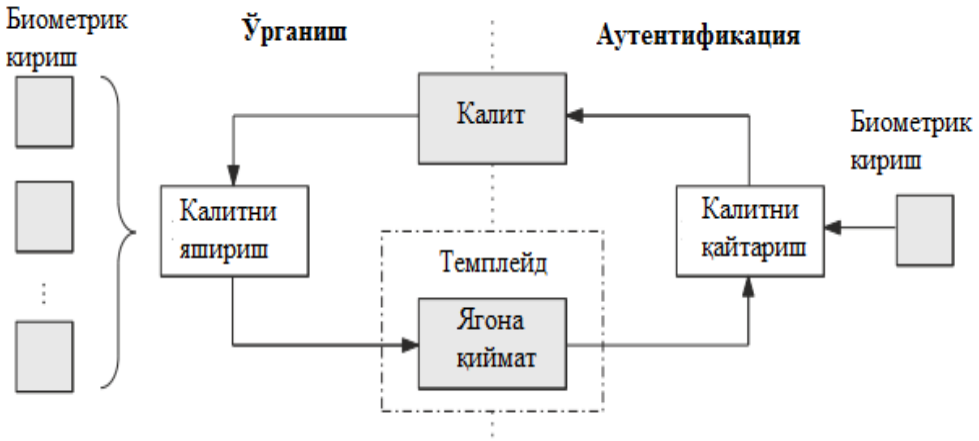
Криптографик калитни озод этиш. Бу ёндашув оддий биометрик аутентификация усулига асосланади. Бирор биометрик аутентификациялаш усулидан муваффаққиятли ўтган фойдаланувчи калитлар сақланадиган маълумотлар базасидан ўз калитини бошқариш ҳуқуқини қўлга киритади. Бошқача айтганда калит ва биометрик параметр бир - бирига алоқадор эмас. Бунда фойдаланилган аутентификациялаш усулида ёлғондан тасдиқлаш кўрсаткичини (*False acceptance rate*) нолга яқинлаштириш тавсия этилади. Бу усулнинг асосий камчилиги - биометрик параметр ва калитнинг бир - бирига боғланмаганлиги ва биометрик параметрнинг хавфсизлиги таъминланмаганлиги.

Криптографик калитни яшириш. Бу ёндашувга асосан криптографик калит ва биометрик параметр асосида ягона катталик (*helper data*) ҳосил қилинади. Бу катталикга мос фойдаланувчи биометрик параметрини аралаштирмасдан калитни ажратиш жуда қийин (назарий томондан иложи йўқ деб ҳисобланади).

Бу жараёнда мавжуд хатоликларни тузатиш учун *хатоликларни тузатиш кодлари*дан кенг фойдаланилади. Бу усулга асосан тасодифий сонлар генератори орқали ҳосил қилинган калитнинг бирор хатоликни тузатиш кодидаги фойдали қолдиғи ҳисобланади. Калит ва унинг фойдали қолдиғи биометрик параметр билан XOR амалида қўшилади ва натижа ягона катталик сифатида калитнинг хэш қиймати билан базада сақланади. Мос фойдаланувчи биометрик параметри киритилганда, уни ягона қиймат билан XOR амалида қўшилганда маълум хатолик билан калит қайта ҳосил бўлади. Мавжуд хатолик даражаси тузатилса ва ундан олинган хэш қиймат базадаги хэш қиймат билан тенг бўлса, калит тўғри деб топилади (1- расм).

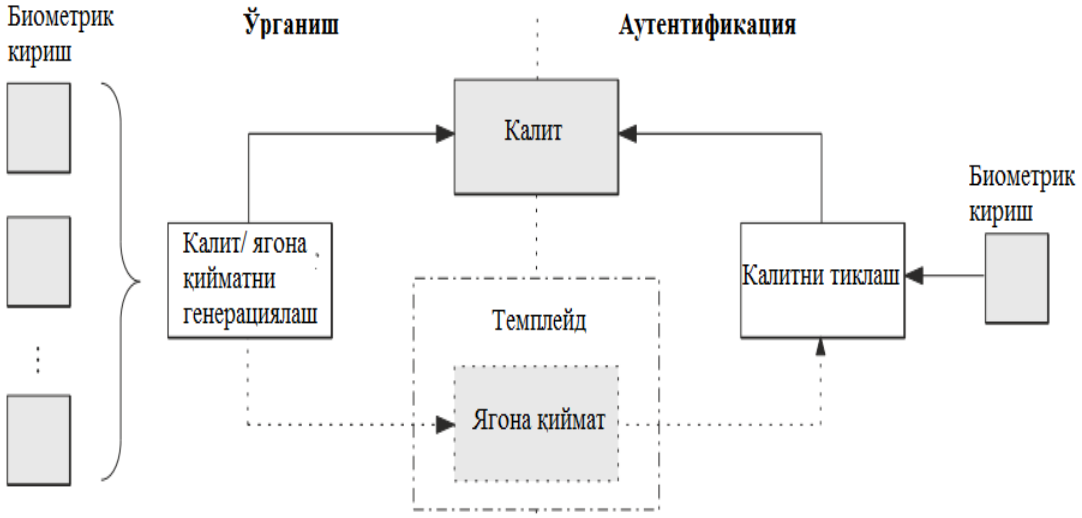
Бу усулда кенг фойдаланилаётган схемалар: *fuzzy commitment* ва *fuzzy vault* лар бўлиб, улар хавфсизлик нуқтаи назаридан ягона қийматни махфий сақлашни, мос

хатоликларни тузатиш кодларини танлашни талаб этади. Бу усулнинг афзаллиги фойдаланилган калитнинг тасодифийлигини ва уни янгилашни амалга ошириш имконияти.



1 - расм. Калитни яшириш

Криптографик калитни генерациялаш. Бу ёндашувга кўра ягона қиймат (*helper data*) фақат биометрик параметрдан ҳосил қилинади. Криптографик калит бевосита ягона қиймат ва киритилган биометрик намунадан ҳосил қилинади (2 - расм). Бу турдаги ёндашувда *fuzzy extractor* ёки *secure sketches* схемалари кенг ишлатилади.



2 - расм. Криптографик калитни генерациялаш

Бунда ҳеч бир керакли ахборот базада сақланмайди. Бу усулнинг асосий камчиларларидан бири - биометрик параметрга калит учун етарли муҳим ахборотнинг мавжуд эмаслиги. Яъни, бармоқ изи ёки юз тасвири учун шахслар ўртасида фарқ қилувчи хусусиятларнинг ўлчами етарлича узунликда эмас (масалан, 128 битли калитни ҳосил қилиш мураккаб).

Юқоридаги барча ёндашувларнинг қиёсий таҳлили 1 - жадвалда келтиралган.

1 - жадвал

Биометрик криптотизимларнинг қиёсий таҳлили

Биометрик криптотизим тури	Афзаллиги	Камчилиги
Криптографик калитни озод этиш	Калитни алмаштириш, фойдаланиш қулай	Биометрик ва калит бир - биридан мустасно, аутентификациядаги муаммолар

Криптографик калитни яшириш	Калитни янгилаш, калит бардошлиги	Муайян хатони тузатиш коди зарур ва ягона қиймат махфий сақланиши шарт
Криптографик калитни ҳосил қилиш	Калит биометрикдан бевосита ҳосил қилинади	Калит энтропияси кам, калитни янгилаш мураккаб

Хулоса сифатида айтиш мумкинки, калитларни алмаштириш зарурияти мавжуд бўлган ва бардошли криптографик калит талаб этилган соҳаларда криптографик калитларни яшириш усуллари самарали ҳисобланади ва уларда юқори энтропияга эга биометриклардан фойдаланиш мақсадга мувофиқ бўлади.

АХБОРОТНИ ҲИМОЯЛАШДА ТИЗИМЛИ ЁНДАШИШДАН ФОЙДАЛАНИШ МАСАЛАСИГА ДОИР

С. К. Ғаниев (ТАТУ, т.ф.д., профессор)
Т.А. Кучкаров (ТАТУ, доцент)

Маълумки, ахборотни ҳимоялашни таъминлаш турли омилларнинг тасодифий таъсири шароитида амалга оширилади. Уларнинг баъзилари стандартларда тартибга солинган, баъзилари олдиндан номаълум ва самарадорликни пасайтиришга қодир ёки ҳатто кўзда тутилган чораларни обрўсизлантиради. Шу сабабли, ҳимоянинг самарадорлигини баҳолашда объектив ҳолатлар ва эҳтимоллик омиллари ҳисобга олиниши шарт.

Кўрилаётган муаммони ечиш учун тизимли ёндашишдан фойдаланиш таклиф этилади. Тизимли ёндашиш - бир бири билан муносабатларнинг комплекси билан боғланган ва ташқи муҳитга нисбатан ягона бутун кўринишли элементларнинг бирлашмаси каби мураккаб субъектларни тадқиқлаш методологияси. Тизимли ёндашишнинг асосий масаласи - маълум ва танланган мезон бўйича оптимал мақсадга эришиш учун мўлжалланган, тизимни лойиҳалашни ва жараёнларни ташкил этишни ўз ичига олувчи синтезлаш.

Хозирда тизимли ёндашиш фан ва техниканинг барча сохаларида – турли биологик ва инсоннинг табиатга таъсир қилувчи тизимларни таҳлиллашда, ахборот тизимларини қуриш назариясида, ишлаб чиқаришни ташкил этиш ва бошқаришнинг турли тизимларида ва ҳ., хатто психологияда ишлатилмоқда.

Тизимли ёндашишнинг афзаллиги аввало билим соҳасини кенгайтириш ҳисобланади. Тизимли ёндашиш объект яҳлитлиги механизмларини қидиришга ва унинг боғланиш технологиясини аниқлашга асосланиб кўпгина ҳодисалар моҳиятини янгича талқин қилишга имкон беради.

Тизимли ёндашишнинг асосий прициплари:

1. Яхлитлик – тизимнинг бир бутун ва юқори сатҳи учун қисмтизим сифатида кўрилиши.
2. Қурилишининг иерархиялиги – паст сатҳ элементларининг юқори сатҳ элементларига тобелиги.
3. Структураланиши – муайян тащкилий структура доирасида тизим элементлари ва уларнинг ўзаро боғланишини таҳлиллаш имконияти.
4. Кўплик – алоҳида элементларни ва тизимни тавсифлашда турли моделлар тўпламидан фойдаланиш имконияти.

Ахборотни ҳимоялаш бўйича чоп этилган илк ишларда, ҳозиргача ўзининг долзарблигини йўқотмаган қуйидаги фаразлар баён этилган:

- мутлақ ҳимояни яратиш мумкин эмас;
- ахборотни ҳимоялаш тизими комплекс характерга эга бўлиши лозим;
- ахборотни ҳимоялаш тизими ўзгарувчи шартларга мослашувчан бўлиши лозим.

Ушбу фаразларга бошқа мулоҳазаларни қўшиш лозим. Биринчидан, ахборотни ҳимоялаш тизими техник воситаларнинг ва ташкилий тадбирларнинг кўпинча тасодифий ва тартибсиз набори бўлиши лозим. Иккинчидан, ахборотни ҳимоялашга тизимли ёндашиш техник топшириқни тайёрлашдан бошлаб ва ахборотни ҳимоялаш тизимини эксплуатация жараёнида унинг самарадорлигини ва сифатини баҳолашни ниҳоялашда қўлланиши лозим.

Аввало, ахборотни ҳимоялаш тизими мақсадли бўлиши лозим. Шу билан бирга ахборотни ҳимоялаш мақсади қанчалик муайян таърифланган, бунинг учун мавжуд ресурслар батафсил аниқланган ва чеклашлар комплекси белгиланган бўлса, исталган натижани олишни кутиш даражаси шунчалик юқори бўлади.

Агар ахборот хавфсизлигини таъминлаш мақсади оддий ва умуман эришишли бўлса, таркиби ва структураси бўйича нисбатан мураккаб бўлмаган ахборотни ҳимоялаш тизими етарли бўлади. Аммо интеграл ахборот хавфсизлигини таъминлаш учун ечиш лозим бўлган муаммолар доирасининг кенгайишида тизимнинг мақсадли мазмуни формаллашган сатҳда кўп ўлчамли ва вектор характерга эга бўлади. Бунда ахборотни ҳимоялаш тизимининг алоҳида элементлари хусусиятларининг аҳамияти пасаяди, биринчи ўринга умумтизим масалалари - тизимнинг оптимал структурасини ва ишлаш режимини аниқлаш, унинг элементлари орасидаги ўзаро таъсирларни ташкил этиш, ташқи муҳит таъсирини ҳисобга олиш ва ҳ. кўтарилади. Элементларнинг аниқ бир мақсадга йўналтириб тизимга бирлаштиришда тизим таркибидаги элементларнинг ҳеч биридаги азалда бўлмаган ўзига хос хусусиятларга эга бўлади. Тизимли ёндашишда фақат бир бири билан ўзаро таъсирни аниқловчи ва бутун тизимга, ҳамда қўйилган мақсадга эришишга таъсир кўрсатувчи хусусиятлари биринчи даражали аҳамиятга эга бўлади.

Хулоса сифатида айтиш лозимки, ахборотни ҳимоялашда тизимли ёндашишдан фойдаланиш фақат мос элементларни яратишдан иборат бўлмай, балки энг самарадор чоралар, воситалар ва ҳимоя усулларидан фойдаланиб тизим хаёт циклининг барча босқичларида амалга оширилувчи мунтазам жараёндир. Ишлаб чиқилган чоралар, воситалар ва ҳимоя усуллари мажмуи ахборотга янги тахдидлар пайдо бўлганида ахборот хавфсизлигининг исталган даражасини мададлашга етарли бўлиши лозим.

БИОМЕТРИК АУТЕНТИФИКАЦИЯЛАШДАН ФОЙДАЛАНИШДАГИ МУАММОЛАР ҲАҚИДА

Ш.З. Исломов (ТАТУ, катта илмий ходим-изланувчи)
Н.К. Нурмухаммедов (ТАТУ, магистр)

Биометрик аутентификациялаш тизимлари талабгорларнинг биометрик параметрлари орқали унинг ҳақиқийлигини текширишни таъминлаш мақсадида қўлланилади. Ҳозирги кунда, анъанавий паролларга асосланган аутентификациялаш усуллари ўз ўрнини биометрик технологияларга бўшатиб бермоқда. Биометрик аутентификациялаш усуллари тезлик билан барча соҳаларда қўлланилмоқда, сабаби у айнан талабгорнинг ажратиб бўлмас параметрлари билан боғлиқдир.

Идентификация талабгорнинг киритилган маълумоти асосида базада сақланаётган рўйҳатдан ўтган маълумоти билан бирга-кўп таққослаш жараёнидир. Биометрик таниб олиш тизимларида асосий эътибор рўйҳатга олиш жараёнига қаратилиб, барча биометрик параметрлар базада сақлаб қўйилади ва ушбу маълумотлар кейинчалик идентификация ёки аутентификация учун қўлланилади. Биометрик факторга боғлиқ равишда кирувчи маълумотларни тизим ўзлаштириши учун бир нечта босқичли жараёнларни амалга оширади. Масалан, расмларни таниб олиш тизимларини оладиган бўлсак, расм хар хил ёритилганликка эга бўлиши мумкин, базада ёзиб қўйиш учун эса, уни нормал ҳолга келтириш талаб этилади. Овоз маълумотлари ҳам частотанинг ўзгаришига қараб бир нечта жараённи ўз ичига олиши мумкин. Биометрик маълумотлар келгусидаги жараёнлар учун

қандай ҳолатда лозим бўлса шунга қараб ўзгартириб сақланади. Талабгор рўйҳатдан ўтгандан кейин, қачон ундан фойдаланмоқчи (аутентификация учун) бўлса, унинг биометрик маълумоти ёзиб олинади ва базада сақланаётган рўйҳатдан ўтган нусхаси билан таққосланади.

Шахсларни таниб олиш жараёни мураккабдир, чунки, биометрик нусхалар рўйҳатга олишда ва киришда хар хил сканерлардан фойдаланилиши, бир вақтнинг ўзида бир эмас бир нечта нуқтани аниқлаши, шунингдек, шароитнинг ўзгариши: шовқинлар пайдо бўлиши, ёрқинликнинг ўзгариши, соялар ҳосил бўлиши, сифатнинг пасайиши ва бошқа ҳолатларни эътиборга олиш лозим. Бу муаммолар таққослаш вақтини самарали вақтга нисбатан кўп сарфлашга олиб келади. Вақтнинг чегаравий қиймати натижавий маҳсулот учун энг охирги босқич ҳисобланади. Чунки биометрик параметрларни таққослаш жараёни чегаравий қийматдан тезроқ бўлиши самарадорликни таъминлайди, айни вақтда тезликнинг пастлиги унинг яроқсизлигини кўрсатиб беради.

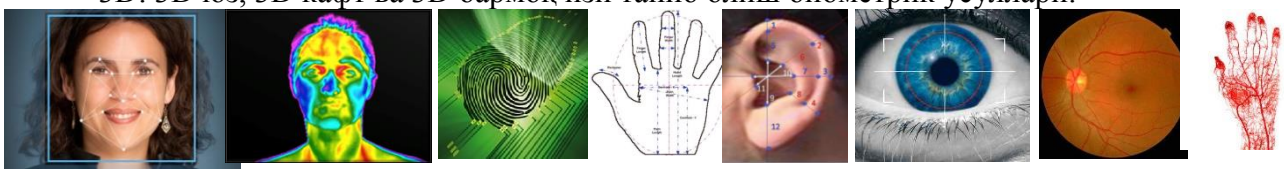
Биометрик усуллар икки хил бўлиб, улар: физик ва хулқ-атвор. Физик биометрик усуллар асосан одамнинг танасидаги хусусиятлар билан, хулқ-атвор кўринишидагилари эса одамнинг ҳаракати билан боғлиқ ҳисобланади. Таниб олишда хулқ-атвор кўринишидаги биометрик тизимлар учун маълум вақтдаги одамнинг кўрсаткичлари асосий параметер бўлиб ҳисобланади.

Ҳозирги кунга келиб биометрик тизимлар, шунингдек, 1D, 2D ва 3D ўлчамли турларга ҳам бўлинади (1-расм).

1D: овоз ва имзо таниб олиш усуллари;

2D: кўз, юз, бармоқ изи, қўл гемометрияси, кафт изи ва бошқа таниб олиш усуллари;

3D: 3D юз, 3D кафт ва 3D бармоқ изи таниб олиш биометрик усуллари.



а. юз | **б.** юз тамографияси | **с.** бармоқ изи | **д.** қўл геометрияси | **е.** кулоқ геометрияси | **ф.** кўз | **г.** кўз қорачиғи | **к.** қон томирларининг изи

1-расм. Физик биометрик усуллар

Кўпчилик биометрик тизимларда мавжуд хавф-хатарларни санашда албатта ёлғондан қабул қилиш (рухсати бўлмаган шахс ёлғондан тизимга кирса) ёлғондан қабул қилиш даражаси (ЙҚҚД) орқали ифодаланса, ёлғондан рад этиш (рухсати бор шахс ёлғондан рад этилса) ёлғондан рад қилиш даражаси (ЙРҚД) билан баҳоланади. Идеал биометрик тизимларда ЙҚҚД=ЙРҚД=0 бўлиши лозим. Реал ҳаётни олиб қарайдиган бўлсак бундай тизим мавжуд эмас. Аммо чегаравий қийматни эътиборга оладиган бўлсак, ушбу икки қиймат ҳар доим тескари ҳисобланади. Батафсилроқ келтирадиган бўлсак, паст чегаравий даража ўрнатиш ЙРҚД ни камайтиришга, ЙҚҚДни оширишига олиб келади. Ушбу ҳолат хавфсизликка талаб паст бўлган иловаларда қўл келади. Дарҳақиқат, юқори даражадаги хавфсизликни талаб этадиган тизимлар эса, ЙҚҚДни камайтириш эвазига, ЙРҚДни оширишига тўғри келади. Рухсатларни назоратлаш ва телекўрсатувларга масофадан уланиш тизимлари қатъий ауторизацияни талаб этади. Қачонки ЙРҚД ва ЙҚҚД тенг бўлса, шунда тенг хатолик даражаси (ТХД) га эга бўламиз ва бу ҳолат биометрик тизим ёки технологиянинг самарадорлиги, сифатини баҳолаб беради.

Энг кенг тарқалган оддий хужум тури бу датчикка қаратилган. Таниб олиш жараёни автоматик равишда (таниб олишни кузатиш имконияти мавжуд эмас) амалга оширилаётган ҳолатда бузғунчи датчикнинг олдида пайдо бўлади ва қонуний фойдаланувчининг биомаълумотларининг нусхасидан фойдаланади. Ушбу усулдан фойдаланган ҳолда биометрик тизимни бузишга урриниш *қалбакилаштириш хужуми* деб номланади. Ҳозирга вақтда ушбу хужумга бардошли хеч қандай биометрик технология

сотувда мавжуд эмас.

Биометрик параметрнинг нусхаси унинг факторидан келиб чиқиб ҳар хил форматда бўлиши мумкин. Ушбу ҳолатда юз бўйича аутентификациялаш тизимини оладиган бўлсак, бузғунчи мавжуд фойдаланувчининг расм, видео, 3D нусха ёки резина маскасидан фойдаланиши мумкин. Ҳозирги кунда машхўр Ленова, Тошиба ёки Асус қўл компьютерларида ўрнатилган юзларни таниб олиш биометрик тизимини қалбакилаштириш хужуми билан осон бузиш мумкин. Ушбу хужумни амалга ошириш эхтимоллиги биометрик тизимнинг заифлиги ҳисобланади, шунинг учун замонавий юзларни таниб олиш тизимларида қалбакилаштиришга қарши бир нечта чоралар кўрилмоқда. Айни вақтда кўпгина илмий изланишлар қалбакилаштириш хужумини текширишга ва қарши туришга бардошлилигини оширишга қаратилган. ICB 2013 конференсиясида бир хил биометрик тизимда бир нечта қалбакилаштириш хужумлари кўриб чиқилиб уларга қарши усуллар яратилган эди.

Бармоқ изи моделлари ҳам осон қалбакилаштирилиши мумкин. Бузғунчилар давлат ташкилотларида ўрнатилган бармоқ изини биометрик тизимлардан олиб ташлаши мумкин. Шунингдек, бармоқ изинининг нусхасини кремний ёки желатин материалидан яратиш мумкин.

2002 йилда Матсумато 11 та хар хил ишлаб чиқарувчи ташкилотларнинг бармоқ изини ўқиб олувчи қурилмаларини оптик ва датчик ёрдамида самарали алдаб ўтган. Унинг натижалари 80% гача аниқликда бўлган. Матсумато мавжуд бармоқ изларини нусхасини яратади, яъни бузғунчи сохта бармоқни датчик ойнасига тегдиради ва гўёки ҳақиқий фойдаланувчидек тизимга уланади. 11 йилдан сўнг яъни 2013 йил CCC (Chaos Computer Club) деб номланган бузғунчи гуруҳ iPhone 5S ва Samsung S5 мобил қурилмаларда ўрнатилган TouchID биометрик хавфсизлик тизимини четлаб ўтишган. Самсунг фирмаси томонидан ишлаб чиқилган ушбу биометрик тизим гуруҳ иштирокчиси томонидан бармоқ изи қалбакилаштирилмайди, балки қурилма ўчириб қайта ишга туширилганда аутентификация жараёни учун чеклов қўяди ва бузғунчи парол киритмасдан, аутентификацияни четлаб қурилма ичига киради. Кўзнинг рангдор пардаси асосидаги таниб олиш тизимларини юқори сифатли тасвирлар билан қалбакилаштириш мумкин. Гупта тижорат SDK, VeriEye маҳсулотларидан фойдаланиб, кўзнинг рангдор пардасининг сурати орқали биометрик тизимни мувафаққиятли қалбакилаштирди.

Овоз маълумотлари автоматлаштирилган ва одамларни таниб олиш овоз аутентификациялаш тизимларида қўлланилади. Қонуний фойдаланувчининг овози ҳар хил йўллар билан ёзиб олинади, унда бузғунчи ёки ҳақиқий фойдаланувчини ажратиш имконияти ва спам қўнғироқлар ёки интернет орқали ёзиб олинган овоз маълумотларини текшириш имконияти йўқ.

Хар хил биометрик тизимларига (юз, кўз, бармоқ изи, ҳаракат) қалбакилаштириш хужумларининг аниқ мақасадлари ва усуллари FP7 да келтирилган ва ТАБУЛА РАСА лойиҳаси ташкил этилган эди. Хулоса ўрнида, қалбакилаштириш хужумини олдини олишга қаратилган бир нечта ишланмалар таклиф этиш мумкин.

Қалбакилаштиришни текширишни тўрта турга бўлиш мумкин:

- фойдаланувчининг ўзаро иштирокини таъминлаш;
- юз ва бош қисмнинг беихтиёр хулқ-атвор ҳаракатларини аниқлаш;
- маълумотларни бошқариш ҳусусиятлари;
- махсус қалбакилаштиришга қарши воситаларни қўллаш.

КРИПТОГРАФИК АЛГОРИТМЛАРНИНГ МАТЕМАТИК АСОСИ

Ҳамдамов Д.Б.(ТАТУ, талаба)

Бугунги кунда криптографик алгоритмларга бўлган талаб ошиб бормоқда. Ахборот хажмининг ошиб бориши, уларни ишончли ҳимоялашга бўлган талабни ошишига сабаб

бўлмоқда. Криптографик алгоритмларнинг криптобардошлилигини оширишда мураккаб математик функциялар самарали ҳисобланади. Шу сабабли криптографик алгоритмларнинг математик асосини ўрганиш, таҳлил қилиш ва улар асосида самарали усуллар ишлаб чиқиш бугунги кунда долзарб масала ҳисобланади.

AES криптоалгоритмининг математик асосини қуйидагилар ташкил этади:

- кўпҳадларни қўшиш ва кўпайтириш;
- кираётган маълумотларнинг ҳолат жадвали;
- шифрлаш калити ҳолат жадвали;
- ***SubBytes***–алгоритмда қайд этилган 16x16 ўлчамли жадвал асосида байтларни алмаштириш, яъни S -блок акслантиришларини амалга ошириш;
- ***ShiftRows***–алгоритмда берилган жадвалга кўра ҳолат байтларини циклик суриш;
- ***MixColumns***–устун элементларини аралаштириш, яъни алгоритмда берилган матрица бўйича акслантиришни амалга ошириш;
- ***AddRoundKey*** **–** раунд калитларини қўшиш, яъни блоклар мос битларни ***XOR*** амали билан қўшиш.

ГОСТ 28147-89 криптоалгоритми ҳозирда Россия Федерацияси давлат стандарт шифрлаш алгоритми ҳисобланади. Бу алгоритм аппарат ва дастурий таъминот учун мўлжалланган бўлиб, ҳимояланадиган маълумотнинг махфийлик даражасига чегаралаш йўқ . Алгоритмнинг калит узунлиги 256 битга шифрлашни 64 бит узунликдаги блокларда амалга оширади ва раундлар сони 32 га тенг.

ГОСТ 28147-89 стандарт симметрик блокли шифрлаш алгоритмининг математик асоси қуйидагилардан иборат:

- блокни 32 битли ўнг қисми ва 32 битли раунд калитини $\bmod 2^{32}$ бўйича қўшиш: $C_i = (R_{i-1} + K_i) \bmod 2^{32}$;
- 32 битли C_i натижа саккизта махфий S-блокларда ўрнига қўйиш акслантириши орқали аксланади ;
- S-блокларда чиқувчи 32 битли блок чапга 11 бирлик циклик сурилади;

DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ) “Миллий Стандартлар Бюроси” томонидан 1977 йилда эълон қилинган.1980 йилда АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” бу алгоритмни давлат ва савдо-сотиқ молияси соҳасидаги маҳфий бўлмаган, аммо муҳим бўлган маълумотларни руҳсат этилмаган жисмоний ва юридик шаҳслардан муҳофаза қилинишида шифрлаш алгоритми сифатида қўллаш стандарти деб қабул қилди.

DES алгоритмида: дастлабки 56 битли калитдан раунд калитларини ҳосил қилишнинг мураккаб эмаслиги, раунд асосий акслантиришларининг аппарат-техник ва дастурий таъминот кўринишларида қўлланилишини таъминлашнинг қулайлиги, ҳамда, улар криптографик ҳоссаларининг самарадорлиги – криптобардошлилигининг юқорилиги, бу алгоритмнинг асосий хусусиятларини белгилайди.

DES шифрлаш алгоритми АҚШда 1998 йилнинг 31 декабргача стандарт шифрлаш алгоритми деб ҳисобланган. Бу алгоритмда қўлланилган акслантиришлар криптографик нуқтаи назардан бардошли, аммо дастлабки 56 - битли калитнинг узунлиги, бугунги кун ҳисоблаш техника ва технологияларининг ютуқларидан фойдаланилганда, мумкин бўлган барча 2^{56} та калитларни тўла танлаб чиқиш имкониятини сезиларли қисқартиради.

DES криптоалгоритмининг математик асосини қуйидагилар ташкил этади:

- L_i ва R_i —ҳар бири 32 битли блоклар бўлиб, Фейстел тармоғини чап ва ўнг қисимларини ифодалайди, $i = 0,1,...,16$;
- $\oplus$ — битлар блоклари векторлари кординаталарини $\bmod 2$ бўйича қўшиш;
- K_i — 48 битли раунд калитлари;
- F — Фейстел тармоғи асосий акслантиришлари функцияси;

– *IP* – ўрин алмаштириш жадвали.

DES алгоритмида шифрлаш жараёни қуйидаги функция орқали амалга оширилади:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \\ i = 1,2,...,16; \end{cases}$$

Дешифрлашда шифрлаш жараёнида бажарилган акслантиришлар тескари тартибда бажарилади:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i), \\ i = 16,15,...,1; \end{cases}$$

– симметрик криптографик алгоритмларда қўлланиладиган математик функциялар кўриб чиқилди;
– криптографик алгоритмларнинг математик асосига параметрли алгебрани жорий қилиш самарали ҳисобланади.

КИРИШНИ НАЗОРАТЛАШ ВА БОШҚАРИШ ТИЗИМИ ТАРКИБИДАГИ КОНТРОЛЛЕРЛАРНИНГ ТАҲЛИЛИ

Д.А. Авлаев (ТДТУ, декан муовини)
А.Т.Имамалиев (ТАТУ, ассистент)

Киришни (фойдаланишни) назоратлаш ва бошқариш тизими таркибидаги маълумотни йиғиш, қайта ишлаш ва бошқариш тизимларини ҳал қиладиган асосий вазифалари кириш режимини ўрнатиш, ўқиб олувчи қурилмадан маълумотни қабул қилиб олиш ва уни қайта ишлаш, идентификация ва аутентификациядан ўтказиш, тўсувчи(чегараловчи) қурилмалар ва бажарувчиларнинг бошқарув сигналларини қайта ишлаш, маълумотларни акслантириш ва регистрация қилишни таъминлайди.

Юқоридагилардан ташқари бу тизим қуйидаги функцияларни бажариши керак:

− шаҳсларни бинога киришни тавсифловчи маълумотларни(кодларни, вақт интервалини, кириш даражасини ва ҳ.к.) маълумотлар базасига киритиш;

− кириш нуқтаси орқали ходимлар ва мижозларни ўтишларини электрон рўйҳатга олиш журналига киритиш;

− кириш(фойдаланиш) нуқтасида фавқулотда ҳолат ҳақида маълумот чиқишининг муҳимлиги;

− ўқиб олувчи, бажарувчи қурилмалар ва алоқа линиясининг ҳолати тўғрилигини назоратлаш.

Қуйидаги маълумотларни йиғиш, қайта ишлаш ва бошқариш тизими воситалари ҳисоблашларни бажариш функциясини амалга оширади:

− аппарат воситалар – кириш контроллерлари, киришни назоратлаш приборлари;

− дастурий воситалар – фойдаланишни(киришни) назоратлаш ва бошқариш тизимининг дастурий таъминоти.

Кириш контроллерлари ўқиб олувчиларнинг идентификаторидаги маълумотни қайта ишлаш учун қўлланиладиган қурилмалар, қарор қабул қилиш қурилмалари, бажарувчиларни бошқарувчи қурилмаларни ўз ичига олади. Контроллерлар бошқариш усули бўйича учта синфга бўлинади: автоном, марказлашган(тармоқли) ва комбинацияланган.

Автоном контроллерлар – бир нуқтадан ўтиш, тартибга солиш ва хизмат кўрсатиш учун мўлжалланган тўлиқ тугалланган қурилма. Автоном контроллерлар ўқиб олувчи

қурилмалар ёки ўрнатилган электромагнит қулуфлар билан конструктив бирлаштирилган бўлиши мумкин. Турли хил ўқиб олувчи қурилмаларни қўлланилишини ҳисоблаб чиқади. Улар киришни (фойдаланишни) назоратлаш ва бошқариш тизимининг унча катта бўлмаган фойдаланувчилар сонига хизмат қилишни кўзда тутади.

Тармоқли контроллерлар – компьютерни бошқаришда ишлатиладиган контроллерлардир. Бундай ҳолларда қарор қабул қилиш функцияси шаҳсий компбютерларга ўрнатилган маҳсус дастурий таъминот орқали амалга оширилади.

Тармоқли контроллерлар, киришни (фойдаланишни) назоратлаш ва бошқариш тизимининг барча мураккаб даражаларини яратиш учун қўлланилади. Бундан ташқари ўтказишга рухсат бериш ёки тақиқлаш каби асосий функциялари ҳам мавжуд бўлиб, улар қуйидаги янги имкониятларни амалга ошириши мумкин:

- ходимнинг иш жойида бор ёки йўқлиги ҳақида ҳисоботни қабул қилиш;
- муайян ходимнинг турган жойини оператив аниқлаш;
- иш вақтини ҳисоблаш табелини автоматик киритиш;
- ихтиёрий вақтда объект бўйича шаҳслар ва мижозларнинг жойларини ўзгариши ҳақида ҳисобот олиш;
- ходимларнинг вақтинчалик ўтиш графигини шакллантириш, яъни ким, қаерга ва қайси вақтда жойини ўзгартириши мумкинлиги;
- ходимларнинг маълумотлар базасини(электрон картотекасини) кўриш.

Комбинацияланган контроллерлар – тармоқли ва автоном контроллерларнинг функцияларини ўз ичига олади. Бошқарилувчи компьютерлар билан алоқа ўрнатилганда тармоқли контроллерлар каби, алоқа йўқлигида эса автоном контроллерлар каби ишлайди.

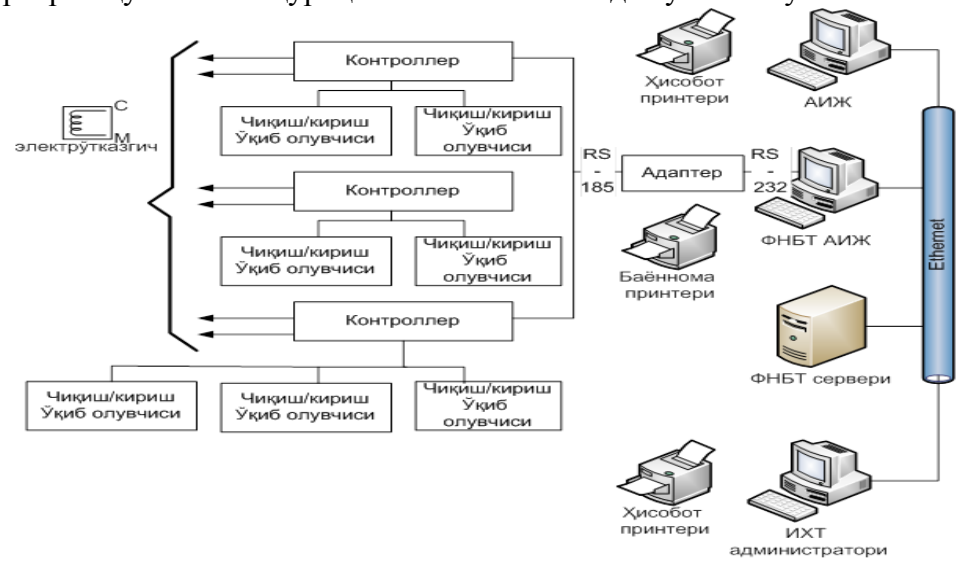
Бу контроллерларнинг яна бир имконияти фойдаланишни(киришни) назоратлаш ва бошқариш тизимининг тақсимланган тармоғини ташкил этишда тўлиқ очиқликдир. Мустақил текшириш процедурасини бажарувчи микрокомпьютерлар(контроллерлар) базасининг периферик пункти локал тармоқ билан жихозланган, бунда серверлар локал маълумотлар базасидаги маълумотларга мантиқий ва статистик ишлов бериш учун ишлатилади. Тақсимланган архитектура ҳолати бўйича фойдаланишни(киришни) назоратлаш ва бошқариш тизимининг асосий фарқланувчи жиҳати шундаки, идентификатор маълумотлар базаси бир эмас, бирнечта контроллерларда сақланади. Бу контроллерлар чиқиш сигналларни, ташқи қурилмалар ва қуриқлаш шлейфларни реле орқали бошқаради. Бу қурилмалар бевосита контроллер платасига ўрнатилади.

Тақсимланган архитектурали киришни (Фойдаланишни) назоратлаш ва бошқариш тизими марказий шаҳсий компьютерларда қайта ишланадиган маълумотларга бўлатиган қарши таъсирлардан, алоқа линиялари ва переферик қурилмалардаги маълумотларни бутунлилигини ва уларнинг ўзларининг бутунлилигини бузилишидан ишончли ҳимоялашга имкон беради. Бундан ташқари, унинг дастурий таъминоти бир неча компьютерларни бирданига бошқаришга ва вазифаларни ўзаро тақсимлашга имкон беради. Бундай тақсимланган фойдаланишни назоратлаш ва бошқариш тизимлари объектнинг бошқа қисмтизимлари билан интеграциялашга имкон беради. Масалан, қўриқлаш сигнализацияси, телвизион қўриқлаш тизимлари ва бошқа шу кабилар.

Қўриқланаётган ҳудудга киришни ташкил этишда хавфсизлик даражасини ошириш учун ўтиш нуқтасига қўшимча қурилмаларни ўрнатиш мумкин. Масалан, икки мартта ўтишни тақиқлаш(anti passback) учун, яъни субъект қўриқланаётган объектга кириб чиққанидан кейин яна қайтиб киришини тақиқлаш.

Икки томонлама ўтишни тақиқлашни амалга оширишда ўтишлар тўлиқ назоратланиши лозим. Бунда иккита ўқиб олувчилар(ридерлар)дан фойдаланилади. Ўтишнинг кириш (нуқтасига)томонига биринчи ўқиб олувчи қурилма, чиқиш томонига эса иккинчи ўқиб олувчи қурилма ўрнатилади. Мазкур функцияни қўллаш, идентификаторни бошқа шаҳсга узатишни қийинлаштиради. Бегона шаҳсларнинг рухсатсиз ўтишидан қўшимча ҳимоялаш чоралари сифатида видеоидентификация функцияси қўлланилиши лозим. Яъни, идентификаторга бириктирилган фоторасм

компьютернинг мониторида акс этирилади. Бундай ўтказиш бўйича ечим автоматик ва контроллерларни қўллаш ёки қўриқлаш хизмати асосида бўлиши мумкин



1-расм. Киришни назоратлаш ва бошқариш тизимининг тақсимланган тармоқ схемаси.

.

КОРХОНАДА АХБОРОТ ХАВФСИЗЛИГИ ИНЦИДЕНТЛАРИНИ ТЕРГОВ ҚИЛИШ УСУЛЛАРИ ВА БАҲОЛАШ

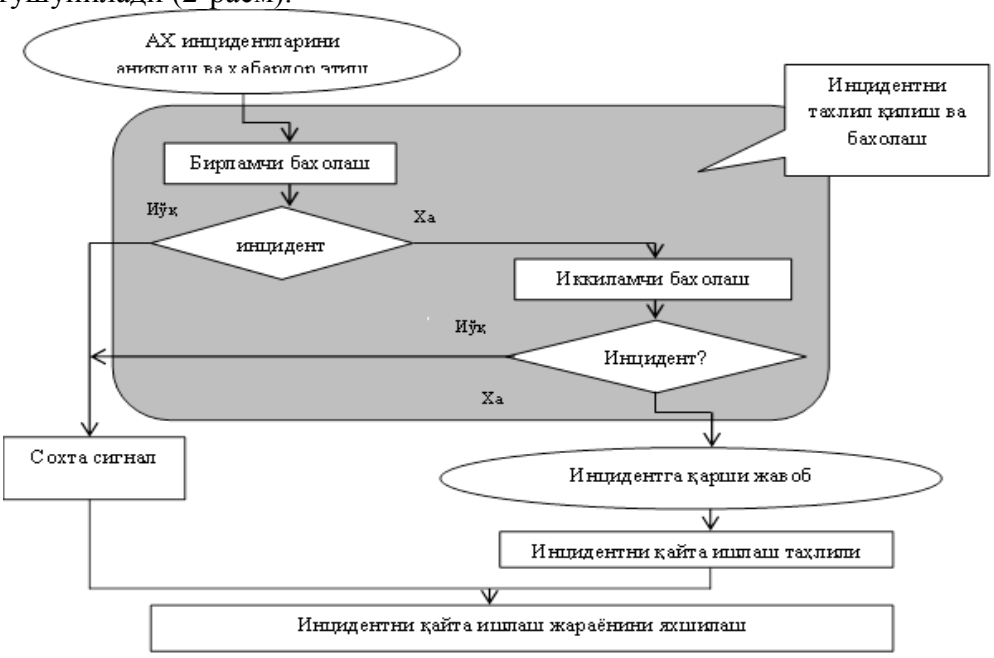
Ш.Р. Ғуломов (ТАТУ, катта ўқитувчи)

Ички терговнинг мақсади – содир бўлган ҳодисада айбдорни топиш, юз берган ҳодисанинг сабабини аниқлаш, келажакда бундай ҳодисаларга дуч келмаслик учун талаб ва таклифлар ишлаб чиқиш.

Ички тергов ўтказишнинг асосий вазифалари: ишчининг нима сабабдан, қандай вазият ва шароитда жиноят содир этганлигини аниқлаш; жиноятга дахлдор аниқ бир шахс ёки шахсларнинг айбдорлик даражасини аниқлаш; жиноят содир этиш турларини, сабабини ва шароитини бартараф этиш учун огоҳлантириш-профилактик турдаги тадбирлар ташкил этиш ва ўтказиш бўйича тавсиялар ишлаб чиқиш (1-расм).

1-расм. Корхонада терговни амалга ошириш архитектураси

Ахборот хавфсизлиги инцидентларини тергов қилиш, аниқлаш, таҳлил қилиш ва баҳолаш. Ахборот хавфсизлиги (АХ) бўйича юз берадиган омилларга асосланган, ахборот хавфсизлиги инцидентларини баҳолаш жараёнлари кўриб чиқиш мумкин. Ахборот тизимлари сонининг ўсиши ва ахборот технологияларининг такомиллашгани сари АХ инцидентларининг сони ҳам ортиб бормоқда. АХ инциденти деганда-бир ёки бир нечта ножўя ходисалар тизимининг ахборот хавфсизлиги активларига таъсир этиб, бизнес жараёнларни узилишига олиб келиши ва салбий оқибатларга олиб келиши тушунилади (2-расм).



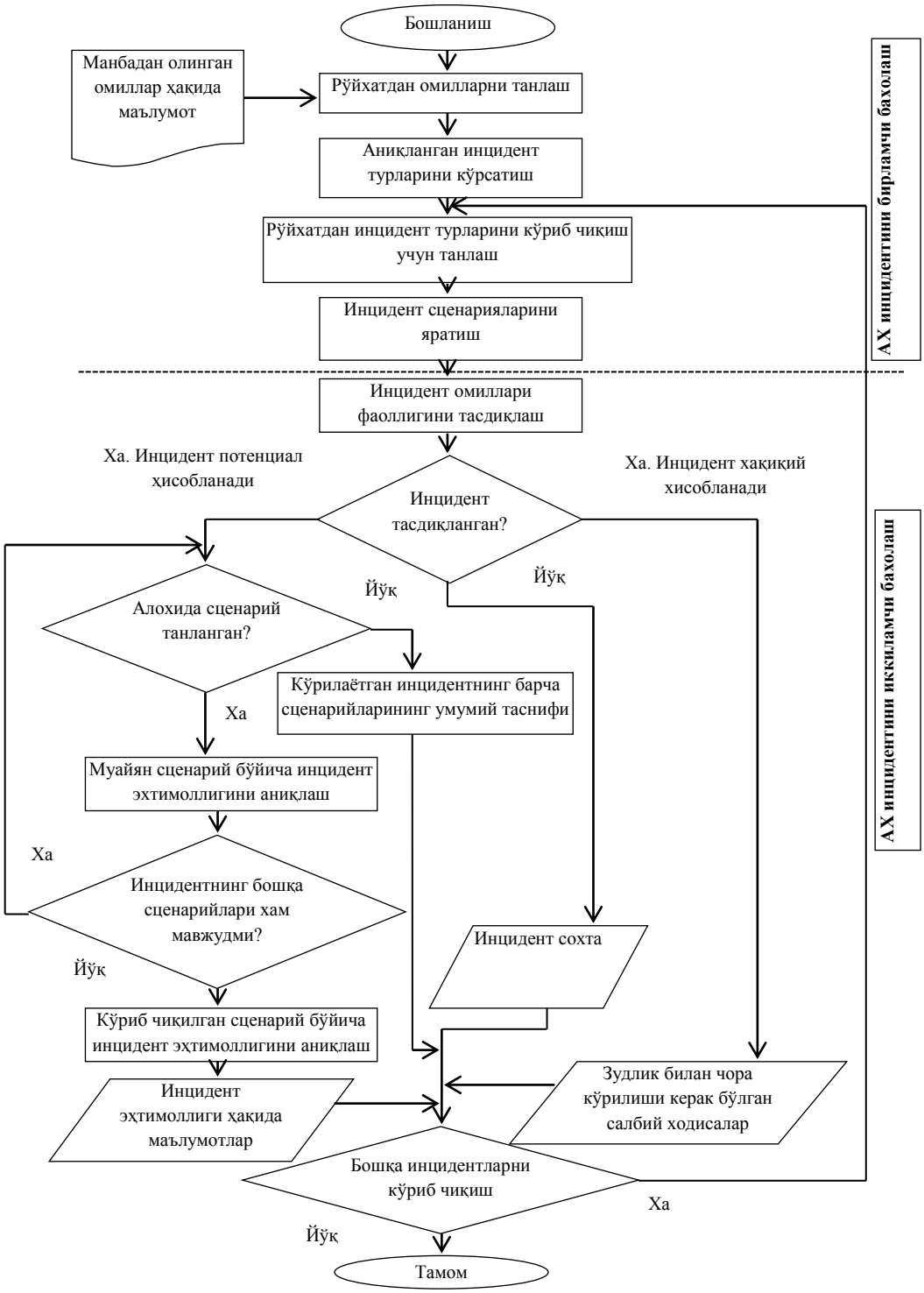
2-расм. АХ инцидентларини ишлашни бошқариш блок-схемаси

Айрим корхоналарда АХ инцидентларини аниқлаш методикаси йўқ, ишчилар хар доим ҳам ишдаги асосий вазифаларнинг узилишларига алоқадар бўлмаганлиги сабабли, қандай ходисалар ахборот хавфсизлиги инциденти эканлиги ҳақида билмайдилар. Шу муаммоларни бартараф этиш мақсадида АХ инцидентлари ва ходисаларининг фаол базасини яратиш муҳим саналади. АХ инцидентлари ва ҳодисалари базаси АХ инцидентларини тартиблвочиларининг шахсий тажрибасига асосланиб яратилиши мумкин. Одатда корхона, хусусан йирик фирма, компанияларда содир этилган ахборот хавфсизлиги инцидентлари ҳақида маълумотлар, тизимга қайта хавфнинг олдини олиш мақсадида ва корхона обрўсига зарар етказмаслик мақсадида нашр этилмайди.

АХ ҳодисаларини инцидент сифатида идентификация қилиш учун зарур бўлган маълумот миқдорининг катталиги сабабли, ушбу ҳодисаларнинг сабаби ва манбаларини аниқлаш, ҳамда салбий оқибатларининг тарқалишида қийинчилик туғдиради, шунинг учун ушбу жараёнлар расмийлаштирилган ва автоматлаштирилган бўлиши зарур.

Ахборот хавфсизлиги инцидентларини уларнинг омиллари асосида баҳолаш. Дастлабки АХ ҳодисаси идентификациясини АХ инциденти сифатида баҳолаш, инцидентнинг муайян бир турига кўрсатувчи АХ ҳодисалари омиллари асосида амалга ошириш мумкин. АХ ходисаси омили бу – АХ ишдан чиққанлигига ишора берувчи АХ ҳодисаси аломати, ҳамда хавфсизлик билан боғлиқ кутилмаган ҳодиса рўй беришидир (3-расм).

АХ инцидентларини тергов қилиш ва уларни баҳолашдаги таҳлил қилинган блок-схемалар АХ инцидентларини ажратиш, эҳтимолий сценарийларини кузатиш, инцидентлар содир бўлиш эҳтимоллигини ҳисоблаш, ҳамда фойдаланувчи томонидан аниқланмаган, содир бўлиши мумкин бўлган инцидентларни аниқлаш имконини беради.



3-расм. АХ инцидентларини баҳолаш блок-схемаси

АХБОРОТ ХАВФСИЗЛИГИДА ХАВФ-ХАТАРЛАРНИ АНИҚЛАШНИНГ УМУМИЙ ТАВСИФИ

О.Н. Бекмирзаев (ТАТУ, ассистент)

Мақолада актив қиймати, таҳдиднинг юзага келиши эҳтимоллиги ва фойдаланишнинг соддалиги хавф-хатарлар ўлчовларини идентификациялаш матрицаси орқали баҳолаш усули таклиф қилинмоқда.

Хавф-хатарларни номақбул воқеа-ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Хавф-хатарларларни

аниқлаш миқдор ёки сифат жиҳатдан хатарларларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ хатарларларни жойлаштириш имкониятини беради.

Хавф-хатарларларни аниқлаш ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган хатарларларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян хавф-хатарларларни жойлаштиради ва контекстни ўрнатишда аниқланган хавф-хатарларларни баҳолаш мезонлари бўйича уларни таснифлайди. Хатарларни аниқлаш кўпинча икки (ёки ундан кўп) итерациядан фойдаланиб ўтказилади. Дастлаб, кейинчалик баҳолашни кафолатлайдиган потенциал юқори хавф-хатарларларни идентификация қилиш учун юқори даражали аниқлаш ўтказилади. Навбатдаги итерация бошланғич итерацияда аниқланган потенциал юқори хатарларларни янада чуқурроқ қараб чиқишни ичига олиши мумкин. Ушбу ишлар хавф-хатарларларни баҳолаш учун етарли ахборот бермаган ҳолларда, бошқа усулдан фойдаланган ҳолда ва хавф-хатарларларнинг таъсир қилиш соҳасининг маълум қисмларигагина татбиқан, янада батафсилроқ таҳлил ўтказилади.

Хавф-хатарларларни аниқлашнинг мақсад ва вазифалари асосида хатарларларни аниқлашга ўз ёндашувини танлаш ташкилотнинг ўзига боғлиқ. Ахборот хавфсизлиги хатарларларини аниқлаш усуллари 1- жадвал келтирилган.

Активларни аниқлашда ахборот тизими фақат аппарат ва дастурий воситалардан иборат эмаслигини назарда тутиш керак. Активларни аниқлаш хавф-хатарларни баҳолаш учун етарли ахборот таъминланадиган тегишли деталлаштириш даражасида амалга оширилиши зарур. Активларни аниқлашда фойдаланиладиган деталлаштириш даражаси хавф-хатарларни баҳолаш вақтида тўпланган ахборотнинг умумий ҳажмига таъсир этади. Бу даража хавф-хатарларни баҳолашнинг кейинги итерацияларида янада деталлаштирилиши мумкин. Ҳар бир актив учун жавобгарликни ва ҳар бир актив ҳисобини таъминлаш учун эгаси аниқланиши керак. Актив эгаси активга бўлган мулкдорлик ҳуқуқларига эга бўлмаслиги мумкин, лекин у активни ишлаб чиқариш, ишлаб чиқиш, унга хизмат кўрсатиш, фойдаланиш ва хавфсизлиги учун тегишли равишда жавобгардир. Кўп ҳолларда, актив эгаси активнинг ташкилот учун ҳақиқий аҳамиятини аниқлашга қодир бўлган энг мос шахс ҳисобланади.

Активларнинг баҳоси, оқибатларнинг ҳар бир турига тааллуқли бўлган заифликлар ва таҳдидларнинг даражалари, ҳар бир комбинация учун 0 дан 8 гача бўлган шкала асосида хавф-хатарларнинг тегишли ўлчовини идентификациялашларни мақсадида, жадвал шаклига (матрицага) келтирилади (1 жадвал). Қийматлар матрицага структураланган тарзда киритилади.

1 жадвал. Хавф-хатарларлар ўлчовларини идентификациялаш матрицаси.

	Таҳдиднинг юзага келиши эҳтимоллиги	Паст(П)			Ўрта(Ў)			Юқори(Ю)		
	Фойдаланишнинг соддалиги	П	Ў	Ю	П	Ў	Ю	П	Ў	Ю
Актив баҳоси	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Ҳар бир актив учун ўринли заифликлар ва уларга мос келадиган таҳдидлар кўриб чиқилади. Агар тегишлича таҳдидсиз заифлик ёки тегишлича заифликсиз таҳдид мавжуд бўлса, ҳозирги пайтда хавф-хатарлар йўқ (лекин, бу вазият ўзгарганда эҳтиёткорлик кўрсатиш керак). Жадвалдаги тегишли сатр актив баҳосининг қиймати бўйича, тегишли устун эса, таҳдиднинг юзага келиш эҳтимоллиги ва фойдаланишнинг соддалиги бўйича белгиланада. Масалан, агар актив 3 баҳога эга бўлса, таҳдид «юқори», заифлик эса, « паст» бўлади, у ҳолда хавф-хатарлар ўлчови 5 га тенг бўлади. Актив 2 баҳога эга деб, ва масалан, ўзгартириш учун таҳдид даражаси « паст», фойдаланишнинг соддалиги эса « юқори» бўлади деб тахмин қиламиз, у ҳолда хавф-хатарлар ўлчови 4 га тенг бўлади. Жадвалнинг ўлчами, таҳдидлар эҳтимоллиги тоифаларининг, фойдаланишнинг соддалиги тоифаларининг сони ҳамда активлар баҳосини аниқлаш тоифаларининг сони нуқтаи назаридан, ташкилотнинг эҳтиёжларига мослаштирилиши мумкин.

Қўшимча хавф-хатарларни ўлчовлари учун қўшимча устунлар ва сатрлар талаб қилинади. Берилган ёндашувнинг аҳамияти, кўриб чиқилиши талаб қилинадиган хавф-хатарларларни ранжлашда ифодаланади. Ўхшаш матрица, 2 - жадвалда кўрсатилганидек, миқдор жиҳатдан баҳоланган бизнес таъсирида акс эттирилган инцидент сценарийси эҳтимоллигини кўриб чиқиш натижаси ҳисобланади. Инцидент сценарийси эҳтимоллиги, муайян эҳтимолликка эга заифликдан фойдаланадиган таҳдид воситасида берилган. Жадвал инцидент сценарийси билан боғлиқ бу эҳтимолликни бизнесга бўладиган таъсирга қарши акс эттиради. Натижада олинадиган хавф-хатарлар 0 дан 8 гача бўлган шкала бўйича ўлчанади, у хавф-хатарларларни қабул қилиш мезонларига нисбатан баҳоланиши мумкин.

Хавф-хатарларларнинг берилган шкаласи қуйидагича тарзда хавф-хатарларларнинг оддий умумий рейтинги учун ҳам акс эттирилиши мумкин:

- паст хавф-хатарлар: 0-2;
- ўрта хавф-хатарлар: 3-5;
- юқори хавф-хатарлар: 6-8.

2 - жадвал. Хавф-хатарларларнинг умумий рейтингининг матрицаси.

	Инцидент сценарийси эҳти-моллиги	Жуда паст (эҳтимол-лиги жуда кам)	Паст (эҳтимол-лиги кам)	Ўртача (мумкин бўлган)	Юқори (эҳти-моллиги бўлган)	Жуда юқори (тез-тез учраб турадиган)
Бизнесга бўладиган таъсир	Жуда паст	0	1	2	3	4
	Паст	1	2	3	4	5
	Ўртача	2	3	4	5	6
	Юқори	3	4	5	6	7
	Жуда юқори	4	5	6	7	8

Хавф-хатарларларни идентификация қилишдан мақсад, потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади. Қуйида тавсифланган қадамлар хатарларларни таҳлил қилиш бўйича табдирлар учун кириш маълумотларини аниқлайди.

Актив қиймати, таҳдиднинг юзага келиши эҳтимоллиги ва фойдаланишнинг соддалигидан келиб чиқиб ахборот хавфсизлигида хавф-хатарларни аниқлашнинг ахборот хавфсизлигига бўладиган хавфларни олдини олиш билан бир қаторда уларга қарши самарали ҳимоя тизимини қуриш имкониятини беради.

ИНТЕРНЕТДА АХБОРОТ АЛМАШИНУВИНИНГ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА SSL ПРОТОКОЛИНИНГ АҲАМИЯТИ

Э.А. Қорабаев (ТАТУ, ассистент)

Ҳозирги кунда компьютер ва интернет технологиялар жадаллик билан ривожланиб бормоқда. Шунингдек бизнес юритишнинг азалий методларига интернет туфайли бир қанча ўзгаришлар киритилмоқда. Интернет орқали савдо-сотиқ қилиш, маълумот алмашишлар, шартномалар имзолаш, келушувлар ва ҳакозолар.

Бундан ташқари интернет магазин, интернет банкинг каби ҳизмат турлари пайдо бўлмоқда. Интернетда, умуман ҳамма тармоқда, ахборотлар «очиқ» кўринишда узатилишини ва уни тармоқ ичидаги ихтиёрий одам ушлаб олиши, ўқиши, ўзгартириши, нусха олиши мумкинлигини инобатга олсак, ахборот алмашинувининг хафвсизлигини таъминлаш қанчалик муҳимлигини англаш қийин эмас.

Айниқса интернетда ахборотлар алмашинувининг хавфсизлигини таъминлаш муҳим аҳамият касб этади. Чунки кўпгина ҳужумлар, таҳдидлар, бузғунчилик ҳаракатлари интернет орқали амалга ошаётган электрон савдо, тижорат ва тўловларда кузатилади. Хавфсизликни таъминлаш учун турли воситалар, дастурлар ишлаб чиқилган. Шулар орасида кенг тарқалгани SSL(Secure Socket Layer) ва SET (Secure Electronic Transactions) протоколодир.

• SSL протоколи маълумотларни канал даражасида шифрлашда қўлланилади;

• SET хавфсиз электрон транзакциялари протоколи яқинда ишлаб чиқилган бўлиб, фақатгина молиявий маълумотларни шифрлашда қўлланилади.

SSL(Secure Socket Layer) протоколи мижоз-сервер иловаларида ахборотни ҳимояланган алмашишни амалга ошириш учун ишлаб чиқилган. Ҳозирда SSL протоколи OSI моделининг сеанс сатҳида ишловчи ҳимояланган канал протоколи сифатида ишлатилади. Бу протокол ахборот алмашиш ҳавфсизлигини таъминлашда ахборотни ҳимоялашнинг криптографик усулларидан фойдаланади. SSL протоколи тармоқнинг иккита абоненти орасида ҳимояланган канал қуришнинг барча функцияларини жумладан, уларни аутентификациялаш, узатилувчи маълумотларнинг конфиденциаллигини ва яхлитлигини таъминлаш функцияларини бажаради. Асимметрик ва симметрик криптотизимлардан комплекс фойдаланиш технологияси SSL протоколининг ядроси ҳисобланади.

SSLда иккала томоннинг ўзаро аутентификациялаш фойдаланувчиларнинг (мижоз ва сервер) махсус сертификация марказларининг рақамли имзоси билан тасдиқланган очиқ калитларининг рақамли сертификатлари билан алмашиш орқали бажарилади. SSL протоколи ҳамма қабул қилган X.509 стандартларга мос келувчи сертификатларни, ҳамда сертифкатларни беришда ва ҳақиқийлигини текширишда ишлатилувчи PKI очиқ калитлари инфраструктураларининг стандартини мададлайди.

Конфиденциаллик уланиш ўрнатилишида томонлар алмашинадиган симметрик сессия калитларида узатилувчи ҳабарларни шифрлаш орқали таъминланади. Сессия калитлари ҳам шифрланган кўринишда узатилади. Бунда улар абонентларнинг сертификатларидан чиқариб олинган очиқ калитларда шифрланади. Ахборотларни шифрлашда симметрик калитларнинг ишлатилишига асосий сабаб-симметрик калитларда шифрлаш ва расшифровка қилиш жараёнининг тезлиги асимметрик калитлар ишлатилишидагига қараганда юқорилиги.

Айланувчи ахборотнинг ҳақиқийлиги ва яҳлитлиги электрон рақамли имзони шакллантириш ва текшириш эвазига таъминланади.

SSL протоколининг ишлаш принципи, 2 та ишочли компютернинг (сизнинг компьютерингиз ёки сизнинг банкингиз сервери) ишончсиз тармоқ (интернет) орқали ҳавфсиз равишда ахборот алмашинувига асосланган.

Бунинг учун аввало иккала тараф шахси аниқланиши лозим. Кўпинча бир тарафнинг

шахси аниқланишиниг ўзи кифоя. Сўнгра маълумотни шифрлаш жараёни. Шифрланган маълумотнинг калити фақат иккала тарафда бўлади ҳолос.

Демак SSL протоколи ахборот алмашинувининг хавфсизлигини таминлашда 2 та қуйидаги элементларни ишлатади:

1. Аутентификация;
2. Шифрлаш.

SSL протоколига мувофиқ криптоҳимояланган туннеллар виртуал тармоқнинг охирги нуқталари орасида яратилади. Ҳар бир ҳимояланган туннелни бошлаб берувчилари–туннел оҳирги нуқталаридаги компьютерларда ишловчи мижоз ва сервер ҳимояланган уланишни шакллантиришда ва мададлашда SSL протоколи мижоз ва сервер ўзаро алоқасининг қуйидаги босқичларини кўзда тутади:

1. SSL сессиясини ўрнатиш;
2. ҳимояланган ўзаро алоқа.

SSL сессияни ўрнатиш жараёнида қуйидаги масалалар эчилади:

1. томонларни аутентификациялаш;
2. ҳимояланган ахборот алмашинувида ишлатилувчи криптографик алгоритмлар ва зичлаштириш алгоритмларини мувофиқлаштириш;
3. умумий махфий мастер-калитни шакллантириш;
4. ахборот алмашишни криптографик ҳимоялаш учун шакллантирилган мастер калит асосида умумий маҳфий сеанс калитларини генерациялаш. Қўл беришиш муолажаси деб ҳам аталувчи SSL-сессияни ўрнатиш муолажаси ахборот алмашишни бевосита ҳимоялашдан олдин пухта ишланади ва SSL протоколи таркибига кирувчи бошланғич саломлаш (HandShake Protocol) протоколи бўйича бажарилади.

Мижоз ва сервер орасида қайта уланиш ўрнатилишида томонлар, ўзаро келишув бўйича, олдинги умумий сир асосида янги сеанс калитларини шакллантиришлари мумкин (ушбу муолажа SSL-сессиянинг давоми деб аталади).

SSL 3.0 протоколи аутентификациялашнинг қуйидаги учта режимини мададлайди:

1. томонларни ўзаро аутентификациялаш;
2. мижозни аутентификацияламасдан серверни бир томонлама аутентификациялаш;
3. тўлиқ анонимлик.

Охирги вариантдан фойдаланилганда томонларнинг ҳақиқийлигини кафолатламасдан ахборот алмашиш хавфсизлиги таъминланади. Бу ҳолда ўзаро алоқадаги томонлар, алоқа қатнашчиларини алмаштириб қўйиш билан боғлиқ хужумлардан ҳимояланмайдилар. SSL протоколига мувофиқ ўзаро алоқадаги томонларни аутентификациялашда ва умумий маҳфий калитни шакллантиришда кўпинча РСА алгоритмидан фойдаланилади.

SSL протоколини кенг миқиёсида қўлланилиши HTTPS (Hypertext Transfer Protocol Secure), шифрлаш имконига эга бўлган яратишга сабаб бўлди. HTTS протоколида узатилаётган маЪлумотлар “жойлаштирилади ”, SSL ёки TLS криптографик томонидан ва шу билан бирга ўзида маълумотлар ҳимояни акс эттиради. Бунда ҳимоя тури ҳимояси жуда муҳим бўлганда Web оламида иловаларда кенг қўлланилади, мисол учун “Тўлов” системаларида. Ҳозирда HTTPS энг машгур броузерлар томонидан кенг қўлланилади. HTTP дан фарқлироқ HTTPS ўзида TCP порт 443 дан фойдаланади. SSL протоколи кенг тарқалган бўлишига қарамай камчиликлардан ҳоли эмас. SSL протоколларининг камчилиги - ўзларининг ҳабарларини ташишда тармоқ сатҳидаги фақат битта – IP-протоколидан фойдаланишлари ва фақат IP-тармоқларда ишлай олишлари. Ундан ташқари, SSLнинг амалда қўлланиши татбиқий протоколлар учун тўла шаффоф эмас. SSLнинг яна бир салбий томони шундай иборатки, агар мижоз ва сервер уланишни узсалар, улар уни маълумотларнинг минимал ҳажмини алмашиш йўли билан тиклашлари ва Session ID нинг эски параметрларидан фойдаланишлари мумкин. Нияти бузуқ одам олдинги сессиялардан бирини обрўсизлантириб уни тиклаш муолажасини сервер билан

ўтказиши мумкин. Натижада бу сессияда узатиладиган кейинги барча маълумотлар обрўсизлантирилади. Ундан ташқари, SSL аутентификациялашда ва ширфлашда бир хил калитдан фойдаланилади. Бу эса маълум бир ҳолатларда заифликка олиб келиши мумкин. Бундай ечим турли калитлар ишлатилганига нисбатан кўп статистик маълумотларни йиғишга имкон беради.

Шундай қилиб, интернетда ахборотлар «очиқ» кўринишда узатилишини ва уни тармоқ ичидаги ихтиёрий одам ушлаб олиши, ўқиши, ўзгартириши, нусха олишига қарши чоралар бўйича тармоқдаги ахборот алмашинувининг конфиденциаллигини ва яхлитлигини таъминлашда SSL протоколининг аҳамияти жуда юқоридир.

ZARARKUNANDA DASTURLARNING KENGAYTIRILGAN DINAMIK TAHLILI VA AMALGA OSHIRISH USULLARI

B.K. Yusupov (TATU, assistent)
S.B.Salimov (TATU, talaba)

Zararkunanda dasturlar paydo bo`lishi uchun, biologik viruslardek, ularning yaratuvchisi bo`lishi kerak. Zararkunanda dasturlar (kompyuter viruslari) tizimga har xil zarar yetkazishi mumkin. Bu zararlarga zararsiz qalqib chiquvchi oynalardan boshlab, hattoki qattiq diskni formatlash bilan yakunlanuvchi jarayonlargacha qarashimiz mumkin. Zararkunanda dasturlardan jabrlanuvchilar har qanday shaxs yoki korxona bo’lishi ehtimoldan holi emas. Uyda foydalanuvchilardan tortib, katta kompaniyalar tarmoq foydalanuvchilari va hukumat foydalanuvchilari ham bu qatorga kiritish mumkin.

Zararkunanda dasturlarni (ZD) tahlil qilish va ularni qidirishning ko’pgina usullari mavjud bo’lib, ular orqali zararli kodlarni aniqlash mumkin. Zararli kodlarni aniqlashning juda keng tarqalgan usullaridan biri ularni statik va dinamik holatda qidirish usulidir. Biz ushbu maqolada ZD kengaytirilgan dinamik tahlilni ko’rib o’tamiz. Tahlilni amalga oshirish uchun kerakli fayllarni (zararli kodlarni) “Practise Malware Analyse” kitobi orqali kerakli manzildan ko’chirib olishimiz mumkin. Bu yo’qoridagi nomi keltirilgan kitobda kengaytirilgan dinamik tahlil haqida umumiy holatda juda ko’plab ma’lumotlar keltirilgan. Zararli kodlarni tez qidirish uchun ularni quyidagi bosqichlar orqali aniqlash kerak bo’ladi:

- Yangi yaratiladigan ZD lar asosan boshqa ma’lum algoritmlardan (antiviruslar qidirish algoritmlaridan) qochish maqsadida yangicha usullar bilan ishlaydi. Ularga qarshi kurashish uchun ularni barcha jihatlarini inobatga olish kerak.

Ko’pincha ZD lar barcha turdagi boshqa viruslarning umumiy kombinatsiyalangan turlarida yaratilib kelinmoqda. Oxirgi bosqichda 4 ta asosiy qism ya’ni:

- ***API*** - Application Programming Interface - Bu orqali zararli kod zararli yoki zararli emasligini u murojaat qilib turgan API funksiyalaridan bilib olish mumkin. Bu usulda faqatgina shubha ostidagi yuklanuvchi fayllarni yuklashni cheklash mumkin.
- ***WinRegistry*** - bu orqali RegShoot dasturnidan foydalangan holatda ZD zararlimi yoki zararli emasligini tekshirish mumkin. Bu jarayon quyidagi bosqichlarni o’z ichiga oladi. Dastur zararli kod yuklanishidan oldingi va yuklanishidan keyingi holatda turgan WinRegistryni farqini oladi va ikkalasini solishtiradi. Bu esa WinRegistryda qilingan barcha o’xgarishlarni yaxlit ravishda ko’rsitiladi. Bu jarayon ZD nima ish lqilishini bilib olish imkonini beradi.
- ***Network*** - tarmoq ZD uchun eng muhim qism hisolanadi. Chunki ZD kerakli barcha maxfiy ma’lumotlarni o’zinig yaratuvchisiga yetkazib berishi kerak va shuning uchun unga taromq kerak bo’ladi. Bu turdagi filtrlar ham ancha qo’l keladi. Negaki, zararli kod qayerga kirib turibdi va u qaysi fayllarni uzatmoqchi bo’layabdi qaysi serverlar bilan muloqotga kirishyabdi, hamma hammasini bilib olishi kerak bo’ladi. Windows operatsion tizimida (OT) NEtFilter - NDIS turdagi driverlar mavjud bo’lib ular yadro darajasida barcha tarmoq paketlarni filtrlash imkoniyatini beradi. Bu bilan esa barcha kiruvchi va chiquvchi tarmoq paketlar nazoratini o’rnatih mumkin. Bundan tashqari Ozeki Software tomonida ishlab chiqilgan WireShark dasturi

orqali ham yaqqol tarzda packetlarni kiruvchi va chiquvchi manzillarni ko'rish ularni qayd etish mumkin. Barcha turdagi tarmoq protokollari ham shu yerda qo'llanilinadi va biz bu yerda filtrlarni o'zimiz maxsus dastur kodlari bilan birga ham berishimiz mumkin bo'ladi.

- ***FileSystem*** **-** bu Windows OT eng yaxshi va kerakli bo'g'ini hisoblanadi, chunki shu tizim orqali barcha yaratiladigan fayllar barcha fayllar bilan bog'langan jarayonlar boshqariladi. Bu yerda FileSystemFilterDriver degan driver mavjud bo'lib u orqlai tizimda bo'ladigan barcha fayllarning monitoringini olish mumkin bo'ladi.

Zararli kodlarni tez qidirish uchun ularni quyidagi kengaytmalar bilan qidirish kerak bo'ladi va ularning ichidagi barcha kodlarini ko'rish kerak bo'ladi.

Hozirgu kunda keng tarqalgan kompyuter viruslari:

- yuklanuvchi fayllar (.exe)
- yorliq fayllar (*.LNK)
- ish stoli foni turidagi (*.scr)
- script fayllar(*.vb,*.com,*.cmd,*.bat)

Kengaytirilgan dinamik tahlil

Kengaytirilgan dinamik tahlilda barcha zararli kodlar virtual mashinada yuklanish orqali tekshiriladi. Bu holatda ular kerakli barcha qiladigan harakatlari nazorat ostida bo'lishi kerak. Agar biror bor xavfli zararli kodni yuklagan taqdirimizda ham virtual mashinamiz buzilishi mumkin xolos.

- ***Virtual Box*** - bu dastur orqali qobit operatison tizim yaratiladi va kerakli shubha ostidagi fayllar shu yerda sinov dan o'tkaziladi.
- ***Strings*** - dasturi orqali dasturning barcha ishlatiladigan o'zgarmas qatorlarni olish mumkin bo'ladi.
- ***ProcessMonitor*** - bu dastur bilan zararli kod yuklanishi va u qayerdan yuklangani va nimalarni yuklagani haqida umumiy ma'lumotl olsih mumkin bo'ladi.
- ***Process Explorer*** - Bu dastur ham biz uchun kerakli bo'lgan kodlarni tahli qilishda ishlatiladi. Farqi shundaki, bunda kerakli protsessni tanlash mumkin va u qiladigan barcah o'zgarishlar fayllarga yozish yoki o'qish registr murojaatlarini ko'rib chiqish mumkin bo'ladi.
- ***Strings*** dasturi orqali yuklanuvchi (*.exe,*.dll) fayllar ichida foydalanilgan barcha qatorlarni olishimiz mumkin. Bu yerda biz uchun kerakli ma'lumotlar: IP manzillar Reg manzillari, yaratilishi mumkin bo'lgan fayl nomlari, kirishi ehtimoli bo'lgan saytlar nomlari bo'lishi mumkin.

Debugging - dastur kodini qadamba-qadam tahlillash

Shu bilan birga biz yana IDA disassembler dasturidan hma foydalanishumiz mumkin. Bu dasturning imkoniyati shundan iboratki, kerakli bo'lgan zararli kodni birinchi kerakli statik tahlilni amalga oshirishimiz mumkin, keyingi bosqich esa dinamik tahlil qilish, yanada to'liq qilib aytadigan bo'lsak kengaytirilgan dinamik tahlilning xuddi o'zginasi deyish mukin. Bu jarayon boshqacha qilib aytganda Debugging jarayoni deyiladi. Jarayonni IDA debugger dasturi orqali zararli kod virtual mashinaga yuklanadi va statik tahlilda ba'zi shubha ostida turgan yoriqnomalarga F2 tugmasi orqali breakpoint (to'xtash nuqtasi) qo'yiladi va shu yerda dastur bajarilishi davomida (yuklangan paytda) breakpointga kelgan payt to'xtash (uzilish) ro'y beradi. Biz usha paytdagi barcha registrlar qiymatlarini ko'rishimiz mumkin.

Debugging jarayonida yuqorida ko'rib turganingizdek barcha funksiyalar argumentlarini ko'rish mumkin bo'ladi. Bu orqali esa biz bemalol qayerga breakpoint qo'yishimizni bilib olishimiz mumkin. Buning natijasida esa ZD operatsion tizimni qaysi registrlar qanday moduldan yoki qaysi dastur nomidan foydalanayotganini aniqlashimiz imkonini beradi.

Shunday qilib, ZD kengaytirilgan dinamik tahlilini amalga oshirish ZD kodlari va ishlash algoritmlarini to'liq o'rganish hamda ulardan himoyalanish uchun maxsus usullar hamda vositalarni aniq tanlash imkoniyatini beradi.

```
push    10Eh                ; uSize
lea     edx, [ebp+Buffer]
push    edx                 ; lpBuffer
call    ds:GetWindowsDirectoryA
push    offset aSystem32Wupd_0 ; "\\system32\\wupdmgr.exe"
lea     eax, [ebp+Buffer]
push    eax
push    offset aSS_0        ; "%s%s"
push    10Eh                ; Count
lea     ecx, [ebp+Dest]
push    ecx                 ; Dest
call    ds:_snprintf
add     esp, 14h
lea     edx, [ebp+var_110]
push    edx                 ; lpBuffer
push    10Eh                ; nBufferLength
call    ds:GetTempPathA
push    offset aWinup_exe ; "\\winup.exe"
lea     eax, [ebp+var_110]
push    eax
push    offset aSS_1        ; "%s%s"
```

1-rasm. ZD Debugging jarayoni

ZD qarshi kurash uchun ZD to'liq tahlilini amalga oshirish va ular foydalanayotgan OT resurslaridan to'liq xabardor bo'lish kerak bo'ladi. Antivirus dasturlarini yaratuvchilar ham ZD larni aniqlash va ularga qarshi kurashish uchun yo'qoridagi tahlil usullaridan keng foydalanib kelishadi. Bu esa o'z navbatida ZD aniqlash va ularga qarshi kurashishda foydalaniladigan eng keng qo'llaniladigan usullardan hisoblanadi.

КОРХОНАДА АХБОРОТ ХАВФСИЗЛИГИ ХАВФ-ХАТАРЛАРИНИ ТАҲЛИЛ ҚИЛИШ УСУЛЛАРИ

Э.Қ. Қахрамонов (ТАТУ, ассистент)

Ҳозирги кунда дунёда ахборот коммуникация технологиялари, маълумотларни узатиш тармоқлари (МУТ) нинг ривожланиши, шу билан бирга, ахборот тизимларининг глобаллашув ва ахборот интеграциялашуви жараёнларии юқори суръатларда давом этмоқда. Ушбу жараёнлар ахборот технологияларининг долзарб муаммоларидан бири ҳисобланган ахборот хавфсизлигини юқори даражада таъминлашни талаб қилади. МУТда ахборот хавфсизлиги (АХ)ни таъминлаш учун биринчи навбатда ахборот хавфсизлиги хавфларини таҳлил қилишимиз керак.

Ушбу мақолада ахборот хавфсизлиги хавфларини таҳлил қилиш усулларини кўриб чиқамиз. МУТда АХни таъминлашда хавфсизлиги таъминланаётган ресурни қийматини билишимиз зарур. Ресурни қиймати унинг бутунлигига, махфийлигига бўладиган бузилишлар тўплами билан аниқланади. Ресурни қийматини баҳолаш – ҳар хил ресурс категориялари учун бўлиши мумкин бўлган зарарларни ҳажми билан аниқланади. МУТда хавфни таҳлил қилишни қуйидаги иккита усулини кўриб чиқамиз.

Асосий усул. Кам меҳнат талаблиги билан ажралиб турувчи хавфни таҳлил қилиш усулидир. Бу усул корхонанинг ахборот ресурслари катта бўлмаганда ишлатилади. Асосий усул корхонада АХ тизими мавжудлигини текширади ва қуйидаги асосий вазифалар орқали амалга оширилади:

- АХ воситаларини мавжудлигини текшириш;
- АХ воситаларини аниқлаш усулларини кўриб чиқиш;
- АХ воситалари тенглигини таҳлил қилиш;
- АХ талаблари тенглигини таҳлил қилиш.

Ушбу усулнинг афзаллик томони ахборот хавфсизлигини бошқариш тизими (АХБТ) воситалари асосида хавфни таҳлил қилишга, ресурслардан минимал сарф-харажат кетишидир. Камчилик томони шундан иборатки, ресурсда ахборотни юқори ҳимоя

воситасига талаб даражаси ўша ресурс учун доимий ошишида билинади. Шу билан бирга корхонанинг ҳимояланадиган ахборот ресурслари катта бўладиган бўлса ушбу усул бўлаётган хавфни таҳлил қила олмайди. Агар барча тизимда АХни фақат минимал талаби таъминланиб, хавфни таҳлил қилишнинг ушбу усули қўлланилса тизим етарлича ишлаб туриши мумкин ва иқтисодий тежамли бўлади, бошқача қилиб айтганда ушбу усул ишласа АХБТ воситаларини қаноатлантиради.

Жадвалли усул. Ҳозирги кунда МУТда хавфни таҳлил қилишнинг жадвалли усулидан фойдаланилади. Бу усулда корхонанинг физик ресурсларини баҳолашни сонли кўрсаткичларини аниқлаш нуқтаи назаридан ишга қобилиятли ресурслар қайта тикланади ёки алмаштирилади. Ресурсларни баҳолашда мавжуд дастурий воситалар ёрдамида уларни қайта тиклаш ёки алмаштиришга кетадиган сарф-харажатлар аниқланади. Умумий ҳолда кўриладиган бўлса, қабул қилинган дастурий таъминот ресурсларни махфийлигига ёки бутунлигига қуйиладиган махсус талабларга эга бўлади. Масалан: дастурий таъминот юқори қийматга эга бўлиши керак, ахборот ресурсларини қийматини ифода этишда бу ресурсларни баҳолаш ўтказилиши керак. Жадвалли усулда салбий таъсирларни келтириб чиқарадиган омиллар ва кўрсатилган заиф жойларда таҳдидларни рўй бериш эҳтимоллиги тасвирланади. Қуйида 1-жадвалда бу усулда хавфни таҳлил қилиш намунаси келтирилган.

Жадвал

Жадвалли усулда хавфни таҳлил қилиш

Таҳдид дескриптори	**A** таҳдид	**B** таҳдид	**C** таҳдид	**D** таҳдид	**E** таҳдид	**F** таҳдид
Салбий таъсирлар кўрсаткичи(a)	5	2	3	1	4	2
Таҳдидни рўй бериш эҳтимоллиги(c)	2	4	5	3	1	4
Хавф кўрсаткичи (d)	10	8	15	3	4	8
Таҳдид анжири(e)	2	3	1	5	4	3

1-босқичда олдиндан аниқланган жадвал бўйича салбий таъсирлар таҳлил қилинади. Масалан, ҳар бир ресурс учун хавфлилик кўрсаткичи аниқланади яъни 1 дан 5 гача (a қатор).

2-босқичда олдиндан берилган жадвал бўйича ҳар бир таҳдидни рўй бериш эҳтимоллиги аниқланади, у ҳам 1 дан 5 гача бўлади (b қатор).

3-босқичда b ва c қаторлар кўпайтирилиб хавф кўрсаткичи ҳисобланади. Ушбу усулдан фойдаланишда хавф кўрсаткичи аниқ ташкил қилиш асосида амалга оширилади.

4-босқичда хавфни келтириб чиқарадиган омиллар бўйича тартибланади.

Ушбу жараён таҳдидларни салбий таъсирлар ҳамда уларни рўй бериш эҳтимоллиги бўйича тартиблашга ва таққослашга имкон беради.

Хулоса қилиб шуни айтиш мумкинки, МУТда АХни таъминлашда хавфсизлиги таъминланаётган ресурни қийматини билишимиз зарур. Ресурни қиймати унинг бутунлигига, махфийлигига бўладиган бузилишлар тўплами билан аниқланади. МУТда АХни таъминлашда хавфни таҳлил қилиш усулларини тўғри танлаш асосий ўрин тутади, яъни ресурс қийматига қараб хавфни таҳлил қилиш усули танланади.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ И ОСНОВНЫЕ ФУНКЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Д.К. Каримова, (ТГТУ, доцент)
М.М. Кадиров, (ТГТУ, старший преподаватель)

В связи с “многопользовательским” режимом работы в компьютерной сети возникает целый набор взаимосвязанных вопросов по защите информации, хранящейся в

компьютерах или серверах компьютерной сети. Следует отметить, что сами сетевые операционные системы также представляют мощные средства защиты от несанкционированного доступа к сетевым ресурсам. Однако, нередки случаи, когда даже такая защита не срабатывает. Практика показывает, что несанкционированный пользователь, имеющий достаточный опыт в области системного и сетевого программирования, задавшийся целью подключиться к сети, даже имея ограниченный доступ к отдельным ресурсам, рано или поздно все равно может получить доступ к некоторым защищенным ресурсам сети. Поэтому возникает необходимость в создании дополнительных аппаратных и программных средств защиты сетевых ресурсов.

К аппаратным средствам защиты относятся различные сетевые экраны, фильтры, устройства шифрования протокола и т.д. К программным средствам защиты можно отнести: программы шифрования данных; программы слежения сетевых подключений (мониторинг сети); программы аутентификации и идентификации и т.д.

При разработке крупномасштабных компьютерных сетей возникает проблема обеспечения взаимодействия большого числа компьютеров и серверов, т.е. проблема поиска оптимальных топологий. Важнейшим компонентом локальных и корпоративных сетей является их системная топология, которая определяется архитектурой межкомпьютерных связей.

Известно, что в компьютерных сетях для обеспечения безопасности подлежит обработке критическая информация.

Под термином «критическая информация» понимается информация: с различными грифами секретности; информация для служебного пользования; информация, составляющая коммерческую тайну или тайну фирмы; информация являющаяся собственностью некоторой организации или частного лица. На рис.1. представлены типичные уязвимые места компьютерных сетей. С точки зрения безопасности компьютерные сети обладают следующими недостатками:

- разделение ресурсов. Поскольку ресурсы и загрузка распределяются по различным узлам сети, многие пользователи имеют потенциальную возможность доступа к сети как к единой компьютерной системе. Иными словами, получив доступ к одной из систем, входящих в сеть, пользователь (или захватчик) имеет реальную возможность атаковать другие системы сети;

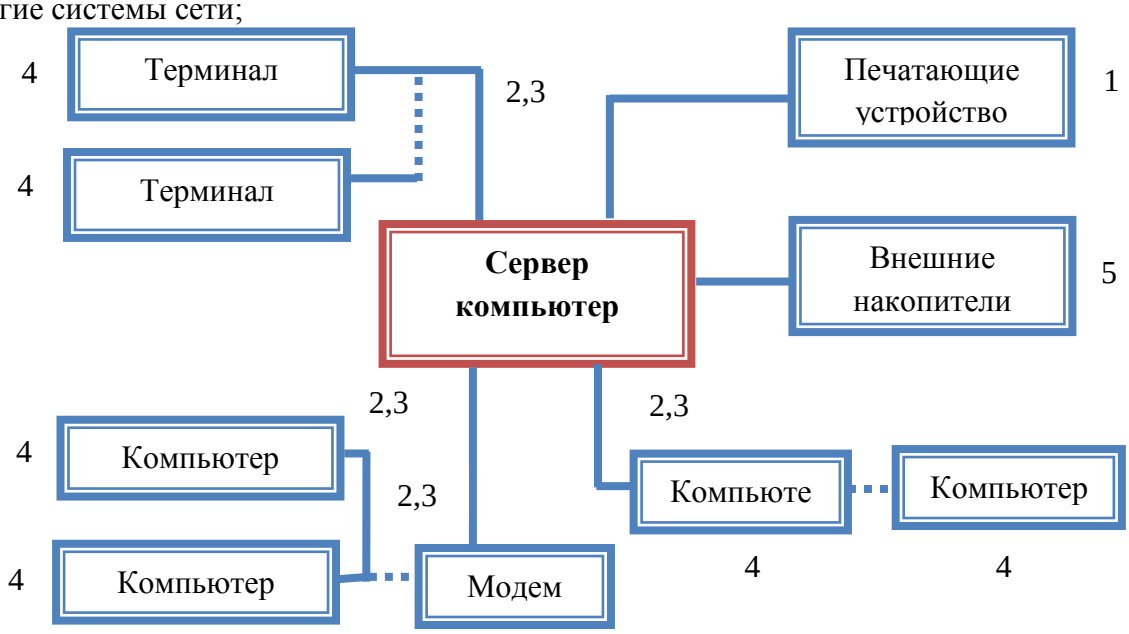


Рис.1. Типичные уязвимые места компьютерных сетей (1-кража результатов выдачи, 2-неразрешенное подключение, 3-неправильная работа линии связи, 4-неправильная работа пользователя, 5-кража внешних носителей информации).

- сложность системы. Во всякой компьютерной системе имеется операционная

система, представляющая сложный комплекс взаимодействующих программ. В силу этого обстоятельство трудно сформулировать четкие требования безопасности, особенно к общецелевым сетям, разрабатывавшимся без учета безопасности;

- неопределенная периферия. На уязвимость сети сильно влияет невозможность определения, в большинстве случаев, точных пределов сети. Один и тот же узел может одновременно работать в нескольких сетях, и следовательно, ресурсы одной сети вполне могут использоваться с узлов, входящих в другую сеть. Такое широкомасштабное разделение ресурсов, несомненно, преимущество. Однако, неопределенное количество потенциально неподготовленных пользователей и потенциальных захватчиков значительно осложняет обеспечение безопасности как сети в целом, так и большинства ее отдельных узлов;

- множественность точек атаки. В отдельной компьютерной системе, можно контролировать доступ к системе пользователей, поскольку этот доступ осуществляется с терминалов компьютерной системы. Ситуация в сети совершенно иная: к одному и тому же файлу может быть затребован так называемый удаленный доступ с различных узлов сети. Поэтому, если администратор отдельной системы может проводить четкую политику безопасности в отношении своей системы, то администратор узла сети лишен такой возможности;

- неизвестная траектория доступа. Пользователь или захватчик может затребовать доступ к ресурсам некоторого узла сети, с которым данный узел не связан на прямую. В таких случаях доступ осуществляется через некоторый промежуточный узел, связанный с обоими узлами, или даже через несколько промежуточных узлов. В условиях сети весьма не проста точно определить, откуда именно пришел запрос на доступ, особенно если захватчик приложит немного усилий к тому, чтобы скрыть это;

- слабая защищенность линии связи. Сеть тем и отличается от отдельной системы, что непременно включает в себя линии связи по которым между узлами передаются данные. Это может быть элементарный провод, а может быть линия радиосвязи, в том числе и спутниковый канал. При наличии определенных условий (и соответствующей аппаратуры) к проводу можно незаметно (или почти незаметно) подсоединиться, радиолинию можно успешно прослушивать - т.е. ничто не препятствует тому, чтобы «выкачивать» передаваемые сообщения из линий связи и затем выделять из всего потока требуемые.

На основе анализа угроз безопасности компьютерных сетей можно сделать выводы о свойствах и функциях, которые должна обладать система обеспечения безопасности корпоративной сети (КС).

1. Идентификация защищаемых ресурсов, т.е. присвоение защищаемым ресурсам идентификаторов- уникальных признаков, по которым в дальнейшем система производит аутентификацию.
2. Аутентификация защищаемых ресурсов, т.е. установление их подлинности на основе сравнения с эталонными идентификаторами.
3. Применение парольной защиты ресурсов.
4. Разграничение доступа пользователей к КС.
5. Разграничение доступа пользователей по операциям (чтение, запись, модификация и т.п.) над ресурсами (программы, файлы, каталоги, диски, сервера и т.д.) с помощью программных средств администрирования.
6. Регистрация событий: вход пользователя в сеть, выход из сети, нарушение прав доступа к защищаемым ресурсам и т.д.
7. Реакция на факты нарушения прав доступа к защищаемым ресурсам сети несанкционированного подключения к КС.
8. Обеспечение защиты информации при проведении ремонтно-профилактических работ.

KOMPYUTER TIZIMLARINI HIMOYALASHDA IKKI OMILLI AUTENTIFIKATSIYALASH USULINING O'RNI

D.Y. Irgasheva (TATU, dekan)
I.M. Nabiyev (TATU, 2-kurs magistranti)

Hozirgi kunda dunyo miqyosida axborot texnologiyalarining jadal sur'atlar bilan rivojlanib borishi qulayliklar bilan bir qatorda yangi muammolarni o‘rtaga qo‘ymoqda. Avtomatlashtirilgan axborot tizimlarida va telekommunikasiya tizimlarida aylanayotgan axborotlar to‘plamiga bo‘lgan tahdidlar keskin oshdi, ayniqsa, Internet paydo bo‘lgandan boshlab, axborot o‘g‘irlash va axborot mazmunini buzib qo‘yish hollari ko‘paydi. Shu sababli ham hozirgi kunda axborotlarni ruxsat etilmagan shaxslar tomonidan foydalanishlarga chek qo'yish masalasi axborot xavfsizligini ta'minlash borasidagi eng asosiy masalalardan biri sifatida qaralmoqda.

Albatta bunday muammoni hal etishda, asosiy masala foydalanuvchining haqiqiy ekanligini tekshirish jarayoni ya'ni autentifikatsiya hisoblanadi.

Hozirgi kunda autentifikatsiyalashning turli xil usullari mavjud bo‘lib, bularga:

- parollar asosida autentifikatsiyalash;
- sertifikatlar asosida autentifikatsiyalash;
- qat'iy autentifikatsiyalash;
- foydalanuvchilarni biometrik identifikatsiyalash va autentifikatsiyalash kabilar kiradi.

Yuqorida keltirilgan autentifikatsiyalash usullarining deyarli barchasi bir omilga asoslangan autentifikatsiyalash usullari bo'lib, barchasining kamchilik tomonlari mavjud. Parollar asosida autentifikatsiyalash jarayonini oladigan bo'lsak uning kamchilik tomoni shundan iboratki:

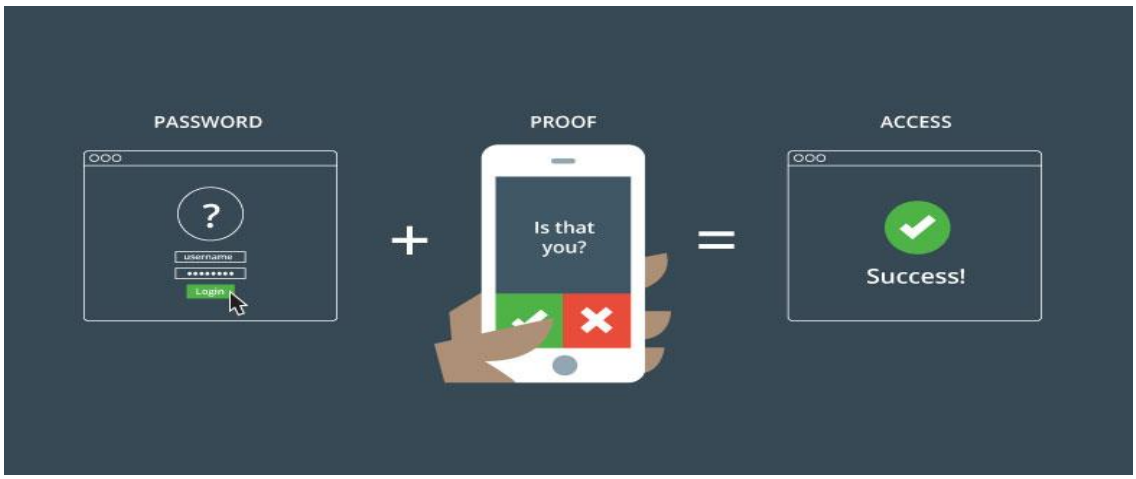
Himoyani mustahkam taminlash uchun parollarni uzunroq hamda turli simvollardan iborat bo'lgan holda qo'yish talab etiladi. Bu o'z navbatida foydalanuvchilarga noqulaylik tug'diradi, chunki murakkab parollarni eslab qolish juda ham qiyin bo'lib, ko'p hollarda foydalanuvchilar ularni yoddan chiqib qo'yishadi. Oddiy qisqa simvollardan tashil topgan parollar qo'yiladigan bo'lsa bunday parollar xavfsizlik talablariga javob bermaydi. Ya'na shuni aytib o'tish joizki qo'yilgan parolni boshqa bir shaxs bilib olgudek bo'lsa u ruhsat etilmagan tizimga bemalol kirishi undagi ma'lumotlardan foydalanishi, o'g'irlashi, mazmunini o'zgartirishi hamda uni yo'q qilishi mumkin bo'ladi.

Qat'iy autentifikatsiyalashda tekshiriluvchi taraf qandaydir sirni bilishni namoyish etgan holda tekshiruvchiga o‘zining haqiqiy ekanligini isbotlaydi. Bu usulning kamchilik taraflaridan biri shuki, birinchidan: birmarta va ko‘p marta foydalaniladigan parollarga asoslanadi, hamda ma'lumotlarni kriptografik usullarini generatsiyalab beruvchi dastur kerak bo‘ladi.

Ko‘p martalik parollardan foydalanishning xavfsizligi darajasi past bo‘lib, bunday parollarni niyyati buzuq shaxslar maxsus algoritmlarga asoslangan holda bilib olishlari mumkin bo'ladi.

Bu kabi kamchiliklar yuqorida keltirilgan boshqa autentifikatsiyalash usullarida ham mavjud. Yuqorilardagi autentifikatsiyalash usullaridagi kamchiliklarni hisobga olgan holda juda muhim ma'lumotlar saqlanadigan davlat organlarida, boshqaruv aparatlarining kompyuter tizimlarida ikki omilli autentifikatsiyalash usullaridan foydalanish yaxshi samara beradi.

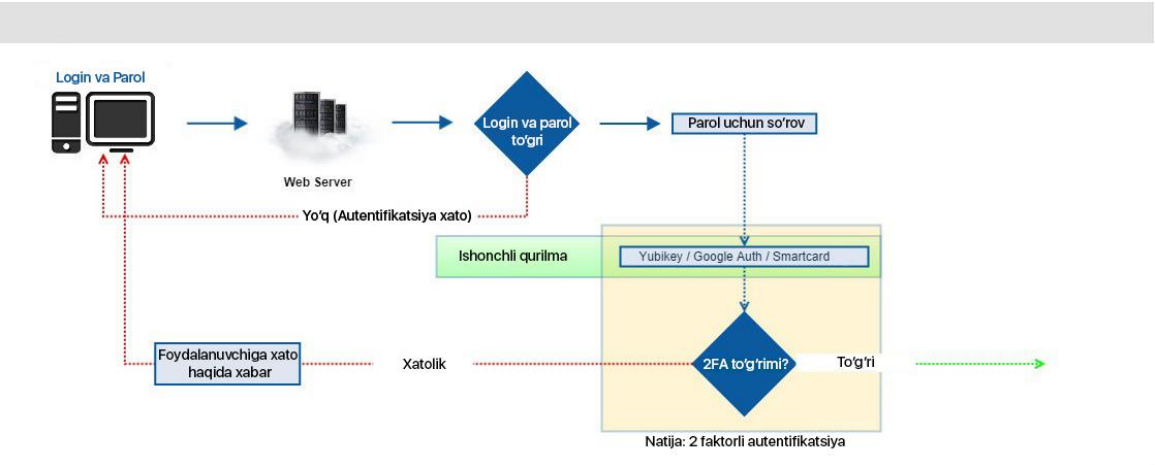
Ikki omilli autentifikatsiya foydalanuvchini aslida haqiqiy va kim ekanligini verifikatsiya qilish uchun ikki qadamdan iborat bo'lgan xavfsizlik jarayoni hisoblanadi *(1-rasm).*



1-rasm. Ikki omilli autentifikatsiya jarayoni

Ikki omilli autentifikatsiyani yaxshi tushunish uchun bir omilli autentifikatsiyani eslaymiz. Bunda foydalanuvchidan biror bir xavfsizlikni ifodalovchi so'rov so'ralar edi. Masalan oddiygina parolni misol keltirish mumkin. Ikki omilli autentifikatsiyada bundan farqli o'laroq, ikkinchi turdagi biror bir omil ham so'raladiki, bunda ushbu omil shu foydalanuvchi uchun identifik bo'lishi shart. Bunday autentifikatsiyalash jarayonlarida ularning biror hissiyoti, odati, tana a'zosi kabi turkumdagi omillar identifik vazifasini bajaradi. Shu uslubda faqatgina bitta omilli paroldan farqli ravishda foydalanuvchining barmoq izi, ko'z gavhari joylashuvini skanerlash, yurish uslubini skanerlash yoki yuz ko'rinishining ifodalanishi kabi qo'shimcha omillar orqali kompyuter tizimlarining xavfsizlik darajasini yanada mukammallashtirish mumkin.

Quyida ikki yoki undan ko'p omillarga ega bo'lgan autentifikatsiya usullarini blok-sxemasini keltirib o'tamiz (2-rasm):



2-rasm. Ikki yoki undan ko'p omillarga asoslangan autentifikatsiyaning blok-sxemasi

Ikki bosqichli autentifikatsiya omillari nimalar bo'lishi mumkin va ulanrni qanday turlarga bo'lish mumkin degan savol tug'ilishi tabiiy. Quyida ushbu usullarni keltirib o'tamiz:

1. Bilimga oid omillar: bunga misol qilib, faqatgina foydalanuvchining o'zi bilishi mumkin bo'lgan parol, PIN kod yoki boshqa shaxslar tomonidan ulashilgan sirlarni keltirish mumkin.
2. Egalik qilishga oid omillar: bunga misol qilib esa, biror ID kartasi, RFID kartalar, biror ko'rinishdagi qurilmalar (smartfon, telefon yoki kompyuterlar)ni misol qilib keltirishimiz mumkin bo'ladi.
3. Jismoniy tegishlilikka oid omillar: bu turdagi autentikatsiya turlari odatda biometrik omillar ham deb ataladi. Bu kabi omillar foydalnuvchiga jismoniy jihatdan aynan tegishli bo'lgan omillar bo'lib, bular barmoq izlari, yuz ko'rinishi yoki ovoz tonlarining farqlanishi orqali

yuzaga chiqadi.

Ayni kunda ko'pgina kompyuter tizimlari yuqoridagi omillardan tashqari, geografik manzildan qilinadigan murojaatlar turiga qarab, murojaat vaqtiga qarab yoki shu turdagi boshqa omillarga tayangan holda 2 yoki undan ko'p qavatlardan iborat multi-omilli autentifikatsiya usullarini ham ishlatishmoqda.

Xulosa qilib shuni aytishimiz mumkinki, ikki omilli autentifikatsiyalash usuli bir omilli autentifikatsiyalash usullariga qaraganda xavfsizligi yuqori hamda ishonchli bo'lib, ular yordamida juda muhim ma'lumotlar saqlanadigan davlat organlari, boshqaruv aparatlarining kompyuter tizimlarida saqlanayotgan axborotlarni ishochli himoya qilish imkoniyati mavjud.

SIMMETRIK KRIPTOTIZIMLAR UCHUN ISHLAB CHIQILGAN KALITLARNI TASODIFIYLIKKA TEKSHIRUVCHI TESTLARNING TAHLILI

S.K. G'aniyev (TATU, t.f.d., professor)
I.S. Olimov (TATU, magistr)

Hozirgi zamon kriptografiyasida bardoshli kalitlarni ishlab chiqish dolzarb muammolardan biridir. Chunki har bir kriptotizimda kalit parametri muhim ahamiyatga ega. Kriptotizim bardoshliligi kalitning qanchalik tasodifiyligiga bog'liq bo'lib, tasodifiy sonlar ketma-ketligini hosil qilish ancha murakkabligi, buning o'rniga esa psevdotasodifiy ketma-ketliklardan foydalanish, psevdotasodifiy ketma-ketliklarni ishlab chiqish muhim vazifa ekanligini anglatadi.

Tasodifiylikka tekshiruvchi testlar 2 xil bo'ladi:

Grafik testlar - grafik testlar foydalanuvchiga tekshirilayotgan ketma-ketlikning ma'lum bir grafik bog'liqligi haqidagi ma'lumotni berib, u bo'yicha tekshirilayotgan ketma-ketlik xossalari to'g'risida xulosa chiqarish imkoniyatini beradi.

Baholash testlari - baholash testlari tekshirilayotgan ketma- ketlik statistik xossalarini taxlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi.

Tasodifiy va psevdotasodifiy ketma-ketliklarni tasodifiylikka tekshiruvchi testlar ko'rib o'tildi. PTSKK tanlashda tasodifiylikka tekshiruvchi testlar muhim ahamiyat kasb etadi. Shunga ko'ra PTSKK qanchalik ko'p tasodifiylikka tekshiruvchi testlardan o'tsa, generator shuncha kriptobardoshli deb topiladi.

Quyidagi jadvalda ushbu tasodifiylikka tekshiruvchi testlarning qiyosiy tahlili keltirilgan.

1-jadval

Tasodifiylikka teshiruvchi testlarning qiyosiy tahlili

Test/ Xususiyat Lar	**Kiruvchi ketma-ketlik uzunligi**	**Asoslanishi**	**Maqsadi**	**Hisoblash darajasi**
Monobit test	100 bit kamida	Nollar va birlar miqdorini hisoblashga	Nollar va birlar orasidagi farqni hisoblash	Taxminiy
Block Frequency Test	100 bit kamida	M bit uzunlikda birlar sonini topishga	Olingan miqdorni kutilgan miqdorga tengligini (m/2) hisoblaydi	Taxminiy, blok uzunligiga bog'liq

Cumulative Sums (Cusum) Test	100 bit kamida	Birlar va nollar miqdorini hisoblashga	Bir va nollar miqdorini tengligini hisoblash	Taxminiy
Runs Test	100 bit kamida	Birlar va nollar miqdorini hisoblashga	Birlar va nollar oraliqlari sonini kutilgan miqdorga tengligini	Taxminiy
Long Runs of Ones Test	128 bit kamida	Ketma-ket Kelgan birlar Sonini hisoblashga	Har bir qismdagi birlar miqdorini kutilganiga qanchalik yaqinligini	Taxminiy
Rank Test	Kamida 38 ta 32x32 matritsa	Matritsa rangini hisoblashga asoslangan	Xar bir qismni bir-biriga bog'liqlik darajasini	Taxminiy
Discrete Fourier Transform	1000 bit kamida	Diskret Fure almashtirish	Davriylik xususiyatini tekshirish	Taxminiy
Non overlapping Template Matchings Test	1 mil. bit kamida	Kiritilgan ketma-ketlikni xosil bo'lish sonini hisoblash	Tanlangan ketma-ketlikni ko'rinmaslik miqdorini	Taxminiy, tekshiriluvchi qism bitga bog'liq
Overlapping Template Matchings Test	1 mil. bit kamida	Kiritilgan ketma-Ketlikni xosil bo'lish sonini hisoblash	Tanlangan ketma-ketlikni ko'rinishlar miqdorini	Taxminiy, tekshiriluvchi qism bitga bog'liq
Universal Statistical Test	Katta uzunlikdagi	Bir xil qismlarni topishga asoslangan	Ketma-ketlikni qisilish uzunligini ko'rsatadi	Taxminiy
Serial Test	Katta uzunlikda	qismlarni paydo bo'lish chastotasini	m-bitli tekshirishda o*m* ~ *2* paydo bo'lish darajasini toppish	Taxminiy
Random Excursions Test	1 mil. Bit	Oraliqda kutilgan Xodisani ko'rinishlar sonini xisobolash	Qism ketma-ketliklarni tasodifiylikka tekshirish	Aniq
Random Excursions Varian Test	1 mil. bit	Oraliqda kutilgan xodisani ko'rinishlar sonini xisobolash	Qism ketma-ketliklarni tasodifiylikka tekshirish	Aniq

Linear Complexity Test	1 mil. bit kamida	Ketma-ketlik oralig'ini hisoblash	O'xshash qismlar orasidagi uzunlikni hisoblash	Taxminiy, blok uzunligiga bog'liq
Xi-kvadrat	Katta uzunlikdagi PTSKK	Olingan va kutilgan natijalar farqini hisoblashga	PTSKK birlar va nollar miqdori ulushini hisoblash	Taxminiy, bardoshsiz kalitga bog'liq
Kol-Smirnov	Kichik uzunlikdagi PTSKK	Olingan va Kutilgan natijalar Farqini hisoblashga	Kichik va katta oqishlarni hisoblash	Aniq

Ushbu tasodifiylikka tekshirish testlari bir-biridan kirish parametrlari va tekshirish usuliga ko'ra farq qiladi. Bu o'rinda shuni hisobga olish kerakki barcha testlarning asosi va testlashning birlamchi sharti sifatida Xi-kvadrat testi olinadi.

PTSKK ni tasodifiylikka tekshirishda ushbu testlar to'plamidan foydalanishda shuni e'tiborga olish kerakki agar psevdotasodifiy ketma-ketlik qanchalik ko'p testlashdan o'tsa uning tasodifiyligi shuncha yuqori hisoblanad

Xulosa:

− psevdotasodifiy ketma-ketlik bloklari belgilarini tasodifiylikka tekshiruvchi testlar haqida fikr va mulohazalar bildirilib, ularning grafik va baxolash testlaridan iboratligi izohlandi;

− keltirilgan testlarning ishlash prinsipi, kirish ketma-ketlik uzunligi va hisoblashning aniqligi bo'yicha tahlil qilindi;

− yakuniy xulosa sifatida shuni aytish mumkinki, ushbu testlash usullari PTSKK testlashda muhim ahamiyat kasb etib, ulardan foydalanish sifatiga, kiruvchi ketma-ketlik uzunligi va soniga bog'liq bo'ladi.

ИСПОЛЬЗОВАНИЕ МАТРИЦЫ УСТАНОВЛЕНИЯ ПОЛНОМОЧИЙ В РАЗГРАНИЧЕНИИ ДОСТУПА

М.М. Кадиров (ТГТУ, старший преподаватель)
М.М. Кадиров (ТГТУ, студент)

Для защиты от несанкционированного входа в персональную компьютерную систему могут использоваться как общесистемные, так и специализированные программные средства защиты. После идентификации и аутентификации пользователя система защиты должна определить его полномочия для последующего контроля санкционированности доступа к компьютерным ресурсам. Полномочия пользователя считываются из базы эталонных данных системы защиты и заносятся в базу данных активных пользователей, которая для достижения более высокой производительности компьютера может располагаться в разделах его оперативной памяти.

При функционировании компьютера система защиты должна постоянно контролировать правомерность доступа пользователей к ресурсам вычислительной системы. Для этого при попытке доступа любого пользователя к какому-либо компьютерному ресурсу система защиты должна проанализировать полномочия этого пользователя, считав их из базы данных активных пользователей, и разрешить доступ только в случае соответствия запроса на доступ пользовательским полномочиям. В случае многопользовательского режима работы компьютера (сервера) для определения системой защиты идентификатора пользователя, пытающегося осуществить доступ к ресурсу, каждой запущенной программе присваивается идентификатор пользователя, который ее запустил.

Процесс определения полномочий пользователей и контроля правомерности их доступа к компьютерным ресурсам называют разграничением доступа, а подсистему защиты, выполняющую эти функции - подсистемой разграничения доступа пользователей к ресурсам КС. Эффективной может быть только та политика разграничения доступа, в основу которой положен принцип - «запрещено все, что не разрешено», а не «разрешено все, что не запрещено». Если при попытке доступа пользователя к ресурсам КС подсистема разграничения определяет факт несоответствия запроса на доступ пользовательским полномочиям, то доступ блокируется, и могут предусматриваться следующие санкции за попытку несанкционированного доступа:

♦ предупреждение пользователя;

♦ отключение пользователя от вычислительной системы на некоторое время;

♦ полное отключение пользователя от системы до проведения административной проверки;

♦ подача сигнала службе безопасности о попытке несанкционированного доступа с отключением пользователя от системы.

Разграничение доступа на основе матрицы установления полномочий является более гибким и удобным в сравнении с разграничением по спискам, так как позволяет всю информацию о пользовательских полномочиях в базе эталонных данных системы защиты хранить и использовать в виде матриц (таблиц), а не в виде разнотипных списков.

В матрице, или как ее еще называют, таблице полномочий строками являются идентификаторы пользователей, имеющих доступ в систему, а столбцами - ресурсы вычислительной системы. Каждая ячейка таблицы для заданного пользователя и ресурса может содержать следующую информацию:

♦ размер предоставляемого ресурса, например, размер области внешней памяти;

♦ имя компонента предоставляемого ресурса, например, имя каталога или логического диска;

♦ код, определяющий права доступа к ресурсу, например, 01_2 -только чтение, 10_2 - чтение и запись и т.д.;

♦ ссылку на другую информационную структуру, задающую права доступа к ресурсу, например, ссылку на другую матрицу полномочий;

♦ ссылку на программу, регулирующую права доступа к ресурсу.

Программа, регулирующая права доступа пользователя к ресурсу, может регулировать права доступа не только в зависимости от времени, но и в зависимости от предыстории работы пользователя, например, пользователь Foydalanuvchi_33 может записывать данные в файл F только в том случае, если он уничтожил файл G. Также может учитываться и состояние КС, например, текущий размер свободной части ресурса.

В качестве простейшего примера матрицы полномочий можно привести следующую таблицу:

	Каталог D:\HUJJAT	Каталог D:\KIRITISH	Каталог D:\NATIJA
Пользователь Foydalanuvchi_1	10	01	10
Пользователь Foydalanuvchi_2	10	10	00
Пользователь Foydalanuvchi_3	00	10	01
……	……..	……..	……..
Пользователь Foydalanuvchi_N	10	00	00

В данной таблице каждая ячейка содержит двоичный код, задающий права доступа к ресурсу: 01 - только чтение, 10 - чтение и запись, а 00 - запрет доступа.

Упрощенная схема обработки запроса на доступ к ресурсу при использовании матрицы установления полномочий представлена на рисунке 1.

Недостатком метода разграничения доступа на основе матрицы полномочий является то, что для большой КС данная матрица может оказаться слишком громоздкой.

Преодолеть данный недостаток можно путем выполнения следующих рекомендаций по сжатию матрицы установления полномочий:

♦ объединение пользователей, имеющих идентичные полномочия в группы;

♦ объединение ресурсов, полномочия на доступ к которым совпадают;

♦ комбинирование метода разграничения доступа на основе матрицы полномочий с методом разграничения по уровням секретности.

Рис. Схема обработки запроса на доступ к ресурсу при использовании матрицы полномочий

Следует отметить, что если задача разграничения доступа пользователей к компьютерным ресурсам является особенно актуальной и КС основана на высокопроизводительной аппаратной базе, то для эффективного контроля установленных полномочий пользователей целесообразно использование операционных систем, имеющих встроенные средства разграничения, либо использовать наложенные средства защиты информации.

CURRENT INTRUSION DETECTION AND PREVENTION METHODOLOGIES

P.Kh. Oripov (TUIT, assistant)

Intrusion detection is a significant focus of research in the security of computer systems and networks. This paper presents an analysis of the progress being made in the development of effective intrusion detection systems for computer systems and distributed computer networks.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

Intrusion detection technologies use many methodologies to detect incidents. Primary classes of detection methodologies: signature-based, anomaly-based, and stateful protocol analysis, respectively. Most Intrusion detection technologies use multiple detection methodologies.

Signature-Based Detection

A signature a pattern that corresponds to a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible incidents.

Examples of signatures are as follows:

- A telnet attempt with a username of “root”, which is a violation of an organization’s security policy
- An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware
- An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled.

Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. For example, if an attacker modified the malware in the previous example to use a filename of “freepics2.exe”, a signature looking for “freepics.exe” would not match it. Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations. Signature-based detection technologies have little understanding of many network or application protocols and cannot track and understand the state of complex communications. For example, they cannot pair a request with the corresponding response, such as knowing that a request to a Web server for a particular page generated a response status code of 403, meaning that the server refused to fill the request. They also lack the ability to remember previous requests when processing the current request. This limitation prevents signature-based detection methods from detecting attacks that comprise multiple events if none of the events contains a clear indication of an attack.

Anomaly-Based Detection

Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. For example, suppose thata computer becomes infected with a new type of malware. The malware could consume the computer’s processing resources, send large numbers of e-mails, initiate large numbers of network connections, and perform other behavior that would be significantly different from the established profiles for the computer.

Stateful Protocol Analysis

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. The “stateful” in stateful protocol analysis means that the Intrusion is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. The “protocol analysis” performed by stateful protocol analysis methods usually includes reasonableness checks for individual commands, such as minimum and maximum lengths for arguments. If a command typically has a username argument, and usernames have a maximum length of 20 characters, then an argument with a length of 1000 characters is suspicious. If the large argument contains binary data, then it is even more suspicious.

The typical components in an IDPS solution are sensors or agents, management servers, database servers, and consoles. Sensors and agents monitor and analyze activity; sensors are used to monitor networks and agents to monitor hosts. Management servers receive information from sensors or agents and manage

them. Database servers are repositories for event information recorded by the sensors or agents and management servers. Consoles are programs that provide interfaces for IDPS users and administrators. These components are connected organization’s standard networks or through a separate network strictly designed for security software management known as a management

network. A management network helps to protect the IDPS from attack and to ensure it has adequate band width under adverse conditions.

In conclusion, a network-based IDPS monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols are identified suspicious activity for protecting network.

TARMOQ TIZIMLARI MONITORINGI VA VOSITALARINI TAHLIL ETISH

M.A. Rashidov (TATU, magistrant)

Hozirgi vaqtda axborot kommunikatsiya texnologiyalarini rivojlanishi tarmoq tizimlarida bir qancha muammolarni paydo bo'lishiga imkoniyat yaratdi. Bularga misol qilib tarmoqda bo'ladigan hujumlar va tahdidlarni oshib borishi kompyuter tizimlari va tarmoqlarini zaiflashiga imkon yaratib berdi. Shu muammolarni qisman echishda tarmoq tizimlari monitoringidan foydalanish maqsadga muvofiqdir.

"Lokal tarmoqlar" (LAN, Local Area Network) aynan, lokal deganda shunday tarmoqlarni tushinish kerakki, o'lchamlari katta bo'lmagan bir biriga yaqin joylashgan kompyuterlarni birlashtiradi. Bunday izohlarni aniq emasligini tushunish uchun ayrim lokal tarmoqlarni xarakteristikalarini ko'rish yetarli bo'ladi. Masalan, ayrim lokal tarmoqlar bir necha kilometr yoki o'nlab kilometrlar masofadagi aloqani oson ta'minlaydi. Boshqa tomondan, global tarmoqlar bo'yicha (WAN, Wide Area Network yoki GAN, Global Area Network) bir xonadagi qo'shni stollarda joylashgan kompyuterlar birlashishi mumkin, buni esa negadir hech kim lokal tarmoq deb atamaydi. Shuningdek, bir biriga yaqin joylashgan kompyuterlar kabel orqali ulanishi mumkun. Bunday aloqa lokal tarmoq deyiladi.

Haqiqatdan ham, real holatda ko'pincha lokal tarmoq ikkitadan bir necha o'nlab kompyuterlarni birlashtiradi. Bir xil lokal tarmoqlarning imkoniyatlari yuqori: abonentlarni maksimal soni mingacha yetishi mumkin.

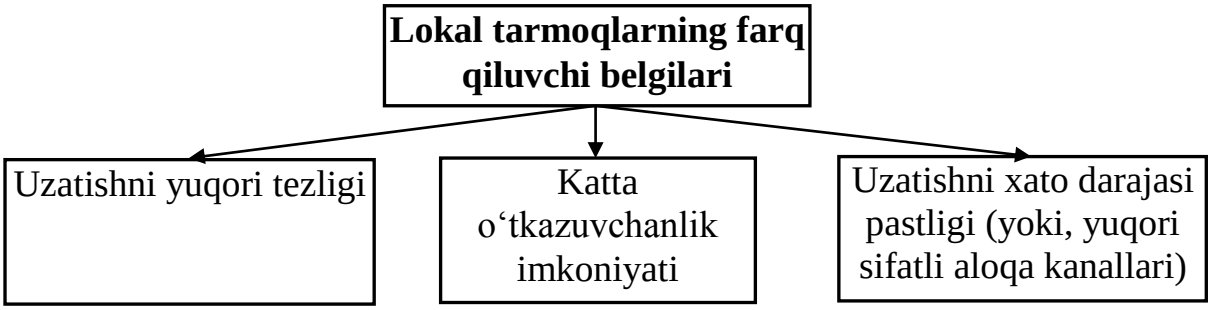
Bir xil mualliflar lokal tamoqni "ko'p kompyuterlarni bevosita ulash uchun sistema" deb ifodalashadi. Bunda faraz qilinadiki, ma'lumot kompyuterdan kompyuterga vositachilarisiz bir xil muhitda uzatiladi. Biroq, zamonaviy lokal tarmog'ida bir xil muhitda uzatish to'g'risida gapirish to'g'ri kelmaydi. Masalan, bir tarmoq ichida ham har xil turdagi kabellar ishlatiladi. "Vositachilarsiz" uzatish deb ifodalash ham juda aniq emas, chunki zamonaviy lokal tarmoqlarda har xil konsentratorlar, komutatorlar, marshrutizatorlar, ko'priklar ishlatiladi. Ular uzatiladigan ma'lumotni juda murakkab qayta ishlashini amalga oshiradi.

Lokal tarmog'i bilan bog'langan kompyuterlar bir virtual kompyuterga birlashadi, uning resurslariga hamma foydalanuvchilar kirishi mumkin bo'ladi, lekin bu kirish bevosita har bir alohida kompyuterga kiradigan resurslarga qaraganda uncha qulay emas.

Bu holatda qulaylik deganda birinchi navbatta kirishni yuqori real tezligi tushiniladi, qo'shish orasidagi ma'lumotlar bilan almashish foydalanuvchi uchun bilinmasdan amalga oshiriladi. Bunday ifodalashdan kelib chiqadiki, lokal tarmoqda uzatish tezligi eng ko'p tarqalgan kompyuterlarni ishlash tezligi oshishi bilan albatta oshishi kerak. Shu sababli lokal tarmoqlar uchun maxsus o'tkazilgan sifatli aloqa liniyalaridan foydalaniladi.

Agar tarmoqda foydalanadigan almashuvni boshqarish mexanizmi unga effektiv bo'lmasa, unda uzatish uchun kompyuterlar o'z navbatini xaddan tashqari uzoq kutishi mumkin va keyin uzatish eng katta tezlikda olib boriladigan va butunlay xatosiz bo'lsa ham tarmoqdan foydalanuvchiga bu baribir barcha tarmoqdagi resurslarga kirish to'g'ri kelmaydigan ushlab qolishlarga aylanadi. Har qanday almashuvni boshqaradigan mexanizm kafolatli shunday ishlashi mumkinki, agar kompyuterlar, abonentlar, uzellar tarmoqqa ulanishi oldindan ma'lum bo'lsa.

Lokal tarmoqlarning farq qiluvchi belgilari quyidagi rasmda keltirilgan.



Rasm. Lokal tarmoqlarning farq qiluvchi belgilari sxemasi

Ma’lumotlar uzatish qo‘yiladigan extimollik xatosi 10~7–10~8 bo‘lishi kerak:

- samarali tezlik bilan almashuvni boshqarish mexanizmi;
- chegaralangan, tarmoqqa ulanadigan aniq ma’lum bo‘lgan kompyuterlar soni.

Tarmoqni monitorlash bu bizga tarmoqda buladigan yoki bo’lishi mumkun bo’lgan hujumlarni va tarmoqdagi nosozliklarni aniqlash va uni cheklash imkonini beradi. Tarmoq monitoringi asosan tashkilot yoki muassasa administratorlari tomonidan bajarilishi mumkun.Tarmoqni monitorlash bizga ko’pgina afzallik yaratadi. Masalan: ma’lumotlar almashinuvini sekinlashini oldini olish tarmoqda ro’y berayotgan hujumlarni aniqlash foydalanuchilarni nazorat qilishdir. Bundan korinib turibdiki har bir administrator tarmoqni monitoring qilishi uning ish faoliyatidan yoki bilim va ko’nikmalaridan kelib chiqqan xolda o’tkaziladi. Tarmoq monitoringidan foydalanib kompyuterlar haqida ma’lumot yoki ularni inventarizatsiya qilishimiz mumkun. Bu tizimning foydali jixati shundaki bu bizga qog’ozdan elektron ko’rinishga o’tish va vaqtni tejash, hamda jismoniy haraktani kamaytirish imkonini beradi. Bu tizimdan foydalanib istalgan kompyuter yoki istalgan hodim, foylanuvchi tarmoqda bajarayotgan ishini nazorat qilish mumkun.

Hisoblash texnikasi paydo bo‘lishidan boshlab, kompyuterlar orasida ma’lumotlar uzatish bo‘lgan. U har bir kompyuterni birgalikda ishlashini tashkil etishga imkon yaratadi. Bir masalani kompyuterlar yordamida yechishga, har bir kompyuterni faqat bitta funksiyani bajarishga maxsuslashtiradi, resurslardan birgalikda foydalanish va boshqa ko‘p muammolarni yechish imkonini beradi.

WEB SAYTLARNI XAVFSIZLIGINI TAMINLASHDA HUJUM TURLARI VA USULLARINI TAHLILI

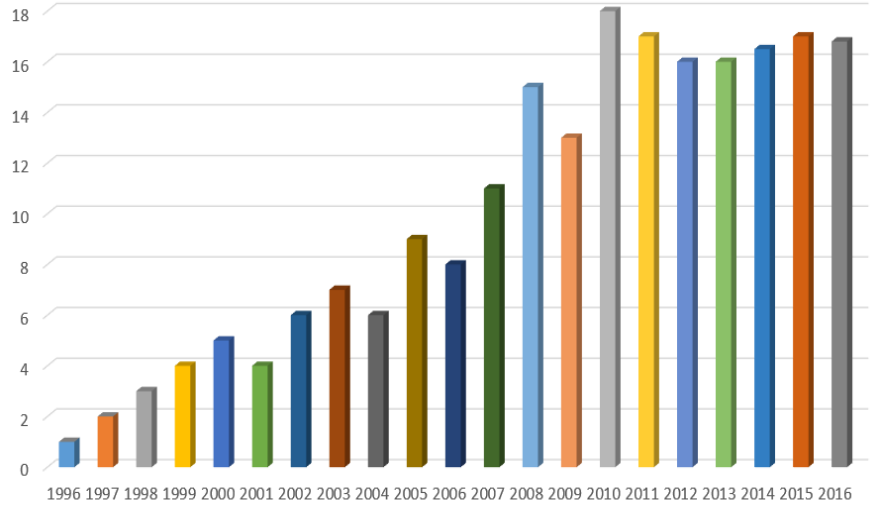
D.R. Gulyamova (TATU, assistent)
S.A. Hojiyev (TATU, talaba)

Barchamizga ma’lumki klient - server texnologiyasida saytlarni tadbiq etish uchun har bir klient kompyuteriga maxsus kod yozilgan. Boshqacha so’z bilan aytadigan bo’lsak dastur foydalanuvchi interfeysi bo’lib xizmat qiladi. Klient va server orasidagi bog’lanish uchun klient kompyuterlari alohida operatsion dasturlar yoki amaliy dastur komponentalarni o’rnatishni talab etadi. Hozirda oldingidan farqli o’laroq ushbu muammolarni bartaraf etgan holda web saytlar turli web brauzerlar qo’llab quvvatlaydigan HTML va JavaScript formatlarida yozilib web hujjatlarda foydalanish uchun ishlatilib kelinmoqda.

Hozirda web saytlarda axborot xavfsizligini ta’minlash juda dolzarb vazifa bo’lib qolmoqda. Web xizmat orqali ma’lumot uzatish tarmog‘ida xizmat qiluvchi dasturlar yaratish juda qulay hisoblanadi. Bunday dasturlar sirasiga elektron hujjat aylanish tizimlari, reklama tizimlari va boshqa tizimlarini kiritish mumkin. Har qanday web texnologiya tizimidagi dasturlarda axborot xavfsizligini ta’minlash asosiy masalalardan biri hisoblanadi. Korporativ tarmoq tizimlari dasturlovchilari har doim ham xavfsizlik qoidalariga amal qilishmaydi, bunga asosiy sabab qilib yetarli malakaga ega bo‘lmaganliklarini yoki tizimlarni dasturlashda boshqa masalalarga e’tiborni qaratishlarini ko‘rsatishishimiz ham mumkin. Web saytlarning axborot xavfsizlik darajasi ularning bevosita zaiflik darajasini aniqlash bilan bog’liqdir. “zaiflik” tizim

xavfsizligi sababli ko‘plab turli mazmunlarda tilga olinadi. Zaiflik bu noto‘g‘ri berilgan qoidalar to‘plami yoki Web saytlar va kompyuter xavfsizligini ta’minlovchi dasturda xato sababli yuzaga kelgan xavfsizlik siyosati buzilishi kabi tushuniladi. Umuman olganda, barcha kompyuter tizimlari kamchiliklarga ega ekanligini aytib o‘tish o‘rinli. Ammo virusli hujumdan mumkin bo‘lgan zarar qanchalik katta bo‘lishiga qarab kamchiliklarni faol foydalaniladigan va umuman foydalanilmaydiganlarga ajratish mumkin. Zaifliklardan foydalanishning ko‘plab usullari mavjud. Bu kamchiliklar yuzasidan qanchadan qancha Web saytlar katta zarar ko’rdi. Bizni maqsadimiz xuddi shunday zararli hujum turlarini ko’rib ularni tahlil qilishdir. Qanday hujum turlari borligini bilish maqsadida , biz veb saytlarda qilingan hujumlar grafigi orqali barcha hujumlarni xavflilik darajasiga qarab baholaymiz.

Web saytlarga qilinadigan hujum turlari haqida gap borganda ularni statistikasini kuzatib boramiz. So’nggi 20 yil mobaynida Web saytlarga bo’lgan hujumlar gistogrammasini 1996-yil hamda 2016-yil oralig’ida o’zgarish statistikasini quyidagi 1-rasmda kuzatishimiz mumkin. Bu statistikada rivojlangan davlatlardagi bo’lib o’tgan hujumlarni darajalari keltirib o’tilgan bo’lib aynan shu hujum turlariga alohida to’xtalib o’tamiz.



1-rasm. Web saytlarga bo’lgan hujumlar gistogrammasi

Web saytlarning rivojlanishi bilan yuqoridagi grafikdan zaiflik darajasining yildan yilga oshib borayotganini kuzatishimiz mumkin. Bu holatga asosiy sabab qilib web saytlarning zaifliklarini oshib borishi bilan tushuntirishimiz mumkin. Mazkur yillik shkalalarning asosiy xarakteristikasi hisoblangan web saytlar kamchiliklari to’grisida batafsil tanishib chiqamiz. Web saytlarga bo’ladigan hujum darajasi statistikalari bo’yicha halqaro OWASP (The Open Web Application Security Project) tashkiloti yillik ma’lumotlarini e’lon qilib boradi. OWASP dasturiy xususan Web saytlarning xavsizligini yanada takomillashtirishga qaratilgan xalqaro notijorat tashkilot hisoblanadi. Tashkilotning maqsadi dunyo bo’ylab dasturiy xavfsizlikni rivojlantirishni ko’zlab shuningdek dunyo bo’ylab, tashkilotlar tizimdagi xavfsizlik darajasini yaratishi to’g’ri qaror qabul qilishi uchun turli xavflarni e’lon qilib boradi va Web saytlarga bo’lgan hujumlar doirasida eng xavfli hujumlar reytingini e’lon qilib boradi. Biz ham shu reyting jihatidan hujum turlarini alohida tartibladik. Quyida OWASP tashkilotining reyting darajasidagi xavflarni ko’rib chiqamiz. 2017 oxirgi nashr qilingan 15 ta hujumlar ro’yxatini batafsil ko’rib chiqamiz. OWASP (The Open Web Application Security Project) agentligining 2017 yil reytingiga ko‘ra:

1. SQL ineksiya (SQL injection)
2. Murojatlarni boshqarish va autentifikatsiyaning buzilishi (Broken Authentication and Session Management)
3. Sayt qatorlarni kesish (Cross-Site Scripting ,XSS)
4. Manba ob’ektlariga yo‘naltirilgan xavflar (Insecure Direct Object
5. Noto‘g‘ri sozlangan xavfsizlik (Security Misconfiguration)

6. Maxfiy axborotlarga ta’sir (Sensitive Data Exposure)
7. Ruxsatlarni nazoratlash darajasidagi vazifalarni kiritish (Missing Function Level Access Control).
8. Soxta so’rovlar kesishuvi (Cross-Site Request Forgery (CSRF))
9. Ma’lum kamchilik komponentlaridan foydalanish (Using Components with Known Vulnerabilities).
10. Ishonchsiz qayta manzillash va davom etish (Unvalidated Redirects and Forwards)
11. XML tashqi obektlari (XML External Entities)
12. Tamg’a ko’chirish (Fingerprinting)
13. Axborotni tarqatish(information leakage)
14. Jarayonni boshqaruv (Credential/Sesion Predection)
15. Tanlov (Brute Force)

OWASP (The Open Web Application Security Project) agentligiga o’xshagan ko’pchilik tadqiqot - izlanuvchi kompaniyalarning yillik tekshiruv natijalariga ko’ra ko’p sonli axborot tizimlari web saytlarida yuqoridagi ro’yxatda keltirilgan bandlar misolidagi zaiflik darajasi yuqori ekanligini ko’rsatadi, bu esa o’z navbatida ham ma’naviy ham moliyaviy zarar yetkazilishiga olib kelishi mumkin. So’ngi yillarda web saytlarga bir nechta hujum turlari oshishi kuzatilmoqda. Web texnologiyalar sohasida web saytlarning xavfsizligini ta’minlash asosiy ustuvor vazifalardan hisoblanadi. Yirik kompaniyalar tarmog’ida bo’ladigan hujumlar aynan web saytlarga birinchi hujum qilishdan boshlanishini alohida ta’kidlash lozim. Web saytlar xavfsizligini ta’minlagan holda bir butun axborot tizimini ta’minlanishini yodda tutgan holda yaratilayotgan tizimlarda xavfsizlik darajasini yuqori holatda himoyalashni ko’zda tutish lozim.Bunday hujum turlarini bilib oganimizdan so’ng biz o’z veb saytlarimizni keraklicha himoyalashimiz mumkin.

Hozirda yurtimizda axborot kommunikatsiya texnologiyalari sohasida jadal su’ratlarda takomillashtirish ishlari olib borilayotganligini nazarda tutib yaratilayotgan Axborot tizimlarini axborot xavfsizlik darajasini oshirgan holatda axborot xizmatlarini joriy etish bugunning dolzarb masalalaridan biridir. Shunday ekan dunyo miqyosidagi axborot hujumlarini tahlil etib axborot xizmatlarini yo’lga qo’yishda mazkur kamchiliklardan holi holatdagi axborot xizmatlarini joriy etish axborot xavfsizligi mutaxassislarining vazifasi ekanligini unutmasligimiz zarur. Zaifliklarning yillar davomida keskin ravishda ortib borishi xususan so‘nggi yillarda web saytlarning zaifligi turli tipidagi tahdidlarni ko’payishiga olib kelmoqda. Biz esa aynan shu tahdidlarga qarshi chora tadbirlarni va dasturlarni yaratyapmiz.

THREATS AND PROTECTION WAYS OF MOBILE NETWORKS

X. Shodmonova (TUIT, master degree)
S. Salimov (TUIT, student)

The sanctity of mobile operators’ networks and brands will depend greatly on their ability to deliver QoS (quality of services) guarantees to roaming and interconnect partners, while simultaneously protecting increasingly multimedia-savvy and socially connected subscribers. The challenge is that the all-IP architecture making mobile networks innovative and monetizable as digital lifestyle-enabling systems are also making them more vulnerable to a multitude of security threats including: Denial of Service (DoS) attacks, IP address, malware, man-in-the-middle (MITM) attacks, botnets, identity theft, TCP sweeps and service thefts. There are several ways protecting from above shown threats.

Mobile network threats are related to mobile network standards, such as, 1G, 2G, 3G, 4G (LTE).

There are quite a few attack types and vectors, and they are unfortunately evolving and multiplying all the time, in this paper we focus on common threats that mobile network operators should be aware of regarding the Gi/SGi interface of the network.

TCP Sweeps. In a TCP sweep-based attack, an attacker can send TCP SYN packets to one or more target mobile devices - possibly a large range of publicly addressable mobile devices on the network. If the devices support to those packets, the attacker learns that a port in the target devices is open, which makes the port vulnerable to attack. The attacker's motivation is to target the weakest link in the mobile chain, such as radio bandwidth or other vulnerable network elements in the mobile operator's cloud, as well as the devices' batteries. By keeping the radio resources in continuous use by waking up some unsuspecting mobile devices, the attacker effectively clogs up the precious radio spectrum resulting in denial of service (DoS) for legitimate mobile initiated transactions and ends up significantly draining the devices' batteries. In this way, attackers can keep hundreds of subscribers from being able to use their mobile devices. While the point to such attacks might not be immediately obvious, Juniper and its MNO customers have witnessed them firsthand and they seem to originate with notoriety-seeking hackers as well as those with a financial motive for negatively impacting subscriber productivity.

Direct Attacks on Mobile Infrastructure. The mobile infrastructure is subject to certain threats including attacks on the Gi/SGi firewall, IPS or both and bandwidth saturation.

Attack on Firewall and IPS Devices. Firewall and IPS devices are stateful inline devices, by virtue of which they are innately vulnerable to DDoS threats that can overwhelm the state capacity of these systems. Therefore, as devices sitting at the Gi/SGi interface of a mobile network, subject to massive mobile traffic, they must be protected.

Gi/SGi Bandwidth Saturation. Gi/SGi bandwidth is one of the weakest links in the mobile packet edge. By entering through the Internet over the Gi/ SGi interface, an attacker can flood the mobile network with excessive network traffic, thereby prohibiting legitimate traffic to pass. This can cause all of the subscribers who are trying to access the Internet on mobile devices to lose network access for some time. In addition, this can completely disable the firewall.

Botnet Attacks. Botnet attacks, which traditionally targeted PCs, are increasingly targeting mobile devices as the latter are becoming more popular and more connected, and the complexity and the number of vulnerabilities in these platforms is increasing. An attacker might launch a mobile device botnet by taking over full control of multiple devices' data connections. The attacker could do so by fingerprinting each of the devices and injecting exploit code customized to these devices by exploiting a known vulnerability in the mobile network operator's network.

Mobile device botnets can then subsequently be used for launching distributed denial-of-service (DDoS) attacks on the mobile network itself, distressing many customers who cannot connect to the network. Alternatively, a spammer could use the botnet to distribute SMS messages from the compromised mobile devices. A botnet could either be fed a list of phone numbers or just randomly try to send messages to every possible phone number in an area code. In the absence of a firewall or spam-blocking software for SMS messages, mobile device SMS spam botnets could be potentially very profitable to spammers. SMS spam messages could also be used to further spread the botnet through Web links or as part of an attack on the mobile network itself. Furthermore, a botnet could send a lot of bogus content to mobile base station towers in a specific region and subsequently degrade the level of service to these towers.

IPv6 DDoS Attacks. The increasing sophistication of mobile devices and the applications that run on them is driving mobile network operators toward public addressing solutions, including IPv6 deployment, to improve scalability and to minimize operating expenses. With the inevitable shift from IPv4 to IPv6, which intermittently requires mobile networks to support both address schemes, large amounts of undesirable state are inserted into the mobile network in the form of 6to4 gateways and carrier-grade NAT (CGN) devices. The large amounts of state present in these devices make them highly vulnerable to both deliberate and inadvertent DDoS attacks.

For protecting from TCP sweeps are used integrated stateful inspection firewall and IPS engine. Protection from mobile infrastructure attacks are designed in such a way as to allow administrators to harden the control plane from any potential attacks and to ensure availability through configuration of filters and rate limiting of the traffic that reaches the route engine.

Special SRX Series Services Gateways protect against botnet attacks through AppDoS. The AppDoS service employs multi-stage detection methods used to identify and mitigate targeted attacks from disrupting critical applications and services, and to identify attacking botnet traffic against legitimate client traffic to prevent DDoS attacks that target applications. Also, IPv6 DDoS Attacks are protected by AppDDoS, a solution that is integrated into the IPS engine to profile the servers that AppDDoS is protecting.

Thus, the firewall, DoS attack prevention, IPS, application protection and QoS is integrated components for uninterrupted connectivity—and implement threat detection, alerting and monitoring as a single holistic solution for protecting the Gi/SGi interface-the operators can reduce risk to their networks and provide a positive customer experience.

ANALYZING E-GOVERNMENT PROTECTION THREATS

M. Tadjieva (TUIT, master degree)
N.Nurmuxamedov (TUIT, master degree)

With the popularity and maturation of computer network technology, the real-time sharing of a large amount of government information and the two-way exchange has been already possible technically. E-government is a kind of governmental administration which based on electronic information technology. The essence of e-government is using electronic information technology to break the boundary of administrative organizations, and build up a virtual electronic government. People can get government information and services through electronic media. Governments can communicate with each other through various kinds of electronic media which can be used inside government bodies, between different governments, or between government and society.

Also, there are many problems exposed in the spread of computer network technology. Security is the most important one. It was said by National Computer Network Emergency Response Technical Team/Coordination Center of China (CERT) in 2007, they had received 26476 network security incident reports. This is three times more than 2005 which was reported 9122 network security incidents. As a result, with the fast development of e- government; it is particularly important to strengthen security consciousness and take strong preventive measures in technology and management aspects.

Views of threats

The development of e-government, which is based on internet, meets fatal security problems due to the complexity and vulnerability of network. Generally speaking, the security risks e-government facing includes the following aspects:

Information intercepting. It means that the related e-government users or invaders capture or steal the e-information from governments or other users.

Information tampering. The internet attackers tamper, insert or delete original data through various technical methods, and transmit them to the destination, in order to damage the integrality of the data.

Services denying. It is the complete invalidation of the network system or the servers system in some period. It mainly comes from the attack of the hackers or the virus, and the man-made destruction of the devices as well.

System resources stealing. In the network system environment, the stealing of the system resources is very common.

Information faking. It means that after the attackers know the rules of the data in the network information or after they have decoded the government information; they could pretend legal users or make false information to cheat other users. The main forms include pretending users to get illegal certifications, forging e-mails, etc.

Risk management system consists of two parts:

– risk identifying;

– risk analyzing;
– risk controlling

Risk identification is based on the collecting of various relevant threats, bugs and corresponding countermeasures, and then recognizes any possible risks or potential threats to the e-government system.

Risk analysis, through various kinds of qualitative or quantitative methods, such as analysis, comparison, evaluation, etc. is to decide the importance of each factor of e-government risks, rank the factors, and then evaluate every possible result to the e-government system. Threat is a kind of potentiality which launched unintentionally by threat source, or threat source attacked the vulnerabilities of the system intentionally. It is that the system has vulnerabilities, so threat sources become risks. So in the process of risk analysis, we must identify and describe threat sources.

Threat sources can be any kinds of environments or events include people, nature, and so on, which do harm to the system. The natural threat that system facing relates to its geographical location; however, the threats from people may have no intention or on purpose. To identify threats the system facing, we can use many different methods, such as brainstorming, Delphi, Scenarios Analysis, etc. Table 1 lists some possible threat sources.

Possible threat sources Table 1.

Threat	**Possible Source**
Intentional threats	terrorists
	people who dissatisfied with the organization, or has a mental imbalance
	criminals
	insiders who colluding with alien enemies
	hackers
Unintentional threats	mis-operations from system users
	mis-operations from system chargers or protectors
Natural threats	earthquake
	volcanic eruption
	hurricane
	flood
	thunder and lightning
	hail

The ultimate goal of threat analyzing is to calculate the general risk probability. The factors influencing risk probability include motivations and ability of threat source, system vulnerabilities, and effect of relative security measures. Calculating risk probability is a course with very strong subjectivity. There may be some history records about natural threats, those records can help to analyze the probability that natural threats happen. But we are often lack of the history information about the technical and operational threats from people. To evaluate probability of these kind threats, we can use analogy method. However, actually it often depends on analyzers' practical experience. We have proposed a simple method to describe the risk probability in three levels: high, medium, and low. Table 3 shows the definitions of risk probability.

We can get the information about vulnerabilities through spot investigation, personnel investigation, network scanning, penetration testing, relative documents analyzing, or other open information sources on vulnerabilities. In the stage of vulnerability analyzing, if the system is still in designing, the emphasis is on the strategies or rules of the system security, and the definitions of security requirements. If the system is already implemented, we should also analyze some more specific information, such as design documents. If the system is in using, we need to do some further analysis, such as the system security functions, actual effects of the security control, etc.

Definitions of Risk Probability Table 2.

Probability	Description
High	Threat source has high motivation and ability, security measures are invalid.
Medium	Threat source has some motivation and ability, but security measure have effect; or threat source does not have motivation; or it does not have obvious ability.
Low	Threat source is lack of motivation and ability, security measures can keep vulnerabilities from attacking effectively.

Risk controlling is to choose and use some risk controlling methods to guarantee the risk can be reduced to an acceptable level. Risk controlling is the most important step in the risk management. It is the key factor to determine whether the risk management is successful or not. The goal of e-government security risk controlling is to reduce the risk degree which e-government projects suffering.

Also, generally speaking, there are two kinds of risk controlling methods. First are risk controlling measures, such as risk reducing, avoiding, or transferring, and losses managing. We often use risk transferring and losses managing in e- government security risk management.

Generally speaking, risk management has three basic countermeasures: (1) managers take some proper measures to reduce the probability of risk accidents; (2) managers prepare an emergency plan and adopt it when contingences happen; or (3) managers do nothing.

For already chosen countermeasures, managers should have a full evaluation of their potential risks. And draw up a relevant emergency plan in order to make the possible risk losses minimum.

There are no golden rules for risk management. For e- government security risk management, the first step is to scan and detect internal and external environment of the e-government system, check the vulnerabilities and weaknesses of the system. Patch or append new devices immediately in order to reduce the losses as much as possible while risks happen. Secondly, do a full analysis about the e-government security risk, and then make relevant plans and measures. Track and monitor those plans and measures in each implement stage. At last, adjust risk management measures at any time according to the environment changes, and draw up a whole disaster recovery plan.

АХБОРОТ ХАВФСИЗЛИГИ ИНЦИДЕНТЛАРИ ТЕРГОВИДА ГУРУҲЛАР ТУЗИЛМАСИНИ ТАШКИЛ ЭТИШ ҲАҚИДА

Б.К. Юсупов (ТАТУ, ассистент)
З.К. Юсупов (ТАТУ, талаба)

Ахборот технологияларини жадал суръатлар билан ривожланиши корхона ва ташкилотларнинг ахборот хавфсизлиги тизимлари билан боғлиқ муаммоларни юзага келишига сабаб бўлмоқда. Бу муаммолардан бири бизнес соҳасида фаолият юритувчи ташкилотларда ахборот хавфсизлиги инцидентлари билан боғлиқ муаммоларни келтириб чиқараябди. Ахборот хавфсизлиги инцидентларини аниқлаш ва терговини амалга оширадиган гуруҳлар тузулмасини ташкил қилиш ахборот хавфсизлиги инцидентларига қарши чораларни асосий босқичларидан бири сифатида қарашимиз мумкин.

Инцидентни тергов этиш қанчалик мураккаблигига қараб унда бир ёки бир нечта иштирокчилар қатнашиши мумкин. Жамоа раҳбари инцидент гувоҳларини таҳлил қилади ва гуруҳда нечта ва қандай йўналишдаги ходимлар бўлиши кераклиги ҳақида қарор қабул қилади. Жавоб қайтариш гуруҳининг тузулмасини уч хил модели мавжуд:

Марказлаштирилган модел – бутун ташкилот доирасида ягона тизим тарзида

ташкил қилинган модел бўлиб, у уч бўлимдан иборат бўлади: call center (телефон қўнғироқларига жавоб маркази), техник ёрдам маркази (маълумотларни йиғиш ва таҳлил қилиш маркази), тергов қилиш гуруҳи (аналитик марказ). Ушбу модел унча катта бўлмаган ташкилотлар учун мўлжалланган.

Тақсимланган модел – марказлаштирилган модел асосида яратилган. Ушбу моделнинг марказлаштирилган моделдан фарқи ташкилот филиаллари географик узоқликда жойлашганлигидадир. Ушбу ҳолатда асосий офиснинг жавоб қайтариш гуруҳи ахборот хавфсизлиги инцидентлари ҳақида мувофиқлаштириш хизмати ва маълумотларни сақлаш билан тўлдирилади.

Корпоратив модел – соҳага оид марказий принципга асосан амалга оширилади. Мувофиқлаштириш бўлими инцидентга жавоб қайтариш саволлари бўйича юридик шахслардан керакли маълумотларни олади, шу билан бирга унинг қарамоғидаги ташкилотларни ҳам бошқаради.

Жавоб қайтариш гуруҳи ходимлари уч асосий модел остида йиғилиши мумкин:

- ташкилот вужудга келган инцидентни қайта ишлаш бўйича барча вазифани ўз зиммасига олади ва ўз ходимларига таянади;
- жамоа таркибига ушбу соҳа вакилларидан аъзолар қабул қилинади. Ушбу модел ўз ресурсларига 24/7 схемаси остида ишлайдиган ташкилотларга тўғри келади. Бундай ҳолатда жавоб қайтариш ва қайта ишлаш масаласини фирма ўз зиммасига олади, тергов ишлари билан эса ташкилот ичидаги гуруҳ шуғулланади;
- инцидентга жавоб қайтариш ва уни қайта ишлаш ишлари тўлақонли бошқа ташкилот ёки фирмага юкаланади. Бу модел ташкилотни қўлидан қайта ишлаш имконияти келмайдиган тақдирдагина қўлланилиши мумкин.

Моделни танлашдаги омиллари:

1. Ахборот тизими доим 24 соат ҳафтасига 7 кун мавжудлиги.
2. Тўлақонли ёки қисман ходимлар бандлиги. Ушбу омилга агар ходимлар тўлақонли банд бўлмасагина аҳамият бериш мумкин. Ходимлар билан кутилмаган ҳолларда боғланиш йўлларини кўриб чиқиш лозим.
3. Ходимлар маҳорати. Ахборот хафсизлиги инцидентларини қайта ишлаш ахборот хавфсизлигини махсус дастурий-аппарат воситаларини билиши талаб этади. Ташкилот ишчи йўллашдан олдин ушбу жиҳатни эътиборга олиши лозим.
4. Ахборот хафсизлиги инцидентларини бошқаришни нархи. Ташкилот ахборот хафсизлиги инцидентларини бошқариш нархини баҳолаши ва ўзи учун фойдали моделни аниқлаб олиши керак.
5. Ташкилий тузулма. Фақат инцидентларни қайта ишлашда корпоратив ёндашувдан фойдаланган ҳолда ахборот хафсизлиги инцидентларини тергов этишда эркин ҳаракат қила оладиган жамоалар тузиш мумкин. Бунда энг яхши ечим марказий офисда мувофиқлашган марказ ташкил этиш бўлади.

Ташқаридан хизмат кўрсатиш омиллари:

1. Кўрсатилган хизмат сифатига жавобгарлик. Ташкилот бошқа фирма томонидан бажариладиган ишнинг сифатини текшириб боради.
2. Маъмурлик ваколатларини ажратиш. Қурилмани ўчириб ёқиш бўйича даража, фойдаланувчилар ҳақидаги маълумотлар ўзгариши ҳамда бошқа ҳаракатлар ҳодиса юз берганда кечадиган жараёнлар олдиндан келишиб олиниши ва ҳужжатлаштирилиши лозим.
3. Ахборотга рухсатни чеклаб қўйиш. Ташкилот ахборот махфийлиги ҳимоясини кўриб чиқади.
4. Ташкилот тузулмасини билиш. Ташкилот ҳизмат кўрсатувчи фирмага ўзи ҳақида тўғри тасаввур яратиш учун ҳаракат қилиши зарур. Ташкилот инцидент қандай юзага келган бўлиши мумкинлиги ҳақидаги ҳужжатни яратади ва ҳар доим уни такомиллаштириб бориши лозим.
5. Юзага келган инцидент коррелцияси. Ташкилот ахборот хафсизлиги инциденти

юзага келганда ушбу вазиятни коррелациялаш тизимини ишга тушириши керак. Ушбу тизим махсус билимни талаб қилади.

6. Инцидентларни қайта ишлаш. Ташкилот ҳизмат кўрсатиш фирмаси ходимини инцидентни тергов этиш жараёнида иштирок этиши ёки этмаслигини аниқлайди.

7. Инцидентларга мустақил равишда жавоб қайтара олиш. Ташкилот ахборот хафсизлигида юзага келадиган инцидентларда мустақил равишда жавоб қайтаришни билиши керак.

Ахборот хавфсизлиги инцидентлари терговида гуруҳлар тузулмасини тўғри ташкил этиш инцидентдан кўриладиган зарарни камайтириш ва инцидентни юзага келишига сабабчи бўлган шахс ёки қурилмани аниқ далиллар асосида топиш ва исботлаш имкониятини оширади.

AN ANALYSIS OF ACCESS CONTROL MODELS

S.K. G`aniyev (TUIT, t.f.d., professor)
B.Y. Turdiboyev (TUIT, student)

Permissions imply a hierarchy of access rights and so users are assigned roles that define what permissions they can exercise and in what context. A role is a set of operations that a user is allowed to perform on a data objects. A user can have more than one role and more than one user can have the same role.

Early research on access control was dominated by two approaches: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). Recently, computer security texts often list Role-Based Access Control (RBAC) as one of the three primary access control policies.

DAC is a user-centric access control model in the sense that a file owner determines the permissions that are assigned to other users requiring access to the file. There is no central control so this model is easy to implement in a distributed applications on the Web. Using a DAC mechanism allows users control over the access rights to their files without the necessity of complying with a set of pre-specified rules. When these rights are managed correctly, only those users specified by the file owner may have some combination of read, write, execute, etc. permissions (privileges) on the file.

An access control matrix (ACM) can be used to keep a global picture of the users on a system and the access rights they have to the files in it. Permissions are defined individually for each combination of users and files/directories in the form of a table. For instance, one might want to implement an access control matrix for a case in which a user, say User_1, creates a folder containing photographs she would like to share. In this case, she decides to allow access only to members who belong in her repertoire of “friends”. As shown in the table given in Figure 1, there are three other users, User_2, User_3 and User_4, on the system. User_3 can view and download files from the Photographs Folder whereas User_4 can only view the photographs and User_2 has no privileges at all with respect to the Photographs Folder.

	Photographs Folder
User_2	-
User_3	{View;Download}
User_4	{View}

Fig.1. An access control matrix

Additionally, since users applying a DAC security model do not have a global picture of the data on the system, it is difficult to take the semantics of the data into consideration in assigning access rights, so information might unknowingly be revealed to unauthorized users. Besides the confinement and information semantics problems that the access control matrix model faces, a key problem that the DAC model faces is vulnerability to Trojan Horse attacks. Trojan horse attacks are typically provoked by deceiving valid users into accepting to run code

that then allows a malicious user to get access to information on the system.

MAC models are typically designed using the concept of information flow control. Information flow control is different from regulating accesses to files by users, as in the ACM model, because it prevents the propagation of information from one user to another. In the MAC model, each user is categorized into a security class and the files are tagged with security labels that are used to restrict access to authorized users. All the valid channels along which information can flow between the classes are regulated.

The collaborative file sharing example shown in Figure 1 can be extended to handle a security scenario in which a security administrator prevents transitive disclosures, by the users accessing User_1's Photographs Folder, by using data labels to monitor information flow. Each data object is tagged with the security clearance labels of each of the users in the system. A transitive disclosure could occur if a user, in this case User_2, gains access to User_1's photographs folder because he belongs in User_3's (who incidentally is on User_1's list of friends) list of "friends". The MAC model prevents such transitive disclosures by labeling information, as shown in Figure 2, to monitor information flow centrally. The users are assigned labels according to their security clearance and information flow is regulated by authenticating a user and then granting access to the file based on their privileges. Since each file is labeled with a security clearance tag, User_2 can no longer access files that User_3 downloads from User_1's Photographs Folder because User_2 does not have a security clearance that allows him access. When the access control policy of a system is based on the MAC model, the security of the system ceases to rely on voluntary user compliance but rather is centrally controlled, making it easier to monitor usage patterns and prevent violations.

In an RBAC model, a user's role is not mutually exclusive of other roles for which the user already possesses membership. The operations and roles can be subject to organizational policies or constraints and, when operations overlap, hierarchies of roles are established. Instead of instituting costly auditing to monitor access, organizations can put constraints on access through RBAC. For example, it may be enough to allow all the users on the system (User_2, User_3 and User_4) to have "view" and "download" access to the Photographs Folder, if their permissions are monitored and constraints used to prevent tampering.

An added drawback that RBAC faces is that roles can be assigned in ways that create conflicts that can open up loopholes in the access control policy. For example in the scenario in Figure 2, we can assume that User_1 is the security administrator for the Photographs Folder and the Movies Folder, and that she chooses to assign roles to users in a way that allow the users to either download or upload movies but not both. Now suppose that at a future date User_1 decides to assign a third role that grants a user, say User_2, the right to veto an existing user's (e.g. User_3's) uploads. In order to veto User_3's uploads, User_2 needs to be able to download as well as temporarily delete questionable uploads, verify the movies and, if satisfied, reload the movies to the site. So, essentially User_2 has the right to both download and upload movies to Movies Folder, a role assignation that conflicts with the first two User_1 specified. Since policy combinations create conflicts that can open up vulnerabilities in a security system designed using the RBAC model, extensions to enable adaptability need to be evaluated with care.

In conclusion, DAC and MAC models compatible with the decline of traditional mechanisms matches in automated information systems. Preveleges to file in objects for DAC, which are appointed by their respective users, shall be determined by the user ID of the process which is performed on behalf of the user. In the MAC, the security level of privacy correspond to objects in the index of documents which they have stored, the security level of subjects determined in accordance with the categories of users. On the contrary, the role model that reflect the security policy applied. That's why close coordination does not exist in this policy. This issue needs to develop a mechanism for the implementation of the policy applied in accordance with the terms and conditions and the method for assigning roles and responsibilities.

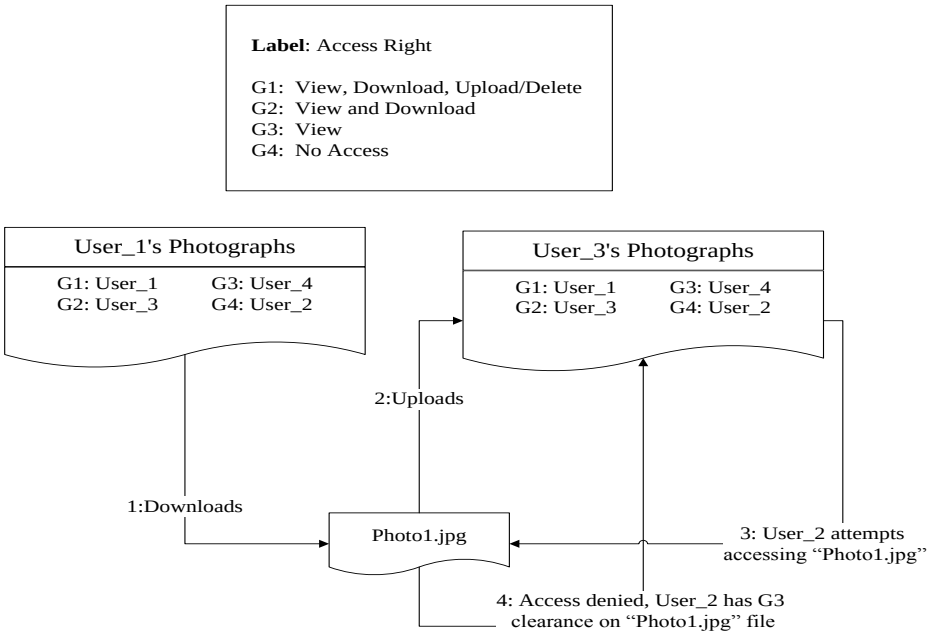


Fig.2. Mandatory access control

KOMPYUTER TARMOQLARIDA AXBOROTDAN RUXSATSIZ FOYDALANISH VA CHIQIB KETISHINI CHEKLASH USULLARI

G.A. Temirova (TATU, talaba)

Hozirgi paytlarda mavjud axborot tizimlarida juda katta xajmda axborotlar saqlanadi va ularni himoyalash eng dolzarb muammolardan bo`lib hisoblanadi.

Zamonaviy avtomatlashtirilgan axborot tizimlari bu taraqqiyot dasturiy-texnik majmuasidir va ular axborot almashuvini talab etadigan masalalarni yechishni ta`minlaydi.

Axborot tizimlarining asosiy ta`sirchan qismlari quyidagilar:

− internet tarmog`idagi serverlar. Bu serverlar: dasturlar yoki ma`lumotlar fayllarini yo`q qilish orqali; serverlarni xaddan tashqari ko`p tugallanmagan protsesslar bilan yuklash orqali; tizim jurnalining keskin tuldirib yuborilishi orqali; brouzer - dasturlarini ishlamay qolishiga olib keluvchi fayllarni nusxalash orqali ishdan chiqariladi;

− ma`lumotlarni uzatish kanallari - biror-bir port orqali axborot olish maqsadida yashirin kanalni tashkil etuvchi dasturlar yuboriladi;

− ma`lumotlarni tezkor uzatish kanallari - bu kanallar juda ko`p mikdorda hech kimga kerak bo`lmagan fayllar bilan yuklanadi va ularning ma`lumot uzatish tezligi susayib ketadi;

− yangiliklarni uzatish kanallari - bu kanallar eskirgan axborot bilan tuldirib tashlanadi yoki bu kanallar umuman yo`q qilib tashlanadi;

− java brouzerlari - SUN firmasi yaratgan java tili imkoniyatlaridan foydalanib, appletlar tashkil etish orqali ma`lumotlarga ruxsatsiz kirish mumkin bo`ladi. Java - appletlari tarmoqda avtomatik ravishda ishga tushib ketadi va buning natijasida foydalanuvchi biror-bir xujjatni ishlatayotgan paytda xaqiqatda nima sodir etilishini hech qachon ko`ra bilmaydi, masalan, tarmoq viruslarini tashkil etish va java-appletlari orqali viruslarni junatish mumkin bo`ladi yoki foydalanuvchining kredit kartalari raqamlariga egalik qilish imkoniyati vujudga keladi.

Demak, yuqorida olib borilgan taxlildan shu narsa ko`rinadiki, hozirgi paytda kompyuter tarmoqlari juda ko`p ta`sirchan qismlarga ega bo`lib, ular orqali axborotlarga ruxsatsiz kirishlar amalga oshirilmoqda yoki ma`lumotlar bazalari yo`q qilib yuborilmoqda va buning natijasida insoniyat millard-millard dollar zarar ko`rmoqda.

Kompyuter tizimlari zaxiralariga ruxsatsiz kirish sifatida mazkur tizim ma`lumotlaridan foydalanish, ularni o`zgartirish va o`chirib tashlash xarakatlari tushuniladi.

Agar kompyuter tizimlari ruxsatsiz kirishdan himoyalanish mexanizmlariga ega bo`lsa, u xolda ruxsatsiz kirish xarakatlari qo`yidagicha tashkil etiladi:

- himoyalash mexanizmini olib tashlash yoki ko`rinishini o`zgartirish;
- tizimga biror - bir foydalanuvchining nomi va paroli bilan kirish.

Agar birinchi xolda dasturning o`zgartirilishi yoki tizim surovlarining o`zgartirilishi talab etilsa, ikkinchi xolda esa mavjud foydalanuvchining parolini klaviatura orqali kiritayotgan paytda ko`rib olish va undan foydalanish orqali ruxsatsiz kirish amalga oshiriladi.

Ma`lumotlarga ruxsatsiz egalik qilish uchun zarur bo`lgan dasturlarni tatbiq etish usullari:

- kompyuter tizimlari zaxiralariga ruxsatsiz egalik qilish;
- kompyuter tarmog`i aloqa kanallaridagi habar almashuvi jarayoniga ruxsatsiz aralashuv;
- virus kurinishidagi dasturiy kamchiliklarni kiritish.

Ko`pincha kompyuter tizimida mavjud zaif qismlarni «teshik» lar, «lyuk» lar deb atashadi. Ba`zan dasturlovchilarning o`zi dastur tuzish paytida bu «teshik» larni qoldirishadi, masalan:

- natijaviy dasturiy mahsulotni yengil yig`ish maqsadida;
- dastur tayyor bo`lgandan keyin yashirincha dasturga kirish vositasiga ega bo`lish maqsadida.

Mavjud «teshik» ka zaruriy buyruqlar quyiladi va bu buyruqlar kerakli paytda o`z ishini bajarib boradi. Virus ko`rinishidagi dasturlar esa ma`lumotlarni yo`qotish yoki qisman o`zgartirish, ish seanslarini buzish uchun ishlatiladi.

Hozirgi paytda lokal hisoblash tarmoqlari (LAN) va global hisoblash tarmoqlari (WAN) orasidagi qirra yuqotilib borilmoqda. Bu esa, ya`ni LAN imkoniyatlarining ortishi, ma`lumotlarni himoyalash usullarini yanada takomillashtirishni talab qilmoqda.

Himoyalash vositalarini tashkil etishda quyidagilarni e`tiborga olish lozim:

- tizim bilan aloqada bo`lgan sub`yektlar sonining ko`pligi, ko`pgina xollarda esa ba`zi bir foydalanuvchilarning nazoratda bo`lmasligi;
- tarmoqda foydalanuvchiga zarur bo`lgan ma`lumotlarning mavjudligi;
- tarmoqlarda turli firmalar ishlab chiqargan kompyuterlarning ishlatilishi;
- tarmoq tizimida turli dasturlarning ishlatilishi;
- tarmoq elementlari turli mamlakatlarda joylashganligi sababli, bu davlatlarga tortilgan aloqa kabellarining uzunligi va ularni to`liq nazorat qilishning qariyib mumkin emasligi;
- axborot zaxiralaridan bir vaqtning o`zida bir qancha foydalanuvchilarning foydalanishi;
- tarmoqqa bir qancha tizimlarning qo`shilishi;
- tarmoqning yengilgina kengayishi, ya`ni tizim chegarasining noaniqligi va unda ishlovchilarning kim ekanligini noma`lumligi;
- xujum nuqtalarining ko`pligi;
- tizimga kirishni nazorat qilishning qiyinligi.

Tarmoqni himoyalash zarurligi quyidagi xollardan kelib chiqadi:

- boshqa foydalanuvchilarning massivlarini o`qish;
- xotirada qolib ketgan ma`lumotlarni o`qish;
- himoya choralarini aylanib o`tib, ma`lumot tashuvchilarni nusxalash;
- yashirincha foydalanuvchi sifatida ishlash;
- dasturiy tutgichlarni ishlatish;
- dasturlash tillarining kamchiliklaridan foydalanish;
- himoya vositalarini bilib turib ishdan chiqarish;
- kompyuter viruslarini kiritish va ishlatish.

Tarmoq muxofazasini tashkil etishda quyidagilarni tashkil etish lozim:

- muxofaza tizimini nazorati;
- fayllarga kirishni nazorati;
- tarmoqda ma`lumot o`zatishni nazorati;
- axborot zaxiralariga kirishni nazorati;
- tarmoq bilan ulangan boshqa tarmoqlarga ma`lumot tarqalishini nazorati.

Axborotni qayta ishlash uchun kerakli tekshiruvdan o`tgan kompyuterlarni ishlatish lozim bo`ladi. Muxofaza vositalarining funksional to`liq bo`lishi muhim hisoblanadi. Bunda tizim administratorining ishi va uning olib borayotgan nazorati katta ahamiyatga egadir. Masalan, foydalanuvchilarning tez-tez parollarini almashtirib turishlari va parollarning juda uzunligi ularni aniqlashni qiyinlashtiradi. Shuning uchun yangi foydalanuvchini qayd etishni cheklash (masalan, faqat ish vaqtida yoki faqat ishlayotgan korxonasida) muhimdir. Foydalanuvchining xaqiqiyligini tekshirish uchun teskari aloqa qilib turish lozim (masalan, modem yordamida). Axborot zaxiralariga kirish xuquqini chegaralash mexanizmini ishlatish va uning ta`sirini LAN ob`yektlariga tulaligicha o`tkazish mumkin.

Tarmoq elementlari urtasida o`tkazilayotgan ma`lumotlarni muxofaza etish uchun quyidagi choralarni kurish darkor:

- ma`lumotlarni aniqlab olishga yo`l qo`ymaslik;
- axborot almashishni taxlil qilishga yo`l qo`ymaslik;
- xabarlarni o`zgartirishga yo`l qo`ymaslik;
- yashirincha ulanishga yo`l qo`ymaslik va bu xollarni tezda aniqlash.

Ma`lumotlarni tarmoqda uzatish paytida kriptografik himoyalash usullaridan foydalaniladi. Qayd etish jurnaliga ruxsat etilmagan kirishlar amalga oshirilganligi xaqida ma`lumotlar yozilib turilishi kerak. Bu jurnalga kirishni chegaralash ham himoya vositalari yordamida amalga oshirilishi lozim.

Kompyuter tarmog`ida nazoratni olib borish murakkabligining asosiy sababi - dasturiy ta`minot ustidan nazorat olib borishning murakkabligidir. Bundan tashqari kompyuter viruslarining ko`pligi ham tarmoqda nazoratni olib borishni qiyinlashtiradi.

Yuqorida keltirilganlardan xulosa qilib, ma`lumotlarga ruxsatsiz egalik qilish uchun dasturiy moslamalar eng kuchli va effektiv instrument bo`lib, kompyuter axborot zaxiralariga katta xavf tug`dirishi va bularga qarshi kurash eng dolzarb muammolardan biri ekanligini ta`kidlash mumkin.

SIMMETRIK KRIPTOTIZIMLARNING MATEMATIK NUQTAI NAZARDAN QIYOSIY TAHLILI

D.B. Xamdamov (TATU, talaba)

Hozirda har bir rivojlangan mamlakatning milliy shifrlash standartlari mavjud. Har bir rivojlangan mamlakat milliy shifrlash algoritmini xech qachon rivojlatirmay qoldirmaydi, ayniqsa bugungi globallashuv jarayonida. Chunki axborot xavfsizligini ta’minlash har bir davlat uchun muhim yo‘nalishlardan biri sanaladi. Shu sababli simmetrik kriptotizimlarni bardoshliligini oshirishda bugungi kunda bir qator ilmiy tadqiqotlar olib borilmoqda. Ushbu jarayonning bir yo‘nalishi sifatida, ya’ni kriptografiya sohasida qo‘llaniladigan simmetrik kriptotizimlarni matematik nuqtai nazardan tahlil qilish, matematik funksiyalar murakkabliklaridan foydalangan holda kriptobardoshli tizimlar ishlab chiqish bugungi kunda dolzarb vazifalardan biri hisoblanadi.

Kriptografik algoritmlarining kriptobardoshliligini belgilovchi eng muhum omil sifatida kalitni ko’rsatish mumkun va uni baxolashda Brute-Forse hujmidan foydalanilagan holda hujimga bir xil qarshilikka ega bo’lishi uchun semmetrik va assimetrik kalit uzunliklari 1-jadvalda berilgan.

1-jadval

Kriptografik algoritmlarining kalit uzunliklari

Brute –Forse hujimi	
Simmetrik kalit uzunligi	Assimetrik kalit uzunligi
56 bit	384 bit
64 bit	512 bit

80 bit	768 bit
112 bit	1792 bit
128 bit	2304 bit

Kriptografik algoritmlarning quyidagi mezonlar asosida baxolanadi algoritm turi bo'yicha, maxfiylik darajasi, autentifikatsiya jarayonlarda qulayligi, yaxlitlikni taminlash funksiyasiga hamda, kalitlarni boshqaruvi;

2-jadval

Kriptografik algoritmlarning imkoniyatlari:

Algoritmlar	Maxfiylik	Autentifikatsiya	Yaxlitlik	Kalitlar boshqaruvi
Simmetrik algoritmlar	Xa	Yo'q	Yo'q	Xa
Assimmetrik Algoritmlar	Xa	Yo'q	Yo'q	Xa
Raqamli belgilash	Yo'q	Xa	Xa	Yo'q
Kalit shartnomasi	Xa	Yo'q	Yo'q	Xa
Bir tamonlama xesh funksiya	Yo'q	Yo'q	Xa	Yo'q
Xabar autentifikatsiya kodi	Xa	Xa	Xa	Yo'q

Simmetrik shiflash algoritmlarini bir qator xususiyatlari orqali baxolash muallifi, kalit uzunligi (bit), kirish blok uzunligi (bit), raund soni, matematik asosi, yaratish asosi

3-jadval

Simmetrik shifrlash algoritmlarining qiyosiy taxlili

Xususiyati	DES	GOCT	AES	Blowfish
Muallifi	IBM tashkiloti	-	Vinsent Rijman va Xuan Daymen	Bryus Shnayer
Kalit uzunligi (bit)	56	256	128,192,256	32-448
Kirish blok uzunligi (bit)	64	64	128	64
Raund soni	16	32	10,12,14	16
Matimatik asosi	Xor, surish va o'rin almashtirish	Xor 2^{32}, surish va o'rin almashtirish	Ko'pxadlar ustida amallar, xor, surish	MOV, ADD, XOR
Yaratish asosi	Feystal tarmog'i	Feystal tarmog'i	SPN tarmoq	Feystal tarmog'i

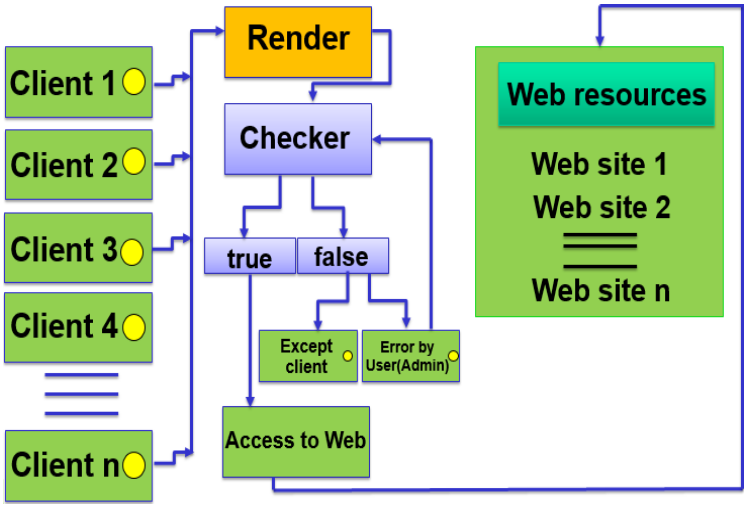
- kriptografik algoritmlarining kriptobardoshliligini baxolashda Brute-Forse hujmidan foydalanilagan holda hujimga bir xil qarshilikka ega bo'lishi uchun semmetrik va assimetrik kalit uzunliklari ko'rib chiqildi
- kriptografik algoritmlarning algoritm turi, maxfiylik darajasi, autentifikatsiya jarayonlari, yaxlitlikni taminlash funksiyasi, kalitlarni boshqaruvi mezonlar asosida baxolanadi
- simmetrik shifrlash algoritmlarining shifrlanadigan ma'lumoti, vaqti, tezlik mezonlariga tayanib qiyosiy taxlili ishlab chiqildi

WEB SAYTLARNI TURLI HUJUMLARDAN HIMOYALASH DASTURIY VOSITASI

Z.Z. Qodirov (TATU, assistent)
S.A. Hojiyev (TATU, talaba)

Bugungi kunda axborotlashtirish hamda interaktiv xizmatlarni yo'lga qo'yish jamiyatning barcha yo'nalishdagi sohalarida birdek rivojlanib bormoqda. Bu xizmatlarni tashkil etishda foydalanilayotgan axborot tizimlarini tashkil etish va foydalanishda web texnologiyalar sohasida web saytlarning xavfsizligini ta'minlash asosiy ustuvor vazifalardan hisoblanadi. Shu sababli web saytlarning xavfsizligi bo'yicha chora tadbir va dasturlar ishlab chiqish rivojlanayotgan elektron hukumat tizimining ishonchliligini va barqarorligini ta'minlaydi. Bu haqida esa xususan axborot xavfsizligini taminlash bo'yicha prezidentimiz Shavkat Mirziyoyevning o'zlari ham alohida urg'u berib o'tdilar.

Hozirgi kunda O'zbekistonda tadbirkorlik va biznesning rivojlanishi turli korxonalarning rivojlanishi kuchli raqobatni keltirib chiqarmoqda. Bu esa ularni reklama qiluvchi va klientlar bilan ma'lumot almashinuvchi veb saytlarga bo'ladigan tahdid va hujumlarni tobora oshirib bormoqda. Bunday himoya tizimini yaratishda ASP.NET Framework bilan birgalikda Web saytlarni yaratuvchi qo'shimcha kuchli himoyaga ega MVC frameworki ham mavjud . Undan oldin esa biz yaratmoqchi bo'lgan tizimni himoyasi bilan algoritm shaklida ko'rsatib o'tsak(1-rasm).



1-rasm. Hujumdan xabardor qilish sxemasi.

Hujum jarayoni tavsifi

- ✓ Bunda **Client 1, Client 2, Client 3…. Client n** lar ichida hujum qilmoqchi bo'lganlar (hakkerlar) bo'lishi mumkin
- ✓ **Render** esa **Client**lar yuborgan so'rovlarni Stek shaklida navbatma navbar, birma-bir **Checker** uzatib turadi.
- ✓ **Checker** so'rovni qanaqa ekanligini aniqlab, to'g'ri(true) bo'lsa Web saytga kirishga ruxsat beradi.
- ✓ **Checker** so'rovni qanaqa ekanligini aniqlab, xato(false) bo'lsa Web saytga kirishga ruxsat bermaydi va Adminga hujum qilinayotgani to'g'risida ma'lumot (SMS-xabar) jo'natiladi va clientga xatolik ko'rsatadi.

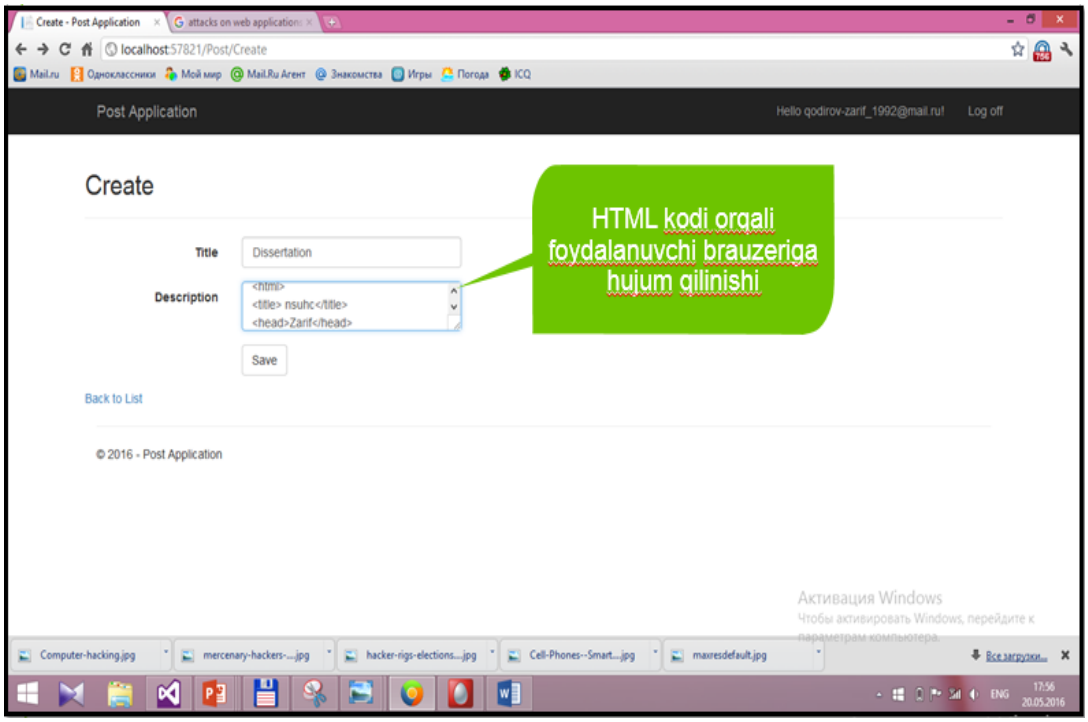
Himoya formasi va hujum turlari

Klientlar kiritgan login va parollar autentifikatsiyalanganini ko'rib turibmiz .

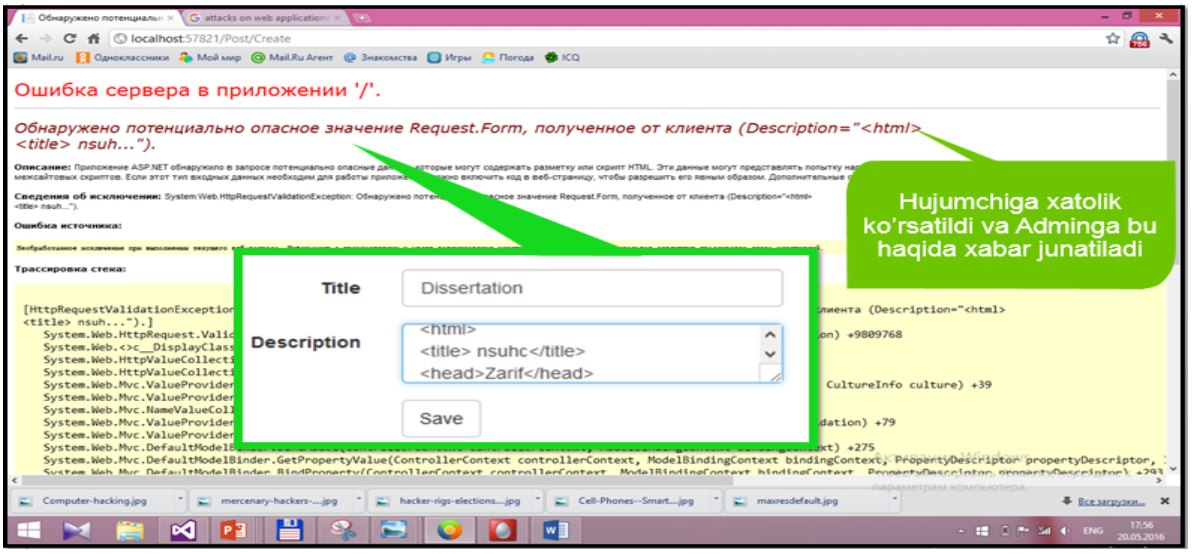
```
<input name="__RequestVerificationToken" type="hidden"
value="4knxtXX-Wmw2UhaLMVS8MUiXozWBCfgoeBGwIlVkweMwRp7r0XBaW9UwD-
```

Cross Site Scripting – JavaScript va HTML kodi orqali foydalanuvchi brauzeriga hujum

qilinishi imkonini beradi. Foydalanuvchi ma'lumotlarni tekshirishi davomida xatoliklarni vujudga keltiradi. Ushbu turdagi hujumlar ko'pincha ularni amalga oshirish mexanizmi **SQL-Injection**ga juda o'xshash, chunki HTML-kodlarida ham shu kabi o’xshashliklar mavjud. Ammo farqli o'laroq foydalanuvchi brauzerida ijro kodni aynan ikkinchisi amalga oshiradi 2-rasm. 3-rasmda xatolik ko’rsatiladi va 4-rasmda administratorga xabar jo’natiladi.

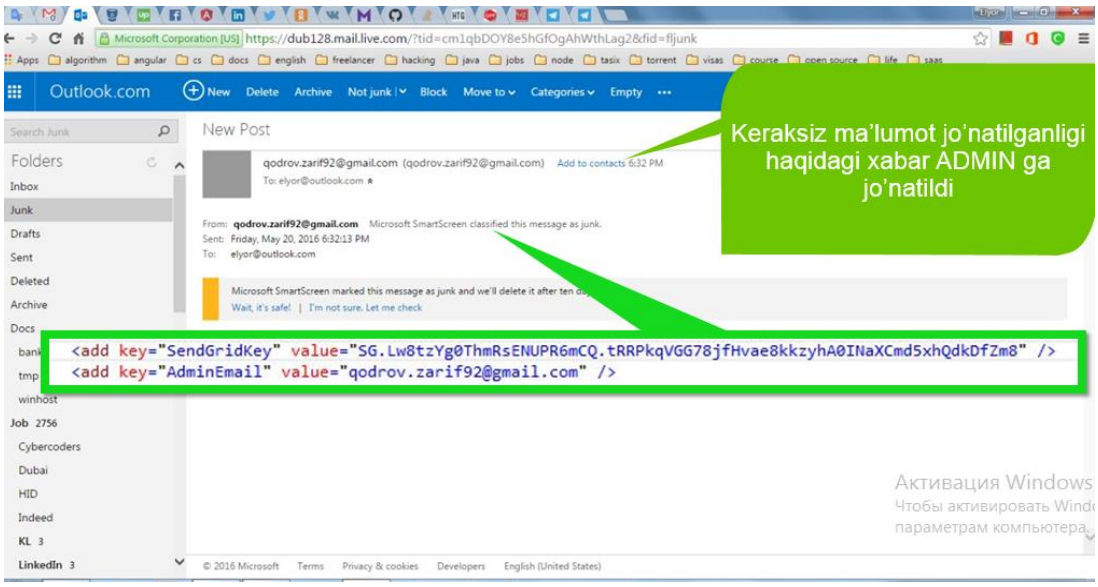


2-rasm. Hujum qilish jarayoni.



3-rasm. Klientga xatolik ko’rsatish jarayoni.

Ushbu dastur orqali veb saytlarni himoya qilish vazifasi bajariladi va administratorga hujum qilinayotgan paytning o’zida xabar jo’natiladi. Kelajakda bu dasturni yanada rivojlantirish maqsadida turli ishlar amalga oshirilmoqda.



4-rasm. Administratorga xabar jo'natish jarayoni.

АХБОРОТ ТИЗИМЛАРИДА ХАВФ ЭҲТИМОЛИНИНГ ТАҲЛИЛИ

А.Н. Қудратов (Гулистон давлат университети, катта ўқитувчи)
Д.Э. Абдураимов (Гулистон давлат университети, катта ўқитувчи)

Бугунги кунда ахборот коммуникация технологияларининг юқори суръатларда ривожланиб бориши ва барча соҳаларда кенг қўлланилиши, янгидан-янги имкониятларни яратиш билан бир қаторда, ўзига хос муаммоларни келтириб чиқармоқда. Бу муаммолардан бири ахборот коммуникация тизимларида ахборот хавфсизлигини таъминлаш хисобланади. Ахборот хавфизлигини таъминлашда хавф эхтимолларини тахлил қилиш ва баҳолаш асосий масалалардан бири хисобланади.

Хавф эҳтимолини батафсил таҳлил қилишда қуйидаги бир қатор мураккаб масалаларни ечиш зарур бўлади:

- белгиланган ресурсларни қадр-қийматини қандай аниқлаш;
- ахборот хавфсизлигига таҳдидларни тўла рўйҳатини тузиш ва баҳолаш;
- хар бир маълум хавф-хатарга қарши самарали ҳимоя чораларини танлаш.

Бу масалаларни ечишда хавф эҳтимолини таҳлил қилиш жараёни бир неча босқичлардан иборат бўлади:

- белгиланган ахборот ресурсларини идентификациялаш;
- баҳолаш мезонларини танлаш ва ресурсларга хамда иловаларга потенциал негатив таъсирларни аниқлаш ва баҳолаш;
- кўрсатилаётган таҳдидларни баҳолаш;
- химоялаш жараёнида заифликларни баҳолаш;
- хавфлар эҳтимолларини баҳолаш;
- ахборот хавфсизлигини таъминловчи мавжуд ва таклиф қилинаётган воситаларнинг самарадорлигини баҳолаш.

Хавф эҳтимолини таҳлили асосида ахборот хавфсизлигини таъминлаш кетма-кетлиги аниқланади. Бизнес учун салмоқли ва маълум даражадаги заифликка эга бўлган ресурсларга нисбатан бирор бир таҳдид мавжуд бўлса, хавф эҳтимоллиги юқори бўлади. Хавф эҳтимолини баҳолашда потенцииал негатив номақбул ходисалардан келиб чиқадиган таъсирлар ва кўрилаётган заифлик хамда таҳдидларнинг муҳим ўрин тутиши кўрсаткичлари ҳисобга олинади.

Хавф эҳтимоли қуйидаги бир қатор омилларга боғлиқ:

- белгиланган ресурсларнинг қадр-қиймати;
- таҳдидларни амалга ошириш эҳтимоллари;
- таҳдидни амалга оширишда заифликдан фойдаланишнинг соддалиги;
- заифликлар кўламини камайтиришга кўмаклашувчи воситалар;
- таҳдидларни юзага келиши эҳтимолини камайтирадиган ва нохуш таъсирлар;
- таҳдидларни амалга ошириш имкониятини камайтирадиган ахборот хавфсизлигини таъминловчи мавжуд ёки тадбиқ қилиниши режалаштирилаётган воситалар.

Ресурсларни қадр-қийматини аниқлаш. Одатда ресурслар бир неча синфларга бўлинади, масалан, жисмоний, дастурий ресурслар, маълумотлар. Хар бир синфга мос келувчи мезонлар тўпламини ва элементлар қадр – қийматини аниқлаш. Бу мезонлар маълумотлар конфеденциаллигини, ахборот тизимининг яхлитлигини, фойдаланиш даражасини бузилиши билан боғлиқ потенциал зарарни ифодалаш учун хизмат қилади.

Жисмоний ресурслар уларни алмаштириш ёки ишлай олиш қобилиятини тиклаш билан боғлиқ харажатлар нуқтаи назаридан баҳоланади. Бу харажатлар кўрсаткичлари сўнгра поғонали (сифат) шкаласига ўтказилиб, ахборот ресурслари учун ҳам қўлланилиши мумкин.

Дастурий ресурслар худди жисмоний ресурслар каби шу усулда баҳоланади, бу холда уларни сотиб олиш ёки тиклаш учун зарур харажатлар асосида аниқланади. Агар ахборот ресурсига конфеденциаллик ва ахборот тизимининг яхлитлигига алоҳида қўшимча талаблар мавжуд бўлса, (масалан, бирламчи матн юқори тижорат қадр – қийматига эга бўлса) бу холда бу ресурсни баҳолаш келтирилган схема бўйича, яъни нарх кўрсаткичларида амалга оширилади.

Тижорат ташкилотлари молиявий зарарни ифодаловчи мезонлардан ташқари, қуйидаги мезонлардан фойдаланишлари мумкин:

- ташкилот обрўсига етган маънавий зарар;
- амалдаги қонунчилик бузилиши сабабли келиб чиққан нохуш холатлар;
- ходимлар саломатлигига етказилагн зарар;
- ходимларни шаҳсий маълумотларини ошкор этилишидан келиб чиқадиган зарар;
- ахборотни ошкор этилишидан келиб чиқадиган молиявий зарар;
- ресурсларни тиклаш билан боғлиқ молиявий зарар;
- мажбуриятларни бажариш имконияти йўқотилиши билан боғлиқ зарар;
- фаолиятни издан чиқаришдан келиб чиққан зарар.

Ташкилотнинг профилига боғлиқ равишда бошқа мезонлар хам қўлланиши мумкин. Масалан давлат органлари учун миллий хавфсизлик ёки халқаро муносабатлар жиҳатларини ифодаловчи мезонлар бўлиши мумкин.

Хавф эҳтимолини баҳолашга сонли ёки сифат ёндашувдан фойдалинишни танлашда ташкилот бизнесининг характерига ва ахборотлаштириш савиясига эътибор берилади, яъни, унга ахборот активларининг муҳимлиги хамда ташкилот савияси билан аниқланади. Ахборот хавфсизлигидаги хавф эҳтимолларини бошқаришнинг самарадорлиги хавф эҳтимолини баҳолашдаги аниқлик ва таҳлилнинг тўлалиги хамда ташкилотда қўлланилаётган ва қабул қилинаётган бошқарув ечимларини қабул қилиш ва улар ижросини назорат қилиш механизмларига боғлиқ бўлади.

КИРИШНИ НАЗОРАТЛАШ ВА БОШҚАРИШ ТИЗИМЛАРИ АРХИТЕКТУРАЛАРИНИНГ ТАҲЛИЛИ

А.Т. Имамалиев (ТАТУ, ассистент)
Б.К. Юсупов (ТАТУ, ассистент)

Кучли марказий контроллерлардан фойдаланиладиган турли хил архитектурали тақсимланган объектлардаги киришни назоратлаш ва бошқариш тизимининг мавжуд

жараёнлари ихтисослаштирилган масофавий модул интерфейслар ёрдамида бошқарилади. Қўлланиладиган талабларни аниқлашнинг ўзига хос хусусияти шундаки, дастурий таъминотга эга бўлган бундай тизимларда ҳар доим марказлашган ёки тақсимланган архитектурали, баъзан, иккаласи бирлаштирилга ҳолдаги архитектурали киришни назоратлаш ва бошқариш тизимларидан фойдаланилади.

Марказлашган архитектурали киришни назоратлаш ва бошқариш тизими. Тақсимланган киришни назоратлаш ва бошқариш тизими асосан қўриқланувчи объектнинг узоқроқ масофада жойлашган алоҳида бинолари билан биргаликда қўлланилади. Бунда ҳар бир бинода марказлаштирилган контроллерлар бўлиши шарт. Бу алоҳида бинода содир бўлиши мумкин бўлган бузғунчиликлардан ҳимоялашда ҳар бир бинонинг хавфсизлик тизимини автоматик равишда функциялаштирилишини таъминлайди. Бир контроллерга уланадиган ўқиб олувчилар сони қоида бўйича, 16 тадан 96 тагача оралиқни ўз ичига олади. Шунинг учун одатда битта контроллернинг қуввати йирик тақсимланган тизимнинг алоҳида объектида киришни назоратлаш ва бошқариш тизимини яратиш учун тўла етарлидир. Марказлашган киришни назоратлаш ва бошқариш тизимининг контроллерлари мантиқий қурилмалардир ва эшикларни бошқармайди яъни, қулуфларни бошқарувчи чиқиш релелари йўқ ва фойдаланишни назоратлаш ва бошқариш тизимининг ўқиб олувчиси(ридери)ни улашда кириш эшикларини, бошқа ташқи қурилмалар ташқи модул интерфейсини бажарадиган бошқариш функцияси ва реле блоклари йўқ. Улар қоида бўйича, бошқариш объектига(эшиклар, қўриқланувчи дарвозалар ва ҳ.к.) яқин бўлган жойга ўрнатилади. Контроллерлар ўртасида мълумот алмашинишда RS-485 интерфейсидан фойдаланилади. Марказлашган контроллерларни бир-бирлари билан улашда асосан RS-485 интерфейси қўлланилади. Марказлашган архитектурали тизимнинг контроллери барча маълумотлар базасидаги идентификаторларни ва ҳолатларни ўзида сақлайди. Юқори ҳимояланадиган жойнинг бошқариладиган компьютерлар(серверлар)дан унча узоқ бўлмаган жойларга ўрнатилади. Катта масштабдаги киришни назоратлаш ва бошқариш тизимини яратишда бундай контроллерларни тармоққа бирлаштириш мумкин. Алоқа бузилганда компьютер тизими билан контроллер автоном режимда ишлайди.

Тақсимланган архитектурали киришни назоратлаш ва бошқариш тизими. Тақсимланган архитектурали киришни назоратлаш ва бошқариш тизимининг ўзига хос жихати шундаки, идентификаторларнинг маълумотлар базиси битта эмас, бир нечта контроллерларда сақланади. Улар одатда контроллер платасига бевосита ўрнатилган кирувчи қўриқлаш сигнализациясини, реле орқали қўриқлаш шлейфларини ва ташқи қурилмаларни бошқариш функциясини бажаради. Бу контроллерлар қоида мувофиқ бинонинг ички ҳимоясини бевосита ўрнатади. Бу контроллерларни рухсатсиз монипуляция қилиш эҳтимоллигини пасайтирмайди, аммо бундай ёндошиш контроллер ва интерфейс модули ўртасида алоқанинг бузилишларини камайтиради. Компьютер тизими ва контроллерлар ўртасидаги алоқа линиялари узилган ҳолларда кириш жараёнини бошқаришнинг асосий функциясини бажариш автоним режимда амалга оширилади. Ўрнатилган контроллерлардан бири бошқасининг ишлашига таъсир кўрсатмайди. Тақсимланган архитектурали тизим контроллери ўтишнинг 4 тагача бўлган эшикларни бошқара олади. Бундай тақсимланган киришни назоратлаш ва бошқариш тизими ўз ичига бир нечта контроллерларни олади ва ҳар бир бино учун алоҳида-алоҳида контроллерлар ўрнатилади. Бу контроллер мустақил таҳлил қилади ва ўз хотирасида киритилган маълумотларни сақлаб қолади. Сақлаб қолинган маълумотлар бошқарувчи компьютерга узатилади. Бу тизим узоқдаги бинолар билан амалий алоқа ўрнатилишида кучайтиргичлар интерфейсини қўллашни талаб қилади. Бу эса ҳар доим ҳам қулай ҳисобланмайди ва ишончлилик даражасини пасайтириб юборади. Шунинг учун бир нечта биноларнинг барча қисмтизимларини бир бутунлилигини кўриб чиқиш талаб этилади.

Аралаш архитектурали киришни назоратлаш ва бошқариш тизими. Одатда бундай тизим марказлашган архитектурали фойдаланишни назоратлаш ва бошқариш тизими

махсус ўқиб олувчилар(ридерлар)ни ўз таркибига қўшишни ёки интерфейсли модулларининг хотира буферларида сақланувчи холатлар ва идентификаторларни ўз ичига олади. Бундай модуллар унча катта бўлмаган киришни назоратлаш ва бошқариш тизимининг контроллерларига эга. Демак, марказлашган архитектурали киришни назоратлаш ва бошқариш тизимининг контроллерлари бир қанча эшикларни бошқара олса, контроллерлар ўртасидаги алоқа линиялари шикастланганда интерфейсли модулнинг бошқариш қурилмаси тизимни қисман ёки тўлиқ блокировка қилиб қўйиши мумкин. Локал ўқиб олувчи ёки интерфейсли блок ўртасида ўрнатилган хотира буфери бўлади.

Киришни назоратлаш ва бошқариш тизимининг архитектурасини тўғри танлаш зарур. Бунда кучли марказий контроллерлардан фойдаланиладиган турли хил тақсимланган объектлардаги киришни назоратлаш ва бошқариш тизимининг мавжуд жараёнлари ихтисослаштирилган масофавий модул интерфейслар ёрдамида бошқарилувчи, локал ўқиб олувчи(ридер), интерфейсли блок ўртасида ўрнатилган хотира буферига эга бўлган аралаш архитектурали киришни назоратлаш ва бошқариш тизимини қуриш тавсия этилади.

ҚЎРИҚЛАНАЁТГАН ОБЪЕКТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ МУАММОСИГА ДОИР

А.Т. Имамалиев (ТАТУ, ассистент)

Объектларни қўриқлаш масаласини самарали хал қилиш учун ҳар бир муайян ҳудудга талаб қилинадиган техник хавфсизликни таъминлаш тизимини танлаш бўйича, таҳдидларни бир вақтнинг ўзида фош этишда кетма-кет жойлашган хавфсизлик худудлари аниқланилади.

Бундай ҳудудлар кетма-кетлик тартибида жойлашган бўлиши керак. Умумун олганда, объект худудини ўрашдан тортиб то обектнинг жиддий элементларигача яъни, сейфлар, сақланадиган қиммат баҳо буюмлар ҳамда маълумотлар ва бошқалар эътиборга олиниши керак. Хавфсизлик зонасини ҳимояси қанчалар мустахкам ва ишончли бўлса, тартиб бузарларнинг бу ҳудудларга кириши шунчалар қийин бўлади.

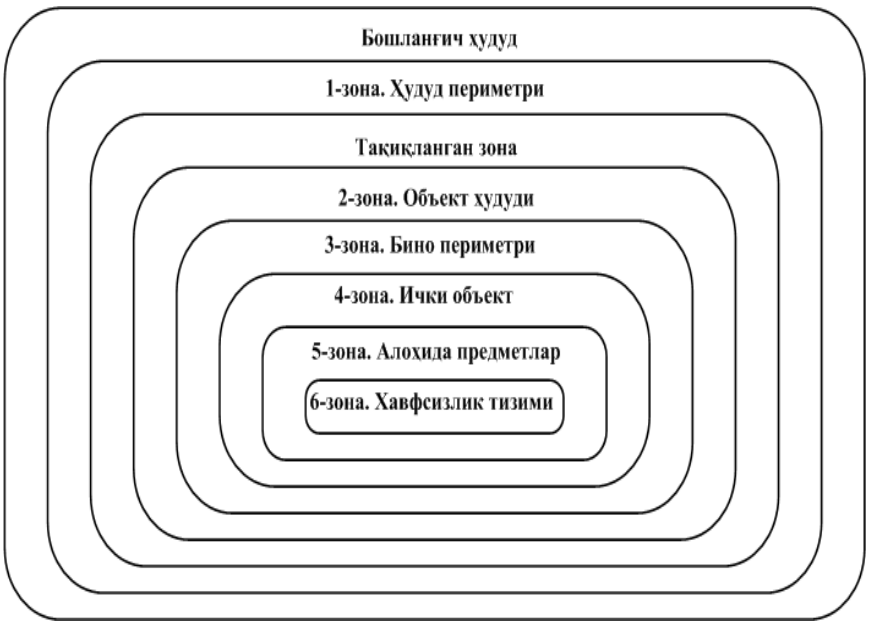
Бу жиноятчилар ёки тартиб бузарларни объектларга киришида кўп вақт сарифлашига олиб келади, натижада огохлантирувчи сигнал ишга тушади ва уларни қўлга олиш имкони туғилади. Демак, таҳдидга қарши тураолиш самарадорлигини ошириш ва огоҳлантириш сабабини аниқлаш учун қўриқлаш хизмати етарлича вақт сарифлайди.

Бошланғич ҳудуд. Хавфсизликни таъминлашнинг бошланғич зонасида майдонлар бирлаштирилади. У объект қисми ҳисобланмайди ва рухсатсиз киришни ташкил этиш бўйича тайёргарлик кўриш ишлари учун бузғунчи фойдаланиши мумкин бўлган жой ҳисобланади. Масалан, объектнинг қўриқлаш тартибини ва унинг қўриқлаш структурасини ўрганиши ва кузатиши мумкин. Шунинг учун худуд атрофи телевизион қўриқлаш воситалари орқали назоратланиши ва хавфсизлиги таъминланиши керак.

Биринчи зона. Бу зона объекет ҳудудининг ташқи периметри ҳисобланади.

Биринчи зонада мустаҳкам инженер-техник воситалардан(девор, тўсиқ), телвизион қўриқлаш тизимларидан, таркибида қўриқлаш сигнализацияси мавжуд бўлган периметрларни қўриқлаш воситаларидан, шунингдек, қоровуллар яъни хавфсизлик хизмати ходимлари ёки идоранинг қоровуллик хизмати ишчиларидан фойдаланилади.

Тақиқланган зона. Объект худудининг ички томонидаги периметир деворларининг баландлигини ва унда назарда тутилган ҳолда техник қўриқлаш воситаларининг жойлаштирилиши ҳамда хизмат вазифаларни бажарувчи қўриқлаш идорасининг шаҳсий таркиби томонидан ташкил этилади.



1-расм. Хавфсизликни таъминлаш бўйича зоналарнинг жойлашиши.

Тақиқланган зона пухталик билан режалаштирилган ва тозалаб қўйилган бўлиши керак. Унда қоровуллар ҳаракатини ва техник қўриқлаш тизимини қўллашга халақит берадиган хеч қандай қурилишлар, нарсалар ва дарахтлар бўлмаслиги керак.

Иккинчи зона. Бу зона қўриқланувчи объект худудини ўз ичига олади.

Мазкур зонанинг ҳимоясида комплекс чора-тадбирлардан, телевизион қўриқлаш воситалари ва қўриқлаш-ёнғин сигнализацияларидан фойдаланилади.

Учинчи зона. Қўриқлашнинг бу зонаси қўриқланаётган бино ёки иншоот периметрининг элементлари таркибига қуйидагилар киради:

- объект биносининг периметри бўйича конструктив қурилишлар, яъни, барча дераза ва эшик ўринлари;
- коммуникацияларнинг кириш жойлари;
- фавқулотда холатлар ва ёнғин нарвонларига чиқиш жойлари;
- асосий ва асосий бўлмаган деворлар; вентеляция қутилари ва ҳавони тозалаш қувурлари.

Бу зона телевизион қўриқлаш тизими, сигнализация қўриқлаш тизими воситалари ва қоровуллар орқали бошқарилади.

Тўртинчи зона – объект биносининг ички қисми.

Киришни назорат қилиш ва бошқариш тизимининг техник воситалари ёрдамида тўртинчи зонанинг ички объекти ва ўтиш тартиби ҳамда объектни қуйидаги учта асосий зоналари ажратиб кўрсатилган бўлиши керак:

- биринчи зона (эркин кириш зонаси) – объектда ишловчи ходимлар, ташриф буюрувчи шаҳсларни бинога, территорияга иншоотга кириши чекланмаган;
- иккинча зона (вақт бўйича чекланган ёки авторизацияланганлик даражаси бўйича кириш зонаси) – бинога кириш чекланган вақтда рухсат этилади(масалан, ишчиларнинг ишлаш вақти ходимларнинг иш тартибига киритилган бўлса) ёки шаҳслар таркибини чеклаш яъни, объектга ташриф буюрувчиларни ўтказиш турлари бўйича ёки объект ходимларининг ҳамрохлигида ўтказиш;
- учинчи зона – объектнинг махсус биносига кириш қатъий тартибда раҳбарият ва хавфсизлик ходимларининг рухсати билан амалга оширилади.

Фойдаланувчилар объектга киришни назоратлаш пунктлари орқали ўтишда қуйидагиларни амалга ошириши керак:

- биринчи зонага биргина идентификациялаш белгиси бўйича кирилади;
- иккинчи зонага кириш иккита идентификациялаш белгиси бўйича амалга оширилади(масалан, электрон карточкалар ва механик қулуфнинг калити);

- учинчи зонага кириш иккитадан кам бўлмаган идентификациялаш белгилари бўйича амалга оширилади.

Бу ерда қуйидаги хавф-ҳатарлар кўзда тутилиши мумкин: молиявий ресурслар ва моддий бойликлар сақланадиган бинога рухсатсиз киришга уриниш; телевизион қўриқлаш тизими ва қўриқлаш сигнализация воситаларининг ишга яроқсиз бўлиб қолиши; ахборот ташқарига чиқиб кетиши мумкин бўлган яширин эшитиш воситаларини ўрнатилиши;

Бу зона сигнализация қўриқлаш, киришни назорат қилиш ва бошқариш тизими, телевизион қўриқлаш тизими воситалари билан биргаликда ахборотни ҳимоялаш воситалари ва қоровуллар орқали назорат қилинади.

Бешинчи зона – бу зонада алоҳида предметлар яъни, сейфлар, картинкалар, хайкалтарошлик асарлари, қимматли маълумотлар, конфиденциал ахборот ва шу кабилар бўлиши мумкин.

Олтинчи зона – ҳусусий хавфсизлик тизими. Бу хавфсизликни таъминловчи техник ва дастурий воситалар ҳимоясини ўз ичига олади.

Хавфсизлик тизимининг асосий функциясини бажара олмаслиги учун уни тўлиқ ишдан чиқариш ёки маълум бир элементларини блокировка қилиш мақсадида улардан руҳсатсиз фойдаланишга бўладиган уринишларни олдини олишда, қўриқланаётган объект ҳимоясини тўғри ташкил этиш ва ҳар бир зоналарда хавфсизликни таъминлашга бўлган талабларни тўғри белгилаш керак.

СИСТЕМЫ МОНИТОРИНГА КАК ОДНО ИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

З. Азизова (ТУИТ, магистрант)

Сегодня, когда мы можем наблюдать тот факт, что масштабное внедрение информационно-коммуникационных технологий в различные виды деятельности способствует развитию таких сфер как экономика, образование, медицина, финансы, культура и другие. Невозможно не уделять должного внимания аспекту безопасности, необходимому для всех процессов, при реализации которых осуществляется та или иная деятельность. В подобных условиях возникает необходимость автоматизированной обработки всей информации с задачей последующего обнаружения угроз информационной безопасности (ИБ) и оценкой возможных рисков, которые могут возникнуть непосредственно при эксплуатации различных систем. В этой связи обеспечение ИБ само по себе требует не только определенных финансовых затрат, но и трудовых. Поэтому у различных организаций и учреждений возникают дополнительные задачи контроля за тем, чтобы эти затраты не были потрачены впустую, а сама система обеспечения защиты информации была достаточно быстрой и продуктивной для данной организации или учреждения.

В последнее время свою актуальность получили проблемы мониторинга ИБ, а также выявление, оценка и обработка возникших инцидентов ИБ в наикратчайшие сроки. Связано это с увеличением зависимости организаций от информации и информационной системы. Возросла уязвимость ИС за счет повышения сложности элементов информационных систем, появления новых технологий передачи и хранения данных, увеличения объема программного обеспечения. Возросло число угроз из-за активного использования организациями открытых глобальных сетей для передачи сообщений и транзакций. Несмотря на выбор традиционных методов защиты с использованием VPN-сетей, средств защиты от НСД, файерволов, для построения надежных и эффективных систем их использование не всегда является достаточным.

Мониторинг безопасности систем позволяет получить информацию в реальном времени о состоянии, активности устройств и о событиях с контекстом безопасности, происходящих в устройствах, например, о потенциальных атаках. Одним из

распространенных способов осуществления мониторинга является мониторинг событий, который может проводиться на основе данных, полученных из журналов событий, средств антивирусной защиты, сетевого оборудования, систем обнаружения вторжений (IDS-систем), систем предотвращения вторжений (IPS-систем) и так далее. Система мониторинга событиями ИБ представляет собой организацию комплексного подхода решению таких задач как сбор, анализ и контроль событий ИБ от различных средств защиты. Это, в свою очередь, дает возможность идентификации инцидентов ИБ в режиме реального времени, при этом получая текущие данные, необходимые для дальнейшего анализа рисков, и принятия решений, относительно имеющихся угроз с целью обеспечения информационной безопасности. В конечном счете, к решающим задачам системы управления событиями или мониторинга можно отнести следующие:

- определение полноты всего происходящего в компьютерных системах;
- управление значительным объемом событий информационной или компьютерной системы;
- наблюдение за текущим уровнем обеспечения безопасности;
- выявление инцидентов информационной безопасности;
- определение данных для оценки и анализа рисков с последующим решением по менеджменту информационной безопасности.

Мониторинг, как и любая система, включает целый ряд компонентов, обеспечивающих её полноценное функционирование. К подобным компонентам общепринято относить подсистему сбора информации, которая поступает от средств защиты уже имеющихся в той или иной системе; сервер событий, главной задачей которого является централизованная обработка поступающей информации о тех событиях, которые имеют отношение к безопасности сети, по заданным правилам администратора; сервер хранения первичной информации или событий, а также полученных результатов проведенного анализа; интерфейс пользователя по управлению системой мониторинга, который позволяет осуществлять контроль и управление в реальном масштабе времени.

Растущее число организаций, заботящихся об ИБ своей деятельности, активно используют системы мониторинга, благодаря чему повышается эффективность процесса выявления угроз и дисфункций сети или системы, а также значительно сокращается время реагирования на инциденты, относящиеся к ИБ и увеличивается качество принимаемых решений. Подобного результата можно добиться посредством автоматизации сбора и анализа данных о всех процессах сети и системы, регистрируемых в системе мониторинга автоматически.

При проектировании и разработке систем мониторинга необходимо учитывать, что в качестве пользователей подобных систем выступают специалисты своей области, это является одной из причин, почему системы должны быть ориентированы именно на них, а не на обычных пользователей.

Применение систем мониторинга в определенной степени повышает эффективность ранее установленных средств защиты за счёт синергетического эффекта, а именно суммирующего эффекта взаимодействия двух или более факторов характеризующегося тем, что их действие существенно превосходит эффект каждого отдельного компонента в виде их простой суммы при обработке данных, имеющих отношение к ИБ.

ТАРМОҚ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ УСУЛИ

О.М. Алланов (ТАТУ, ассистент)

Мамлакатимиз сиёсатининг устувор йўналишларига киритилган компютер ва ахборот технологиялари, телекомуникация, маълумотларни узатиш тармоқлари, Интернет

хизматларидан фойдаланиш ривожланмоқда ва модернизациялашмоқда. Жамиятимизнинг барча соҳаларига кундалик ҳаётимизга замонавий ахборот технологияларини кенг жорий этиш истиқболдаги мақсадларимизга эришишни таъминлайди. Ҳар бир соҳа фаолиятида Интернет тармоғидан фойдаланиш иш унумдорлигини оширмоқда.

Айнан тармоқдан фойдаланган ҳолда тезкор маълумот алмашиш вақтдан ютиш имконини беради. Хусусан, юртимизда Электрон ҳукумат тизими шакллантирилиши ва унинг замирида давлат бошқарув органлари ҳамда аҳоли ўртасидаги ўзаро алоқанинг мустаҳкамланишини ташкил этиш тармоқдан фойдаланган ҳолда амалга ошади. Тармоқдан самарали фойдаланиш демократик ахборотлашган жамиятни шакллантиришни таъминлайди. Бундай жамиятда, ахборот алмашинув тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича тезкор натижага эга бўлинади.

Бироқ тармоққа ноқонуний кириш, ахборотлардан фойдаланиш ва ўзгартириш, йўқотиш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди. Иш фаолиятини тармоқ билан боғлаган корхона, ташкилотлар ҳамда давлат идоралари маълумот алмашиш учун тармоққа боғланишидан олдин тармоқ хавфсизлигига жиддий эътибор қаратиши керак. Тармоқ хавфсизлиги узатилаётган, сақланаётган ва қайта ишланаётган ахборотни ишончли тизимли тарзда таъминлаш мақсадида турли воситалар ва усулларни қўллаш, чораларни кўриш ва тадбирларни амалга ошириш орқали амалга оширилади. Тармоқ хавсизлигини таъминлаш мақсадида қўлланилган восита хавф-хатарни тезда аниқлаши ва унга нисбатан қарши чора кўриши керак. Тармоқ хавфсизлигига таҳдидларнинг кўп турлари бор, бироқ улар бир неча
тоифаларга бўлинади:

- ахборотни узатиш жараёнида ҳужум қилиш орқали, эшитиш ва ўзгартириш (Eavesdropping);
- хизмат кўрсатишдан воз кечиш; (Denial-of-service);
- портларни текшириш (Port scanning).

Ахборотни узатиш жараёнида, эшитиш ва ўзгартириш ҳужуми билан телефон алоқа линиялари, интернет орқали тезкор хабар алмашиш, видеоконференция ва факс жўнатмалари орқали амалга ошириладиган ахборот алмашинувида фойдаланувчиларга сездирмаган ҳолатда ахборотларни тинглаш, ўзгартириш ҳамда тўсиб қўйиш мумкин. Бир қанча тармоқни таҳлилловчи протоколлар орқали бу ҳужумни амалга ошириш мумкин. Ҳужумни амалга оширувчи дастурий таъминотлар орқали CODEC (видео ёки овозли аналог сигнални рақамли сигналга айлантириб бериш ва аксинча) стандартидаги рақамли товушни осонлик билан юқори сифатли, аммо катта ҳажмни эгаллайдиган овозли файллар (WAV)га айлантириб беради. Одатда бу ҳужумнинг амалга оширилиш жараёни фойдаланувчига умуман сезилмайди. Тизим ортиқча зўриқишларсиз ва шовқинсиз белгиланган амалларни бажараверади. Ахборотнинг ўғирланиши ҳақида мутлақо шубҳа туғилмайди. Фақатгина олдиндан ушбу таҳдид ҳақида маълумотга эга бўлган ва юборилаётган ахборотнинг ўз қийматини сақлаб қолишини хоҳловчилар махсус тармоқ хафвсизлик чораларини қўллаш натижасида ҳимояланган тармоқ орқали маълумот алмашиш имкониятига эга бўладилар. Тармоқ орқали маълумот алмашиш мобайнида юборилаётган ахборотни эшитиш ва ўзгартиришга қарши бир неча самарали натижа берувчи технологиялар мавжуд:

- IPSec (Internet protocol security) протоколи;
- VPN (Virtual Private Network) виртуал хусусий тармоқ;
- IDS (Intrusion Detection System) рухсатсиз киришларни аниқлаш тизими.

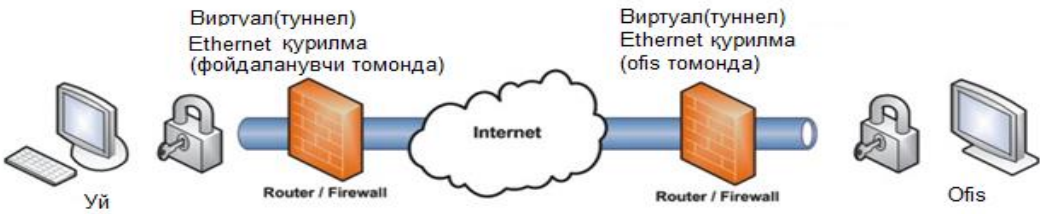
IPSec (Internet protocol security) бу хавфсизлик протоколлари ҳамда шифрлаш алгоритмларидан фойдаланган ҳолда тармоқ орқали хавфсиз маълумот алмашиш имконини беради. Бу махсус стандарт орқали тармоқдаги компютерларнинг ўзаро алоқасида дастур ва маълумотлар ҳамда қурилмавий воситалар бир-бирига мос келишини таъминлайди. IPSec протоколи тармоқ орқали узатилаётган ахборотнинг сирлилигини,

яъни фақатгина юборувчи ва қабул қилувчига тушунарли бўлишини, ахборотнинг софлигини ҳамда пакетларни аутентификатсиялашни амалга оширади. Замонавий ахборот технологияларни қўллаш ҳар бир ташкилотнинг ривожланиши учун зарурий восита бўлиб қолди, IPSec протоколи эса айнан қуйидагилар учун самарали
ҳимояни таъминлайди:

- бош офис ва филиалларни глобал тармоқ билан боғлаганда;
- узоқ масофадан туриб, корхонани интернет орқали бошқаришда;
- ҳомийлар билан боғланган тармоқни ҳимоялашда;
- электрон тижоратнинг хавфсизлик даражасини юксалтиришда.

VPN (Virtual Private Network) виртуал хусусий тармоқ сифатида таърифланади. Бу технология фойдаланувчилар ўртасида барча маълумотларни алмашиш бошқа тармоқ доирасида ички тармоқни шакллантиришга асосланган, ишончли ҳимояни таъминлашга қаратилган. VPN учун тармоқ асоси сифатида Интернетдан фойдаланилади.VPN технологиясининг афзаллиги. Локал тармоқларни умумий VPN тармоғига бирлаштириш орқали кам харажатли ва юқори даражали ҳимояланган тунелни қуриш мумкин. Бундай тармоқни яратиш учун сизга ҳар бир тармоқ қисмининг битта компютерига филиаллар ўртасида маълумот алмашишига хизмат қилувчи махсус VPN шлюз ўрнатиш керак. Ҳар бир бўлимда ахборот алмашиши оддий усулда амалга оширилади. Агар VPN тармоғининг бошқа қисмига маълумот жўнатиш керак бўлса, бу ҳолда барча маълумотлар шлюзга жўнатилади. Ўз навбатида, шлюз маълумотларни қайта ишлашни амалга оширади, ишончли алгоритм асосида шифрлайди ва Интернет тармоғи орқали бошқа филиалдаги шлюзга жўнатади. Белгиланган нуқтада маълумотлар қайта дешифрланади ва охирги компютерга оддий усулда узатилади. Буларнинг барчаси фойдаланувчи учун умуман сезилмас даражада амалга ошади ҳамда локал тармоқда ишлашдан ҳеч қандай фарқ қилмайди. Eavesdropping ҳужумидан фойдаланиб, тингланган ахборот тушунарсиз бўлади. Бундан ташқари, VPN алоҳида компютерни ташкилотнинг локал тармоғига қўшишнинг ажойиб усули ҳисобланади. Тасаввур қиламиз, хизмат сафарига ноутбукингиз билан чиққансиз, ўз тармоғингизга уланиш ёки у ердан бирор-бир маълумотни олиш зарурияти пайдо бўлди. Махсус дастур ёрдамида VPN шлюз билан боғланишингиз мумкин ва офисда жойлашган ҳар бир ишчи каби фаолият олиб боришигиз мумкин. Бу нафақат қулай, балки арзондир. VPN ишлаш тамойили. VPN тармоғини ташкил этиш учун янги қурилмалар ва дастурий таъминотдан ташқари иккита асосий қисмга ҳам эга бўлиш лозим: маълумот узатиш протоколи ва унинг ҳимояси бўйича воситалар. Рухсатсиз киришни аниқлаш тизими (IDS) ёрдамида тизим ёки тармоқ хавфсизлик сиёсатини бузиб киришга ҳаракат қилинган усул ёки воситалар аниқланади. Рухсатсиз киришларни аниқлаш тизимлари деярли чорак асрлик тарихга эга. Рухсатсиз киришларни аниқлаш тизимларининг илк моделлари ва прототиплари компютер тизимларининг аудит маълумотларини таҳлиллашдан фойдаланган. Бу тизим иккита асосий синфга ажратилади. Тармоққа рухсатсиз киришни аниқлаш тизими (Network Intrusion Detection System) ва компютерга рухсатсиз киришни аниқлаш тизимига (Host Intrusion Detection System) бўлинади.

Қуйидаги 1-расмда икки томон ўртасидаги маълумот алмашиш учун хавфсиз усул таклиф қилинган. Унда фойдаланувчининг уйи ва офиси ўртасида VPN тармоғини ташкил қилиш усули келтирилган.



1-расм. VPN тармоғини ташкил килиш схемаси

Юқорида таклиф қилинаётган усул тармоқдан фойдаланган ҳолда маълумот алмашинилганда унинг хавфсизлигини таминлаш учун самарали ечим ҳисобланади. Унда фойдадланувчи уйидан туриб офисидаги махфий маълумотларидан бемалол фойдаланиши мумкин. Фойдаланувчи махфий маълумотларидан хавфсиз фойдаланиш учун ташкил қилинган VPN тармоғи ва аутентификация тизими ишончли восита бўлиб ҳисобланади.

КРИПТОГРАФИК ХЭШ ФУНКЦИЯЛАРНИНГ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДАГИ ЎРНИ

О.М. Алланов (ТАТУ, ассистент)

Ушбу мақола криптографик хэш функцияларни ўз ичига олган. Бир қарашда криптграфик хэш функциялар мураккаб сирлидек кўринади. Шунга қарамасдан, хэш функциялар ахборот хавфсизлиги соҳасида муҳим аҳамиятга эга. Криптографик хэш функциялар асосан электрон рақамли имзода ва хэшланган МАС да қўлланилади. Бу ерда эса криптографияга алоқадор бўлган муҳим жиҳатлари келтирилган.

Компьютер саводхонлигида “хэшлаш” деган тушанча жуда кенг қўлланилади. Криптографияда, хэш функциянинг жуда қимматли маънога, шуниндек вақтга алоқадор хусусияти муҳим бўлиб, қолган хусусиятларни эсдан чиқариш мақсадга мувофиқдир.

Криптографик хэш функция $h(x)$ қуйидагиларнинг барчасини таминлаши шарт:

- **сиқиш** – ихтиёрик узунликдаги кирувчи x учун, чиқувчи $y=h(x)$ нинг узунлиги етарлича кичик бўлиши керак. Амалда чиқувчи узунлик кирувчи қиймат узунлигидан қатий назар фиксирланган бўлади (масалан, 160 бит).
- **самарадорлик** – ихтиёрий узунликдаги кирувчи x учун $h(x)$ ни ҳисоблаш содда бўлсин. Ҳисоблашдаги самарадорлик катта ресурсни талаб этмайди.
- **бир томонламалик** – ихтиёрий y учун, x ни топиш имкони бўлмаслиги керак, яъни, $h(x)=y$. Бошқа сўз билан айтганда, хэшни орқага қайтариш имкони бўлмаслиги шарт.
- **заиф коллизияга бардошлик** – берилган x ва $h(x)$ учун, қуйидаги шартни бажарувчи y топиш имконсиз бўлсин, $y\neq x,\ h(x)=h(y)$. Бошқа сўз билан айтганда, хабар хеш қийматини ўзгартирмасдан, хабарни ўзини ўзгартириш имконсиз бўлсин.
- **кучли коллизияга бардошлик** – қуйидаги шартни бажарувчи x ва y ни топиш имконсиз бўлсин, $y\neq x,\ h(x)=h(y)$. Яъни, хэш қиймати бир хил бўлган, иккита хабарни топиш имконсиз бўлсин.

Чиқиш қиймати соҳасига қараган кириш қиймати соҳасининг катта бўлган ҳолда, кўплаб коллизиялар бўлиши мумкин. Масалан, бирор хэш функция 128 – битли қийматни генерация қилади. Агар 150 – битли кирувчи барча маълумотлар сони 2^{22} га тенг бўлишини (4 000 000 дан кўпроқ) ҳисобга олсак, ҳар бир кирувчи маълумотга такрорланмас чиқувчи маълумот мос келишини назарга тутсак, коллизия ҳодисаси бўлиши мумкин.

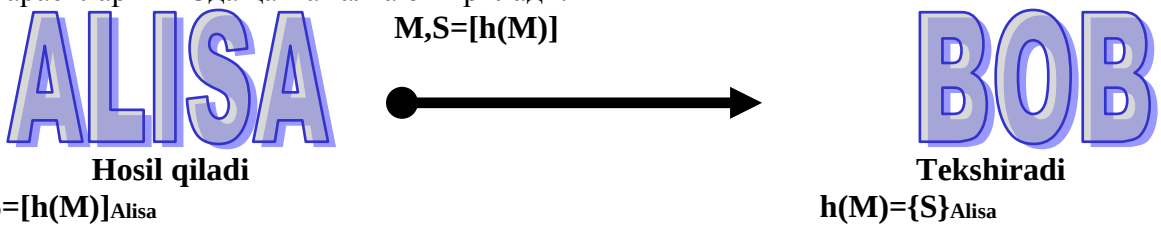
Хэш функция хавфсизлик соҳасида жуда муҳимдир. Биринчи кенг фойдаланиладиган йўналиш бу – электрон рақамли имзони ҳисоблашда ишлатилади. Масалан: Алиса M маълумотга имзо қўйишни ўзининг шахсий калити билан уни “шифрлаш” орқали амалга оширади, яъни у $S=[M]_{Алиса}$. Агар Алиса хабар M ва имзо S ни Бобга юборса, у ҳолда Боб имзо тўғрилигини қуйидаги тенгликни текшириб билади, $M=\{S\}_{Алиса}$. Шунга қарамасдан, агар M хабар жуда катта хажмда бўлса, у ҳолда $[M]_{Алиса}$ ҳисоблаш катта имкониятни, бундан ташқари M ва S ни юбориш катта трафикни талаб қилади. Тескари томондан, МАС ҳисобланган вақтда эса шифрлаш тезкор ва унга қўшилувчи маълумот бити кичик бўлиши керак.

Фараз қилайлик Алисада h криптографик хэш функция мавжуд. У ҳолда $h(M)$ қиймат M маълумотнинг “хэш қиймати (бармоқ изи)” сифатида кўринади, яъни, $h(M)$ қиймат M маълумотга қараганда жуда кичик, аммо, уни идентификациялайди. Агар M`

маълумот *M* маълумотдан ҳаттоки бир битга фарқ қилган тақдирда ҳам, уларнинг хэш қийматлари етарлича катта фарқ қилади. Бундан ташқари криптографик хэш функцияларнинг коллизияга бардошлилик хусусияти, *M* маълумотни *h(M)=h(M`)* шартни бажарувчи бошқа *M`* маълумот билан алмаштириш мумкин эмаслигини билдиради.

Алисада *h* криптографик функция мавжуд экан, *M* маълумотга имзо қўйишдан олдин, маълумотнинг хэш қийматини ҳисоблайди ва унга имзо қўйади, $S=[h(M)]_{Алиса.}$ Хэш қиймат самарали ва фақат кичик сондаги бит имзоланади.

Шундан сўнг, Алиса *M* ва *S* ни қуйидаги 1 – расмда кўрсатилганидек Бобга юборади. Боб имзони текшириш учун *M* маълумотни хешлайди қабул қилинган *S* қийматни Алисани очиқ калити билан дешифрлайди ва натижаларни солиштиради. Яъни, Боб, $h(M)=\{S\}_{Алиса}$ тенгликни текширади. Шуни эсда сақлаш лозимки, Алиса маълумот, *M* ва унга мос кичик ҳажмдаги имзо, *S* ни бобга юбориши талаб этилади. Шунингдек, бу жараёнлар МАСда ҳам амалга оширилади.



Расм 1. Имзо қўйишнинг мақбул йўли

Юқоридаги янги – такомиллаштирилган имзо схемаси хавфсизми? Агар коллизия бўлмаслигини ҳисобга олсак, имзо ва маълумот хавфсиз. Шу нарса аниқки, маълумотни ўзини имзолагандан кўра уни хэш қийматини имзолаган хавфсизроқ. Аммо, шуни эсдан чиқармаслик керакки, электрон рақамли имзо алгоритмларининг хавфсизлиги ҳар иккала, очиқ калитни шифрлаш алгоритми ва хэш функцияга боғлиқ бўлади. Улардан биттаси заиф бўлган тақдирда ҳам имзо хавфсиз бўлмайди.

Хэш функциялардан бундан ташқари спам хабарларни камайтирш учун фойдаланиш мумкин. Спам исталмаган ва сўралмаган хабарлар сифатида қаралади. Бу схемада, Алиса хабарларни токи юборувчи хабарни яратиш учун этарлича ҳаракатни оширганлиги ҳақида исбот бўлмагунга қадар рад этади. Бу ерда, “ҳаракат” ҳисоблаш ресурсида, хусусан, CPU даври орқали ҳисобланади. Амалий бўлиши учун, у қабул қилувчи, Алиса текшиши, яъни, у ҳақиқатда ҳисоблашни амалга оширганлигини текшириш учун осон бўлиши керак. Бу схема айнан спамларга қаратилмаган бўлсада, ихтиёрий фойдаланувчи юборган ҳажмини чегаралайди.

Келинг, M e-mail хабар ва T эса жорий вақт бўлсин. Хабар M ўзида юборувчи ва қабул қилувчининг e-mail манзилларидан иборат бўлади, аммо, бирор қўшимча манзилга эга бўлмайди. M хабарни юборувчи R қийматни қуйидагидек ҳисоблаши шарт:

$$h(M,R,T) = (\underbrace{00\ldots0}_{N},X) \quad (1)$$

Юборувчи шундай R сонин топиш керакки, (1) тенгликдаги хэш қийматнинг биринчи N бит чиқиши нол бўлсин. Бу амалга оширилса, юборувчи, учлик, (M,R,T) ни юборади. Алисадан олдин, қабул қилувчи хабарни қабул қилади, у вақт T ни текшириши шарт ва $h(M,R,T)$ қийматни дастлабки N бити ноллигини текшириши шарт.

Қайтадан, юборувчи тасодифий R сонини танлайди ва дастлабки N бити нол бўлмагунга қадар уни хэшлайди. Шунинг учун юборувчи, тақрибан 2^N та ҳисоблашни амалга ошири шарт. Бошқа томондан эса, қабул қилувчи биргина хэшлаш орқали $h(M,R,T)$ ни N та нол билан бошланишини билиши кифоя. Шунинг учун, юборувчининг иши ўртача 2^N та хэшлашдан, қабул қилувчиники эса битта хэшлашни амалга оширишдан иборат. Бу юборувчининг иши N га боғлиқ экспонентал равишда ортишини, қабул қилувчиники эса N га боғлиқ эмаслигини билдиради.

Бу тизимни амалий равишда бажариш учун, N даражани нормал хабар юборувчи

учун мос, спам юборувчилар учун эса юқори қилиб танлашимиз зарур. Бу тизим билан, фойдаланувчилар ўзлари учун спам хабарларга турли даражали қийматларни танлашлари мумкин. Масалан, Алиса спамдан безор ва шунинг учун N=40 деб танлади. Бу танлов нафақат спам хабар юборувчиларни, балки қонуний хабар юборувчиларни ҳам тўхтатиб қолиши мумкин. Бошқа томондан, агар Бобга спам хабарларни чеклаш унчалик ҳам шарт эмас ва қонуний фойдаланувчилардан хабарларни қабул қилиш шарт бўлса, унда N=10 тарзида танлайди.

Спам юборувчилар буни ёқтирмасликлари аниқ. Қонуний хабар юборувчилар ҳам буни ортиқча ресурс талаб этганлиги боис унчалик хуш кўрмайдилар. Ихтиёрий ҳолатда ҳам, бу усулда хабарларни юбориш сарф харажатларни ошишига олиб келади.

Криптографик хеш функциялар кулай ва самарали томони у бир тамондан маълумотнинг хеш қийматини ҳисобласа, иккинчи томондан уни имзо қўйувчининг ёпиқ калити билан шифрлайди. Бундан кўриниб турибдики криптографик хеш функциялар маълумотни ҳимоялашда бир томонлама функция ва криптографик усулни уйғунликда фойдаланишга хизмат қилади.

АНАЛИЗ СПОСОБОВ ОБЕСПЕЧЕНИЯ СЕТЕВОЙ АДМИНИСТРАТИВНОЙ БЕЗОПАСНОСТИ

Б.М. Шамшиева (ТУИТ, ассистент)

Административная безопасность – это те решения, которые соответствуют политикам и процедурам, ресурсам, степени ответственности, потребностям в обучении персонала и планам по выходу из критических ситуаций. Эти меры призваны определить важность информации и информационных систем для компании и объяснить персоналу в чем именно заключается эта важность. Наши рекомендации по обеспечению административной безопасности определяют ресурсы, необходимые для осуществления должного управления рисками и определения лиц, несущих ответственность за управление безопасности организации.

Политики безопасности определяют метод, согласно которому обеспечивается безопасность внутри организации. После определения политики предполагается, что большинство сотрудников компании будут ее соблюдать. Следует понимать, что полного и безоговорочного выполнения политики не будет. В некоторых случаях политика будет нарушаться из-за требований, связанных с деловой деятельностью организации. В других случаях игнорирование политики обусловлено сложностью ее выполнения.

В качестве рекомендаций бозопасности можно рассмотреть следующие меры политики.

- Политика использования. Определяет допустимый уровень использования компьютерных систем организации и штрафные санкции, предусмотренные за их нецелевое использование. Данная политика приемлемого использования.
- Политика безопасности. Определяет технические средства управления и настройки безопасности, применяемые пользователями и администраторами на всех компьютерных системах.
- Информационная политика. Определяет степень секретности информации внутри организации и необходимые требования к хранению, передаче, пометке и управлению этой информацией.
- Политика резервного копирования. Определяет периодичность резервного копирования данных и требования к перемещению резервных данных и требования к перемещению резервных данных в отдельное хранилище. Кроме того, политики резервного копирования определяют время, в течение которого данные должны быть зарезервированы перед повторным использованием.

Политики сами по себе не формируют исчерпывающих инструкций по

выполнению программы безопасности организации. Следует определить процедуры, согласно которым сотрудники будут выполнять определенные задачи, и которые будут определять дальнейшие шаги по обработке различных ситуаций с точки зрения безопасности. Внутри организации должны быть определены следующие процедуры.

- Процедура системного администрирования. Описывают, каким образом в данный момент времени применяются политика безопасности на различных системах, имеющихся в организации. Это процедура подробно определяет, каким образом должна осуществлятся работа с обновлениями и их установка на системы.
- Процедура управления конфигурацией. Определяют шаги по внесению изменений в функционирующие системы. Изменения могут включать в себя обновление программного и аппаратного обеспечения, подключение новых систем и удаление ненужных систем.
- Процедура управления пользователями. Определяет, кто может осуществлять авторизованный доступ к тем или иным компьютерам организации, и какую информацию администраторы должны предоставлять пользователям, запрашивающим поддержку. Процедуры управления пользователями также определяют, кто несет ответственность за информирование администраторов о том что сотруднику больше не требуется учетная запись.

Во многих организациях управление обновлениями представляет собой большую проблему. Отслеживание обновлений для снижения уровня уязвимости систем, а также тестирование этих обновлений перед установкой на функционирующие системы занимает очень много времени, но эти задачи очень важны для любой организации.

Наряду с процедурами по управлению конфигурацией устанавливаются методологии разработки новых систем. Они очень важны для управления уязвимостями новых систем от несанкционированного изменения. Методология разработки определяет, как и когда должны разрабатываться и применятся меры защиты. Необходимо делать акцент на этих сведениях при проведении любых инструктажей разработчиков и менеджеров проектов.

Для применения корректных рекомендаций по безопасности необходимо осуществить присвоение ресурсов. К сожалению, не существует формулы, которую можно использовать для определения того, сколько ресурсов должно быть выделено в соответствии с программой безопасности, руководствуясь лишь размерами организации. В этом уравнении слишком много переменных. Необходимые ресурсы обуславливаются размером организации и опасностями, угрожающими ей. Количество ресурсов должно определятся на базе корректной и полной оценки рисков, в соответствии с алгоритмом обработки рисков. Каждая политика организации должна предусматривать даты пересмотра политики. Отдел безопасности должен разрабатывать планы для начала пересмотра и оценки политики по мере приближения даты пересмотра.

Если программа безопасности воспринимается как проект, то организация должна выделить достаточно ресурсов для уравновешивания треугольника либо расширить время или уменьшить область.

РАСМ МАЪЛУМОТЛАРДА АХБОРОТНИ СТЕГАНОГРАФИК ЯШИРИШНИНГ САМАРАЛИ УСУЛИ

З.Т. Худойқулов (ТАТУ, ассистент)
А.Т. Имомалиев (ТАТУ, ассистент)

Ахборотнинг криптографик ҳимоя усули ҳозирда жуда ишончли усуллардан бири саналиб, хусусан, маълумотларни яшириш усуллари, стеганография усулларига бўлган талаб сўнги йилларда ортмоқда. Бунинг асосий сабаби, стеганографик усулларини амалга ошириш учун кам ресурс талаб этишидир. Стеганографик ҳимоя усуллари нафақат

маълумотларни яшириш имкониятини, балки уни узатишда махфийлиги ва бутунлигини таъминлаш имкониятини ҳам яратади.

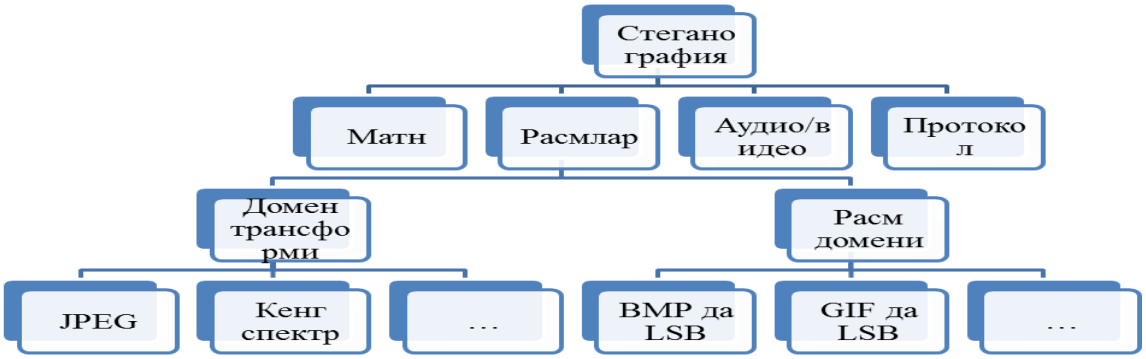
Маълумотларни яшириш (information hiding ёки data hiding) қадимдан фойдаланилиб келинган ва долзарб бўлган соҳа саналган. Маълумотларни яшириш деганда контент (расмлар, қўшиқлар, видеолар ва ҳак.) ичида керакли маълумотларни яшириш тушунилади. Бу ерда, яшириш тушунчаси, маълумотни сезилмайдиган кўринишда келтириш ёки маълумот махфийлигининг мавжудлигини сақлаш учун фойдаланилади. Қадимда турли маълумотларни яшириш усулларидан фойдаланилган ҳолда, маълум доирадаги одамлар орасида маълумотлар алмашинилган. Умумий ҳолда маълумотлари яшириш тузулмаси қуйидагича:

1-расм. Маълумот яширишнинг умумий тузилмаси.

Одатда маълумотларни яшириш соҳаси иккита катта қисмга ажратилади:

- Стеганография;
- Watermarking (сув шаклидаги белги).

Watermarking соҳаси контенга алоқадор бўлган бирор хусусиятни аниқлашда, таниб олишда ёки эгалик ҳуқуқини таъминлашда фойдаланилса, *стегонография* контентга махфий ахборотни яшириш усулларини ўрганади.



2 – расм. Расм стеганографияси категориялари.

Расм маълумотлар стеганографияда енг кўп тарқалган маълумот ташувчи контент ҳисобланади. Расм маълумотларнинг рақамли ишлов беришда уларнинг форматларидан фойдаланилган ҳолда ёндошилади. Расм маълумотларнинг кўп турлари мавжуд бўлиб, улар тузилишлари билан бир – биридан фарқ қилади. Ҳозирда амалда .JPEG, .GIF, .BPM, .PNG, .TIFF каби кенг тарқалган турлари мавжуд (2 - расм).

Расм маълумотларди ахборотларни яширишнинг мавжуд усулларининг таҳлили қуйидаги жадвалда келтирилган.

1- жадвал

	BMP да LSB	**GIF да LSB**	**JPEG сиқиш**	**Patchwork**	**Кенг спектрлар**
Кўринмаслик	Юқори	Ўртача	Юқори	Юқори	Юқори

Қўшимча қўшиладиган маълумот ҳажми	Юқори	Ўртача	Ўртача	Паст	Ўртача
Статистик таҳдидга бардошлилик	Паст	Паст	Ўртача	Юқори	Юқори
Расмни бузишга асосланган таҳдидга бардошлилик	Паст	Паст	Ўртача	Юқори	Ўртача
Файл форматига боғлиқлилик	Паст	Паст	Паст	Юқори	Юқори
Шубҳаланмаслик даражаси	Паст	Паст	Юқори	Юқори	Юқори

Контентга яширилган маълумотни нисбатан қуйидаги турдаги таҳдидлар мавжуд:

Рухсатсиз белгини бириктириш. Кўплаб рухсатсиз белгини бириктириш усулида ихтиёрий олинган контентга ҳақиқий хабар белгиси қўйилади.

Рухсатсиз белгини аниқлаш. Бу турдаги таҳдидда белгини аниқлаш рухсатига эга бўлмаган фойдаланувчи томонидан белгини аниқлаш амалга оширилади.

Қўйилган белгини рухсатсиз олиб ташлаш. Бу таҳдид натижасида контентдан белги рухсатсиз олиб ташланади ва белги қўйилмаган ҳолда келтирилади.

Юқоридаги таҳдидлардан ҳимоялаш учун одатда криптографик ҳимоя усулларидан кенг фойдаланилади. Масалан, контентга яширилган ахборотни рухсат этилмаган аниқлашдан ҳимоялаш учун шифрлаш алгоритмларидан фойдаланилса, рухсат этилмаган ўзгартиришдан ҳимоялаш учун хэш фунция, ЭРИ ёки HMAC тизимларидан фойдаланиш мумкин.

Расм маълумотларда ахборотларни яширишда стеганографик алгоритмлар ёрдамида яширганда уларни аниқлаш имконияти мавжуд бўлади. Бу заифликни олдини олиш учун одатда стеганографик алгоритмлар криптографик алгоритмлар билан комплекс ҳолда фойдаланилади. Бу комплекс усул маълумотни махфийлигини таъминлаш ва бутунлигини текшириш имконини беради. Ушбу ғояга асосланиб таклиф этилган усул кўриниши қуйидагича:

Таклиф этилган усулда қуйидаги алгоритмлардан фойдаланиш мумкин:

- маълумотларни шифрлашда AES, DES, CAMELLIE шифрлаш алгоритмидан;

маълумотни бутунлигини таъминлашда SHA1, SHA-2 оиласига тегишли хэш функцияси асосида HMAC тизимидан фойдаланиш мумкин

3- расм. Таклиф этилган усул

Маълумот яширинган расмни сақлашда эса йўқотилишсиз сиқишга асосланган расм форматларидан фойдаланиш тавсия этилади.

ХАВФСИЗ SMS - ХАБАР АЛМАШИНИШ УСУЛЛАРИНИНГ ТАДҚИҚИ

И.У. Халимтаева (ТАТУ, ассистент)

Ҳозирги кунга келиб мобил телефонлар инсонларнинг ажралмас ҳамроҳига айланиб бўлди. Мобил телефонлар нафақат суҳбатлашиш ва хабарлашиш учун, балки маълумотларни алмашиниш, банк амалиётларини бажариш ва кўплаб бошқа вазифаларни бажариш учун фойдаланилмоқда. Бу эса ўз навбатида мобил қурилмаларда юбориладиган, қайта ишланадиган ва сақланаётган маълумотлар хавфсизлигини таъминлаш муаммосини келтириб чиқаради. Бу ўринда SMS хабарларни хавфсиз узатиш ва сақлаш муҳим аҳамиятга эга.

Short Message Service (SMS) бу телефон, Web ёки мобил алоқа тизимларининг текст хабарлар хизматидир. У стандарт алоқа протоколидан фойдаланиб, мобил қурилмаларда матнли хабарларни алмашинишда имкон беради. SMS хизмати 2010 йилда 3.5 млрд актив фойдаланувчи томонидан фойдаланилган.

Ушбу хизмат GSM тармоқ технологиясининг ажралмас қисми бўлиб, ҳозирда GSM провайдерлар томонидан кенг фойдаланилмоқда. У хизмат сифатида Global Switched Telephone Network (GSTN) ва Integrated Services Digital Network (ISDN)нинг бошқа хизматларига қараганда самаралироқдир. Бунинг асосий сабаби, SMS – агент ҳам хабарни жунатувчи ва қабул қилувчи вазифасини бажариши мумкин.

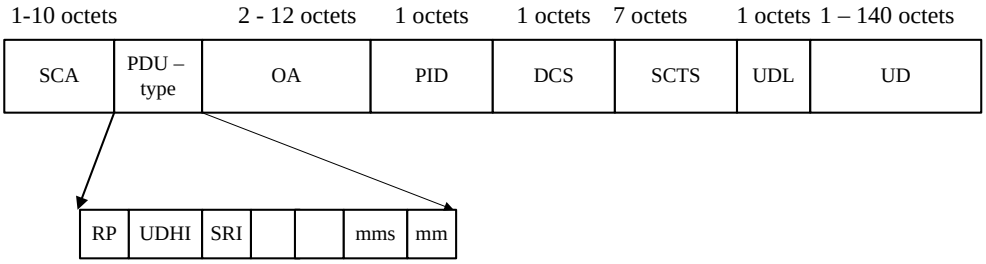
GSM SMS хабарлари SMS фойдаланувчилари орасида асосан алфавит ва рақамлардан ташкил топган бўлиб, уларнинг максимал узунлиги 160 белигига тенг (7 – битли белгилар). Бундан ташқари, 70 – та белгидан иборат тури мавжуд.

GSTN тармоқ бўйлаб хабарларни узатишда, хабарлар SMS Center (SMSC) да сақланади ва қабул қилувчи тармоқда уланган вақтда унга юборилади. Бунда бир нечта SMSC лар биргаликда ишлайди. Одатда ҳар бир фойдаланувчи SMS хабарни юбориш учун SMSC нинг рақамини билиши талаб этилади.

SMS хизмати SS7 протоколи оиласининг MAP (Mobile Application Part) протоколи асосида амалга оширилади. MAP нинг тўрт жараёни орқали SMS хизмати назорат қилинади:

- Mobile Oriented (MO) қисқа хабарлар хизмати трансфери;
- Mobile Terminated (MT) қисқа хабарлар хизмати трансфери;
- қисқа хабарлар огоҳлантиришлари жараёни;
- қисқа хабарларни кутиш жараёни маълумотлари.

Қуйидаги 1 - расмда юборилган SMS - хабар пакетининг умумий кўриниши келтирилган. Бундан кўриниб турибдики, маълумот очиқ ҳолда узатилади. Бу ҳолда юборилган SMS - хабарни конфиденциаллиги ва яхлитлигига бушизга қаратилган таъсирлар бўлиши мумкин.



1 - расм. Юборилган SMS хабар пакети формати

Мобил телефонларда SMS хабарлар учун уларнинг махфийлик ва яхлитлик хусусиятларини таъминлаш муҳим аҳамиятга эга. SMS хабарнинг махфийлиги деганда уни фақат рухсат берилган фойдаланувчиларга ўқиш мумкин эканлиги тушинилса, SMS хабарни бутунлигини таъминлашда уни ўзгартирилмаганлигига ишонч ҳосил қилиш тушинилади.

Ахборотни махфийлигини таъминлашда одатда шифрлаш алгоритмларидан, очиқ

калитли ва симметрик шифрлаш алгоритмларидан фойдаланиш мумкин (масалан, AES, DES, RSA ва х).

SMS хабарларни шифрлаганда симметрик шифрлаш алгоритмлари мос бўлиб, шифрлангандан сўнг хабарнинг ўлчами ҳам ўзгармайди. Бу эса фойдланувчини ортиқча маблағ сарфлашини олдини олади.

Ахборотларни яхлитлигини таъминлашда эса электрон рақамли имзо алгоритмлари ва калитли хэш функциялар муҳим рол ўйнайди.

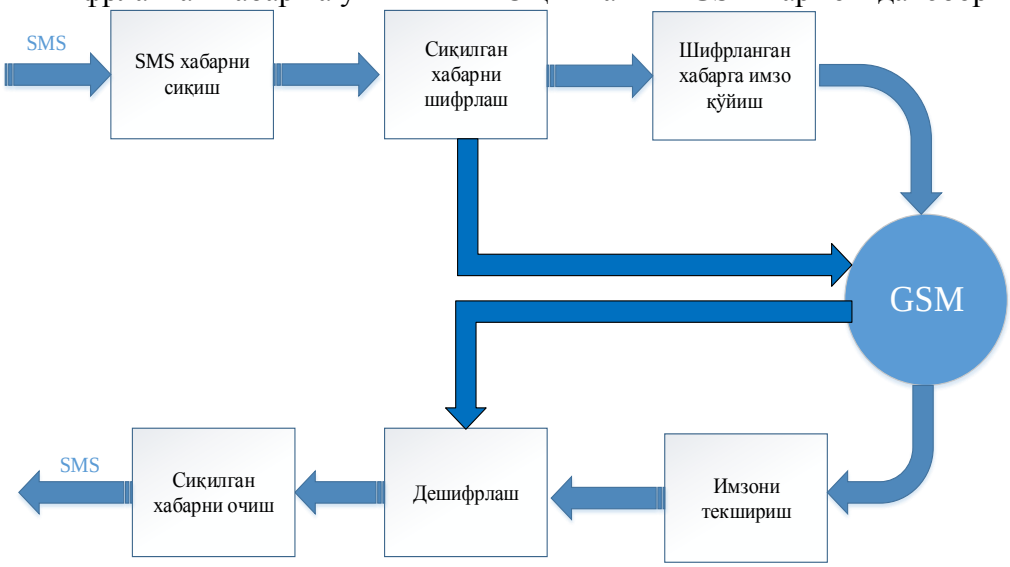
SMS - хабарларни бутунлигини таъминлашда ёки аутентификациялашда маълумотга ортиқча ахборот қўшилади ва бу фойдаланувчидан ортиқча маблағ таълаб этади.

Бу муаммони ҳал қилиш учун маълумотларни сиқиш алгоритмларидан фойдаланиш катта самара беради. Сиқиш алгоритмлари сифатида Хаффмен ёки LZ сериясидаги кодларни мисол қилиш мумкин.

Юқоридаги ҳимоя ва маълумотларни узатиш усулларидан фойдаланиб, SMS хабарларни узатишда қуйидаги хавфсиз узатиш усули таклиф этиш мумкин (2 - расм).

SMS хабарни бутунлигини ва махфийлигини таъминлаш қуйидагича амалга оширилади:

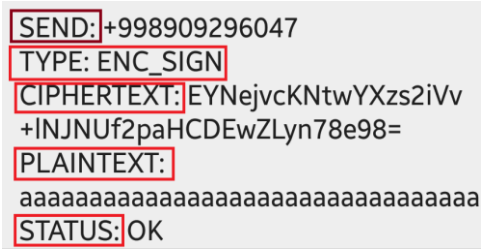
- SMS хабарни сиқиш;
- сиқилган SMS хабарни шифрлаш;
- шифрланган хабарни HMAC қийматини ҳисоблаш;
- шифрланган хабар ва унинг HMAC қийматини GSM тармоғида юбориш.



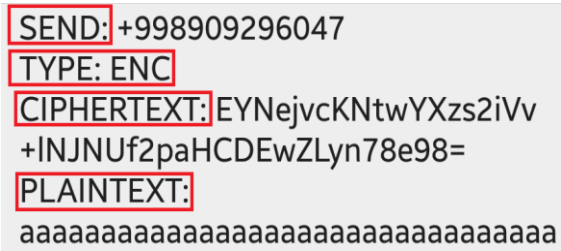
2 – расм. Таклиф этилган усулнинг умумий кўриниши

Ушбу усулни дастурий таъминотини ишлаб чиқишда қуйидаги алгоритмлардан фойдаланилди:

- GZIP сиқиш алгоритмидан;
- AES симметрик шифрлаш алгоритмидан;
- SHA1 хэш функциясига асосланган HMAC алгоритмидан.



а) махфийлиги&бутунлиги таъминланган SMS хабар кўриниши (SEND – юборувчи TYPE: ENC_SIGN – махфийлик&бутунликни таъминлаш



б) махфийлиги таъминланган SMS хабар кўриниши (SEND – юборувчи TYPE: ENC – махфийликни таъминлаш CIPHERTEXT – шифрматн

CIPHERTEXT – шифрматн PLAINTEXT – очиқ матн)
PLAINTEXT – очиқ матн
STATUS:OK – имзо тўғри)

3 – расм. SMS хабарларни Secure SMS дастурида кўриниши

Таклиф этилган усул катта ҳажмдаги хабарларни алмашинишда уларни сиқиш, махфийлигини, бутунлигини таъминлаш имкониятини беради. Бу имкониятлар эса ўз навбатида хавфсизликни таъминлайди ва сарфланадиган харажатни ва қувватни тежайди. Ушбу таклиф этилган усулни нафақат қисқа хабарлар алмашинувида, балки ижтимоий тармоқларда, почта хабарларини хавфсиз узатишда ҳам қўллаш мумкин.

ПРИМЕНЕНИЕ DPI КАК СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

Р.Р. Ибрагимов (ТУИТ, студент)

С каждым днем расширяется сфера применения информационных технологий, повышается их роль в повседневной жизни каждого человека. Развитие мультимедийных технологий, повышение доступности сети Интернет, а также предоставление широкого спектра услуг клиентам с различными объёмами запрашиваемых услуг приводят к значительному увеличению объемов передаваемой по сетям связи информации. В связи с этим для операторов особенно остро встают вопросы инжиниринга трафика для повышения эффективности использования сетевых ресурсов – актуальными являются задачи контроля, управления, приоритетного обслуживания и оптимизация общей нагрузки на сетевую инфраструктуру. Так же критической является задача обеспечения безопасности информационных систем.

Для сбора и обработки данных об активности пользователей сети и управления трафиком применяются DPI-системы (DPI - Deep Packet Inspection). Решения, основанные на использовании данной технологии, позволяют как рассмотреть происходящие в сети процессы с различных сторон, так и увидеть полную картину, выявляются наиболее активные потребители трафика, становится возможным эффективное управление трафиком в режиме реального времени на основе получаемых данных. Использование данной технологии позволяет учитывать особенности конкретных сетей при организации сервисов, при создании и проведении сервисных политик, также повышается эффективность организации защиты пользователей и самой сети. Собираемая DPI-системой статистика позволяет облегчить поиск и устранение неисправностей, а также запланировать развитие сети и предоставляемых сервисов.

Системы DPI позволяют блокировать вредоносный трафик DoS, DDoS, SPAM-рассылок и вирусов, сканирование сети - решение позволяет обнаруживать и блокировать «зараженных» абонентов, чьи компьютеры создают угрозу другим пользователям Интернета.

DPI-системы представляют собой идеальную среду для выявления и фильтрации широкого спектра вредоносных программ и вирусов, таких как черви, троянские кони, программы-шпионы, рекламные программы и другие виды вредоносных приложений. Большая часть DPI-систем может быть сконфигурирована для обнаружения и устранения подавляющего большинства этих угроз, также DPI-система может быть расширена с использованием решений сторонних разработчиков. Почти все угрозы могут быть перехвачены, если система использует трехсторонний подход к безопасности:

- распознавание URL-адресов – сравнение поступающих в чистом виде и вложенных URL-адресов с базой данных известных вредоносных сайтов;
- распознавание объектов – поиск в потоке данных потенциально опасных исполняемых файлов или объектов (например, изображений в формате JPEG) с проведением дальнейшего их анализа;

- распознавание сигнатур – использование базы данных сигнатур для обнаружения определенных видов вредоносных программ, особенно вирусов, которые мутируют при репликации.

Каждый из этих подходов к распознаванию может и должен быть обновлен с помощью сторонних разработчиков, например, с помощью продуктов Лаборатории Касперского.

Возможность оперативного обновления профилей распознавания без нарушения работы системы является важной характеристикой в DPI-решениях, особенно для центров обработки данных и хранилищ данных. По этой причине системы распознавания должны быть реконфигурируемыми без необходимости перезагрузки системы. Надежная DPI система должна быть в состоянии обнаружить протоколы и приложения, подверженные риску заражения вредоносными программами и кодами, с использованием следующих таких методов, как распознавание портов, распознавание сигнатур и эвристический анализ.

Другие характеристики высокоэффективной системы DPI включают распознавание на уровне потоков (для TCP, UDP и WAP), поддержка IPv4 и IPv6, нормализация TCP/IP, а также повторная сборка и извлечение метаданных на основе установленных правил.

Для обеспечения безопасности информационных систем также применяются системы предотвращения вторжений (Intrusion Prevention System, IPS) и системы обнаружения вторжений (Intrusion Detection Systems , IDS). Обе системы обнаруживают попытки вторжения и разделяют много особенностей. Они используются для обнаружения хакеров и неавторизованных пользователей, пытающихся получить доступ к сети или компьютеру, обычно эксплуатируя уязвимости приложений, возможно с использованием вредоносных и вирусных программ для сокрытия факта вторжения. Но эти две системы различаются в одном важном аспекте: IDS – прежде всего инструмент регистрации нарушений, чьи данные используются для дальнейшего анализа, в том числе судебного. IPS, с другой стороны, автоматически принимает решения, когда обнаружена злонамеренная деятельность. Системы DPI способны обеспечивать оба этих сервиса, особенно в аспекте обнаружения попыток сокрытия или маскировки злонамеренной деятельности, как то использование нестандартных протоколов или встраивание вредоносного кода в доверенные программные продукты.

Таким образом, применение систем DPI позволит лучше управлять сетевым трафиком, обеспечивая принятие решений для конкретной сети на основе динамически обновляемых данных, а также повысить уровень безопасности информационных систем, обеспечивая надежное средство фильтрации вредоносных программ и вирусов и блокировки нежелательного трафика.

ИНТЕРНЕТ ТАРМОҒИДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ

Н.Б. Насруллаев (ТАТУ, катта илмий ходим-изланувчи)
А.А. Ганиев (ТДТУ, ассистент)
Л.Т. Ширинов (ТАТУ, талаба)

Бугунги кунда Республикамизда ахборот-коммуникация технологияларини, шунингдек, Интернеттармоғининг миллий сегменти жадал суратлар билан ривожланиб бормоқда.

Глобал тармоқнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб бўлмоқда. Ҳозирги кунга келиб, дунё аҳолисининг 44% и (3,2 миллиард аҳоли) Интернеттармоғидан фойдаланувчилар ҳисобланади. Бу эса ўз навбатида маълумотларни йўқолиши ёки ўғирланиши натижасида улардан бошқа ёвуз мақсадларда фойдаланилиши кабиахборот хавфсизлигига таҳдид солиш эҳтимолининг кескин даражада ошишига олиб келмоқда.

Интернет деярли бир ондаёқ турли хил бўлган кенг кўнгилочар ва ахборот ресурсларига йўл очиб беради. Соатлаб виртуал алоқаларда қатнашиш, янги ахборотларни ўрганиш, интернет-дўконларда савдо қилиш ва онлайн режимда компьютер ўйинларини ўйнаш қанчалик ўзига жалб қилмасин, шуни эсдан чиқармаслик керакки, ҳар бир фойдаланувчи учун энг асосийси - ахборот хавфсизлиги ва шахсий маълумотларни ҳимояланганлигидир.

Интернет тармоғида ахборот хавфсизлигига таҳдид солувчи асосий манбаалар:

1. Компьютер вируслари, троянлар ва бошқа зарар келтирувчи дастурлар - ушбу дастурларни электрон почта ёки ташувчи орқали қабул қилган компьютер иш фаолиятини бузишга қодир бўлган дастурлардир.

Эҳтиёт чоралари:

- Антивирус дастурий таъминотини ўрнатиш. Антивирус дастурлари компьютерни вирусларга қарши текшириб, улар компьютергазарар келтирмасдан олдин аниқланган вируслар ҳақида огоҳлантиришга хизмат қилади.
- Нотаниш бўлган электрон почта манзилларидан келган хатларни очмаслик. Айниқса, “.vbs”, ”.exe”, “.bat”, ёки “.scr” кенгайтмали файлларни очмаслик ва юкламаслик керак бўлади.
- Лицензияга эга бўлмаган (пиратский) маҳсулотларни юкламаслик. Лицензиясизмаҳсулотлардан фойдаланиш, шахсий маълумотларни қўлга киритиш учун уринишлар эҳтимоллигини оширишга хизмат қилади. Интернетдан маълумот олишда иложи борича расмий манбаалардан фойдаланиш лозим.
- Ташувчилардан фойдаланишда эҳтиёткорликка риоя қилиш. Чунки, бир нечта компьютерда фойдаланилган флеш-хотира ва компакт-дискларда вируслар бўлиши мумкин.
- Доимий равишда ташқи хотираларда маълумотларни захира нусхасини сақлаб бориш. Маълумотларни захира нусхасини олиш, компьютер вируси билан зарарланганда қимматли маълумотларни йўқолишини олдини олади.

2.Фишинг - турли хил хизмат кўрсатувчи корхоналар, фирмалар ва банк сайтлари ва эелектрон почта манзилларини сохталаштириш натижасида махфий маълумотлар, айнан пароль ва кредит карта рақамларини қўлга киритишни кўзловчи интернет фирибгарлик йўлларидан бири.

Эҳтиёт чоралари:

- Нотаниш электрон почта манзиллари орқали юборилган хаволаларга ўтиш тавсия этилмайди. Шуни инобатга олиш лозимки, ёвуз ниятли кишилар ўз мақсадига эришиш учун сохта сайтларни ҳосил қилишлари мумкин.
- Маълумотларни киритишдан олдин улар ҳимояланган режимда юборилишига ишонч комил қилиш. Ҳимояланган режим ёқилган ҳолатда сайт манзилидаги "http" номли сатр "https" сатри билан алмашади, экраннинг қуйи қисмида эса қулф тасвири пайдо бўлади.

3. Спам - ушбу термин қабул қилучининг олдиндан розилигисиз оммавий равишда электрон хатларни унга юборишни англатади.

Эҳтиёт чоралари:

- Сайтларда рўйхатдан ўтиш жараёнида рўйхатдан ўтган фойдаланувчиларнинг электрон почтаси манзилларидан фойдаланиш қоидаларини синчиклаб ўрганиш лозим.
- Интернеттармоғида ахборот хавфсизлигини таъминлаш ва юқорида келтирилган таҳдидларни олдини олиш мақсадида қуйидаги умумий тавсияларга риоя қилиш лозим бўлади:

1. Шубҳага эга бўлган иловаларга ўтмаслик, чункизарарланган иловаларга ўтиш оқибатида турли хил конфиденциал маълумотлар, яъни логин, пароль, кредит карта рақами ва бошқаларни ўғирланиши мумкин;

2. Лицензияга эга бўлган дастурий таъминотлардан фойдаланиш, чунки ахборот хавфсизлиги бўйича экспертларнинг фикрига кўра, лицензияга эга бўлмаган дастурий

таъминотларнинг 94%дан ортиғи,бузғунчи - хакерлар томонидан ёвуз мақсадлар учун қўлланилади;

3. Дастурларни доимий равишда янгилаб бориш, чунки тараққиёт натижасида янги технологияларни пайдо бўлиши ва бу жараён доимо ҳаракатдалигисабабли, ҳимояни мутлоқ таъминлашнинг йўли мавжуд эмас.Шунинг учун тизимдаги мавжуд камчиликларни бартарафқилиш мақсадида дастурларни янгилаш зарур;

4.Имконияти борича Mozilla Firefox ва Google Chrome браузерлардан фойдаланиш, чунки ҳозирги кунда Internet Explorer ва Opera браузерларида кўплаб заифликлар аниқланган бўлиб, улар тўлиқлигича бартараф этилмаган;

5. Ҳимоянинг комплекс тизимини ўрнатиш. Бу антивирус дастурий маҳсулотлари, тармоқлараро экран ва бошқа бир қатор ҳимоя воситаларини ўз ичига олади. Улар ёрдамида Интернетдан кириб келаётган зарар келтирувчи дастурлар, вируслар ва бошқа таҳдидлардан ҳимояланиш мумкин.

КОРХОНАЛАРДА АХБОРОТ ХАВФСИЗЛИГИ ХАВФ-ХАТАРЛАРИНИ БАҲОЛАШ АЛГОРИТМИ

М.Б. Мирзаева (ТАТУ, ассистент)

Ахборот хавф-хатарларини баҳолаш учун ахборот тизимига таъсир қилувчи заифликлар орқали амалга оширилиши мумкин бўлган таҳдидларни таҳлил қилиш зарурдир. Ахборот тизими эгаси томонидан тақдим этилган ҳисоботлар таҳлилидан фойдаланиб, корхона ахборот тизими учун таҳдидлар ва заифликлар моделини қуриши мумкин. Тақдим этилаётган ушбу алгоритмда ҳар бир ресурс учун ахборот хавфсизлиги тахдидларини амалга ошириш эҳтимоллиги таҳлили олиб борилади ва шу асосда ахборотда бўладиган хавф-хатарлар ҳисоблаб чиқилади.

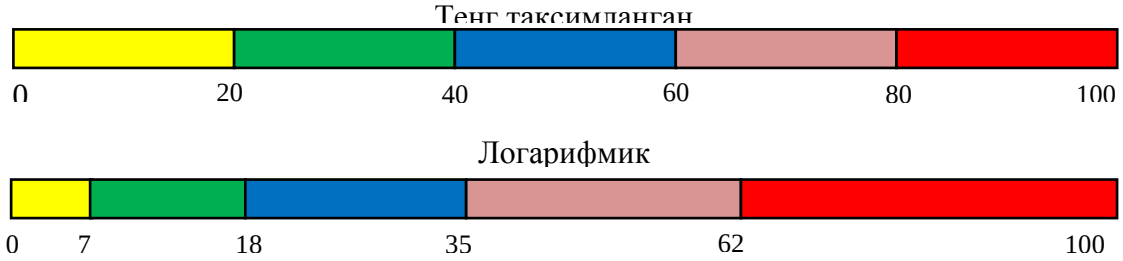
Ахборот хавфсизлиги хавф-хатарлари алгоритмини ишлаш тамойили қуйидагилардан ташкил топган:

- ресурслар;
- бўлимларга алоқадор ресурслар;
- ресурслага таъсир этадиган тахдидлар;
- таҳдидларни амалга ошириладиган заифликлар;
- заифлик орқали таҳдидни амалга ошириш кескинлиги;
- заифлик орқали таҳдидни амалга ошириш эҳтимоллиги.

Ахборот хавфсизлигини таянч таҳдидлари алгоритмини иккита ишлаш режими мавжуд:

- битта таянч тахдид (жамланган);
- учта таянч тахдидлар.

Шкалани даражаларга бўлиш тамойиллари. Алгоритм билан ишлашда 0 дан 100% гача бўлган шкаладан фойдаланилади. Даражанинг максимал қиймати - 100, шкалани 100 та даражага ажратиш мумкин. Шкала кичик қийматли даражага бўлинганда, ҳар бир даража шкалада муайян оралиқни эгаллайди. Бундан ташқари, ажратишни иккита варианти мавжуд:



Расм. Ахборот хавфсизлиги тахдидлари бўйича хавф-хатарларни ҳисоблаш

1. Биринчи босқичда заифлик орқали амалга ошириладиган таҳдидлар кескинлиги ва эҳтимоллиги асосида Th заифлик бўйича тахдидлар даражаси хисобланади. Таҳдид даражаси, ушбу таҳдидни уни амалга ошириш эҳтимоллиги ҳисоби билан ресурсга таъсирини қанчалик кескинлигини кўрсатади.

$$Th_{c,i,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100} \quad (1)$$

бу ерда $ER_{c,i,a}$ — тахдидларни амалга ошириш кескинлиги (% да кўрсатилади);

$P(V)_{c,i,a}$ — заифлик орқали таҳдидни амалга ошириш эҳтимоллиги (% да кўрсатилади).

Таянч тахдидлар сонига қараб битта ёки учта қиймат хисобланади. Тахдидлар даража қийматлари 0 ва 1 оралиқда олинади.

2. Иккинчи босқичда барча заифликлар CTh учун таҳдидлар даражасини хисоблашда қуйидаги формула бўйича аниқ заифликлар орқали олинган таҳдидлар даражалари қўшиб чиқилади:

Бир таянч таҳдид режими учун:

$$T_h = \frac{ER}{100} \times \frac{P(V)}{100} \quad (2)$$

бу ерда T_h — заифликлар бўйича таҳдидлар даражаси;

ER — тахдидни амалга ошириш кескинлиги, %;

$P(V)$ — заифликлар орқали тахдидни амалга ошириш эҳтимоллиги, %.

Учта таянч таҳдидлар режими учун қуйидаги формула қўлланилади:

$$T_{h_C} = \frac{ER_C}{100} \times \frac{P(V)_C}{100} \quad (3)$$

бу ерда T_{h_C} —махфийликни заифликлари бўйича тахдидлар даражаси;

ER_C — махфийликда тахдидни амалга ошириш кескинлиги, %;

$P(V)_C$ — махфийликда тахдидни амалга ошириш эҳтимоллиги, %.

$$T_{h_i} = \frac{ER_i}{100} \times \frac{P(V)_i}{100} \quad (4)$$

бу ерда T_{h_i} — бутунлик заифликлари бўйича тахдидлар даражаси;

ER_i — бутунликда таҳдидни амалга ошириш кескинлиги, %;

$P(V)_i$ — бутунликда тахдидни амалга ошириш эҳтимоллиги, %.

$$T_{h_a} = \frac{ER_a}{100} \times \frac{P(V)_a}{100} \quad (5)$$

бу ерда T_{h_a} —фойдаланувчанлик заифликлари бўйича тахдидлар даражаси;

ER_a — фойдаланувчанликда таҳдидни амалга ошириш кескинлиги, %;

$P(V)_a$ — фойдаланувчанликда тахдидни амалга ошириш эҳтимоллиги, %.

Заифликлар бўйича тахдидлар даражасининг қийматлари 0 ва 1 оралиқда жойлашади.

Бир неча заифликлар бўйича тахдидлар даражасини хисоблаш учун аниқ заифликлар орқали олинган таҳдидлар даражалари қўшиб чиқилади:

Бир таянч таҳдид режими учун қуйидаги формула қўлланилади:

$$CT_h = 1 - \prod_{i=1}^{n}\left(1 - T_{h_i}\right) \quad (6)$$

бу ерда CT_h —бир неча заифликлар бўйича тахдидлар даражаси;

T_h — заифликлар бўйича тахдидлар даражаси.

Бир неча заифликлар бўйича тахдидлар даражасининг қийматлари 0 ва 1 оралиқда

жойлашади.

Учта таянч тахдидлар режими учун:

$$CT_{h_C} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{Cj}}\right) \quad (7)$$

бу ерда CT_{h_C} – махфийлик тахдиди мезонлари бўйича бир неча заифликларни тахдид даражаси;

$T_{h_{Cj}}$ – махфийликдаги заифликлар бўйича таҳдид даражаси.

$$CT_{h_i} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{ij}}\right) \quad (8)$$

бу ерда CT_{h_i} –бутунлик таҳдиди мезони бўйича бир неча заифликларни таҳдид даражаси;

$T_{h_{ij}}$ – бутунлик заифлиги бўйича таҳдид даражаси.

$$CT_{h_a} = 1 - \prod_{j=1}^{n}\left(1 - T_{h_{aj}}\right) \quad (9)$$

бу ерда CT_{h_a} – фойдаланувчанлик тахдиди мезони бўйича бир неча заифликларни тахдид даражаси;

$T_{h_{aj}}$ – фойдаланувчанлик заифлиги бўйича тахдид даражаси.

Барча заифликлар бўйича таҳдидлар даражасининг қийматлари 0 ва 1 оралиқда жойлашади.

Худди шундай ресурс бўйича умумий тахдид даражаси хисобланади (ресурсага таъсир қилувчи барча тахдидлар хисобга олинади):

Бир таянч тахдидлар режими учун:

$$cT_h R = 1 - \prod_{i=1}^{n}\left(1 - T_{h_i}\right) \quad (10)$$

бу ерда $cT_h R$- ресурслар бўйича тахдидлар даражаси;

T_h –заифликлар бўйича тахдид даражаси.

Умумий тахдидлар даражаси қийматлари 0 ва 1 оралиқда жойлашади.

Баҳолаш натижасидан келиб чиқиб шуни таъкидлаш лозимки корхона ёки ташкилотда ахборот хавфсизлиги хавф-хатарларини баҳолаш ахборот тизимлари ва тармоқлари ҳимояланганлигини оширади ва ахборот хавфсизлиги асосий функциялари (махфийлик, яхлитлик ва бутунлик) да бўладиган хавф-хатарларни ва таҳдидларни бартараф этишга имкон беради.

ДОСТОИНСТВА И НЕДОСТАТКИ ПОЛИТИКИ БЕЗОПАСНОСТИ В РЕЛЯЦИОННЫХ БАЗАХ ДАННЫХ

М.В. Лазарева (ФФ ТУИТ, старший преподаватель)
А.А. Горовик (ФФ ТУИТ, старший преподаватель)

В настоящее время особенно актуальную роль приобретают средства защиты информации от несанкционированного доступа. Современные системы управления базами данных обладают достаточно развитыми различными средствами защиты. Это связано с тем, что деятельность любой базы данных связана с переработкой и хранением значительных объемов информации. С другой стороны, доступ к этой информации имеет широкий доступ различных лиц. Гарантировать абсолютную защиту практически не возможно. Существуют два типа политики безопасности: дискреционная и мандатная. Дискреционная защита является логической многоуровневой защитой.

Дискреционная защита (discretionary access control – дискреционное управление

доступом) — это разделение доступа между субъектами и объектами, которое определяется двумя свойствами:

1. все субъекты и объекты должны быть определены (идентифицированы);
2. права доступа субъекта к объекту определяются на основании некоторого заранее не вносимого в системы правила.

Субъект с определенным правом доступа может передать такое право любому другому субъекту. По отношению к защищаемому объекту полностью разделен набор привилегий. Владелец таблицы реляционной базы данных может ограничить доступ, расширить, снять привилегии. Привилегии конкретному пользователю могут быть назначены администратором явно и неявно, например через роль. Роль — это еще один возможный носитель привилегий. Роли удобно использовать, когда набор привилегий необходимо назначить группе пользователей. Это облегчает администратору управление привилегиями и вносит определенный порядок в случае необходимости изменить набор привилегий для группы пользователей сразу.

Администратор каждой базы создает круг возможных пользователей базы данных и разграничивает полномочия этих пользователей. Такие данные хранятся в системных таблицах реляционных баз данных и отделены от самих таблиц баз данных. Очевидно, что эти данные могут быть использованы для несанкционированного доступа и поэтому также подлежат защите. Такая защита осуществляется самой системой управления базами данных. Система управления позволяет зарегистрировать пользователя и хранит информацию о нем.

Но такая защита имеет недостаток: она защищает только объекты базы данных, но не хранящиеся в них данные.

К достоинствам дискреционной политики защиты можно отнести простую реализацию механизмов защиты. Большинство распространенных систем обеспечивают выполнение именно такой политики безопасности.

Мандатная политика безопасности (mandatory access control) – политика безопасности основанная на совокупности предоставления доступа, определенного на множестве атрибутов безопасности субъекта и объекта, которая подразумевает, что:

1. все субъекты и объекты системы должны быть однозначно определены (идентифицированы);
2. задан упорядоченный (обычно линейно) набор меток секретности;
3. каждому объекту присвоена метка секретности, определяющая обычно ценность имеющейся информации (уровень секретности);
4. каждому субъекту системы также присвоена метка секретности, определяющая уровень доверия к нему - максимальное значение метки секретности объектов, к которым субъект имеет доступ. Такая метка секретности (именно субъекта) называется его уровнем доступа.

Основная задача мандатной политики – слежение за передачей информации. Основная цель мандатной политики безопасности - предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа. Таким образом, невозможно возникновение информационных каналов сверху-вниз.

Недостатки такой политики – реализация довольно сложна и требует значительных ресурсов вычислительной системы.

К достоинствам мандатной политики защиты можно отнести более высокую степень надежности. Правила такой политики достаточно ясны и понятны.

КИБЕРТЕРРОРИЗМ – НОВЫЕ УГРОЗЫ XXI ВЕКА

М.В. Лазарева (ФФ ТУИТ, старший преподаватель)

Противодействие все возрастающим и усложняющимся угрозам информационной безопасности в последнее время является самым актуальным вопросом эпохи становления глобального информационного общества. Проблема сдерживания и предотвращения реальных и потенциальных угроз в информационной сфере относится к числу наиболее серьезных вызовов национальной и международной безопасности нашего века.

Неправомерный доступ к информации, повлекший ее уничтожение, блокирование, модификацию, копирование, нарушение работы различных микропроцессорных устройств, систем и сетей, может нарушить деятельность различных систем, повлечь не только значительный материальный ущерб, но и причинение вреда здоровью людей и их гибель. Особенностями развивающихся информационно-коммуникационных технологий являются:

- общедоступность;
- возможность замаскированного или анонимного вторжения;
- отсутствие каких-либо территориальных и национальных границ;
- избирательная деятельность;
- экономичность;
- высокая эффективность и др.

Глобальное информационное пространство и его основная составляющая - сеть Интернет с одной стороны используется для обеспечения работоспособности объектов инфраструктур, расширения доступа граждан к информации, а с другой стороны может быть использовано криминальными структурами, международными террористическими организациями и враждебными государствами. Необходимо постоянно уточнять и классифицировать угрозы, делать подробную оценку этих угроз и уточнять планы противодействия на перспективу.

На современном этапе использование террористами последних достижений в сфере высоких технологий представляет собой одну из главных угроз международной и национальной безопасности. Понятие кибертерроризма становится все более ощутимым. Растущая компьютеризация и информатизация жизненно важных сфер деятельности общества и государства создает условия для широкого распространения террористических акций с помощью социальных сетей.

Используя глобальную сеть Интернет, террористы имеют возможность не только обмениваться информацией между собой, тем самым координировать совместные действия, но и вести пропаганду с целью вербовки новых членов.

При этом посредством компьютерных программных закладок и вирусов – «логических бомб», «троянских» программ, программ-снифферов и иных видов информационного оружия – кибертеррористы способны модифицировать либо уничтожить любую информацию.

Неотъемлемой частью современного Интернет пространства является также развитие социальных сетей и микроблогов, количество которых постоянно увеличивается, параллельно с геометрической прогрессией растет и количество их пользователей. Такая социальная сеть как «Facebook», насчитывающая на сегодняшний день порядка 1 миллиарда пользователей по всему миру.

Рост популярности социальных сетей в мире (особенно их мобильных версий), сопряженный с общим увеличением количества пользователей сети-Интернет, обусловлен тем, что социальные сети превратились в открытую площадку не только для оперативного обмена информации, но и для продвижения услуг и товаров. В то же время информационный и мобилизационный ресурс социальных сетей и микроблогов может быть использован определенными силами и в других целях, в частности, посредством

распространения в сети призывов к террористическим актам, общественным протестам и многого другого.

В этой связи перед мировым сообществом стоят задачи:

- согласования и разработки требований, обязательств, необходимых для противодействия компьютерным преступлениям, заключение соответствующих межгосударственных соглашений;
- определение основных путей создания эффективных механизмов предотвращения и устранения угрозы миру, подавление актов агрессии или других нарушений мира, связанных с враждебным использованием информационно-коммуникационных технологий;
- активизация международного сотрудничества в целях укрепления безопасности и функционирования открытых информационных сетей, в частности сети Интернет;
- развитие международного сотрудничества по стандартизации требований по обеспечению информационной безопасности информационно-телекоммуникационных систем и информационных ресурсов.

Выработка и принятие таких международных стандартов позволит сформировать единые подходы к обеспечению глобальной информационной безопасности и даст возможность согласовать уровни безопасности и механизмы защиты различных информационных систем.

ОРГАНИЗАЦИЯ ЗАЩИТЫ МУЛЬТИСЕРВИСНОЙ СЕТИ С ПОМОЩЬЮ МЕЖСЕТЕВЫХ ЭКРАНОВ

Н.А. Сайфуллаева (ТУИТ, старший преподаватель)

Для обеспечения безопасности информационных ресурсов и оптимальной работы мультисервисных сетей необходимо применение комплексной системы защиты информации, которая позволит эффективно использовать преимущества межсетевых экранов и компенсировать их недостатки с помощью других средств безопасности.

Полнофункциональная защита мультисервисной сети должна обеспечить:

-безопасное взаимодействие пользователей и информационных ресурсов, расположенных в мультисервисных сетях, с внешними сетями, например с Интернетом;

-технологически единый комплекс мер защиты для распределенных и сегментированных локальных сетей подразделений мультисервисных сетей;

-наличие иерархической системы защиты, предоставляющей адекватные средства обеспечения безопасности для различных по степени закрытости сегментов мультисервисной сети.

Характер современной обработки данных в мультисервисных сетях требует наличия у межсетевых экранов следующих основных качеств:

-мобильность и масштабируемость относительно различных аппаратно-программных платформ;

-возможность интеграции с аппаратно-программными средствами других производителей;

-простота установки, конфигурирования и эксплуатации;

-управление в соответствии с централизованной политикой безопасности.

В зависимости от масштабов организации и принятой политики безопасности могут применяться различные межсетевые экраны. Для небольших сетей, использующих до десятка узлов, подойдут межсетевые экраны с удобным графическим интерфейсом, допускающие локальное конфигурирование без применения централизованного управления. Для крупных сетей предпочтительнее системы с консолями и менеджерами управления, которые обеспечивают оперативное управление локальными межсетевыми экранами, поддержку виртуальных частных сетей.

В настоящее время все выпускаемые межсетевые экраны можно классифицировать по следующим основным признакам:

-по исполнению: аппаратно-программный, программный;

-по функционированию на уровнях модели OSI:шлюз экспертного уровня, экранирующий шлюз (прикладной шлюз), экранирующий транспорт (шлюз сеансового уровня), экранирующий маршрутизатор (пакетный фильтр);

-по используемой технологии:контроль состояния протокола,на основе модулей-посредников (proxy);

-по схеме подключения:схема единой защиты сети, схема с защищаемым закрытым и не защищаемым открытым сегментами сети, схема с раздельной защитой закрытого и открытого сегментов сети.

Увеличение потоков информации, передаваемых по Интернету пользователями, а также потребность в сетях удаленного доступа к мультисервисным сетям являются причинами постоянного совершенствования технологий подключения мультисервисных сетей к Интернету.

Следует отметить, что в настоящее время ни одна из технологий подключения, обладая высокими характеристиками по производительности, в стандартной конфигурации не может обеспечить полнофункциональной защиты мультисервисной сети. Решение данной задачи становится возможным только при использовании технологии межсетевых экранов, организующей безопасное взаимодействие с внешней средой.

При подключении мультисервисной сети к Интернету можно защитить сеть от несанкционированного доступа с помощью одного из следующих решений:

-аппаратно-программный или программный межсетевой экран;

-маршрутизатор со встроенным пакетным фильтром;

-специализированный маршрутизатор, реализующий механизм защиты на основе списков доступа;

-операционная система семейства UNIX или, реже, семейства Windows, усиленная специальными утилитами, реализующими пакетную фильтрацию.

Защита мультисервисной сети на основе межсетевого экрана позволяет получить высокую степень безопасности и реализовать следующие возможности:

-семантическая фильтрация циркулирующих потоков данных;

-фильтрация на основе сетевых адресов отправителя и получателя;

-фильтрация запросов на транспортном уровне на установление виртуальных соединений;

-фильтрация запросов на прикладном уровне к прикладным сервисам;

-локальная сигнализация попыток нарушения правил фильтрации;

-запрет доступа неизвестного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась;

-обеспечение безопасности от точки до точки: межсетевой экран, авторизация маршрута и маршрутизатора, туннель для маршрута и криптозащита данных и др.

Следует отметить, что межсетевые экраны позволяют организовать комплексную защиту мультисервисной сети от несанкционированного доступа, основанную как на традиционной синтаксической (IP-пакетной) фильтрации контролируемых потоков данных, осуществляемой большинством ОС семейства Windows и UNIX, так и на семантической (контентной), доступной только специальным решениям.

В современных условиях более 50% различных атак и попыток доступа к информации осуществляется изнутри локальных сетей. Мультисервисную сеть можно считать действительно защищенной от несанкционированного доступа только при наличии в ней как средств защиты точек входа со стороны Интернета, так и решений, обеспечивающих безопасность отдельных компьютеров, мультисервисных серверов и фрагментов локальной сети. Безопасность отдельных компьютеров, мульти-сервисных

серверов и фрагментов локальной сети наилучшим образом обеспечивают решения на основе распределенных или персональных межсетевых экранов. Чтобы эффективно обеспечивать безопасность сети, комплексный межсетевой экран обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние.

Простейший способ защиты серверов — установка между серверами и Интернетом межсетевого экрана, например Firewall-1 компании Checkpoint. При правильной конфигурации большинство межсетевых экранов может защитить внутренние серверы от внешних злоумышленников, а некоторые выявляют и предотвращают атаки типа «отказ в обслуживании». Тем не менее, этот подход не лишен некоторых недостатков. Когда мульти-сервисные серверы защищены однимединственным межсетевым экраном, все правила контроля доступа и данные оказываются сосредоточенными в одном месте. Таким образом, межсетевой экран становится узким местом и по мере нарастания нагрузки значительно теряет в производительности.

Итак, межсетевой экран:

- защищает передаваемую информацию в мультисервисных сетях независимо от средств и среды передачи данных (спутниковые каналы, оптические линии связи, телефонные соединения, радиорелейные линии);
-выполняет защиту любых приложений, не требуя их изменений;
-прозрачен для конечных пользователей;
-позволяет реализовать масштабируемые системы защиты с возможностью дальнейшего их наращивания и усложнения по мере роста и совершенствования требований политики безопасности;
- защищает отдельные сетевые информационные системы и приложения независимо от топологии сетей, которые они используют;
- защищает информационную систему мультисервисных сетей от атак из внешней среды;
- защищает информацию от перехвата и изменения не только на внешних открытых соединениях, но и во внутренних сетях мультисервисных сетей;
- может быть легко переконфигурирован по мере развития политики информационной безопасности, добавления ресурсов, обновления технологий, роста мультисервисной сети.

В результате того, что межсетевой экран становится выделенным ресурсом сервера, решается проблема узкого места и уменьшается влияние отказа отдельного межсетевого экрана на общее состояние сети. Однако и данный подход нельзя назвать идеальным, поскольку резко увеличиваются затраты сети на приобретение оборудования. А так же возрастают трудозатраты на администрирование и обслуживание сети.

СПОСОБЫ ОРГАНИЗАЦИИ И МЕХАНИЗМЫ ЗАЩИТЫ БЕСПРОВОДНЫХ СЕТЕЙ

Н.А. Сайфуллаева (ТУИТ, старший преподаватель)

Беспроводные сети используются практически во всем мире. Это обусловлено их удобством, гибкостью и сравнительно невысокой стоимостью. Беспроводные технологии должны удовлетворять ряду требований и качеству, скорости, радиусу, приема и защищенности, причем, защищенность является самым важным фактором. Несмотря на различия в реализации, подход к безопасности беспроводных сетей и их проводных аналоговых идентичен: здесь присутствуют такие же требования к обеспечению конфиденциальности и целостности передаваемых данных и, конечно же, к проверке подлинности ка беспроводных клиентов, так и точек доступа.

Для защиты беспроводных сетей соответствующие стандарту IEEE 802.11 предлагают четыре уровня средств безопасности: физический, идентификатор набора служб (SSID – Service Set Identifier), идентификатор управления доступом к среде (MAC

ID – Media Access Control ID) и шифрование.

Технология DSSS для передачи данных в частотном диапазоне 2,4 ГГц за последние 50 лет нашла широкое применение в военной связи для улучшения безопасности беспроводных передач. В рамках схемы DSSS поток требующих передачи данных "разворачивается" по каналу шириной 20 МГц в рамках диапазона ISM с помощью схемы ключей дополнительного кода (Complementary Code Keying, CCK**).** Для декодирования принятых данных получатель должен установить правильный частотный канал и использовать ту же самую схему CCK. Таким образом, технология на базе DSSS обеспечивает первую линию обороны от нежелательного доступа к передаваемым данным. Кроме того, DSSS представляет собой "тихий" интерфейс, так что практически все подслушивающие устройства будут отфильтровывать его как "белый шум".

Идентификатор SSID позволяет различать отдельные беспроводные сети, которые могут действовать в одном и том же месте или области. Он представляет собой уникальное имя сети, включаемое в заголовок пакетов данных и управления IEEE 802.11. Беспроводные клиенты и точки доступа используют его, чтобы проводить фильтрацию и принимать только те запросы, которые относятся к их SSID. Таким образом, пользователь не сможет обратиться к точке доступа, если только ему не предоставлен правильный SSID.

Возможность принятия или отклонения запроса к сети может зависеть также от значения идентификатора MAC ID - это уникальное число, присваиваемое в процессе производства каждой сетевой карте. Когда клиентский ПК пытается получить доступ к беспроводной сети, точка доступа должна сначала проверить адрес MAC для клиента. Точно так же и клиентский ПК должен знать имя точки доступа.

Механизм Wired Equivalency Privacy (WEP), определенный в стандарте IEEE 802.11, обеспечивает еще один уровень безопасности. Он опирается на алгоритм шифрования RC 4 компании RSA Data Security с 40- или 128-разрядными ключами. Несмотря на то, что использование WEP несколько снижает пропускную способность, эта технология заслуживает более пристального внимания. Дополнительные функции WEP затрагивают процессы сетевой аутентификации и шифрования данных. Процесс аутентификации с разделяемым ключом для получения доступа к беспроводной сети использует 64-разрядный ключ - 40-разрядный ключ WEP выступает как секретный, а 24-разрядный вектор инициализации (Initialization Vector) - как разделяемый. Если конфигурация точки доступа позволяет принимать только обращения с разделяемым ключом, она будет направлять клиенту случайную строку вызова длиной 128 октетов. Клиент должен зашифровать строку вызова и вернуть зашифрованное значение точке доступа. Далее точка доступа расшифровывает полученную от клиента строку и сравнивает ее с исходной строкой вызова. Наконец, право клиента на доступ к сети определяется в зависимости от того, прошел ли он проверку шифрованием. Процесс расшифровки данных, закодированных с помощью WEP, заключается в выполнении логической операции "исключающее ИЛИ" (XOR) над ключевым потоком и принятой информацией. Процесс аутентификации с разделяемым ключом не допускает передачи реального 40-разрядного ключа WEP, поэтому этот ключ практически нельзя получить путем контроля за сетевым трафиком. Ключ WEP рекомендуется периодически менять, чтобы гарантировать целостность системы безопасности.

Еще одно преимущество беспроводной сети связано с тем, что физические характеристики сети делают ее локализованной. В результате дальность действия сети ограничивается лишь определенной зоной покрытия. Для подслушивания потенциальный злоумышленник должен будет находиться в непосредственной физической близости, а значит, привлекать к себе внимание. В этом преимущество беспроводных сетей с точки зрения безопасности. Беспроводные сети имеют также уникальную особенность: их можно отключить или модифицировать их параметры, если безопасность зоны вызывает сомнения.

Благодаря средствам аутентификации и шифрования данных WEP злоумышленнику почти невозможно получить доступ к сети или перехватить передаваемые данные. В сочетании с мерами безопасности на сетевом уровне протокола (подключение к сети, парольный доступ и т.д.), а также функциями безопасности тех или иных конкретных приложений (шифрование, парольный доступ и т.д.) средства безопасности продуктов беспроводной связи открывают путь к безопасной сети.

АХБОРОТ ТИЗИМЛАРИ САМАРАДОРЛИГИНИ БАҲОЛАШНИНГ ДОЛЗАРБЛИГИ ВА МУАММОЛАРИ

А.А. Ганиев (ТДТУ, ассистент)
Н.Ф. Ахмедова (ТАТУ, талаба)

Жахон бозор тизими ривожланишининг ҳозирги босқичи юқори мавхумлик ва иқтисодиёт субъектларининг бизнес муҳитига доимий ўзгаришларни ошиб бориши динамикаси билан характерланади. Глобал ўзгаришлар иқтисодиётнинг юқори технологик секторининг ролини ошиши ва уни ахборот жамиятига ўтиши оқибатида юзага келади. Иқтисодиёт субъектлари борган сари мураккаб ва динамик бизнес – тизим бўлиб бормоқда. Бунда уларни бошқариш тузилмаси ҳамда уларнинг бизнес жараёнларини муҳим қисми бўлиб бораётган тегишли ахборотни ишлаш ва узатиш ҳам мураккаблашади.

Ҳозирги рақобат шароитида ўз бизнес натижаларини (маҳсулотлар ёки хизматлар) тезлик билан яратиб, умумий бозорнинг мавхум талабларига эмас, балки ҳар бир ноёб истеъмолчи эхтиёжига етказиб берса, шундай бизнес тизимлари устунликка эга бўладилар. Ишлаб чиқарувчиларнинг шахсий афзал кўрган истеъмол эхтиёжлари билан ўз бизнесларини мос натижаларини ва адекват бошқарув тизимлари билан биргаликда мутаносиблаштиришлари бу тизимларни самарали ривожланишида ҳал қилувчи омил бўлиб ҳисобланади. Ҳозирги вақтда ахборот коммуникация технологиялари иқтисодиёт субъектларини адаптивлиги ва рақобатбардошлилигини таъминлашнинг асосий воситаларидан бири ҳисобланади. Бизнес муҳит талабларини ўзгариши билан аппарат воситаларга, дастурий махсулотларга ва IT-сервислари (IT-хизматлари)га қўйиладиган талаблар ҳам ўзгаради ва бу уларни мададловчи ахборот инфратузилмасига янада янги аппарат-дастурий платформаларни қўшиб боришга олиб келади. Бунда уларнинг ўсиб бораётган мураккаблиги ва хилма-хиллиги субъектларни бутун бир ахборот тизимларини бошқарилувчанлигига, уларни ишлашининг барқарорлиги ва самарадорлигига таъсир этади.

Ахборотни тўплаш, сақлаш, излаш, унга ишлов бериш ҳамда ундан фойдаланиш имконини берадиган, ташкилий жиҳатдан тартибга солинган жами ахборот ресурслари, ахборот технологиялари ва алоқа воситаларидан таркиб топган ахборот тизимларининг фойдалилигига нисбатан ишончга эҳтиёж, улар билан боғлиқ хатарларни бошқариш ва ахборот устидан назоратга ортиб бораётган талаблар, ҳозирги вақтда корпоратив бошқарувнинг асосий элементлари ҳисобланади. Қиймат, хавф-хатар ва назорат бутун бир бизнес тизимни, хусусан унинг ахборот тизимини нафақат жорий вақт даврида, балки узоқ муддатли истиқболдаги корпоратив бошқарув моҳиятини аниқлайди.

Мавжуд ва эҳтимолий хавф-хатарларни ҳамда бизнес тизимларни ишлаш жараёнида юзага келадиган турли туман муаммоли вазиятларни тадқиқ этишнинг энг мукаммал, кўпфункцияли ва юқори малакали асбоб-ускунаси бўлиб, ихтиёрий хўжалик субъекти ахборот тизими ҳолатини ахборот технологияларини бошқаришни мақсад вазифалари билан ўзаро алоқада ўрганиб чиқиш ва тавсифлаш, кўрсатилган мақсаддан оғиш билан боғлиқ бизнес хавф-хатарларни аниқлаб олиш, ҳамда бу мақсадга эришиш усулларини таклиф этувчи, ахборот тизимлари аудити ҳисобланади.

Ҳозирги шароитда аудит ахборотни ҳар томонлама тадқиқ этишда ва баҳолашда, бошқарув қарорларини қабул қилишда, бутун бир бизнес тизимни, хусусан унинг ахборот

тизимини ривожланиш истиқболини белгилашда деярли унинг ўрнини босиб бўлмайдиган ҳамда бу тизимларни бошқаришни мададлаш асбоби бўлиб қолмоқда. Умумий ҳолда ахборот тизими моҳияти бўйича ўзи ишлаётган бизнес тизимнинг модели ҳисобланиб, жуда ҳам мураккаб ва кўпфункцияли шаклланган тузилма бўлиб, уни тадқиқ этиш ўзига хос, кўп меҳнат талаб этадиган, комплекс ёндошувни талаб этади.

Шу сабабли, бу шароитда аудит, анъанавий бухгалтерия аудитидан фарқ қилиб, бизнес, хусусан унинг ахборот моделининг (ахборот тизимини) аудити бўлиши керак.

Таъкидлаш лозимки, бу ҳолатда аудит фақат бўлиб ўтган ходиса ва далилларни қайд этиш ва тасдиқлаши эмас, балки яхлит бир бизнес тизимни ва хусусан унинг ахборот тизимини ривожланишини оптималлаштириш бўйича бошқарувчи тавсияларни ишлаб беришга йўналтирилган бўлиши керак. Ахборот технологиялари йилдан-йилга мураккаблашиб бормоқда. Уларга катта молиявий ва вақт ресурслари сарфланмоқда ва ҳар доим ҳам шунга адекват самара олинаётгани йўқ. Лекин ҳозирги кунда ахборот технологиялари ҳар бир иқтисодиёт субъектлари учун ҳаётий зарурият, уларни ривожига, уларга хизмат кўрсатувчи персонални мужассамлаштирган ахборот тизимлари ҳозирги замонда рақобатга ҳаракат этувчи ҳар қандай бизнес тизимларнинг ажратиб бўлмайдиган ва муҳим қисми ҳисобланади. Лекин ахборот технологиялари билан боғлиқ бўлган барча ижобий аспектларга иқтисодиёт субъектлари учун мутлақо янги хавф-хатарлар хамроҳлик қилади ва бу субъектларни бошқариш тизимининг юқори бўғинлари томонидан қўшимча назоратни талаб этади. Шу сабабли ахборот тизимларининг аудитининг роли унинг ривожланишининг барча сатҳлари ва босқичларида кескин ортади.

Аудит ахборот тизимларини жорий ҳолатини баҳолаш учун тизимли ва ишончли ахборотни тез олиш билан, бу тизимларни бошқариш ва ривожлантириш бўйича адекват қарорлар қабул қилишга имкон беради.

Ахборот тизимлари аудити анъанавий бухгалтерия аудитига нисбатан мураккаброқ аудиторлик тадқиқоти йўналиши бўлиб ҳисобланади. Уни амалга ошириш учун зарур шарт-шароитларни яратиш бўйича кўп меҳнат талаб этилади. Бунда биринчи навбатда ҳозирги жамиятда мулкчилик шаклидан қатъий назар ҳар қандай иқтисодиёт субъектлари фаолиятининг самарадорлигини ошириш учун аудитни ўтказиш муҳимлиги ва зарурлиги ҳақидаги мувофиқ фикрларни шакллантириш зарур бўлади.

КОРХОНА ВА ТАШКИЛОТЛАРДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ БЎЙИЧА МАЖБУРИЯТЛАРНИ ТАҚСИМЛАШ

О.Н. Бекмирзаев (ТАТУ, ассистент)
Ж.А. Негматов (ТАТУ, талаба)

Ушбу мақолада корхона ва ташкилотларда фаолият кўрсатувчи ходимларнинг ахборот хавфсизлигини таъминлашдаги мажбуриятлари, вазифалари кўриб чиқилган.

Ахборот хавфсизлигини таъминлаш бўйича барча мажбуриятлар аниқ белгиланган бўлиши керак.

Ахборот хавфсизлиги бўйича мажбуриятларнинг тақсимланишини ахборот хавфсизлиги сиёсатига мувофиқ бажариш лозимдир. Шахсий маълумотларни муҳофаза қилиш ва хавфсизликнинг муайян жараёнларини бажариш бўйича мажбуриятларни аниқ белгилаш зарурдир. Зарурат бўлганда мажбуриятларни муайян объектлар ва ахборотга ишлов бериш воситалари учун янада аниқроқ тавсиялар билан тўлдириш лозим. Активларни муҳофаза қилиш ва хавфсизликнинг узлуксиз ишни режалаштириш каби аниқ жараёнларини бажариш бўйича ички мажбуриятларни аниқ белгилашдан иборатдир. Ахборот хавфсизлигини таъминлаш бўйича масалаларни бажариш учун жавобгар ходим ўз мажбуриятларини кимгадир юклаши мумкин. Шундай бўлса ҳам, у жавобгар бўлиб қолади ва ҳар бир юкланган топшириқнинг тўғри бажарилишини таъминлаши лозимдир.

Ходим жавобгар бўлган соҳаларни аниқ ифодалаш керак; хусусан қуйидаги

тадбирларни амалга ошириш зарур:

a) хавфсизликнинг ҳар бир алоҳида тизим билан боғлиқ активлари ва жараёнларини аниқлаш ва аниқ белгилаш керак;

b) хавфсизликнинг ҳар бир актив ва жараёни учун жавобгарни тайинлаш, шунингдек, ушбу мажбуриятларни ҳужжатлаштириш керак;

c) ваколатлар даражасини аниқ белгилаш ва ҳужжатлаштириш.

Кўпгина ташкилотларда ташкилот раҳбарлари аъзоларидан ахборот хавфсизлиги билан боғлиқ барча масалаларга жавобгар тайинланади.

Бироқ активларни қидириш ва бошқриш воситаларини жорий этиш учун жавобгарлик кўпинча алоҳида раҳбарлар зиммасида қолади. Ҳар бир активга унинг кундалик муҳофазаси учун жавобгар бўлиб қоладиган эгасини тайинлаш кенг тарқалган тажрибага айланмоқда.

Ахборотга ишлов беришнинг янги воситаларидан фойдаланиш учун рухсат олиш процедураларини аниқлаш ва жорий этиш зарур.

Рухсат олиш процедураларини жорий этиш учун қуйидаги тадбирлар бажарилиши лозим:

1. янги воситалар ва уларнинг вазифаси фойдаланувчиларнинг раҳбарлари томонидан тасдиқланган ва ички ахборот тизимлари ишлашининг хавфсиз муҳитини кузатиш учун жавобгар маъмур томонидан маъқулланган бўлиши зарур. Ушбу чоралар хавфсизликнинг тегишли сиёсатлари ва талабларини бажаришни кафолатлашга имкон беради;

2. аппарат воситалари ва дастурий таъминотни тизимнинг бошқа компонентлари билан мослашувчанлигига текшириш керак;

3. иш жойида хизматга оид ахборотга ишлов бериш учун ахборотнинг шахсий ишлов бериш воситаларидан, масалан, ноутбуклар, уй компьютерлари ва бошқалардан фойдаланиш янги заифликларнинг сабаби бўлиши мумкин ва бинобарин таъсири баҳоланган ва тасдиқланган бўлиши лозимдир.

Конфиденциалликни сақлаш ва ошкор этмаслик тўғрисида контрактларга қўйилган талабларни белгилашда қуйидаги жиҳатларга амал қилиш лозим бўлади:

1. Муҳофаза қилинаётган ахборотнинг таснифи;

2. Контрактнинг кутилаётган амал қилиш муддати, жумладан конфи-денциалликка риоя қилиш муддатсиз бўлган ҳолларни ҳам ҳисоблаганда;

3. Контрактнинг амал қилиш муддати тўхтатилган ҳолларда зарур чоралар;

4. Ахборотни («билишнинг зарурлик принципи», «фақат билиш зарур бўлган нарсани билиш» каби) рухсатсиз ошкор этилишига йўл қўймаслик учун контрактни имзоловчи шахслар жавобгарлиги ва хатти-ҳаракатлари;

5. Конфиденциал ахборотни муҳофаза қилиш билан тижорат сири ва интеллектуал эгалик ўртасидаги боғлиқлик;

6. Конфиденциал ахборотдан фойдаланишга рухсат беришда контракт- ни имзолаётган шахснинг мажбуриятлари ва ҳуқуқлари;

7. Конфиденциал ахборотдан фойдаланиш аудити ва мониторингини ўтказиш;

8. Рухсатсиз ошкор этиш ва конфиденциалликни бузиш ҳолатлари тўғрисида хабар ва ҳисобот бериш тартиби;

9. Контрактнинг муддати тугаган ҳолларда ахборот йўқ қилиниши ёки қайтарилиши керак бўлган муддатларни белгилаш;

10. Контракт бузилганда кўриладиган чоралар.

Ташкилотдаги хавфсизлик сиёсати талабларига асосан конфиденциалликка риоя қилиш ва ошкор этмаслик тўғрисида бошқа контрактларга зарурат туғилиши мумкин.

Конфиденциалликка риоя қилиш ва ахборотни ошкор этмаслик тўғрисидаги контрактларга қўйилган талабларни ушбу талабларга таъсир қиладиган ўзгаришлар бўлганда вақти-вақти билан қайта кўриб чиқиш керак.

Турли ҳолатларда ташкилотга конфиденциалликка риоя қилиш ва ошкор этмаслик

тўғрисидаги контрактларнинг турли шакллари керак бўлиб қолиши мумкин.

Хулоса қилиб айтадиган бўлсак ахборот хавфсизлиги бўйича мажбуриятларнинг тақсимланишини ахборот хавфсизлиги сиёсатига мувофиқ бажариш керак.

ИМИТАЦИОННАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ В ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ

О.Х. Кулдашов (Ферганский филиал ТУИТ, декан)
К.З. Муминов (Ферганский филиал ТУИТ, студент)

Волоконно-оптические системы связи находят широкое применение для передачи больших объемов информации на значительные расстояния. Одним из основных требований, предъявляемых к современным волоконно-оптическим системам передачи информации, является обеспечение их защищенности от несанкционированного доступа.

Анализ существующих методов и средств обеспечения информационной безопасности в волоконно-оптической линии связи показал, что наиболее актуальным является метод зашумления линейного тракта оптического волокна со стороны приемника информации.

Предложена модель защиты информации от несанкционированного доступа в волоконно-оптической линиях связи. На передающей стороне волоконно-оптической линии связи формируют суммарный сигнал путем смешивания шумового и информационного сигнала и вводят в волоконно-оптическую линию связи, а на приемной стороне волоконно-оптической линии связи из принятого оптического излучения выделяют информационный сигнал.

Имитационная модель защиты информации в волоконно-оптической линии связи (рис.1) состоит из следующих основных элементов:

Источник данных, генератор случайных целых чисел – Random-Integer (Communications Blockset/Random Data Sources), вырабатывающий числа в интервале от 0 до N-1. Выход генератора нужно сделать в виде кадра из K чисел.

Кодер Рида-Соломона – RS encoder (Communications Blockset/Block). Он по сообщению K формирует передаваемый код из N символов.

Декодер Рида-Соломона – RS decoder (Communications Blockset/Block), имеющий два выхода. На верхнем выходе из принятого кода R формируется декодированное сообщение, на нижний выход выводится кратность исправленных ошибок.

Сумматор Sum (Simulink/Math Operation). В нем осуществляется смешивание шумового и информационного сигнала и выделение информационного сигнала.

Блоки Unbuffer (Signal Processing Blockset/Buffers) преобразуют кадры в линейные последовательности, направляемые к виртуальному двухвходовому наблюдателю Scope.

Наблюдатель Scope (Simulink/Sinks) позволяет в общем масштабе времени наблюдать сигналы от блоков Buffer.

При рассматриваемом подходе защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации противником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем канал законного пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возрастало, обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь.

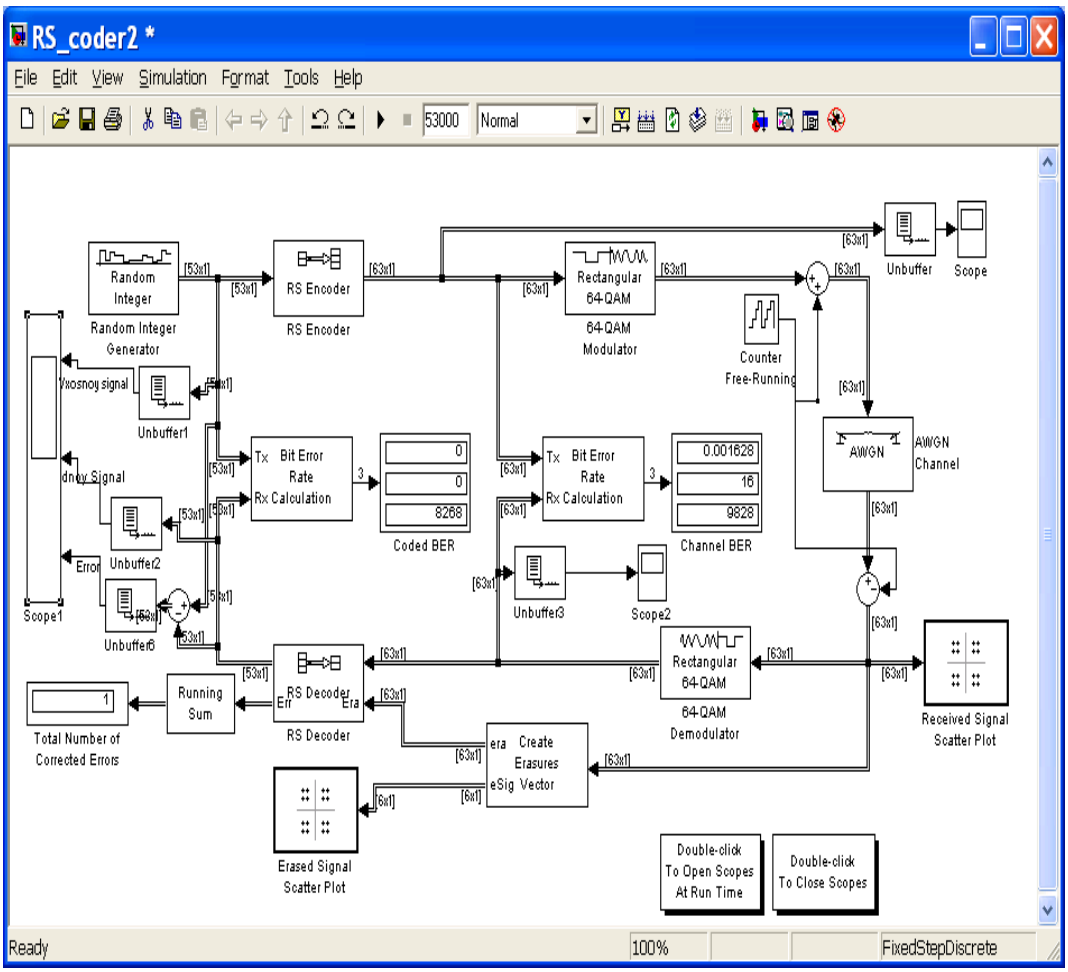


Рис.1. Имитационная модель защиты информации в волоконно-оптической линии связи

ТАРМОҚ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА ТАРМОҚЛАРАРО ЭКРАН (FIREWALL) ДАСТУРЛАРИНИНГ АМАЛИЙ АХАМИЯТИ

Б.К. Юсупов (ТАТУ, ассистент)
У.О. Мамажонов (ТАТУ, магистрант)

Ахборотни ҳимоялаш муаммолари инсониятни қадим-қадим замонлардан бери қизиқтириб келади. Ахборотни ҳимоялаш зарурати ҳам харбий, ҳам дипломатик маълумотларни сирли равишда узатиш талабидан келиб чиқди.

Масалан, антик даврдаги спарталиклар ўз хабарларини шифрлаганлари маълум. Хитойликларда эса маълумотларни иероглифлар ёрдамида ёзишининг ўзиёқ уларни ўзга юртликлар учун сирли қилар эди.

Дастлабки алоқа каналлари ғоят содда бўлган. Уларни ташкил этишда ишончли чопарлардан фойдаланилган. Бундай алоқа тизимларининг хавфсизлиги чопарларнинг содиқлиги ҳамда уларнинг маълумот очилиб қолиши мумкин бўлган ҳолатларга тушиб қолмаслик қобилиятига боғлиқ бўлган.

Криптологиянинг қадимги даврлардан бошлаб, то 1949 йилгача бўлган тарихини илмий криптологиягача бўлган давр деб аташ расм бўлган, чунки у давр ютуқлари интуицияга асосланган бўлиб, далиллар билан исботланмаган эди. Ўша даврда криптология билан фан сифатида эмас, балки фақат санъатнинг бир тури сифатида шуғулланганлар. Бу ўтган даврлар криптология тарихи биз учун ҳеч қандай қизиқиш туғдирмайди деган гап эмас, албатта. қарийб 2000 минг йил аввал Юлий Сезар Римдаги Сицеронга ва бошқа дўстларига ҳозирда ўзининг номи билан аталган шифрдан

фойдаланиб мактублар йўллаган эди.

Саройлар ва бошқа стратегик обектларда қўриқчилар орасида ўзаро махфий сўзлардан фойдаланган ҳолда мурожаатлар амалга оширилган. Махфий сўзлар соқчилар бошлиқлари томонидан маълум муддатларда янгиланиб турган ва шу орқали ташқаридан бўладиган рухсатсиз ташрифлардан химояланилган ва маълумотлар хавфсизлиги таъминланган.

Юқорида айтиб ўтилган ва шу каби бошқа муаммоларни ҳал қилиш учун қандайдир битта техник усул ёки қоида мавжуд эмас. Бироқ уларни ечишда криптографияни ва ахборотни криптографик ўзгартиришларни қўллаш қандайдир умумий йўналиш беради.

Бугунда замонавий компютер тизимларининг яратилиши ва глобал компютер тамоқларининг пайдо бўлиши ахборот ҳимояси муаммосининг мазмуни ва кўламини бутунлай ўзгартириб юборди. Кенг кўламда компютерлаштирилган ва ахборотлаштирилган бизнинг жамиятимизда реал қимматликларга эга бўлиш, уларни бошқариш, қимматликларни узатиш ёки уларга кириб бориш кўп ҳолларда моддийлашмаган ахборот билан, яъни мавжудлиги бирон-бир жисмоний ташувчига ёзилган бўлиши шарт бўлмаган ахборот билан боғлиқ. Баъзида жисмоний ва юридик шахсларнинг катта аҳамиятга эга бўлган ёки конфиденциал (махфий) ахборотдан фойдаланиш, уни модификация қилиш, ундан нусха кўчиришга бўлган ваколатлари ҳам айнан шундай белгиланади. Шунинг учун ахборот конфиденциаллиги ва бутлигини таъминлаш билан боғлиқ барча зарур функцияларни ишга солиш учун самарали воситаларни яратиш ва қўллаш ғоят катта аҳамият касб этади.

Ахборот ғоят қимматли ёки жуда муҳим бўлиши мумкин экан, демак бундай ахборотни сақлаётган, унга ишлов бераётган ёки уни узатаётган компютер тизимларига нисбатан турлича бузғунчи хатти-ҳаракатлар содир қилиниши мумкин.

Шундай экан мазкур муаммони ҳал этишнининг ҳам замонавий усулларини ишлаб чиқиш талаб этилади. Бугун дунёни глобал тармоқсиз тасаввур этиб бўлмайди. Тармоққа уларган қурилма бор экан демак унга тармоқ орқали мурожаат ҳам мавжуд. Тармоқ орқали бизнинг маълумотларимизга бўладиган мурожаатларни эса назорат қилиб боришимиз талаб этилади. Ким бизнинг маълумотларимиздан фойдаланмоқда?, унга ушбу маълумотдан фойдаланишга рухсат берилганми? каби бир қанча саволларга жавоб беришимиз керак.

Бу борада бизга “Firewall” (“Оловли девор”) аппарат ва дастурий воситалари ёрдам беради. Мазкур амалий дастурлар тармоқ орқали мурожаатларни назорат қилишга мўлжалланган бўлиб, у турли усул ва алгоритмларга асосланган. “Firewall” дастури компютернинг кириш - чиқиш портларини назорат қилиб туради, ҳар бир мурожаатни таҳлил қилади. Мурожаатга рухсат берилган ёки йўқлигига қараб киришига рухсат беради ва чеклов қўяди.

“Firewall” локал тармоқни глобал тармоққа чиқиш қисмига ўрнатилади. Шу билан бутун глобал тармоқ ташқи ҳавлардан ҳимоя қилинади. Глобал тармоқ орқали тизимга киришга уринган бузғунчилар аввало “Firewall” нинг ҳавфсизлик тазимини бузиб ўтиши керак бўлади.

Замонавий “Firewall” лар OSI моделининг тармоқ сатхида (TCP/IP протоколида) ишлайди ва пакетли филтрлаш қоидаларига асосланган. “Firewall” администраторн мурожаатлар учун роллар ажратиш имкониятига эга яъни кирувчи ёки чиқувчи IP адресс учун маълум мурожаатларга руҳсат бериш ёки чеклом қўйиш имконияти мувжуд. Бундан ташқари “Firewall” лар нафақат ҳужумларни, руҳсат берилмаган мурожаатларни назорат қилади, бундан ташқари тармоқ трафигини ҳам назорат қилади.

Тармоқ трафигини назорат қилиш компютеригизга ўрнатилган дастурлар ёки операцион тизимингизни сизни “огоҳлантирмасдан” янгиланишларига йўл қўймайди. Бу эса кутилмаган носозликлар келиб чиқишини олдини олади ва сизнинг тармоқ трафигингизни тежайди.

Юқоридагиларни хисобга оладиган бўлсак “Firewall” дастурий ва аппарат

воситалари тармоғимизда аҳборот хавфсизлигини таъминлашимизда биз учун муҳим омиллардан бири экан. Шунинг учун мазкур воситалардан фойдаланиш мақсадга мувофиқ бўлади деб хисоблаймиз.

ОЛИЙ ТАЪЛИМ МУАССАСАЛАРИ АХБОРОТ ТИЗИМЛАРИДАН ФОЙДАЛАНИШНИ БОШҚАРИШДА РОЛЛИ МОДЕЛИНИНГ ЎРНИ

Қ.С. Рахманов (ДБА, кафедра мудири)
Б.Қ. Махманов (ТАТУ, магистратура талабаси)

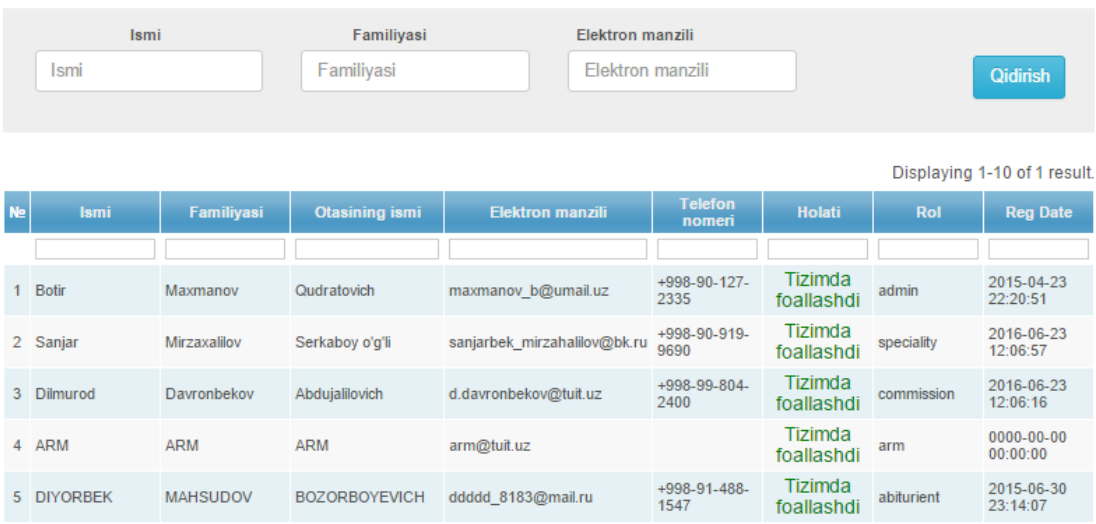
Барчамизга маълумки, ҳозирги ахборот технологиялари асрида маълумотларни хавфсизлигини таъминлаш энг устувор вазифалардан бири бўлиб бормоқда. Ахборот хавфсизлигига бўлган эхтиёжларнинг тобора ортиб бориши, янги ҳимоя қилиш тизимларини турлари ва усулларини яратиш самарали ишларни олиб боришни талаб қилади. Шу нуқтаи назардан ҳар бир ташкилот ва корхоналарни ўзига тегишли ахборот тизимлари ва технологияларидан тўғри ва самарали фойдаланишида уларни қандай ва нима асосида қурилиши муҳимдир.

Юқоридагилардан келиб чиққан ҳолда, олий таълим муассасаси (ОТМ) қабул жараёни ахборот тизими билан ишловчи фойдаланувчилар бўлиб, уларни дастурда бажарадиган ишлари ва маълум бир фаолиятни амалга оширишда зарур ваколатларини амалга ошириш учун роллар аниқ қилиб ишлаб чиқилган (1-расм ва 2-расм). Бу билан эса маълумотларнинг ахборот хавфсизлиги таъминлаган. Ахборот хавфсизлигида рол сиёсати бошқа қатъий ва расмий сиёсатлардан фарқли ўлароқ реал ҳаётга жуда яқин. Ҳақиқатан, тизимда ишловчи фойдаланувчилар шахсий исмидан ҳаракат қилмай, маълум хизмат вазифаларни амалга оширади, яъни ўзларининг шахси билан боғлиқ бўлмаган қандайдир ролларни бажаради.

id	name	surname	password	status	role
1	Botir	Maxmanov	25f9e794323b453885f5181f1b624d0b	0	admin
2	Sanjar	Mirzaxalilov	25f9e794323b453885f5181f1b624d0b	0	speciality
3	Dilmurod	Davronbekov	25f9e794323b453885f5181f1b624d0b	0	commission
4	ARM	ARM	25f9e794323b453885f5181f1b624d0b	0	arm
329	DIYORBEK	MAHSUDOV	2a46ceb76ea727c24e793fa4f82aed6a	0	abiturient
330	MASHHUR	UKTAMOV	e10adc3949ba59abbe56e057f20f883e	0	abiturient
331	AHIL	SAMANDAROV	f5efd45c6d00facd9bbd48a683bf0ad0	0	abiturient
334	FURQATJON	MIRZAJONOV	e10adc3949ba59abbe56e057f20f883e	0	abiturient
338	Bahadir	Begilov	e10adc3949ba59abbe56e057f20f883e	0	speciality

1-расм. Ахборот тизими маълумотлар базасида роллар тақсимоти

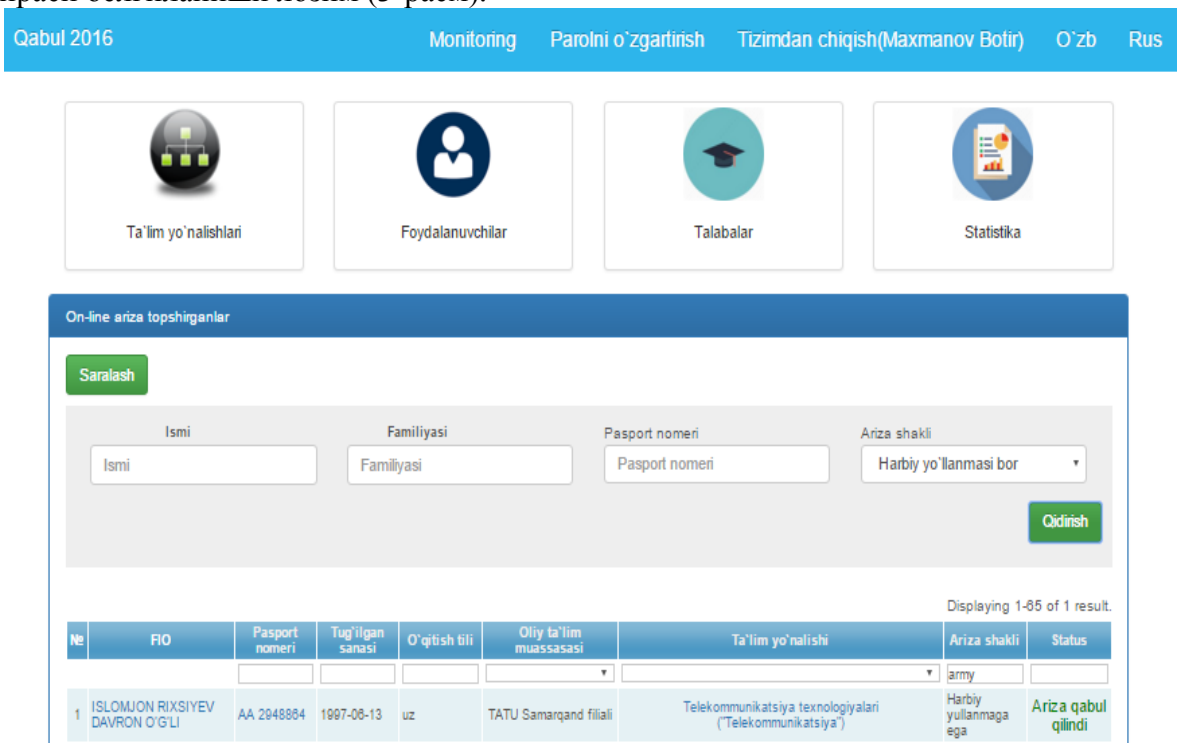
Бу тизимда роллар бошқаруви бир нечта хил кўринишини ташкил этиб (администратор,университет қабул комиссияси котиби, ОТМ таълим йўналиши, Абитуриент) ҳар бири ўзи бажарадиган вазифасига қараб, турлича интерфейсларда шаклланади. Белгиланган роллар кўрсатилган тартибда тўлиқ қўйилган бўлса, шу фойдаланувчи тўлиқ имкониятли рухсат доирасига эга бўлади. Бундай ролни дастур администратори, масъул шахсга бериш тавсия қилинади. Сабаби, фойдаланувчи ўзига берилган рухсатлар доирасида конфигурацияни бошқариш ҳуқуқига эга бўлиб, ишлаб чиқарилган дастурий тасодифий рақамлар генераторларини қўллаш натижасида олинган рақамларни қайта олиш ёки чеклаш имкониятини эга бўлиши мумкин.



№	Ismi	Familiyasi	Otasining ismi	Elektron manzili	Telefon nomeri	Holati	Rol	Reg Date
1	Botir	Maxmanov	Qudratovich	maxmanov_b@umail.uz	+998-90-127-2335	Tizimda foallashdi	admin	2015-04-23 22:20:51
2	Sanjar	Mirzaxalilov	Serkaboy o'g'li	sanjarbek_mirzahalilov@bk.ru	+998-90-919-9690	Tizimda foallashdi	speciality	2016-06-23 12:06:57
3	Dilmurod	Davronbekov	Abdujalilovich	d.davronbekov@tuit.uz	+998-99-804-2400	Tizimda foallashdi	commission	2016-06-23 12:06:16
4	ARM	ARM	ARM	arm@tuit.uz		Tizimda foallashdi	arm	0000-00-00 00:00:00
5	DIYORBEK	MAHSUDOV	BOZORBOYEVICH	ddddd_8183@mail.ru	+998-91-488-1547	Tizimda foallashdi	abiturient	2015-06-30 23:14:07

2-расм. Автоматлашган тизимда роллар тақсимоти

Хар бир фойдаланувчини бажарадиган иши ва ўрнига боғлиқ равишда рухсатлар доираси белгиланиши лозим (3-расм).



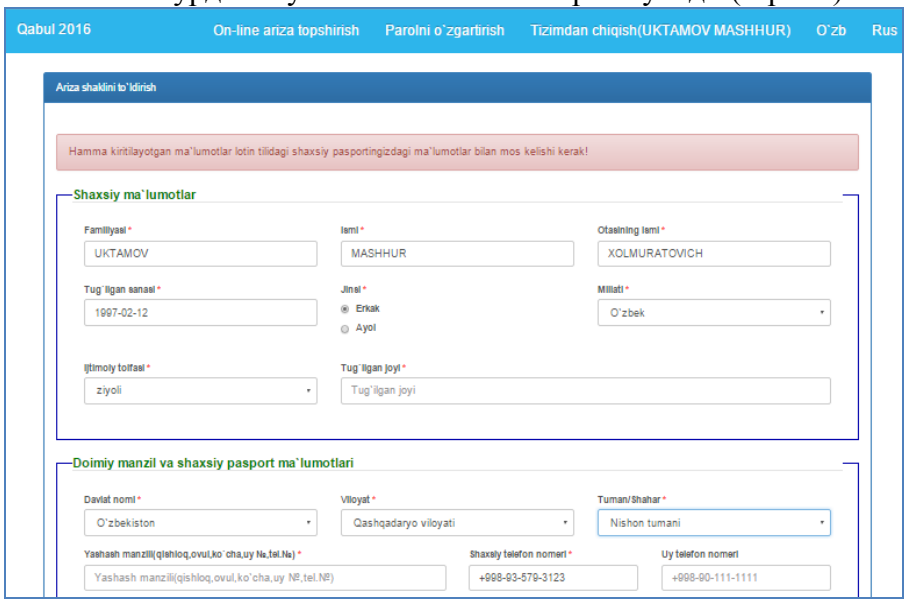
№	FIO	Pasport nomeri	Tug'ilgan sanasi	O'qitish tili	Oliy ta'lim muassasasi	Ta'lim yo'nalishi	Ariza shakli	Status
							army	
1	ISLOMJON RIXSIYEV DAVRON O'G'LI	AA 2948864	1997-06-13	uz	TATU Samarqand filiali	Telekommunikatsiya texnologiyalari ("Telekommunikatsiya")	Harbiy yullanmaga ega	Ariza qabul qilindi

3-расм. Тизим администратори шахсий профили

Тизим администраторига тизимда амалга оширадиган вазифаларига қараб интерфейс шакллантирилган. У таълим йўналишлари ва тушган электрон аризалар контенгентини қўриш, қабул жараёнлари мониторингини юритиш, фойдаланувчиларни бошқариш имкониятларига эга (3-расм). Қабул комиссияси котиби шахсий профилида эса ОТМга тушган барча электрон ҳужжатларни кўриб чиқиши ва тасдиқлаши, мониторингини юритиш имконияти мавжуд (4-расм).

4-расм. Қабул комиссияси котиби шахсий профили

ОТМ таълим йўналишидан маъсул шахс шахсий профилида эса ўзига тегишли йўналишдаги тушган элекрон ҳужжатларни кўриб чиқиш, тасдиқлаш ва мониторингини юритиш имкониятиша эгадир. ОТМга ҳужжат топширмоқчи бўлган абитуриент биринчи навбатда тизимдан рўйҳатдан ўтиши ҳамда тизимга киришни амалга ошириши мумкин бўлади. Абитуриент шахсий профилида мос ариза шаблонини тўлдириш интерфейси ва тўлдирилган ариза шаблонини электрон файлини юклаб олиш, ҳарбий имтиёзга эга бўлса ва таълим йуналишига мос турдош йўналишни танлаш керак бўлади (5-расм).



5-расм. ОТМга ҳужжат топширмоқчи бўлган абитуриент шахсий профили

Ҳудудий жойлашишидан қатъий назар, кундалик ҳаётимизга турли хилдаги ахборотлар халқаро компьютер тармоғи орқали кириб келади. Шунинг учун ҳам мавжуд ахборотларга рухсатсиз кириш, улардан фойдаланиш ва ўзгартириш, йўқотиш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қелмоқда. Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон тамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратиш жуда муҳим саналади.

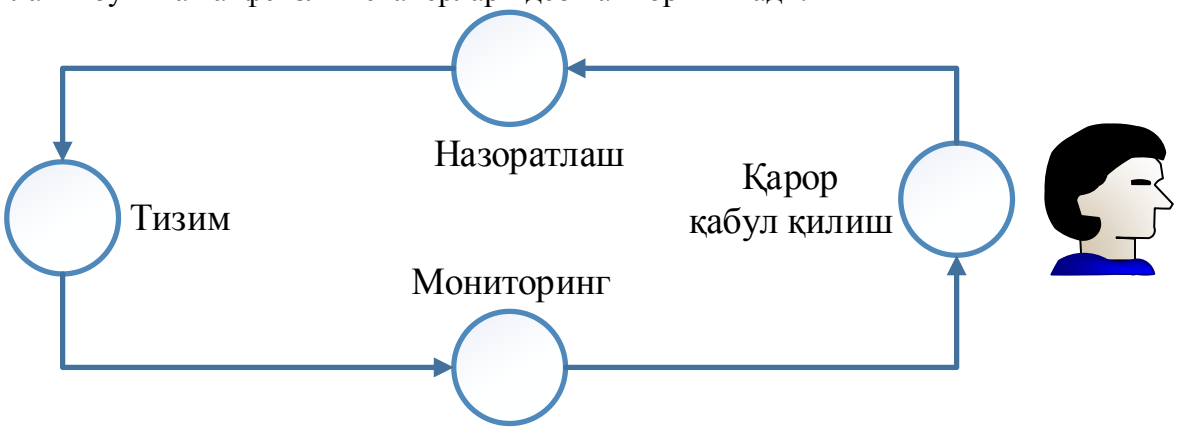
ТАҚСИМЛАНГАН ТИЗИМЛАРНИ МОНИТОРИНГЛАШ УСУЛЛАРИ ТАҲЛИЛИ

С.А. Нематова (ТАТУ ФФ, ассистент)

Ахборотни ҳимоялашда унинг фойдаланувчанлигини таъминлаш муаммоси кўплаб тизимларда долзарб ва бирламчи талаб сифатида қаралади. Ахборотни фойдаланувчанлигини таъминлаш ва бўладиган таҳдидларни олдиндан аниқлаш, ҳужумни

бартараф этишдан самаралирокдир. Тизимга бўладиган тахдидларни олдиндан аниқлашда ва тизимдаги заифликларни аниқлашда одатда мониторинг жараёнидан фойдаланилади. Мониторинг жараёни тизимнинг ҳолатини кузатишни амалга ошириб, вақт онида тизимдан маълумотлар олиб, тизимнинг ишлашини назорат қилиб боради.

Ахборот хавфсизлиги тизимининг мониторинги вазифаларини химояланишни тахлиллаш ва хужумларни аниқлаш воситалари бажаради. Ҳимояланишни тахлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим химояси элементларининг созланишини тадқиқлайди. Улар тармоқ топологиясини тадқиқлайди, химояланмаган ёки нотўғри тармоқ уланишларини қидиради, тармоқлараро экранлар созланишини тахлиллайди. Химояланишни тахлиллаш воситаларини, уларнинг ишлаши бўйича хавфсизлик сканерлари деб хам юритишади.



1-расм. Мониторинглаш ва бошқарув орасидаги боғлиқлик

Тахлиллаш натижасида сканер маъмурга юборилувчи, таркибида аниқланган заифликлар ва уларни йўқотиш қоидалари бўлган хисоботни шакллантиради. Агар сканер таркибида хавфсизлик воситалари созланишини бошқарувчи воситалар бўлса, у мустақил тарзда уларни қайта созлаши мумкин.

Мониторинглаш ва унинг бошқаруви ўрганилаётган тизимнинг талаб қилинаётган моделини қуриш мақсадида керакли маълумотларни тўплаш билан шуғулланади.

Марказлашган ва тақсимланган тизимларда мониторинглаш жараёнида қуйидаги муаммолар мавжуд:

- бевосита ва билвосита кузатиш;
- тугалланган ва тугалланмаган кузатиш;
- тақдимот муаммоси;
- мониторинг ва халақитлар.

Ҳозирги кунда марказлашган тизимлардан фарқли бўлган, тақсимланган тизимлар ҳам кенг фойдаланиб келинмоқда. Қуйидаги жадвалда бу икки турдаги тизим хусусиятлари келтирилган.

1-жадвал

Марказлашган ва тақсимлашган тизимлар хусусиятлари

Марказлашган тизимлар	**Тақимланган тизимлар**
- автоном саналмаган қисмлардан ташкил топган бир ташкил этувчи; - ресурслар барча фойдаланувчилар учун ихтиёрий вақтда тақсимланган; - барча ресурсларни бошқариш имконияти мавжуд; - дастурий таъминот ягона процессорда юкланади; - бошқарувнинг ягона нуқталиги; - ишламай қолишнинг ягона нуқталиги.	- кўплаб автоном ташкил этувчилар; - ташкил этувчиларилар фойдаланувчилар орасида тақсимланмайди; - ресурсларни бошқариш имконияти бўлмаслиги мумкин; - дастурий таъминот турли процессорларда юкланади; - бошқарувнинг кўп нуқталиги; - ишламай қолишнинг кўп нуқталиги.

Тақсимланган тизимларнинг кенг фойдаланилишининг асосий сабаблари қуйидагилар:

- амалга ошириш даражасининг юқорилиги/ нархнинг пастлиги;
- ресурсларни тақсимлаш;
- тизимни ривожлантиришнинг ишончлилиги ва мавжудлиги;
- модулли кенгайтириш;
- боғланиш.

Умумий ҳолда тақсимланган тизимларнинг камчиликлар қуйидагилар:

- мураккаблик;
- тармоқ муаммолари;
- хавфсизлик муаммолари.

Одатда тармоқланган тизимларда мониторинги амалга оширишда қуйидаги учта усулдан фойдаланилади:

- агенгга асосланган;
- агентсиз;
- тартибга асосланган.

Қуйидаги жадвалда бу усулларнинг бир неча хусусиятлар бўйича таҳлил натижалари келтирилган.

2-жадвал

Агентга асосланган, агентсиз ва тартибга асосланган мониторинг усулларининг таҳлили

Усул/ хусусият	Агентга асосланган усул	Агентсиз усул	Тартибга асосланган усусл
Платформага боғликлик	Бор	Йўқ	Бор
Мониторинглаш ҳажми	Талабга кўра созланувчан	Олдиндан аниқланган хусусиятлар	Талабга кўра созланувчан
Мониторинглашни мавжудлиги	Йўқ	Боб	Бор
Ресурслардан фойдаланиш ва ҳодисаларни мониторинглаш	Бор	Бор, чекланган	Бор
Мониторинг маълумотларни теранлиги	Аниқ, тўлиқ	Умумий, чекланган	Аниқ, тўлиқ
Мониторинг маълумотларини алмашиниш режими	Суриш	Сўров – жавоб	Тортиш
Скрипт тили имкониятлари	Талаб этмайди	Талаб этмайди	Талаб этади
Ечим тури	Оғир, содда	Содда	Содда
Ташкилот учун таёйрлилик	Бор	Умумий ҳол учун бор, истемолчи талабига кўра йўқ.	Бор
Мониторинг тизимида дастурий таъминотни ўрнатиш зарурияти	Бор	Йўқ	Истемолчи талабига кўра талаб этади, умумий ҳолда талаб этмайди.

Таҳлил натижаларига таянган ҳолда айтиш мумкинки, тартибга асосланган мониторинглаш усули тақсимланган тизимлар учун мос бўлиб, ташкилот ҳажмига мослашувчанлиги, оптимал архитектурага эгалиги ва натижаларни олишда юқори тезликга эгалиги билан ажралиб туради.

ТАРМОҚ ҲУЖУМЛАРНИ АНИҚЛАШ УСУЛЛАРИНИНГ ТАДБИҚИ

Д.Я.Иргашева (ТАТУ, декан)
Ш.Ж.Ҳамидов (ТАТУ, магистрант)

Ушбу мақолада бугунги кунда тармоқ орқали ҳужумларни аниқлаш усуллари, тармоқда бўладиган ҳужумларни аниқлаш тизимлари ва архитектураси баён этилган.

Бугунги кунгача “ҳужум” (суқилиб кириш, ҳужум) иборасининг аниқ таърифи йўқ. Хавфсизлик соҳасидаги ҳар бир мутаҳҳасис уни ўзича таърифлайди. Ахборот тизимларига ҳужум деб, тизимнинг заифликларидан фойдаланиб, қайта ишланаётган ахборотнинг бутунлиги, маҳфийлиги ва фойдаланувчанлигини бузилишига олиб келувчи таҳдидчининг атайлаб қилган ҳаракатларига айтилади.

Ахборот ва тармоқ технологиялари жуда тез ривожланиб, ўзгариб бормоқда. Бунда статик ҳимоялаш воситалари, кириш ҳуқуқларини чеклаш ҳамда аутентификация тизимлари самарали ҳимояни таъминлай олмайди. Ҳозирги кунда хавфсизлик меёрлари бузилишини аниқловчи, олдини олувчи динамик ҳимоялаш усулларидан фойдаланилади. Ана шундай тизимлардан бири бўлиб, анъанавий фойдаланиш ҳуқуқларини назорат қилувчи моделлар аниқлай олмайдиган бузилишларни кузатишга имкон берувчи ҳужумларни аниқлаш технологияси ҳисобланади.

Ҳужумларни аниқлаш - ҳисоблаш ёки тармоқ ресурсларига йўналтирилган шубҳали ҳаракатларни идентификациялаш ва уларга реакция кўрсатиш жараёни. Технологияларнинг самарадорлиги кўп жиҳатдан тўпланган ахборотни таҳлил қилишда фойдаланилган усулларга боғлиқ. Айни пайтда, статистик усул билан бир қаторда эксперт тизимлари ва нейрон тармоқлар каби янги усуллардан фойдаланилмоқда. Ҳозирда ҳужумларни аниқлаш тизимларида қуйидаги усуллар ишлатилади:

- статистик усул;
- эксперт тизимлар;
- нейрон тармоқлар.

Статистик усул. Статистик ёндашишнинг асосий афзаллиги аллақачон ишлаб чиқилган, ўзини танитган математик статистика аппаратини ишлатиш ва субъект характерига мослаш. Ушбу усулдан фойдаланишдан аввал таҳлил қилинаётган тизимнинг ҳар бир субъекти учун профиллар аниқлаб олинади. Фойдаланилган профил мезонига мос келмаган ҳаракатлар рухсат этилмаган ҳаракат деб қабул қилинади. Статистик усуллар умумий хисобланади улар тизимга бўладиган ҳужумлар ва заифликлар ҳақида билимларни талаб этмайди. Бироқ улардан фойдаланганда баъзи бир қийинчиликлар пайдо бўлиши мумкин, мисол учун рухсат этилмаган харакатларни нормал ҳаракат деб кўрсатиб қўйиш мумкин. Шунинг учун, статистик таҳлил қилиш билан биргаликда қўшимча усуллар ишлатилади.

Эксперт тизимлари. Эксперт тизими эксперт билимларини қамраб олувчи қоидалар тўпламидан ташкил топган. Эксперт тизимидан фойдаланиш хужумларни аниқлашнинг кенг тарқалган усули бўлиб, ҳужумлар ҳусусидаги ахборот қоидалар кўринишида ифодаланади. Бу қоидалар ҳаракатлар кетма-кетлиги ёки сигнатуралар кўринишида ёзилиши мумкин. Бу қоидаларнинг ҳар бирининг бажарилишида рухсатсиз фаолият мавжудлиги ҳусусида қарор қабул қилинади. Бундай ёндашишнинг муҳим афзаллиги - ёлғон тревоганинг умуман бўлмаслиги. Эксперт тизимларини доимо фаол сақлаш учун фойдаланиладиган маълумотлар базаларини янгилаб бориш зарур. Ушбу усулнинг камчилиги номаълум бўлган хужумларни бартараф этиш имкониятининг

мавжуд эмаслиги. Агар маълумотлар базасидан хужумни бир оз ўзгартириб қўйилса уни аниқлашда муҳим тўсиқ бўлиб қолади. Шуни таъкидлаш зарурки оддий IDS фақатгина маълум бўлган хужумларни ўз вақтида аниқлайди. Улар ҳам антивирус дастурларининг режимида ишлайди: маълумлари - аниқланади, номаълумлари - аниқланмайди. Жорий ходисаларни таҳлил қилишда содир бўлган хужумлар ҳам хисобга олиниши мумкин, бу ҳужумларни идентификация қилишга ва келажакда содир бўладиган ходисаларни прогноз қилишга имкон яратади.

Нейрон тармоқлари. Хужумларни аниқлаш усулларининг аксарияти қоидалар ёки статистик ёндашиш асосида назоратланувчи муҳитни таҳлиллаш шаклларидан фойдаланади. Назоратланувчи муҳит сифатида қайдлаш журналлари ёки тармоқ трафиги кўрилиши мумкин. Бундай таҳлиллаш маъмур ёки ҳужумларни аниқлаш тизими томонидан яратилган, олдиндан аниқланган қоидалар тўпламига таянади.

Ҳужумларни аниқлаш тизимлари (IDS) - ҳимояланган компютер тизим(ҳисоблаш тармоқ)ларининг турли нуқталаридан маълумот йиғувчи, ушбу маълумотларни бузишга уринишларни аниқлаш учун таҳлил қилувчи ва хақиқий ҳимоянинг бузилиш(суқилиб кириш)ларини аниқловчи тизим.

Замонавий ҳужумларни аниқлаш тизимлари мантиқан қуйидаги асосий элементларга ажратилади: ахборот йиғувчи қисм тизим, таҳлил қилувчи қисм тизим ва ҳисобот тақдим қилувчи модул.

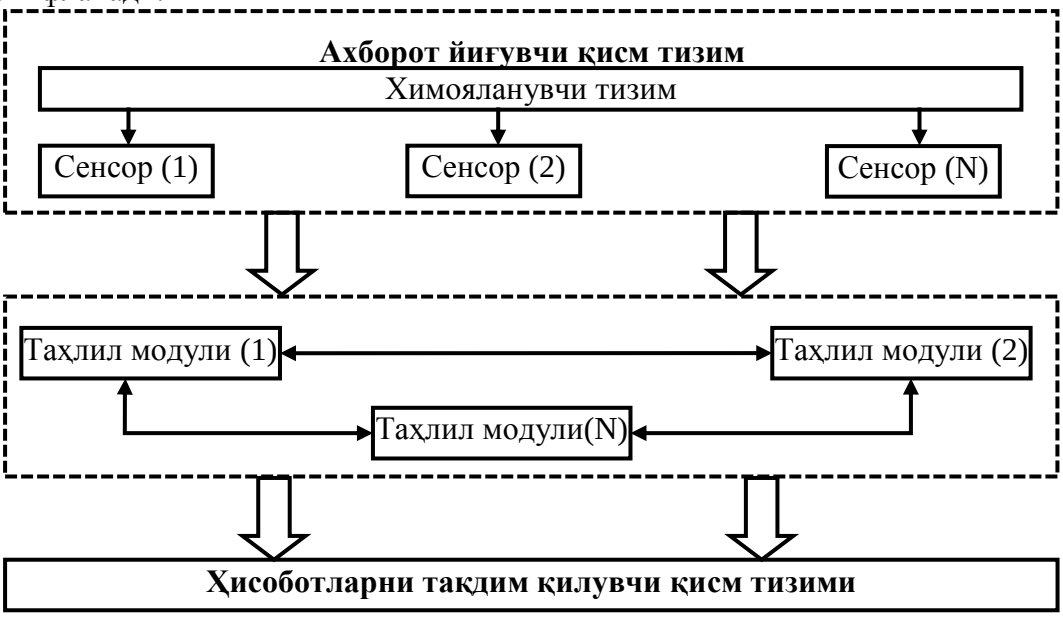
Ахборот йиғувчи қисм тизим ҳимояланаётган тизим иши ҳақида бошланғич маълумотларни тўплаш учун ишлатилади.

Таҳлил қилувчи қисм тизими (аниқлаш) ҳимояланган тизимга нисбатан ҳужум ва суқилиб киришларни қидиришни амалга оширади.

Ҳисоботларни тақдим қилувчи қисм тизими (фойдаланувчи интерфейси) DNS фойдаланувчиларига ҳимояланаётган тизим ҳолатини кузатиб бориш имконини беради.

Ахборот тўплаш қисм тизимида ҳимояланаётган тизим иши ҳақида маълумотларни тўпланади.

Ахборот тўплаш учун автоном модулар-сенсорлардан фойдаланилади. Ишлатиладиган датчиклар сони ҳар хил бўлади ва ҳимояланаётган тизимининг ҳусусиятларига боғлиқ бўлади. IDS даги датчиклари тўпланадиган маълумотлар турига қараб синфланади.



1-расм. Ҳужумларни аниқлаш тизими архитектураси

Ахборот тизимларининг умумий тузилиши мувофиқ қуйидаги турларга ажратилади:

- илова сенсорлари - ҳимояланаётган тизимнинг дастурий таъминоти иши ҳақида маълумот тўплайди;

- ҳост сенсорлари - ҳимояланаётган тизим ишчи станцияси фаолияти ҳақида маълумот тўплайди;

- тармоқ сенсорлари - тармоқ трафигини баҳолаш учун маълумотлар тўплайди;

- тармоқлараро сенсорлар - тармоқлар орасидаги алмашинувчи маълумотлар хусусиятларини ўз ичига олган.

Таҳлил қилувчи қисм тизими - бир ёки бир неча таҳлил модуллари, анализаторларни ўз ичига олади. Бир неча анализаторларнинг мавжудлиги аниқлаш самарадорлигини ошириш учун керак. Ҳар бир анализатор муайян турдаги ҳужумлар ёки суқилиб киришларни излашни амалга оширади. Анализатор учун кириш маълумотлари бўлиб ахборот йиғувчи қуйи тизимдан ёки бошқа анализатордан олинган ахборот хизмат қилади. Замонавий IDS ларнинг таҳлил қилувчи қуйи тизимларида фойдаланилган усулларни икки йўналишга ажратиш мумкин: биринчиси химоя қилинаётган тизимда аномал ходисаларни аниқлашга, иккинчиси рухсат этилмаган хатти ҳаракатларни қидиришга йўналтирилган.

Юқоридагилардан келиб чиқиб, хозирги кунда ҳужумларни аниқлаш тизимлари ҳужумларни аниқлаш ва уларга реакция кўрсатишда муҳим ўрин эгаллайди. Ташкилот тармоқ ҳимоясини қуришда, ҳимоялаш механизмаларини тадбиқ этишда ҳужумларни аниқлаш тизимининг эксперт тизимларига асосланган тизимидан фойдаланиш самарали ва ишончли ҳисобланади.

“ЭЛЕКТРОН ҲУКУМАТ” ТИЗИМИНИ САМАРАЛИ ТАШКИЛ ЭТИШДА АХБОРОТНИ РУХСАТСИЗ ЧИҚИБ КЕТИШИДАН ҲИМОЯЛАШ

С.Ш. Муминова (ТАТУ, ассистент)

Ахборот технологияларининг кенг доирадаги соҳаларни қамраб олиши тўқсонинчи йилларда WorldWideWeb нинг пайдо бўлиши билан бир қаторда шаклланиб борди. Фойдаланувчилар интернетда ҳукумат ва корпоратив ташкилотлар томонидан кўплаб ахборот ва хизматларни талаб қилиниши натижасида фуқаролар ўзларининг фуқаролик, касбий ва шахсий ҳаётлари тўғрисида ахборотни алмашиш ва сақлаш мақсадида фойдаланиб келишмоқда. Бунинг натижасида доимий равишда ўсишнинг сабаби сифатида электрон ҳукумат тизими барча соҳаларни қамраб олиш ва хизмат кўрсата олиш қобилиятиги эга эканлиги тан олинди. Аммо, бу талабни бажариш жараёнида ахборотни қайта ишлаш ва хизматларни кўрсатиш учун алоқа, тармоқ ва тизимни яратишда АКТ воситаларидан фойдаланиш зарур.

Маълумки, электрон ҳукумат – бу давлат бошқарув органларида ахборот ва коммуникацион технологияларни қўллаш орқали янги кўникмаларни жорий қилиш ва ташкилий ўзгартиришлар асосида давлат хизматларини ва демократик жараёнларни, давлат сиёсий институтларига ёрдам беришни таъминлашни такомиллаштиришга қаратилган тизимдир.

Сўнгги йилларда “Электрон ҳукумат” тизими бир неча сабабларга кўра ҳукумат органлари томонидан оммалашиб бормоқда. Бу сабабларга қуйидагиларни киритиш мумкин:

- давлат хизматларини самарали ва тезлаштирилган босқичда кўрсатилиши;
- ички самарадорликни ўзгартириш;
- фуқаролар, корхоналар ёки бошқа давлат муассалари ўртасида ахборот алмашинуви;
- харажатларни камайтириш ва даромадни ошириш;
- маъмурий жараёнларни тузилмасини қайта тузиш.

Бироқ қандай тизимда ишлашингиздан қатъий назар тизимнинг ахборот

хавфсизлигини таъминлаш асосий муаммо бўлиб қолмоқда. Ахборотнинг хавфсизлигини таъминлаш учун, аввало, унга бўлиши мумкин бўлган хавфларни ўрганиб чиқиб, турли усул ва воситалардан фойдаланиш зарур.

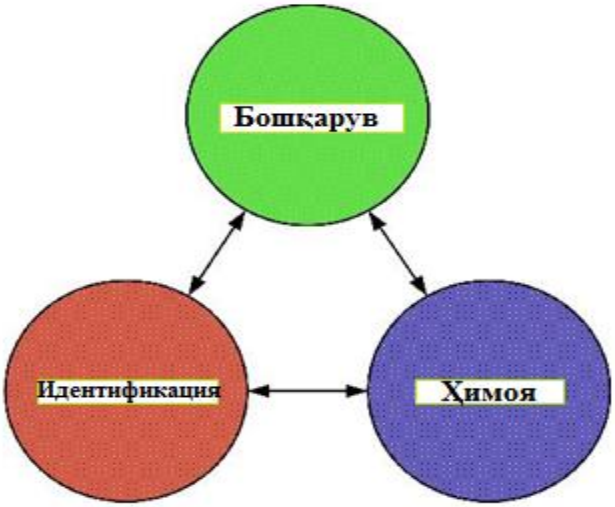
Электрон ҳукумат тизимини хавфсизлигни таъминлаш учун ундаги таркибий қисмларнинг тузилиши ва улардаги ҳимояланиши зарур бўлган ахборотлар аниқланиши зарур.

Конфиденциал маълумотлар ҳимоясини автоматлаштиришда ҳаттоки етук мутахассислар ҳам хато қилиш мумкинлигини кўзда тутиш лозим. CompTIA нашриёти ахборот хавфсизлиги сохаси 2008 йил натижалари бўйича тайёрлаган докладига кўра, ахборот бузилиши сабабларининг 30% ходимларнинг хатолари юзасидан, 30% хаккерларнинг ходимлар хатоларидан фойдалангани натижасида ва 40% хаккерларнинг хужуми натижасида амалга ошрилиши келтириб ўтилган. Ҳозирги кунга келиб бу кўрсаткичлар бир мунча ўзгарган бўлиб, шу нашриётнинг соха бўйича янги докладига кўра, жиддий ахборот бузилишларининг 8% гина ходимларнинг иштирокисиз амалга оширилган. Қолган 92% ҳолатда албатта инсон фактори иштирок этгани қайд этилган.

Инсонлар конфиденциал маълумотларни ҳимоясига жиддий киришишган, бироқ барибир етарли даражада эмас. Шунинг учун ҳам ахборотни ҳимоялаш жараёнини автоматлаштириш яхши натижаларни беради. Бу вазифани бажаришда DLP технологияси қўл келади.

DLP – Data Loss Prevention – “Ахборотларни йўқолишини олдини олиш” термини конфиденциал маълумотларни ҳимоясини ва идентификациясини автоматлаштириш технологиясини ифодалайди.

DLP тизими 3 та асосий функцияни амалга оширувчи компонентга эга: бошқариш, идентификация ва ҳимоя. Бошқариш компоненти маъмур томонидан яратилган хавфсизлик сиёсати қоидалари асосида ишлайди ва маълумотларни хисоботларни кўринишида сақлайди.



1-расм. DLP тизимининг функционал компоненталари.

Идентификация жараёнида эса тизим сигнатуравий тахлил ёрдамида конфиденциал маълумотларни аниқлашни амалга оширади. Ҳимоя компоненти идентификация жараёнида аниқлнаган конфиденциал маълумотларни ҳимоялайди. Қуйидаги 1-расмда ушбу учта компонентнинг ўзаро боғланиши кўрсатилган.

Ҳозирги кунда DLP тизими икки ҳил мақсадда тармоқ ҳимоясини ташкил этишда ҳамда тармоқ терминалларидаги маълумотларни ҳимоялашда қўлланилади.

Тармоқ DLP тизими конфиденциал маълумотларни электрон почта ёки веб орқали чиқиб кетмаслиги учун маълумотнинг узатилишини назорат қилиб туради. Бунда маълумотларнинг химояси ва индентификацияси тармоқда узатилиши орқали назорат қилинади (2-расм).

2-расм. Тармоқ DLP тизимининг ишлаш механизми

Тармоқ терминалларини ишини таҳлил қилиш ва маълумотларини ҳимоялаш телекоммуникацион тармоқларни таҳлил қилишга нисбатан бир осонроқ. Шунинг учун амалиётда тармоқ терминаллари DLP тизимлари нисбатан кўп учрайди. Улар ишчи станциялар ва сервердаги маълумотлар базаларини назорат қилади (3-расм).

3-расм. Сервер ва ШКлар DLP тизимининг ишлаш механизми

Хулоса қилиб шуни айтиш мумкинки, электрон ҳукумат тизими – давлат бошқарув органлари (вазирликлар, қўмиталар, марказлар ва б.қ.) ва фуқаролари ўртасидаги алоқа таъминловчи, интерактив хизмат кўрсатувчи ва ахборот берувчи ва бошқа тизимлар мажмуини ўзи ичига олувчи йирик тизим. Тизимнинг таркибий қисмлари ўртасида ахборот алмашиш, сақлаш ва қайта ишлаш жараёнларида қўлланиладиган ахборот хавфсизлигини таъминловчи усуллар ва воситалар муҳим аҳамиятга эга. Бу ўринда DLP технологияси маълумотларни хавфсизлиги таъминлаш, шунингдек, ходимларнинг иш вақтини мониторинг қилишда самарали восита бўлиб ҳисобланади. Тажрибалар шуни кўрсатдики, DLP технологиясидан фойдаланиш маълумотларни руҳсатсиз чиқиб кетиши ёки йўқолиши миқдорини сезиларли даражада пасайтиради. Шунингдек ушу тизимнинг тўлиқ ишлаб чиқилиши конфиденциал маълумотларни излаш, аниқлаб олиш ва ҳимоялашда самарали натижаларни беради.

МАРШРУТИЗАЦИЯ ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ СМЕШАННОГО ТИПА

М. И. Рашидов (ТУИТ, магистр)
Т.А. Кучкаров (ТУИТ, доцент)

Задача маршрутизации данных в беспроводной сети разбивается на несколько этапов. Первый этап – определение требований к маршруту передачи данных. Критериями требований могут выступать: пропускная способность канала, величина задержки при передаче данных, надежность выбранного маршрута и т.д. Второй этап – отыскание одного или нескольких маршрутов от источника передачи данных к их получателю,

удовлетворяющих этим требованиям, или установление невозможности найти такой маршрут. Третий этап – выбор из множества найденных маршрутов одного, являющегося оптимальным по заданному набору критериев.

Первый этап обычно выполняется протоколами более высокого уровня на основании информации, к какому типу относится передаваемый трафик. В задачи алгоритма маршрутизации входит выполнение второго и третьего этапа. Подавляющее большинство алгоритмов выполняют поиск маршрутов передачи данных без учета требований к типу передаваемого трафика. Это значит, что все существующие алгоритмы маршрутизации предполагают использование только одного типа коммутации (либо пакетов, либо каналов) в беспроводной сети и оказываются неэффективными или даже неприменимыми для задач маршрутизации данных в сетях со смешанными типа передаваемой информации.

Наибольшее распространение получили 3 группы протоколов: проактивные, реактивные и гибридные. Проактивные протоколы (известные также как протоколы маршрутизации с использованием таблиц) применяются для поиска маршрута непосредственно на стороне узла-источника. Реактивные протоколы, или протоколы маршрутизации по запросу, не хранят таблицу маршрутизации в памяти узла. Вместо этого они для каждого ранее неизвестного получателя выполняют рассылку пакетов поиска маршрута и по получению ответа начинают процесс установления соединения и передачи. Гибридные протоколы используют смешанный подход, когда для маршрутизации до определенного множества узлов «ближней зоны» используется проактивный протокол, а до узлов «дальней зоны» – реактивный протокол.

У каждого из подходов есть свои достоинства и недостатки. Например, проактивные протоколы обеспечивают самую высокую скорость маршрутизации, но генерируют при этом значительный объем служебных пакетов. Реактивные протоколы, хотя и оказывают минимальное влияние на пропускную способность сети, предоставляют маршрутную информацию со значительной задержкой. Гибридные протоколы, сочетающие в себе достоинства проактивных и реактивных протоколов (хотя и не лишены недостатков) в целом являются более эффективными. Однако как было отмечено ранее, в настоящее время не существует протоколов маршрутизации, которые были бы эффективны в сетях со смешанными типами коммутации ресурсов, поэтому требуется разработать новый протокол, который мог справляться с данной задачей. Такой алгоритм маршрутизации можно назвать алгоритмом для трафика смешанного типа.

В задачи алгоритма маршрутизации входит отыскание всех возможных ациклических путей от источника к получателю и последующий выбор одного из них, наиболее эффективного по заданному критерию.

В основе разрабатываемого алгоритма лежит модифицированный волновой алгоритм Ли, использующийся для поиска маршрутов в «ближней зоне», т.е. отыскания всех ациклических маршрутов от узла-источника к узлу-потребителю, и принцип минимальности занятых каналов.

Принцип состоит в следующем: из двух зависимых маршрутов более эффективным считается тот маршрут, длина которого меньше. Данное ограничение основывается на следующем:

- меньшая длина маршрута обеспечивает меньшую задержку при передаче данных;
- маршруты по определению являются зависимыми, следовательно, всегда как минимум для одной пары узлов одного маршрута, найдется соответствующая пара узлов множества другого маршрута, между которыми будет находиться, по меньшей мере, один узел, не входящий в состав первого маршрута. Работа алгоритма маршрутизации должна завершиться 3 возможными способами:

– узел-получатель оказывается соседом узла-источника;

– после очередного увеличения индекса волны оказывается, что нет ни одного узла с таким индексом;

– узел-источник ограничивает максимальный индекс волны определенным значением, по достижении которого поиск прекращается.

После завершения работы алгоритма поиска, протокол маршрутизации должен осуществить выбор одного из этих маршрутов, оптимального по определенному критерию. Набор критериев зависит от типа передаваемых данных и политики управления ресурсами сети. Для потокового трафика (который использует коммутацию каналов) необходима дополнительная проверка на наличие достаточного количества доступных выделенных каналов для организации сквозного соединения на всем маршруте от источника до получателя.

В случае, когда длина маршрута больше одного пролета должна производиться ретрансляция данных. При этом возможно повторное использование каналов.

В результате работы алгоритма должны быть получены результаты, позволяющие говорить о значительном выигрыше от использования предлагаемого протокола в сетях смешенного типа.

АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИДА АХБОРОТ ХАВФСИЗЛИГИНИ БАҲОЛАШНИНГ ЗАМОНАВИЙ УСУЛЛАРИ

О.У.Халмуратов (ТАТУ УФ, катта ўқитувчи)
Д.Ж.Хўжамов (ТАТУ УФ, талаба)

Ахборот коммуникация технологияларида ахборот хафсизлигини баҳолаш тизимларида баҳолаш усуллари бўйича умумий қабул қилинган стандартлар ва хужжатларнинг тўлиқ эмаслигига қарамасдан, бу сохада кенг тарқалган усулбий таҳлиллари мавжуд. Ахборот коммуникация технологияларида ахборот хафсизлигини баҳолаш тизимларида баҳолашнинг учта асосий усули мавжуд бўлиб улар:

- таҳлилий;
- статистик;
- синфлаш каби усулларни ажратишга имкон беради.

Ахборот коммуникация технологияларида ахборот хафсизлигини баҳолаш тизимларида баҳолашнинг амалий ёндашуви – бу хавф-хатар ва ҳимоя механизмларида калит тушунчалари билан боғлиқ жиддий қийинчиликлар борлиги сабабли кенг тарқалмаган.

Ўз вақтида, статистик ёндашув ахборот хафсизлигини баҳолаш тизимларида у ёки бу ҳолатларнинг юзага келиши частотаси ҳақида статистик ахборотни йиғиш ва улар асосида мос таҳдидларнинг юзага келишини статистик эхтимоллик қийматларини ҳисоблашларни кўзда тутади. Эхтимоли жуда кичик бўлган ходисалар ҳақида реал маълумотлар олиш ва АКТ га ҳар йили қўйилувчи янги ускуналар ва дастурий воситалар бўйича реал статистикаларни йиғиш амалда мумкин эмас. Бу эса нима сабабдан ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашда статистик ёндашувдан амалиётда қисман фойдаланишни тушинилади, ундан ёндашувчи восита ва статистик маълумотлар ишончлилигини жиддий исботлашда фойдаланилади.

Амалиётда ноформал ҳимоя моделларидан фойдаланувчи ноформал синифлфрга болинувчи ёндашув кенг тарқалган, унда объектлар характеристикалари қийматлари сифатида аниқ категорияларга тегишлилигидан фойдаланилади. Ушбу ёндашув ҳимояланганлик кўрсаткичларининг аниқ қийматларини белгилаб бермайди, лекин ахборот коммуникация технологиялари ни ҳимоя даражаси бўйича синифларга бўлиш ва таққослаш имконини беради.

Хавфсизлик регуляторларини қўллаш даражасини баҳолаш учун, ахборот ҳимоя тизимини тестлашнинг фаол ва пассив усулларидан фойдаланилади, яъни потенциалли зараркунанданинг ҳимоя механизимларини алдаш бўйича ҳаракатларини имитациялайди ёки текширув ва сўровномалар ёрдамида ускуналар, операцион тизимлар ва иловалар

конфигурациясини таҳлил қилади. Тест ўтказиш қўлда ёки махсус дастурий воситаларни қўллаш билан амалга оширилади.

Кўрсатилган дастурий воситалар мисоли – бу қуйдаги тизимларни ўз ичига олувчи Internet Security Systems компанияси махсулотлари оиласидир;

- Ахборот коммуникация технологиялари даражадаги ҳимоя тахлили-Internet Scanner, ОТ даражадаги ҳимоя тахлили – System Scanner;
- ММБТ даражасидаги ҳимоя тахлили – Database Scanner;
- Симсиз тармоклари даражасидаги ҳимоя тахлили – Wireless Scanner.

Бундай дастурий махсулотлар турли компаниялар (Network Asseociates, Cisco Systems, Symantec, “Информ зашита” ва бошкалар) ва мустақил дастурчилар гуруҳи билан бирга ишчилаб чиқилган. Ахборот хавфсизлигини баҳолашнинг барча мавжуд усуллари маълумотлар базаси технологияларига асосланган автоматлаширилган шахсий воситалардан фойдаланилади ва сифат, миқдорий усулларга бўлинади.

Сўнги 15 йил мобайнида, оддийлиги билан ажралиб турувчи ҳимоянинг усули кенг тарқалди. Турли автоматлаштирилган воситалардан кўп сонли услубиётлар ишлаб чиқилди. Уларнинг ичида энг машхурлари қуйдагилардан иборат:

Англянинг GOBRA, Германиянинг RA software Tool ва Австралиянинг Method Warc усуллари. Ушбу методикалар ташклот ҳимоя тизимининг халқаро стандартлар, яъни ISO 17799-2002 га ёки миллий стандартларга мос равишда баҳолаш имконини беради. Баҳолаш бошланғич маълумотлар асосида, сифатли шкалалардан фойдаланилиб амалга оширилади.

Ҳавфларни баҳолаш ва бошқариш маълум миқдорий методлари тизимини таҳлилининг объектга йўналтирилган усулларга асосланган нозик томонлар маълумотлар базасидан ва махсус ишлаб чиқилган мураккаб ускунавий воситалардан фойдаланилади. Кўрсатилган методларга биринчи навбатда, Англянинг CRAMM , Американинг Risk Watch ва Россиянинг “Гриф” ва “АванГард” ларни мисол қилиш мумкин. Аммо, таҳлилидан кўринадики, бу методлар миқдорий деб фақат шартли равишда номланиши мумкин. Чунки унда қўлланилувчи балли баҳо субъективлигининг йирик қисмларига эга сифат шкалаларидан яхши эмас.

Ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолаш учун асосий усул – бу синфларга ёндашув деб таъкидлаш мумкин. Бу усулда интерваллар шкаласидан фойдаланилади ва асосий параметрларни синфлаш йўли билан балли баҳолашга имкон беради. Олинган сифат катигорияларида чизиқли функйиялардан фойдаланилиб, мос равишда айрим мидорий катталикларга қўйилади. Таҳлилдан кўринадики, ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашда лингвистик шкалалардан фойдаланиш мақсадга мувофиқдир. Мажмуавий баҳолашда эса, лингвистик шкалалар базасида тўлиқ ортоганал семантик фазони қуриш зарур бўлади. Бугунги кунда, ноаниқ баҳоларнинг мақсадга мувофиқлиги шубҳа уйғотмайди.

Ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашнинг замонавий усулларининг жиддий камчиликларига экспертлар билимидан самарали фойдаланилмаганликни киритиш мумкин. Қоида бўйича, нисбатан муҳим кўрсаткичлар ва уларнинг нуқтали қийматлари баҳосини олиш билан чегараланади.

Мавжуд ишларда мезонлар туридаги асослашлар деярли йўқ. Унда чизиқли белгини танлаш яхши усул ҳисобланади, бунда нисбатан муҳим кўрсаткичларнинг амалда доимий бўлмаганлиги муҳокама қилинмайди.

Ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашнинг замонавий методлари камчилиги – бу чегараланган меъёрий услубий базани қўллаб олинган мажмуавийликнинг йўқлигидир.

Деярли барча ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашда замонавий усуллар кўп меҳнат сарфлашни таълаб қилади ва ишларда лингвистик шкала белгилари градацияси сони етарлича асосланмаган.

Шундай қилиб, ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолашнинг замонавий усуллари бир қатор аҳамиятли камчиликларга эга. Буларга, улардан амалий фойдаланишнинг қийинчилиги ва олинган натижалар қийматларини пасайтиради. Ўтказилган таҳлиллардан кўринадики, ҳозирги вақтда баҳонинг объективлиги, мажмуавийлиги ва меҳнат сарфи замонавий талабларни қондирувчи ахборот коммуникация технологиялари ахборот хавфсизлиги тизимларини баҳолаш усул ва услубиятлари мавжуд эмас.

AXBOROT XAVFSIZLIGI HODISASINI KO'CHIRISH QOIDALARI

K.A.Tashev (TATU, dekan)
Y.A. Bo'riyev (TATU, magistr)

Axborot xavfsizligi hodisasi bu ko'chirishda ishlatiladigan atama "xavfsizlik voqeasi" bilan bog'liq har qanday axborot xavfsizligi voqeasini anglatadi. Bu axborot kamchiligini anglatadi, bu esa Hukumat yoki salbiy voqea manfaatlari, maxfiylikka nisbatan kompyuter yoki tarmoq xavfsizligiga tahdid solmoqda, qaysiki nomaqbul axborot tizimini ishonchliligi, butunligi va mavjudligiga ta'sir qiladi. Biroq, bunday tabiiy ofat kabi salbiy hodisalar, apparat / dasturiy ta'minot va hokazolarni buzilishi, ma'lumotlar liniyasi yetishmovchiligi, elektr uzilishi, bu dasturil amal qilish doirasidan tashqari, va tizimga texnik xizmat ko'rsatish va falokatda qutqaruv rejasi bilan hal qilinishi lozim.

Xavfsizlik voqealari misollari o'z ichiga oladi: ruxsatsiz kirish, ruxsatsiz foydalanish xizmatlari, xizmatlarni rad etish, himoyalangan ma'lumotlar / dastur / tarmoq tizimi murosali imtiyozlari, elektron shaklda, zararli qirg'in yoki modifikatsiya mahfiy ma'lumotlarni oqish va ma'lumotlarga kirilganda va aralashayotganini, tizim resurslarini noto'g'ri, kompyuter viruslari va soxta tarzda qotgan va zararli kodlariga yoki tarmoq tizimlariga ta'sir qiladi.

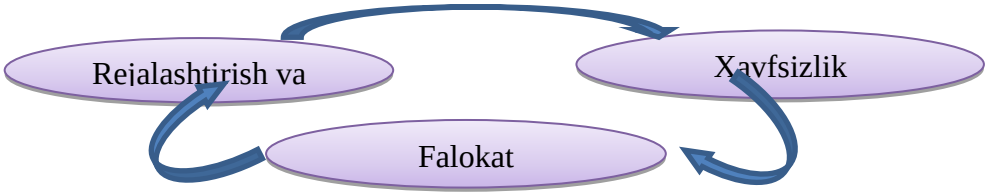
Xavfsizlik hodisasini ko'chirish

Xavfsizlik hodisasini ko'chirish bu faoliyatini tartibga soluvchi harakatlar oldin, davomiy va axborot xavfsizligi sodir bo'lganda keying davomiy jarayonlarning jamlanmasi bo'lib hisoblanadi.Xavfsizlik voqeadan foydalanishda rejalashtirish bilan boshlanadi va resurslar uchun tayyorlash va to'g'ri tartibda rivojlanayotgan bunday ko'lamining kengayishi va xavfsizlik voqea sifatida, javob tartibida ta'qib qilinadi.

Xavfsizlik voqeasini aniqlanganda, xavfsizlik voqeasiga javobgar mas'ul tomonidan oldindan belgilangan tartibda quyidagi tomonlar amalga oshiriladi. B/ D Hukumat axborot xavfsizligi voqealar aralashishi offisi (GIRO) doimiy office sifatida iloji boricha tezroq maslahat berishi va yangilashi kerak. Xavfsizlik voqeasiga javobgarlik xavfsizlik hodisasini hal qilish va normal operatsiyalarni yig'ishda olib borilgan say harakatlar va hatti harakatlarni ifodalab beradi. o'ziga xos hodisaga javobgar jamoalar odatda talab qilingan vazifalarni amalga oshirish uchun tashkil etilgan.

Qachonki hodisa tugaganda, hodisani aniqlashga va qaytishni oldini olishda xafvsizlikni himoya qilishga kuzatilayotgan harakatlar qilinishi kerak. Rejalashtirish va tayyorlanayotgan mashqlar qayta ko'rib chiqilishi va qayta tekshirilishi yetarli mabnalar mavjudligiga binoan tekshirilishi kerak (inson resurslari, asbob-uskunalar va texnik bilimlar, shular jumlasidandir). Axborot xavfsizligi hodisasini ko'chirishda bir nechta amallar mavjud:

Rejalashtirish va tayyorlash, falokat, xavfsizlik xodisasiga javobgarlikdan iborat:



Rasm. Xavfsizlik Hodisasini Ko'chirish Aylanishi

Quyidagi bo’limlarda xavfsizlik hodisasining ko’chirilishini aylanishining 3 ta jarayonlari mavjud:

Xavfsizlik hodisasini ko’chirishning muhimligidagi takliflar

Yaxshi aniqlangan xavfsizlik hodisasini ko’chirish rejasi bu xavfsizlik hodisasining, ta’sirni kamaytirish va zararning va kompyuter tizimining tez yig’uvchi operatsiyalarining samarali va foydali ko’chirishda muhim bo’lib hisoblanadi.

Quyida xavfsizlik voqeasining asosiy vazifalaridan foydalanish:

a. Zarur resurslar, jumladan, voqealar bilan shug'ullanish uchun mavjud ekanligiga ishonch hosil qilish, kadrlar, texnologiyalar va boshqalar

b. Barcha mas'ul tomonlar vazifalar haqida aniq tushunchaga ega bo'lishi lozim, ular kuzatilayotgan qayta aniqlangan jarayonlar tomonidan hodisa davomida ko’rsatilishi kerak

c. javobgar tizimli va samarali ekanligini ta'minlash va xavf tizimi uchun tezkor tiklash borligiga ishonch hosil qilish.

d. javob faoliyati e'tirof etilgan va muvofiqlashtirilganligiga ishonch hosil qilish.

e. axborot kamchiligi, korrupsiya va tizimni yo’qolishi jihatida hodisaning bo’lishi mumkin bo’lgan ta’sini kamaytirish

axborot oqish jihatidan voqea ta'sirini kamaytirishi mumkin va hokazo korruptsiya va tizim buzilish

f. B / DS ichida voqeaga javoban tajribani ulashish.

g.qo’shimcha hujumlar va zararni oldini olish.

h. tegishli huquqiy masalalari bilan shug'ullanish.

Hukumatda axborot texnologiyalarini jadal rivojlantirish uchun, xavfsizlik hodisa tashish rejasi barcha B/D larda muhim bo’lib hisoblanadi, ayniqsa, kuzatilayotgan axborot tizimlari quyidagilar bo’lsa:

a. Tashqi bog’lanish bilan tizimlar, masalan, Internet.

b. Nozik ma'lumot va axborot ishlash tizimlari.

c. Muhim vazifa tizimlari.

d. Boshqa tizimlar qaysiki xavfsizlik agar voqea sodir bo'lganda juda noqulay ta'siri lozim bo'ladi.

Xulosa qilib aytganda Hukumatda axborot texnologiyalarini jadal rivojlantirish uchun, xavfsizlik hodisa tashish rejasi barcha B/D larda muhim bo’lib hisoblanadi.

ВОЗМОЖНОСТИ RFID ТЕХНОЛОГИИ

С.Г. Кудратов (ТУИТ, доцент)
И.А. Холбоев (ТУИТ, студент)

Технология RFID может эффективно улучшить самообслуживание персоналов и управление ресурсами библиотеки, что соответственно приводит к улучшению удобства для пользователей библиотеки.

Радиочастотная идентификация (RFID) представляет собой автоматический метод идентификации, который может хранить и удаленно получать данные с помощью устройств, называемых RFID-метки. Технология требует сотрудничества читателя RFID и RFID-метки. RFID-основанные LMS (Library Management System) облегчает быструю выдачу, переоформление и возвращение книг с помощью RFID-модулей включена. Он непосредственно предоставляет информацию о книге и пользователе библиотеки в системе управления библиотекой в и не требует ручного ввода. Эта технология медленно начали заменить традиционные штрих-коды на библиотечных делах, и имеет свои преимущества, так и недостатки по сравнению с существующими штрих-коды. RFID тег может содержать идентификационную информацию, например, название или код, который предоставляет книги, без того, чтобы быть указал на отдельную базу данных. Информация считывается с помощью считывателя RFID, который заменяет стандартный

считыватель штрих-кодов обычно встречаются при хождении регистрации библиотеки. За что самое пристальное внимание было принято, чтобы удалить вручную бухгалтерский учет записей, сократить затраты времени в пределах прямой видимости и ручного взаимодействия не нужны для чтения RFID-тегов и повысить эффективность использования ресурсов, как людских ресурсов, инфраструктуры и т.д. Существуют много причин, чтобы использовать технологию RFID в последние годы. Исследования и разработки в этой области сделало эту технологию передовой, которая будет использоваться в управлении цепочками поставок, управление посещаемости, управление библиотекой, автоматизированный сбор платных и т.д.

Есть несколько стандартов RFID, которые используются в промышленности. Существование этих многочисленных стандартов помогает пользователям этой технологии, чтобы сделать выбор между различными стандартами и выбрать подход, который наилучшим образом подходит им, а затем реализовать его для связи между считывателем (RFID-считыватель) и RFID-меткой. В более конкретных терминах, относящихся к RFID библиотеки, RFID в библиотеках была впервые разработана и предложена в мире в конце 1990-х годов. RFID-технологии, направленные на повышение общего рабочего процесса в библиотеке по максимуму, насколько это возможно и сделать все, как книга выдачи, так и заказ и возвращение книг в автоматическом режиме. Сингапур была первой страной, которая ввела RFID технологию в библиотеках. Университет Рокфеллера в Нью-Йорке была первой академической библиотекой в США, которая использовала эту технологию. Фармингтон Community Library был первым государственным учреждением, использующий технологию RFID. Рокфеллер Университет и Фармингтон Community Library начали использовать RFID в конце 90-х годов. В Европе первой публичной библиотекой, использовавшей RFID технологию является Hoogezand-Sappemeer в Нидерландах в 2001 году. Исследование показало, что более 70% людей использует продукты, адаптированные к технологии RFID. В целом, RFID-технология используется больше всего в Соединенных Штатах, а затем в Великобритании и в Японии. Но есть проблема, что эта технология все еще дорого в условиях современного рынка для небольших организаций, по сравнению с более крупными организациями. Концепция RFID можно рассматривать в качестве дополнения к электронным штрих-кодом, который может быть использован для идентификации и отслеживания в ежедневном обслуживании библиотеки. Эта система, состоит из смарт-тегов RFID, что обеспечивает библиотеку с более эффективным способом управления своими коллекциями, обеспечивая при этом большую обслуживания клиентов для своих пользователей. Технология работает на малых и тонких тегов, что позволяет ему быть размещены на внутренней стороне обложки каждой книги в библиотечной коллекции. Тег состоит из антенны и крошечного чипа, который хранит небольшое количество данных для идентификации каждого элемента. Эти теги применяются непосредственно на библиотечных книгах и могут быть прочитаны с помощью RFID Reader. Линия прямой видимости не является обязательным для чтения тегов с читателем, поэтому процесс требует гораздо меньше человеческого участия. Серверное программное обеспечение интегрируется с аппаратным обеспечением для бесшовного функционирования бухгалтерского учета. Информация, содержащаяся на микрочипах, прикрепленных к библиотечным материалам для чтения, не зависит от ориентации или выравнивания элемента. Она обеспечивает связь беспроводной передачи данных, без необходимости прямой видимости. В дополнение к меткам, система RFID требует средства для чтения, чтобы получить сохраненные данные, а затем некоторые средства передается этой меткой данных в библиотечной информационной системы. RFID-метка принимает по радио запрос от читателя и ответить посредством передачи их уникального идентификационного кода. Когда данные, хранящиеся в микросхеме передается читателю, читатель сохраняет эти данные в файле журнала. Радиочастотная идентификация (RFID) системы может быть использована в библиотеках для идентификации книг, для самостоятельного оформления

заказа, для управления запасами, а также для сортировки и транспортировки библиотечных книг. Эти приложения могут привести к значительной экономии затрат рабочей силы, повысить качество обслуживания клиентов, к предотвращению кражи книг и обеспечить постоянное обновление записи новых коллекций книг.

В заключении отметим, что RFID технология является одной из самых быстрорастущих и наиболее выгодных технологий, принимаемых сегодня в народном хозяйстве. Но, очевидно, использование RFID технологии в информационно-библиотечных учреждениях приносит хорошие результаты. Применение RFID технологии в средних и крупных библиотеках даёт эффективность при самообслуживании пользователей, значительно улучшает рабочее время персонала. Сэкономленное рабочее время персоналов может быть использовано в других целях, что приводит к повышению производительности библиотеки.

ОБ ОДНОМ ПОДХОДЕ НАПИСАНИЯ БЕЗОПАСНЫХ ВЕБ-ПРИЛОЖЕНИЙ

Самаров Х.К. (ТУИТ, доцент)

Среди задач, решаемых современными PHP - фреймворками можно выделить организацию удобной среды разработки, использующие проверенные временем паттерны программирования, набора надежных инструментов для решения типовых задач веб-приложений, уменьшение времени написания безопасного кода, введение правил безопасной разработки.

Стандартная, используемые к установке сборок фреймворков «из коробки» обеспечивают защиту от большинства угроз, актуальных для веба на сегодняшний день. В данной статье приводится обзор основных механизмов, делающих разработку на Symfony2 безопасной.

Преобразование используемых языком разметки спецсимволов в безопасные эквивалентные конструкции защищающих от XSS-атак.
Использование XSS-атаки позволяет злоумышленнику возможность эксплуатировать вредоносный код на стороне.

Помимо того, что базовое решение опять сопряжено с высокими издержками на написание дополнительного кода, оно оставляет разработчику большой простор для ошибки при формировании самой фразы запроса. В определенных ситуациях неправильно организованный код может породить валидные, но нежелательные запросы, которые нарушат целостность или доступность информации.

Для работы с базой данных Symfony2 использует сторонний проект Doctrine.
Главная компонента, Doctrine DBAL (Database Abstraction Layer), дает возможность быстро и удобно подставлять экранированные данные в тело запроса.

Такой подход исключает появление в запросе неожиданных конструкций. В случае нарушения каких-либо структурных правил построения запроса библиотека выдает ошибку на уровне PHP, а не на уровне синтаксического анализатора SQL. Это изолирует данные от ошибочных запросов.

В стандартную сборку Symfony2 также интегрирована библиотека Doctrine ORM, которая позволяет работать не с самим SQL-запросом или его конструктором, а непосредственно с PHP-объектами. Классы моделей размечаются определенным образом (например, при помощи аннотаций в phpDoc), в результате чего свойства объектов проецируются на колонки таблиц в базе данных (БД). Взаимодействие между объектом и строкой в БД (создание, редактирование, удаление) происходит автоматически через отлаженные механизмы, что помимо повышения скорости разработки сводит к минимуму возможность ошибки.

Неотъемлемой частью веб-приложения являются формы. Существует множество подходов к проверке входящих данных. Все они используют простые функции вроде

in_array, is_numeric, filter_var, preg_match для проверок на тип или соответствие шаблону. Главная сложность состоит в выработке цельного универсального подхода к валидации форм, который будет игнорировать лишние параметры, максимально контролировать нужные и возвращать после обработки чистые безопасные данные или ошибку. Валидация в Symfony2 глубоко интегрирована в сам механизм конструирования форм. Например, при объявлении поля типа выпадающий список (или группы радиокнопок) обязательным является указание списка опций. Получив заполненную форму, фреймворк автоматически проверяет данные на соответствие предлагавшимся опциям.

В Symfony2 по умолчанию включена защита от CSRF-атак. Во все формы автоматически добавляется CSRF token, уникальный для каждого пользователя. При получении ответа, фреймворк первым делом сверяет полученный токен с токеном из сессии.

Symfony2 делает акцент на разделении двух ключевых в безопасности понятий – аутентификации и авторизации.

Из вышесказанного следует, что в предусматривающей аутентификацию части приложения любой запрос должен быть аутентифицирован. Для этого по умолчанию всем пользователем ставится, например, метка аноним, которая временно является их идентификатором в системе. Фреймворк использует мандатный принцип контроля доступа. Каждый пользователь имеет своё место в иерархии ролей; для каждого ресурса можно указать, какие роли имеют к нему доступ.

Безусловно, Symfony2 позволяет модифицировать и расширять оба механизма в разных его частях. Например, можно организовать несколько независимых или связанных защищенных зон, реализовать неограниченное количество провайдеров пользователей (имплементировав соответствующие интерфейсы), использовать различные способы аутентификации. Отдельное внимание в фреймворке уделяется криптографии. Через конфигурацию для класса пользователя можно определить любой тип шифрования пароля:

Инструменты фреймворка Symfony2, позволяют решить главные вопросы безопасности веб-приложения. Стандартная сборка фреймворка предусматривает защиту от XSS- и CSRF-атак, SQL-инъекций, включает инструменты быстрой и понятной валидации форм, механизмы аутентификации и авторизации. Важно понимать, что помимо реализации самих механизмов, немалое значение имеет общая архитектура фреймворка, которая обязывает разработчика следовать определенным канонам проектирования.

АХБОРОТ ХАФСИЗЛИГИ ИНЦИДЕНТЛАРИГА ЖАВОБ ҚАЙТАРИШ ПРОЦЕДУРАСИНИНГ ҲАЁТ ДАВРИ

С.Ю. Юсупов (ТАТУ, доцент)
А.А. Ганиев (ТДТУ, ассистент)

Ахборот хавфсизлиги инцидентларига жавоб қайтариш процедураси бир нечта босқичлардан таркиб топган. Ходимларни ўқитишдан бошлаб махсус қурилмалар ва ҳодисалардан чиқиб кетишгача бўлган вақтни ўз ичига олади. Ташкилот бундай ҳодисаларга тайёргарлик қилиш вақтида ҳар доим кутилмаган ҳодисалар сонини камайтиришга интилади.

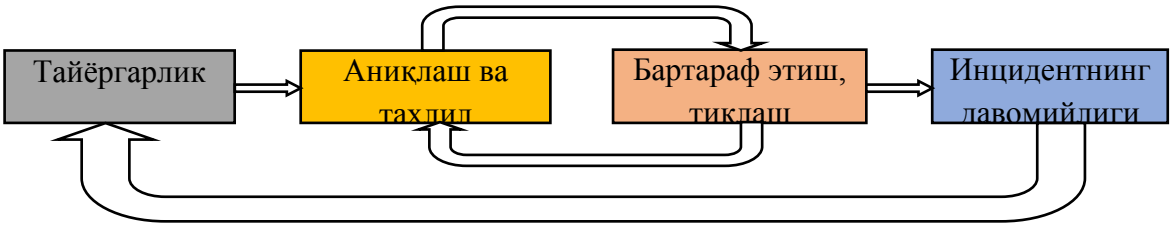
Ташкилотлар бундай вазиятларда ахборот хавфсизлигини бошқаришни қўллашади, бу эса ўз навбатида кутилмаган ҳодисаларни ўрганишини соддалаштиради.

Ахборот хавфсизлигини таминловчи механизмларни ишга тушириш ва ташкил қилиш анча катта меҳнатни талаб қилади ва алоҳида хизмат кўрсатиш керак бўлади. Инцидентларга жавоб қайтариш қуйидаги даражаларни ўз ичига олади:

– тайёргарлик;

– аниқлаш ва таҳлил;
– бартараф қилиш/қайта тиклаш;
– инцидентларнинг давомийлигини.

Инцидентларга жавоб қайтаришни ҳаёт даври қуйидаги расмда келтирилган.



Расм. Инцидентларга жавоб қайтаришни ҳаёт даври

1. Тайёргарлик.

Инцидентларга қарши ҳар ҳил усуллар ёрдами тайёргарлик кўриш, бу фақатгина инцидентларга тайёр туриш эмас, шу билан бирга уларни олдини олиш ахборот хавфсизлигини яхшилаш ҳам саналади.

2. Аниқлаш ва таҳлил.

Ҳужум йўналишлари бу шундай тушунчаки унинг ичида ҳужум қилиниши мумкин бўлган умумий усуллар келтирилади, булар:

1. Ташқи хотира қурилмалари.
2. Тизим унумдорлигини пасайиши.
3. Web дастурлар.
4. Электрон почта.
5. Рухсатсиз фойдаланиш.
6. Қурилмалар йўқолиши ёки ўғирланиши.

Инцидентларни ҳужжатлаштириш. Инцидентни ҳужжатлаштиришда қуйидагиларни ҳисобга олиш зарур ҳисобланади:

– инцидентларнинг жорий ҳолати;
– инцидентлар ҳақида қисқача маълумот;
– инцидентларни қайта ишлашда қатнашаётган ходимлар;
– зарарни баҳолаш;
– тергов жараёнида аниқланган далиллар рўйхати.

Инцидент аломатлари. Инцидент аломатлари икки турга бўлинади: бўлиши мумкин инцидентлар ва индикаторлар. Бўлиши мумкин бўлган инцидентлар келажакда бўлиш эхтимоли бор инцидентлардир. Индикатор эса инцидент бўлиб ўтгани ёки ҳозирда бўлаётганини англатади.

3. Бартараф этиш ва тиклаш.

Ҳар қандай далил учун маълумотларни сақлаш керак ва улар қуйидагиларни ўз ичига олиши зарур:

– идентификацияланадиган маълумот (масалан IP-адрес , MAC адрес ва бошқалар);
– инцидент билан ишлаган ҳар бир одамнинг Ф.И.О., лавозими ва телефон номери;
– вақт;
– сақлаш жойи.

Ҳужум қилувчининг идентификацияси. Ҳужум қилаётган шахсни аниқлаш учун қилинадиган амаллар қуйидагилардир:

– қидирув тизимлари орқали ҳужум қилаётган шахсни қидириш;
– ички ёки ташқи маълумотлар базасидан фойдаланиш;
– ҳужум қилиниши мумкин бўлган каналлар мониторинги.

Ҳужумларни бартараф этиш ёки қайта тиклаш. Инцидентларни аниқлаб уни тўхтатишга эришилгандан кейин у етказган зарарни қайта тиклашга тўғри келади. Қайта

тиклаш ҳолати маълум дастур ёки ОТ туридан келиб чиққан ҳолда ҳар хил бўлиши мумкин.

4. Инцидентнингдавомийлиги.

Инцидент асосида тўпланган маълумотларни қайта ишланиши.

Ўлчаш лозим бўлган бирликлар:

- қайта ишланган инцидентлар;
- ҳар бир инцидент учун йўқотилган вақт бирлиги;
- ҳар бир инцидентни қайта ишлаш унумдорлиги;
- ҳар бир инцидентни субъектли баҳоланиши.

Таҳлил натижасидан шуни таъкидлаш мумкинки, инцидентларга жавоб қайтариш процедурасининг ҳаёт даври тармоқ ва тизимга бўладиган хавф-хатарларни бартараф этишга ёрдам беради, ҳамда инцидентлар ҳақида маълумот тўплаб кейинги бўлиши мумкин бўлган инцидентларни қисман камайтиришга замин яратиб беради.

A BIOMETRIC APPROACH TO LINUX LOGIN ACCESS CONTROL

U.R.Mardiyev (TUIT, assistant)

Login access control refers to securing the entry point to a computing system. The login system is responsible for this service and must provide a number of tasks, the main task being that of user authentication. This research focused on overcoming the vulnerabilities of password verification, which has been identified as the greatest gap in computer security, through the development of a biometric (facial recognition) login system.

In any “secured” computing system, the login procedure is the only port of entry, hence login access control plays a crucial role in its security. The login system is responsible for this assurance and must provide a number of tasks, the main task being that of user authentication. Biometric signatures are essentially unique and difficult to forge, thereby presenting a rational alternative to password systems. The main contribution of this paper is to change the authentication system for Linux operating system and use two basic face recognition techniques to verify its effectiveness. More advanced authentication techniques can be embedded into this system easily. Authentication management involves the validation of a user to the system, through biometric techniques. Session management provides the mechanisms for assigning authenticated users’ privileges on the system, initializing the users X11-windowing session and assigning additional constraints on the user, such as when, and for how long certain users can login to the system.

Figure 1 shows a generalization of the defined architecture of the implemented login system (grey shaded box) and how it was deployed into the current Linux architecture.

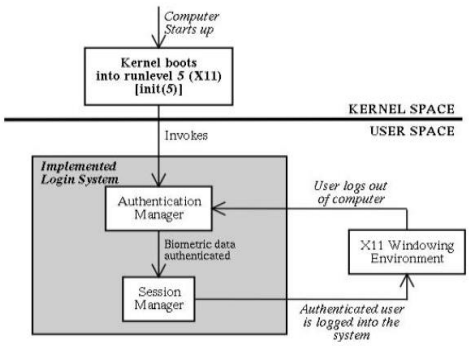


Fig. 1. The Login System Architecture

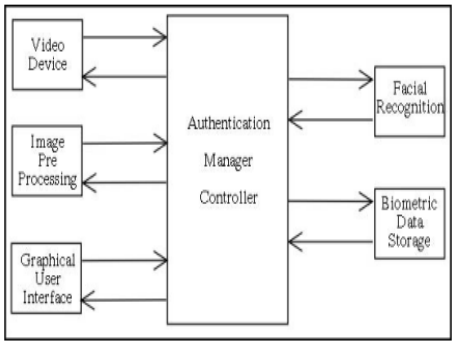


Fig.2. Developed Components of the Authentication Manager

When the computer starts up, the Linux kernel begins its boot sequence, where the

essence of its work is to abstract the underlying hardware from the software and provide an environment in which application software can run. The implemented login system then waits for a valid user to present their biometric data. The authentication manager implemented in the developed login system is made up of the components shown in *Figure 2*, where all components, except the video device, were designed and implemented from scratch. The authentication manager controller is the authentication managers main thread of execution and is responsible for issuing the tasks between the various components that make up the authentication manager. The implementation methodology outlined in this paper is specific to the current facial recognition system, however during all stages of development emphasis was placed on easy configuration of the system for various other biometric techniques, once the relevant drivers become available.

The algorithm describes an abstract view of the control-flow and interaction between the various components that make up the implemented authentication manager. Once the system has established a users identity it then passes control of the system to the session manager.

The session manager implemented in the login system provides the functionality necessary to allow the authenticated user access to the system's resources. Once called, the session manager creates a new control process with access restricted according to the user's privileges on the system. This newly created process is configured according to the users preferences with numerous environment variables being set as well.

Algorithm 1 controller main loop

1: **loop**
2: **if** capture image event occurs **then**
3: signal video device component to grab current video frame.
4: **end if**
5: **if** new RGB image captured event occurs **then**
6: signal *GUI* component to draw image to screen.
7: signal image pre-processing component to convert captured image.
8: end if
9: **if** new 255 grey image event occurs **then**
10: signal facial *recognition component* to identify image.
11: **end if**
12: **if** biometrc data matched event occurs **then**
13: signal *video device component* to terminate.
14: signal *GUI component* to terminate.
15: signal *facial recognition component* to terminate.
16: close down authentication manager and pass system control to the **session manager**.
17: **end if**
18: **if** login process timed out event occurs **then**
19: signal *video device component* to terminate.
20: signal *GUI* component to terminate.
21: signal *facial recognition component* to terminate.
22: notify the user that login attempt failed.
23: restart authentication manager and await a new login attempt.
24: **end if**
25: **end loop**

The implemented session manager awaits a signal from the desktop environment that the user wishes to log out. On this request, the session manager removes all access rights assigned to the user and passes control back to the authentication manager. This research developed a complete prototype login system for Linux that provided authentication services through biometric techniques. Considerable research was required to identify how biometrics could be integrated into an application capable of providing authentication services, and how this application was to be deployed into the Linux operating system.

Preliminary investigations identified a suitable biometric technique for which authentication could be achieved. Due to the limited hardware support currently available for Linux, facial recognition was the only suitable biometric technique for which hardware

supported was identified. Analysis into alternative facial recognition algorithms identified the Eigen face approach as the most suitable candidate for providing user authentication in the login system, primarily as it was able to handle the system's environment (in which images were captured) and requirements better than the other algorithms.

In conclusion, it should be noted, that developed login system is complete and functional within a Linux environment and currently implements Eigen-faces facial recognition for user authentication with promising results. Current results suggest the login system is perfect with both precision and recall rates of 100%. However, the precision and recall rates are unlikely to always be 100%, especially as the number of users enrolled in the system grows.

ПРИМЕНЕНИЕ WIRESHARK ДЛЯ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ СЕТЕВЫХ АТАК

Р.Р. Ибрагимов (ТУИТ, студент)

Методы обнаружения сетевых атак по способам выявления атак подразделяются на методы обнаружения злоупотреблений и методы обнаружения аномалий. Методы обнаружения злоупотреблений опираются на знания об особенностях проведения тех или иных атак, записанных в виде сигнатур, сценариев или последовательности переходов между состояниями системы. Методы обнаружения аномалий базируются на характеристиках поведения системы, которые могут оцениваться по собранной статистике – среднеквадратическое отклонение, пороговый анализ, анализ временных рядов или анализ распределений интенсивности передачи/приема пакетов. Развивающейся областью в вопросе обнаружения сетевых атак является применение методов машинного обучения и методов вычислительного интеллекта.

Основное преимущество методов обнаружения злоупотреблений заключается в том, что обнаружение известных образцов аномальных событий осуществляется максимально эффективно. Недостатком методов на основе знаний является невозможность обнаружить вредоносное воздействие при отсутствии данных о конкретной модификации вредоносной деятельности. Методы обнаружения аномалий, в перспективе, должны справляться не только с уже существующими типами сетевых атак и их разновидностями, но и атаками «нулевого дня».

Одним из способов совершенствования систем обнаружения и предотвращения вторжений является анализ образцов трафика различных сетевых атак, с целью выделения наиболее характерных черт для каждой атаки. По результатам проведённого анализа создаются или уточняются сигнатуры атак, переоцениваются пороговые значения для детекторов аномалий. Наряду с публикациями списков известных эксплоитов и уязвимостей существуют также базы данных образцов трафика сетевых атак. Для работы с образцами трафика применяются программы-анализаторы трафика, одной из таких программ является Wireshark.

Основной возможностью Wireshark является перехват пакетов со всех подключенных сетевых интерфейсов и отображение их содержимого в детальном виде. Wireshark поддерживает работу с сетями на основе технологий Ethernet, FDDI, PPP, Token-Ring и ряда других, широкий набор протоколов, включающий в себя TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG, в общей сложности 2157 протоколов (версия Wireshark 2.2.4). Перехваченные пакеты могут сохраняться в большом количестве форматов других пакетных анализаторов, таких как: libpcap, tcpdump, Sun snoop, atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer, Microsoft Network Monitor, AIX's iptrace. Каждый захваченный пакет может быть подробно рассмотрен по полям заголовков данных – флаги, проверочные суммы, приоритет, адреса получателей и отправителей, MAC адреса задействованных интерфейсов. Wireshark позволяет фильтровать трафик

протоколов канального, сетевого, транспортного и прикладного уровней по множеству критериев. Фильтрация подразделяется на два вида – времени захвата пакетов и времени отображения пакетов. Фильтры позволяют обнаруживать пакеты с некорректной проверочной суммой, больше установленной максимальной или нулевой длины, перекрытие областей данных при приемё за счёт отрицательного смещения и другие, ошибочные или неправильно сформированные пакеты. Так как значительная часть данных в сети Интернет передается с использованием протокола TCP, предусмотрены фильтры для обнаружения сегментов TCP, содержащих ошибочные данные - Spurious Retransmission (случайная повторная отправка TCP сегмента), сегменты с несколькими поднятыми флагами, пропуск ожидаемого сегмента, сегменты с флагом ACK ненулевой длины или дубликаты, содержащие уже полученный флаг ACK. Количество одновременно применяемых фильтров не ограничено, возможно использовать комбинации, необходимые для обнаружения тех или иных событий, используются операторы сравнения, поиск или соответствие подстроке. Также, для каждого конкретного фильтра и события может быть предусмотрена собственная цветовая схема, позволяющая легче отделять редкие события от часто встречающихся событий и классифицировать их по степени серьезности. Для наглядного отображения накопленной статистики Wireshark предоставляет средства для построения графиков интенсивности трафика различных протоколов с высокой детализацией по времени, что позволяет выделять периоды возникновения и спада сетевой активности, возможно соответствующие сетевой атаке – например, начинающиеся атаки класса DoS/DDoS. Немаловажным для предотвращения дальнейших атак является выявление задействованных в атаке хостов, для этого в Wireshark есть возможность отследить пути входящих и исходящих пакетов. Например, сеансы связи по протоколу DHCP или DNS, которые ведутся с соответствующими серверами, соединения по протоколам SSL и TLS 1.2, использующие шифрование для защиты данных, передача данных по протоколам TCP и UDP – каждый из потоков данных отражается подробно от начала и до конца.

Таким образом, при помощи Wireshark возможно собрать статистические данные по интенсивности трафика различных протоколов, отобразить их в графической форме, отфильтровать по протоколам, по IP-адресам участвующих в сеансе обмена данными хостов, выделить нестандартные или содержащие ошибки пакеты. Собранные данные можно использовать при формировании конфигурации для IDS/IPS.

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ НА КОМПЬЮТЕРАХ И НОУТБУКАХ

О.В. Порубай (ФФ ТУИТ, старший преподаватель)

На сегодняшний день одной из самых опасных угроз является несанкционированный доступ к информации, а также кража носителей информации. В результате комбинации этих двух угроз, убытки могут возрасти в несколько раз. Следовательно, помимо защиты конфиденциальной информации от несанкционированного доступа необходимо оберегать и сам физический носитель. Но при этом надо учитывать то, чтобы система безопасности не доставляла пользователю трудностей при работе с персональным компьютером.

Уже много лет, самым эффективным средством защиты конфиденциальной информации, является шифрование данных. При условии сохранности криптографических ключей, шифрование гарантирует безопасность данных.

Пригодность различных подходов к шифрованию данных

Для защиты информации от несанкционированного доступа, применяются технологии шифрования.

Пофайловое шифрование (Рис.1). Пользователь сам выбирает файлы, которые следует зашифровать.

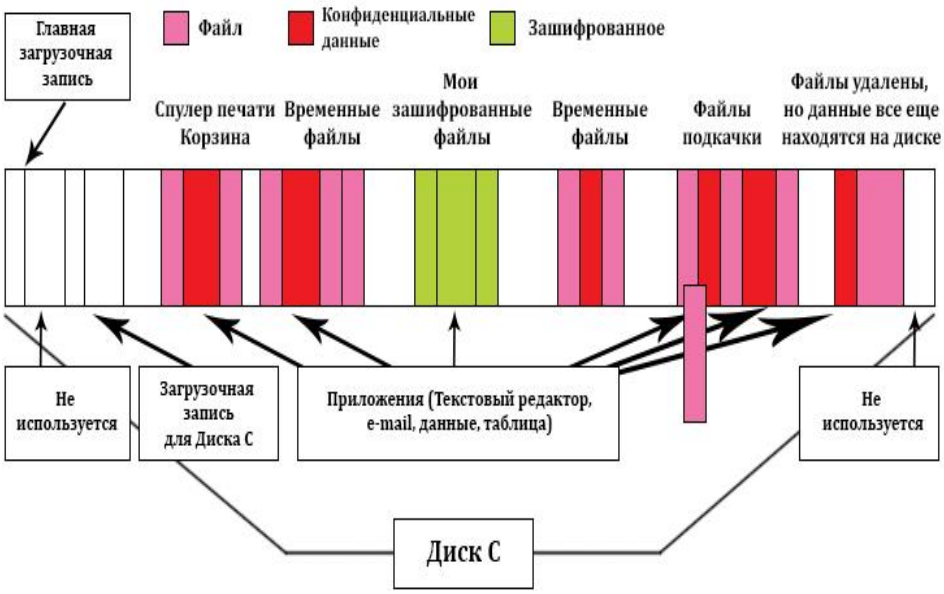


Рис.1. Пофайловое шифрование

Чаще всего данный метод используется в тех случаях, когда нужно послать зашифрованные файлы средствами сети Интернет. В этом случае пользователь шифрует определенный файл, который необходимо защитить. Минус данного подхода в том, что он ограничен низкой скоростью работы, в особенности, когда нужно отправить информацию больших объемов. Еще одной проблемой является то, что шифруется лишь файл-оригинал, а временные файлы и файл подкачки остаются полностью незащищенными, поэтому защита обеспечивается только от злоумышленника, пытающегося перехватить сообщение в Интернете, но не против преступника, укравшего ноутбук или КПК.

Шифрование каталогов. Данный метод не сильно отличается от предыдущего, т.к. в основе шифрования папок лежит пофайловое шифрование, отличие в том, что данный подход позволяет переносить файлы в папку, где они будут зашифрованы автоматически. Оба метода не обеспечивают надежной защиты временных файлов, файлов подкачки, не удаляют физически данные с диска и т. д. Для шифрования каталога процессору требуется время для постоянного шифрования/дешифрования файлов, что делает этот процесс очень ресурсоемким и медленным.

Шифрование виртуальных дисков (Рис.2). Данный подход подразумевает создание скрытого файла большого размера, находящегося на жестком диске. Операционная система «видит» его как новый логический диск, вся информация, хранящаяся на диске, является зашифрованной. Здесь данные шифруются автоматически сразу, когда они записываются на виртуальный диск или считываются с него.

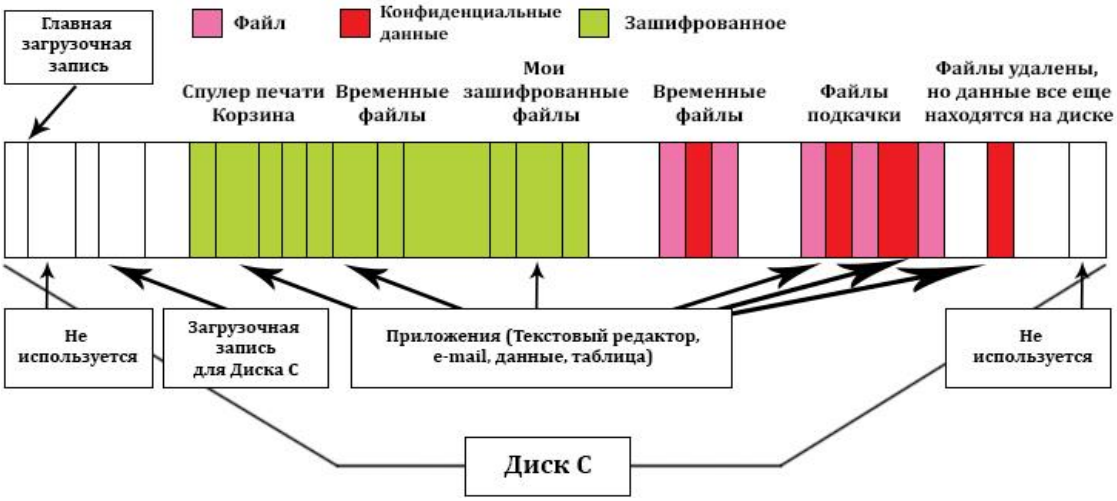


Рис.2. Шифрование папок и виртуальных дисков

Концепция виртуальных дисков имеет как плюсы, так и минусы. Например, зашифрованный виртуальный диск защищает имена файлов, размещенные в виртуальных файловых таблицах. Однако этот виртуальный диск не может быть расширен столь же просто, как обыкновенная папка, что очень неудобно, и так же может оставить без защиты временные файлы и файлы подкачки.

Шифрование всего диска (Рис.3). В основе данной концепции лежит посекторное шифрование, шифруется абсолютно все: загрузочный сектор, все системные файлы и любая другая информация на диске. Криптографические программы шифруют данные прежде, чем операционная система поместит их на диск. Для этого криптографическая программа перехватывает все попытки операционной системы записать данные на физический диск и производит операции шифрования на лету. Благодаря такому подходу зашифрованными окажутся еще и временные файлы, файл подкачки и все удаленные файлы.

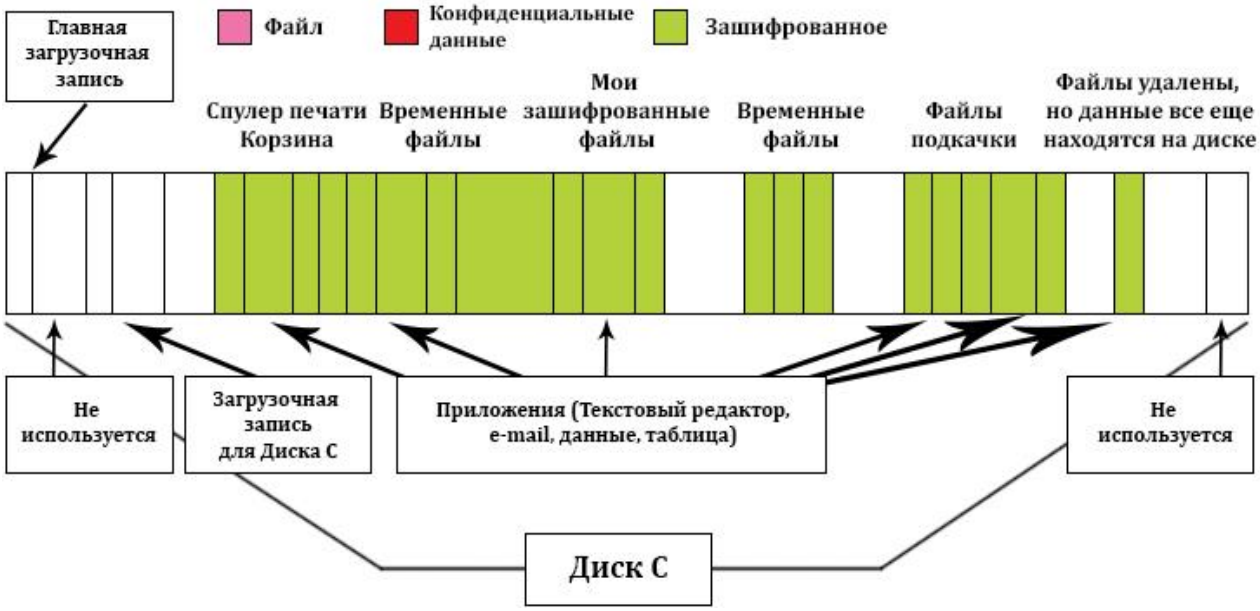


Рис.3. Шифрование всего диска (включая загрузочные записи)

Защита процесса загрузки. Шифрование всего диска подразумевает и защиту процесса загрузки. Операционная система не сможет запуститься если зашифрован весь диск целиком. Чтобы запустить процесс загрузки нужно расшифровать файлы загрузки. Для этого пользователю требуется ввести пароль, чтобы операционная система могла стартовать. После правильно введенного пароля программа шифрования получит доступ к ключам шифрования, что позволит читать дальнейшие данные с диска.

Шифрование с использованием сильной аутентификации

Для еще более надежного сохранения данных требуются не только криптографические технологии, но и средства, которые предоставляют персональный доступ. В этом нам смогут помочь ключи ЭЦП, основанные на строгой двухфакторной аутентификации. Чтобы успешно пройти процедуру сильной аутентификации, пользователю необходимо предъявить операционной системе ключ ЭЦП (находящийся на USB-флеш-накопителе), а потом доказать свое право владения этим электронным ключом (ввести пароль).

Таким образом, задача злоумышленника, пытающегося получить доступ к чувствительным данным, сильно осложняется: ему требуется не просто знать пароль, но и иметь физический носитель, которым обладают лишь легальные пользователи.

РАСПРОСТРАНЕНИЕ DDOS-АТАК ПОСРЕДСТВОМ БОТ-СЕТЕЙ

О.В. Порубай (ФФ ТУИТ, старший преподаватель)

Одним из самых распространенных инструментов для совершения преступлений в киберпространстве на сегодняшний день, являются Бот-сети, которые в основном используется для передачи огромного количества спама.

Ботнет или бот-сеть представляет из себя совокупность компьютеров, зараженных вредоносными программами - ботами, с помощью которых можно удаленно управлять ничего подозревающими пользователями.

Бот-сеть, может включать в себя более ста тысяч инфицированных машин, и может быть использована как средство для проведения DDoS-атаки. В результате такой атаки сервер может полностью отключается из-за перегрузки. Это открывает путь для преступлений с материальным мотивом.

В настоящее время самыми крупными являются бот-сети: Storm, Rustock, Sribi, Kraken, Mega-D и Bobax.

DDoS-атаки (от англ. *Distributed Denial of Service, распределённый отказ в обслуживании*) в последние несколько лет стали одним из самых распространенных преступлений в киберпространстве. Чаще всего хакеры организуют подобные нападения на серверы бизнес-структур с целью получения прибыли, а так же возможное использование DDoS-атаки в виде шантажа. Бот-сети сейчас являются самой эффективной системой информационной войны. Во-первых, из-за проблем с законодательством и с правовым беспорядком в сети Интернет, бот-сети в ближайшие несколько лет будут основным нелегальным источником дохода в сети. Криминальные структуры уже давно стали частью данного сообщества. Владельцы бот-сетей инвестируют, проводят исследования и разработки направленные в первую очередь на:

- увеличение числа ботов;
- анонимность;
- распределенность;
- стабильность.

Бот-сети уже превратились в сферу бизнеса и развивается, как обычная компания: маркетинг, разработка, безопасность.

Основным источником дохода для владельцев бот-сетей является:

1. Рассылка спама. Бизнес фактически легальный, т.к. явных законов, запрещающих рассылку спама нет.
2. DDOS атаки. Нелегальный, но один из лучших способов ведения информационной войны. Для защиты от DDOS атак компании – тратят огромные деньги, но тем не менее остаются уязвимыми перед серьезной бот-сетью.
3. Подбор паролей для дальнейшего взлома какого-либо сервиса.

Вопрос зарождения бот-сетей носит важный характер. Даже сейчас, многие, кто читают эту статью, ничего не подозревая, являются соучастниками DDOS атаки. Постараюсь расписать все по пунктам:

1. Любое заражение начинается со «спама». Т.е. e-mail приходит письмо с зараженным сайтом. Ничего не подозревающий пользователь, переходит по ссылке и ему на компьютер автоматически загружается вирус.
2. После чего вирус глубоко прячется в компьютере и ждет команды из управляющего центра, который, как правило, находится в отдаленный стране, и засечь владельца практически не возможно.
3. Владелец сети ждет момента, когда заразятся порядка 1000 машин и, зайдя в управляющий центр, дает команду или определенный запрос для вызова большого количества атак, направленных на определенный ресурс. И буквально в течение 10 минут сервер, не справляясь с количеством запросов, начинает виснуть. Существует всего

несколько способов использовать «выращенные» бот-сети, например атака по заказу конкурирующей компании или же просто атака с целью вымогательства.

Основной способ влияния – DDOS атака. При мощной бот-сети практически 100 % результат.

1. Межхакерские войны или anticyber-crimes акции. Атаки на управляющий центр для отражения атаки, попытки завладеть чужими ботами, маркетинговая акция (атакуем чужой управляющий центр, показываем, что чужая сеть не работает – получаем заказ).
2. Банковский сектор, сектор электронных платежей. Атакуется сервер банк-клиента, или коммуникационный сервер системы электронных платежей. Предполагаемые цели – маркетинг. Использование информации для понижения имиджа банка. В случае систем моментальных платежей – клиент просто пользуется системой конкурента.
3. Политический сектор. Средство ведения информационной войны. Интернет как основное средство СМИ. Атакуются сайт политических партий, организаций связанных с религией.
4. Сектор телекоммуникаций – связь/хостинги/провайдеры. Атаки по заказу конкурентов с целью, как и в первом пункте. Атакуются не сайты, а телекоммуникационные узлы.

В заключении хотелось бы написать о том, что нынешние финансовые учреждения недооценивают риски, связанные с бот-сетями. Уже сейчас банки обязаны возмещать ущерб клиентам, со счета которых будут похищены денежные средства. Большинство банков совершенно не готово к угрозам, которые несут бот-сети. Перспективы использования бот-сетей будут привлекать все большее количество участников на этот рынок. В последнее время тенденция такова, что каждые два месяца фиксируется появление новой преступной группы с собственной бот-сетью. Естественно, что таких групп будет все больше, троянские программы будут все совершеннее, а методы и объемы их распространения будут стремится к результатам распространения обычных вредоносных программ.

СПЕЦИАЛЬНАЯ ФИЛЬТРАЦИЯ ТРАФИКА С ИСПОЛЬЗОВАНИЕМ ПЛАТФОРМЫ ФИЛЬТРАЦИИ WINDOWS

М. Салимов (ТУИТ, магистрант)

Одной из угроз, рассматриваемой при создании информационных систем, является несанкционированное воздействие на устройства защиты, в частности атаки на МЭ. Для отражения угроз такого типа в компьютерных сетях применяется режим специальной фильтрации трафика и скрытность функционирования.

Специальная фильтрация подразумевает фильтрацию трафика на нескольких уровнях сетевой модели OSI. Основным элементом специальной фильтрации трафика является фильтрация пакетов. Изначально эта технология использовалась на сетевом уровне, поэтому фильтрация только подвергают воздействию источника и назначения IP-адресу. В настоящее время, анализ сетевого трафика и фильтрации пакетов выполняется на транспортном уровне.

Каждый IP-пакет проверяется на соответствие установленным правилам, в результате чего пакет либо перемещается через сетевой стек для дальнейшей обработки или передачи, либо отклоняется.

Обеспечить такого рода фильтрацию трафика для операционных систем семейства Windows позволяет платформа фильтрации Windows (Windows Filtering Platform или сокращенно WFP).

WFP представляет собой набор API и системных служб, которые предоставляют платформу для создания приложений фильтрации сети. API WFP позволяет разработчикам писать код, взаимодействующий с обработкой пакетов, которая

происходит на нескольких уровнях в сетевом стеке операционной системы. Данные сети могут быть отфильтрованы, а также изменены, прежде чем они достигнут своего назначения. Обеспечивая более простую платформу разработки, WFP призвана заменить предыдущие технологии фильтрации пакетов, таких как Transport Driver Interface (TDI) фильтры, сетевой драйвер интерфейса спецификации (NDIS) фильтры и провайдеров Winsock Layered Service (WLS).

WFP обеспечивает фильтрацию в двух режимах: user (пользовательский режим) и kernel (режим ядра), которые вместе выполняют все операции фильтрации сетевых пакетов или потоков. Структура WFP приведена на рис.

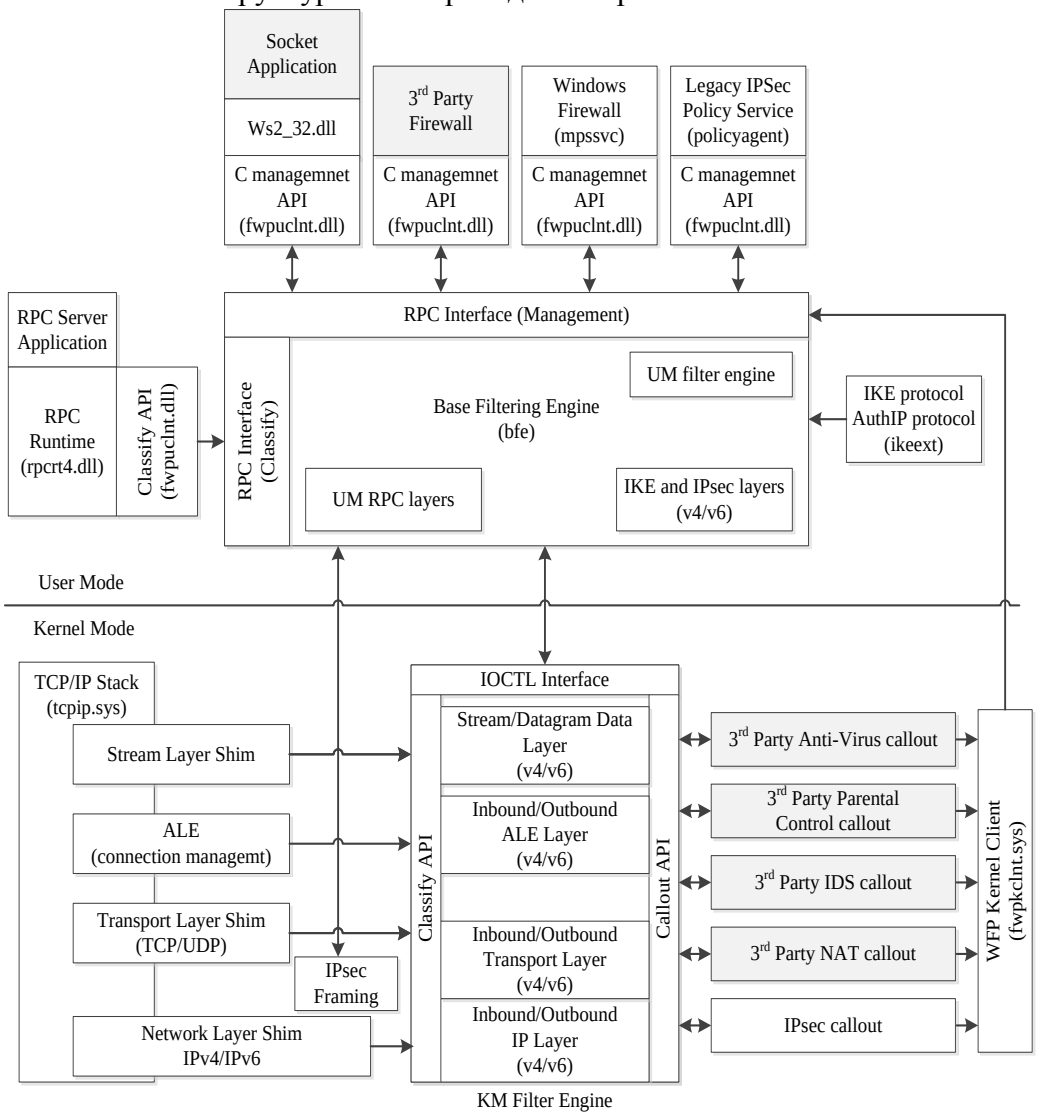


Рис. Структура платформы фильтрации WFP

Механизм фильтрации содержит несколько слоев фильтрации для каждого сетевого уровня в сетевом стеке операционной системы. Разделение слоев фильтра двигателя в пользовательском режиме слоев и режима ядра слоев основан на компоненте фильтра двигателя, который владеет им. Компонент User Mode (пользовательского режима) выполняет RPC и IPsec фильтрацию. Фильтр двигателя содержит приблизительно 10 слоев пользовательского режима фильтрации. Компонент Kernel Mode (режима ядра) выполняет фильтрацию на сетевом и транспортном уровнях стека TCP/IP. Этот компонент также отвечает за обращение на доступные функции выноски в процессе классификации. Фильтр двигателя содержит максимум 50 фильтрующих слоев в режиме ядра.

Базовый механизм фильтрации (BFE) принадлежит к компоненту пользовательского режима и координирует компоненты WFP. Основными операциями,

выполняемыми BFE, являются добавление и удаление фильтров из системы, хранение конфигураций фильтров, и применение политики безопасности WFP.

Связь между приложением и BFE осуществляется с помощью конкретных функций управления WFP. Драйверы выноски (callout драйверы) обеспечивают дополнительные функциональные возможности фильтрации путем добавления функций пользовательских настроек к фильтру двигателя на одном или нескольких из режима ядра фильтрующих слоев. Callout драйверы поддерживает глубокую инспекцию пакетов, а также изменение потока. После того, как callout драйвер добавил свои функции в фильтр двигателя, фильтры, которые определяют функции callout могут быть добавлены в процессе фильтрации.

Таким образом, основу новых технологий и продуктов в сфере фильтрации трафика составляют сервисы, которые позволяют повысить качество фильтрации и степень защищенности не только от существующих угроз, но также предотвратить целый класс новых угроз.

ВЕБ-ИЛОВАЛАР ЗАИФЛИКЛАРИНИ АНИҚЛАШ УСУЛЛАРИНИНГ ТАҲЛИЛИ

Г.С. Рахманова (ТАТУ, катта ўқитувчи)

Бугунги кундаги олиб борган изланишларга кўра веб-иловалардаги заифликларни аниқлашнинг самарали усули веб-иловаларнинг кодларини экспертлик таҳлили (code review) хисобланади. Бу усул қийин ҳисобланиб, юқори малакали экспертларни талаб қилади. Веб-иловаларнинг заифликларини автоматик аниқлаш усулларини иккита асосий гуруҳларга ажратиш мумкин:

– веб-иловаларнинг кодларига мурожатни амалга оширмайдиган веб-иловалар ишини таҳлил қилиш усули;

– веб-иловалар кодларини ва конфигурация созланмаларини таҳлил қилиш усули.

Биринчи гуруҳ усулларида веб-иловаларни ташқи фойдаланувчи, потенциал бузғунчи сифатида кўриб чиқилади. Бу гуруҳга қуйидаги усуллар киради:

– веб-илова ҳақида идентификация маълумотларини олиш;

– суқилиб киришни текшириш усули.

Иккинчи гуруҳ қуйидаги усуллардан иборат:

– веб-илова кодларини статик таҳлил қилиш усули;

– веб-илова кодларини динамик таҳлил қилиш усули.

Суқилиб киришни тестлаш усули. Суқилиб киришни тестлаш (penetration testing) усули веб-иловага ташқи фойдаланувчи, потенциал бузғунчи нуқтаи назаридан қаралади. Бунда бузғунчи веб-илова кодига, созланмаларига кириш хуқуқига эга бўлмаган оддий фойдаланувчи каби имкониятларга эга деб қаралади. Усул ишлаётган веб-иловага бузғунчи ҳаракатларига мос фойдаланувчи фаоллигини эмуляция қилувчи ва хато сўровлар юбориш орқали тестлашни амалга оширишни назарда тутади. Веб-иловани суқилиб киришга тестлаш усули ёрдамида заифликларини қидиришда учта асосий вазифа мавжуд:

– веб-илова структурасини олиш ва ўрганиш;

– веб-илова қурилган структура асосида HTTP-сўровларни яратиш;

– заифликларни аниқлаш учун веб-сервер жавобларини таҳлили асосида тестлашни кучайтириш.

Статик таҳлил усули. Веб-илованинг кодларини статик таҳлил қилиш веб-иловани реал бажарилишини назарда тутмайди. Бунинг ўрнига бошқарув ва маълумотларга боғлиқлик графиклари қурилади ва заифликларни ушбу графикларини таҳлил қилиш орқали аниқланади. Заифликларни аниқлашнинг иккита асосий ёндашуви мавжуд: хавфсизлик турларини таҳлили ва маълумотлар оқимини таҳлили.

Веб-илованинг кодларини статик таҳлил қилиш усули веб-иловаларнинг баъзи хато

киритилувчи маълумотлар билан боғлиқ заифликларини аниқлашга имкон беради. Бу усул бошқа заифликлар синфини аниқлашга имкон бермайди.

Динамик таҳлил усули. Веб-илованинг кодларини динамик таҳлил қилиш кодларни статик таҳлил қилиш усулига ўхшайди, лекин ундан фарқлироқ график қурмасдан веб-илова бажарилиш жараёнидан таҳлил қилинади. Ўтказилган таҳлил асосида веб-иловалар заифликларини автоматик аниқлаш усулларининг имкониятлари қуйидагилардир:

– максимал заифликлар синфини қамраб олиш;

– заифликларни аниқлаш тўлиқлигини назоратлаш, автоматик таҳлил натижасида кўрсатилган синфдаги заифликлар йуқлиги ҳақида кафолат бериш.

Ҳимояланганликни таҳлил қилиш тизими. Ҳимояланганликни таҳлил қилиш тизими веб-порталнинг дастурий-аппаратларидаги заифликларини аниқлаш учун мўлжалланган. Бундай заифликларга мисол қилиб тармоқ портали хизмати конфигурациясини нотўғрилиги, янгиланиш модулисиз ўрнатилган дастурий таъминотлар (service packs, patches, hotfixes)ни келтириш мумкиндир. Ҳимояланганликни таҳлил қилиш тизими натижаларига кўра аниқланган заифликлар ва уларни бартараф қилиш бўйича тавсияномаларни сақловчи ахборотлардан иборат ҳисобот шакллантирилади. Ушбу тизим ёрдамида аниқланган заифликларни ўз вақтида бартараф этилиши мумкин бўлган ҳужумларни бартараф этишга имкон беради.

Криптографик ҳимоялаш тизимлари. Криптографик ҳимоялаш усуллари веб-портал билан масофадаги мулоқотни ҳимоялаш учун мўлжалланган. Тизим ҳимояланган тармоқ яратиш имконини берувчи, VPN (Virtual Private Network) виртуал ҳимояланган тармоқга аосланади, бунда фойдаланувчиларни аутентификацияси амалга оширилади, шунингдек узатилаётган маълумотларни махфийлиги ва бутунлиги таъминланади. Бундай уланишлар махсус криптогарфик протоколлар ёрдамида амалга оширилади. Бу криптографик протоколлар TCP/IP стекининг турли сатхларида ишлайди (жадвал).

Жадвал

TCP/IP стекининг турли сатхларидаги криптографик протоколлар

TCP/IP стекининг сатхлари номи	Криптопротокол номи
Тадбиқий сатхи	SSL (Secure Sockets Layer) / TLS (Transport Layer Security) Secure HTTP
Тармоқ сатхи	IPSec (Internet Protocol Security) SKIP (Secure Key Interchange Protocol)
Канал сатхи	PPTP (Point-to-Point Tunneling Protocol) L2F (Layer 2 Forwarding Protocol) L2TP (Layer 2 Tunneling Protocol)

Таҳлил натижасисидан шуни маълум қилиш мумкинки веб-иловалар заифликларини аниқлаш статик ва динамик усуллари орқали амалга оширилади. Бу усуллар веб технологияларда бўладиган хавф-хатарларни олдиндан аниқлаш ва уларга қарши ҳимоя усулларини ишлаб чиқиш имкониятини беради.

7-Шўъба.

ТЕЛЕКОММУНИКАЦИЯ ТАРМОҚЛАРИ ВА КОММУТАЦИЯ ТИЗИМЛАРИНИНГ РИВОЖЛАНИШ ТАМОЙИЛЛАРИ

OPTIK TOLALI ALOQA LINIYALARINING RIVOJLANISH ISTIQBOLLARI

K.B.Abdurakhmonova (TATU, 2-bosqich talabasi)

Insoniyat taraqqiyotida aloqaning, xususan, optik aloqaning roli katta bo‘lgan, bunga sabab uning tarqalish tezligining juda kattaligidir, (vq3*1010 sm/s) ham to‘g‘ri chiziqli tarqalish va boshqa xususiyatlariga bog‘liq. Masalan, XVIII asrdayoq quyosh nurini qaytaruvchi ko‘zgulardan foydalanish asosida ishlaydigan optik telegraf va murakkab signallarni uzatish qobiliyatiga ega bo‘lgan semoforlar yaratildi. Axborotni masofaga uzatishda yorug‘lik nurining qulayligini sezgan amerikalik telefon ixtirochisi A. Bell bundan 125 yil avval optik telefon (fotofon)ni yaratdi.

U o‘zining qurilmasi yordamida odam ovozini nur orqali 200 metr masofaga uzatdi. Bunda mikrofonning tebranishidan qaytuvchi quyosh nuri ovozni tashuvchi bo‘lib xizmat qildi. Hozirgi kunda deyarli har bir uyda radio, televizor va telefon bor, shaharlar va maydonlar o‘rtasida yotqizilgan kabellar yordamida koinotdan yerning sun’iy yo‘ldoshlari orqali keng miqyosda axborotlar uzatilib turiladi. Ammo aloqa texnikasining rivojlanishi, elektronikaning zamonaviy yutuqlari, elektromagnit to‘lqinlarining sm va mm diapazonining o‘zlashtirilishi ham hozirgi paytda mislsiz ko‘payib ketayotgan axborot talablariga javob bermay qoldi: amaliyot axborotning zichligi, uzatish chastotasining oshirilishi aloqa kanallarini zichlashtirish kabi qator talablarni qo‘ymoqda. Shuning uchun ham dunyo mutaxassislari birinchi navbatda optik diapazonga qayta-qayta e’tibor bera boshladilar. Shuningdek, dunyodagi mis konlari borgan sari kamayib bormoqda. Vaholanki, texnikada juda kerak bo‘lgan bu metallning deyarli yarmi kabellar uchun ishlatiladi. Olimlarning taxmini bo‘yicha mis ishlab chiqarish XXI asrda keskin ravishda kamayadi. Demak, biror chora topilmasa, kabel ishlab chiqarish tushkunlikka uchrashi turgan gap. Shuning uchun ham mis simlardan voz kechib, axborotni shaffof shisha tolalar orqali nur yordamida uzatishga o‘tish lozimligini tushunib yetildi. Demak, shisha tolalarni ishlatish ikki ijobiy yutuqqa — axborot uzatish tezligini keskin oshirib, qimmat hisoblangan misni katta miqdorda iqtisod qilishga imkon beradi. Ta’kidlash lozimki, O‘YuCh -diapazoni (q=1-20sm) bo‘lgan elektromagnit to‘lqinlar mukammal o‘zlashtirilgandan so‘ng navbat optik diapazonga yetib keldi. 60-yillarda kashf etilgan lazerlar ham katta samara bermadi. Chunki axborotni lazer nuri bilan ochiq atmosferada uzatish yaxshi natija bermadi. Bunga sabab atmosferadagi temperatura, havo oqimi, changlar, tuman va h.k. lar tinimsiz o‘zgarib turganligi uchun ochiq havo nur o‘tkazuvchi muhit sifatida ishlatishga yaroqsizligi aniqlandi. Lazer nurini trubalar ichida uzatib ko‘rildi, lekin bu yo‘l ham foyda bermadi. Shuni aytish kerakki, nur o‘tkazuvchi shisha tolalar 60 — yillarda ma’lum edi. Ularning diametri 100 mkm bo‘lib, o‘zak va uni o‘rab olgan qobiqdan iborat edi. O‘zakning sindirish ko‘rsatkichi qobiqning sindirish ko‘rsatkichidan biroz katta bo‘lishi kerak. Lazer nurini shunday tolalar orqali uzatishga urinib ko‘rildi, ammo bunday tolalar juda katta yutish koeffisiyentiga ega bo‘lib, taxminan 1000 db/km ga teng. Bunday tolaga kiritilgan nur bir necha metr masofadan so‘ng deyarli butunlay yutilib ketadi. Ammo 1966 yilda ingliz olimlari Kao va Xokxem o‘zlarining ilmiy izlanishlarida optik shishalardagi nurning yutilish sabablarini taxlil qilib, nurning yutilishiga asosiy sabab He, Ni, Si, Sg va shunga o‘xshash metallar shisha sintez qilinayotganda tashqaridan (havodan, tigeldan) kirib qolgan metall ionlari ekan. Maqola mualliflari agar shishalar ana shu ionlardan tozalansa, yutish koeffisiyenti a<20db/km bo‘lgan tolalar olish mumkinligini isbotlab berdilar. Bu maqoladan so‘ng dunyo miqyosida yutish koeffisiyenti kichik bo‘lgan nur o‘tkazuvchi tolalarni olish bo‘yicha ishlar juda kuchayib ketdi. Nihoyat, 1970 yil "Korning Glass" firmasi mutaxassislari to‘lqin uzunligi qq063 mkm bo‘lgan nur uchun yutish koeffisiyenti 20 db/km dan

kichik bo‘lgan nur uchun nur o‘tkazuvchi tolalarni yaratdilar. Bunday tolalar uzun to‘lqinli optik aloqa liniyalarida ishlatsa bo‘ladigan sifatlarga ega edi. Shuning uchun 1970 yil tolali optikaning tug‘ilgan yili deb sanala boshlandi. Ana shundan so‘ng tolali optika aloqasi misli ko‘rilmagan tezlik bilan rivojlanib ketdi, ular ishlatiladigan sohalar ko‘paya boshladi: telefon tarmoqlari orqali ishlaydigan televideniye, aviatsiya va dengiz flotida, bort aloqasi, hisoblash texnikasi, texnologik jarayonlarni boshqarish va nazorat qilish tizimi va h.k.larda ham ishlatila boshlandi. Bundan tashqari, nurli tolalarning tashqaridan tushuvchi elektromagnit to‘lqinlarning ta'sirini sezmasligi, vaznlari kam va ixchamligi ham aniqlandi. Shunday qilib, optik aloqa tizimlarining negizi shaffof va toza shishadan qilingan tola bo‘lib, u yaxshi xizmat qiladi.

Optika qonunlaridan ma’lumki, tola ichiga kiritilgan nur tashqariga chiqmasdan tarqala oladi. Bunda tola to‘g‘ri chiziq bo‘yicha yo‘nalgan yoki barabanga o‘ralgan bo‘lishi mumkin. Buning sababi nur tola ichida tarqalar ekan, uning chegarasiga tushadi va yana ichkariga to‘la qaytadi. Bu nur tolaning ikkinchi chegarasiga tushadi va yana undan ichkariga to‘la qaytadi va h.k., bu jarayon uzluksiz davom etadi.

Demak, nurning tarqalish sharti uning tola yon chegarasida to‘la ichki qaytishi ekan. Bu juda oddiy va optikada keng qo‘llaniladigan hodisadir. Faraz qilaylik (1-rasm), nur sindirish ko‘rsatkichi p1 va radiusi g bo‘lgan silindr shaklidagi muhitda tarqalayotgan bo‘lsin. Tashqi muhitning sindirish ko‘rsatkichi p2 bo‘lsin. U holda nur ikki muhit chegarasiga tushganda sinadi va qisman qaytadi. Sinish (q2) va tushish (q1) burchaklari Snellius qonuniga bo‘ysinadi: n1Sin a1qn2Sina2 yoki Sin a1qn2/n1 Sin a2 Agar biz tushish burchagini (q1) kattalashtirib borsak, sinish burchagi a2 ham ortib boradi va ikkinchi muhitga singan nur tola chegarasiga qarab ko‘proq egila boshlaydi. q1 burchak ma’lum kritik qiymatga erishganda q2q90° bo‘ladi. Bu holda singan nur tola chegarasi bo‘ylab tarqaladi va ikkinchi muhitga o‘tmaydi, to‘la ichki qaytish sodir bo‘ladi. Bu burchak Sin a1Tqn2/n1 ga teng biladi. Nihoyat tushish burchagi a1 q a1T bo‘lganda tola chegarasiga tushayotgan nur energiyasining deyarli hammasi yana tola ichiga qaytadi.

Shisha tola nur tarqatishga juda qulay muhit bo‘lsa ham, uning kamchiliklari bor. Bu haqida anjuman ishida tu’laqonli ma’lumot berilib tahlil etiladi.

ATMOSFERALI OPTIK ALOQA LINIYASIGA KO‘P KANALLI TIZIMINI QO‘LLASH

K.B.Abdurakhmonova (TATU, 2-bosqich talabasi)
A.M.Eshmuradov (TATU, TI kafedrasi mudiri)

Istiqbolli, shu bilan birga kam tadqiq etilgan, yuqori tezlikdagi raqamli aloqa kanali tashkil etish bu atmosferali optik aloqa liniyasini qo‘llash hisoblanadi. Shu usulda ma’lumotlarni yuqori tezlikda uzatish, shovqinbardoshlikni oshirish va kam vaqt ichida bu tizimni ishga tushirish mumkin. Tizimni qo‘llashda unga to‘siq bo‘ladigan asosiy faktor – aloqa kanali uzunligining cheklanishi. Atmosferali optik aloqa liniyalari (AOAL) stansiyalarining tuzilishi asosan o‘xshash: interfeys moduli, modulyator, lazer, uzatgichning optik tizimi, qabul qilgich optik tizimi, demodulyator va qabul qilgich interfeys modullaridan tashkil topgan bo‘ladi. Foydalanuvchilar qurilmalaridan uzatilayotgan ma’lumotlar oqimi interfeys moduliga kelib tushadi, keyin esa nurlatgichning modulyatoriga beriladi. Modulyatorda signal yuqori samaradorli injeksion lazer orqali yaqin IQ – diapozonli optik nurga o‘zgartiriladi va optika orqali tor oqim (2-4 mrad) hosil qilinadi. IQ – oqim atmosfera orqali qabul qilgichga uzatiladi. Qabul qilish punktida optik nur qabul qilish ob’ektivi yordamida yuqori sezuvchan, tez harakatlanuvchi fotoqabul qilgich maydoniga fokuslanadi va unda detektorlanadi.

Kuchaytirilgandan va qayta ishlovdan o‘tgandan keyin signal qabul qilish interfeysiga tushadi, keyin esa foydalanuvchi qurilmasiga uzatiladi.

Optik tizimlarni hisoblash fotoqabul qilgichga tushayotgan IQ nurning quvvatini aniqlash bilan olib boriladi. Ma’lumki, bu qiymat qancha katta bo‘lsa, nurning uzatgichdan qabul qilgichga tushish samaradorligi shuncha yaxshi bo‘ladi. Axborotlashtirilgan optik signalning optik oqim tarqalishi evaziga tushishi soddalashtirilgan holatda geometrik optika qonuniga binoan aniqlanadi. Bu foto qabul qilgichning linza tekisligida optik dog‘ maydonining qabul qilgich linzasining maydoniga nisbatiga teng bo‘ladi.

Atmosferali optik aloqa liniyasi hisoblashni ma’lum dastur yordamida bajarishi mumkin. Kompyuterda modellashtirishni Mathlab dasturlash muhitida amalga oshirish mumkin. Optik aloqa liniyalari uchun maxsus dasturiy echim OptiSystemdan foydalanish mumkin. Lazerli aloqa liniyasi ikkita bir xil stansiyadan tashkil topgan bo‘lib, ular bir - biriga qarama - qarshi va bir - birini ko‘rish masofasida o‘rnatiladi.

Maqolada, uzatish qurilmasida uchta lazer, qabul qilish qurilmasida uchta fotodiod ishlatilgan variant holatida tadqiqot ishlari olib borilgan.

Uzatgichlar 910 nm to‘lqin uzunligida nur tarqatadi. Har bir lazerning nurni tarqatish quvvati 8 dBm. Axborotni uzatish tezligi – 155,52 M bit/s. qabul qilishda – uchta fotodiod ishlatilgan.

Tadqiqot jarayonida quvvati 20 dBm bo‘lgan bitta uzatgich va qabulda bitta fotodiodi bo‘lgan atmosferali optik aloqa liniyasi bilan solishtirish o‘tkazildi.

VIRTUAL XUSUSIY TARMOQLAR TRANSPORTINING ASOSIY TEXNOLOGIYALARI

N.X.Gulturaev (TATU, dotsent)
S.Q.Qadamov (TATU, magistrant)

VPN qurish asosiy texnologiyalari orasidan quyidagilarni ko`rsatish mumkin: IPSecVPN, MPLS VPN,RRTR vaL2TP tunnellashtirish asosidagi VPN. Barcha sanab o`tilgan xolatlarda provayder tarmoғiga trafik IP protokoli bo`yicha uzatiladi, u provayderga nafaqat VPN xizmatlarini, shuningdek turli qo`shimcha xizmatlarni ko`rsatadi.

VPN qurishga yordam beruvchi texnologiyalar, ularning xususiyatlariga sezilarli ta’sir ko`rsatishini, ta’kidlash lozim.

***Virtua lkanallarni qo`llab-quvvatlash texnologiyasi bazasidagi VPN.*** Amalda bunga o`xshash texnologiyalarni ro`yxatiATMvaFR bilan cheklanadi.Virtual kanallarni qo`llab-quvvatlovchi va xususiy VPN ega X.25 texnologiyasinig hayot tsikli tamom bo`lib bormoqda. Ma’lumotlar uzatishda ATM va FR faqat ikki darajada stek protokollaridan foydalanganligi sababli, ular asosida qurilgan VPN variantlari ham 2-darajali VPN (L2VPN) deb ataladi. "Nuqta-nuqta" virtual kanallari ajratilgan kanallarning servisini imitatsiyalaydi, mijoz bitta uzelining (SE) chegaraviy qurilmasidan provayder tarmoғi orqali boshqa uzel mijozining chegaraviy qurilmasiga o`tadi.

ATM va FR texnologiyalarida QoS ni qo`llab-quvvatlash mehanizmlar mavjudligi ajratilgan kanallar sifatini etarlicha yaxshi emulyatsiyalaydi. Xavfsizlikka magistral tarmoqda barcha trafik marshrutlanmaydi, balki virtual kanallar bo`yicha lokal belgilar VPI/VCI (ATM) yoki DLCI (FR) asosida kommutatsiyalanishi sababli erishiladi.

Virtual kanallar (L2VPN) asosidagi VPN ning murakkabligi uning qiymatiga o`xshab etarlicha yuqoridir. Aloqa operatori tomonidan mijoz uzellarining to`liq boғlanishli topologiyasi tashkil etilganda konfiguratsiyalash operatsiyalari va ichki tarmoqlar soni munosabati kvadratli boғlanishda bo`ladi.

Faqat Intranet xizmatlari qo`llab-quvvatlanganda konfiguratsiyalangan ulanishlar umumiy soni mijozlar soniga to`ғri proportsionaldir. Lekin Extranet xizmatlarini ko`rsatish

vaziyatni yomonlashtiradi, chunki mijozlarning turli ichki tarmoqlari uzellarida aloqani ta'minlash zarur bo`ladi.

Operatorning umumiy kirishli IP-tarmoƶi baƶasidagi VPN. Bu kategoriyaga turli texnologiyalar kiradi: IP Sec VPN, MPLS VPN va IP orqali tunnellanadigan boshqa texnologiyalar asosidagi VPN kiradi, masalan GRE, RRTR yoki L2TP. Barcha hollarda, mijoz IP protokoli yordamida provayder tarmoƒiga trafikni yuboradi, shuning uchun provayder nafaqat VPN xizmatlarini, shuningdek, qo`shimcha xizmatlarni, jumladan, amaliy darajadagi xizmatlarni ko`rsatishga qodir bo`ladi.

IPSec VPN.IPSec texnologiyasi - Internet standartidir, bu xolda uni IP-tarmoqlarda xavfsizlikni ta'minlovchi eng ommaviy va istiqbolli texnologiya zkanligini aytish mumkin. IPSec standartlari yuqori darajali moslashuvchanlikni ta`minlaydi, bu himoyaning kerakli rejimini (shifrlangan yoki faqat autentichlikni va ma`lumotlar yaxlitligini ta`minlash) tanlash, shuningdek autentifikatsiyalash va shifrlashning turli algoritmlaridan foydalanish imkoniyatini beradi. IPSec ning inkapsulyatsiya rejimi ikkita tashqi va ichki IP-adreslarni qo`llash hisobiga mijoz va provayder adreslar fazosini ajratish imkonini beradi.

IPorqali tunnellashga asoslanganVPN. Bu atama operator IP-tarmoƒi orqali VPN xosil qilish uchun foydalanadigan turli texnologiyalarni birlashtiradi. Tunnellar mijozning adresli fazosini ajratishni ta`minlaydi, u shifrlanmagan trafikni (GRE, L2TP) tashishi mumkin yoki uni shifrlashi (RRTR) mumkin.

MPLS VPN. VPN ning bu turlari 2-nchi va 3-nchi darajadagi VPN xususiyatlarini qamraydi, chunki trafikni tarmoq operator ining chegara qurilmasigacha etkazish IP protokoli (3-nchi daraja) yordamida, operator tarmoƒi doirasida esa MPLS yordamida etkaziladi, bunda paketlarni lokal belgilar asosida siljishi 2-nchi darajaga mos keladi. Umumiy xolda magistral IP tarmoq ATM transport tarmoƒi asosida yaratiladi, uning ustida MPLS qo`llab-quvvatlaydigan IP-marshrutizatorlar ishlab turadi. Bugungi kunda, MPLS VPN tashkil etilishini tavsiflovchi asosiy hujjat Cisco Systems mutaxassislari tomonidan tayyorlangan deb, RFC2547 axborot hujjat hisoblanadi.

MPLS VPN tarmoƒi yadro, chegara xudud va foydalanuvchilar tarmoƒiga ajratiladi. Har bir foydalanuvchi o`z navbatida bir nechta ajratilgan regional IP- tarmoqlar bo`lishi mumkin, ularning xar biri o`z navbatida, marshrutizatorlar bilan boƒlangan bir nechta quyi tarmoqlarni o`z tarkibiga kiritishi mumkin. Bitta iste`molchiga mansub ichki tarmoqlar IP-paketlarni operatorning yagona tarmoƒi orqali almashtirishadi va ular o`zining VPN ni tashkil etadi. Ichki tarmoqlarni operator magistraliga ulanishiga yordam beradigan marshrutizator, foydalanuvchining chegeraviy marshrutizatori SE (Cystomer Edge) deb ataladi. U iste'molchi tomonidaniste'molchi va operator orasidagi tranzit uzeli bo`lib xizmat qiladi.Operator magistral tarmoƒi – bu MPLStarmoƒidir, unda IP-paketlar belgilar asosida xarakatlanishadi.

Operator tarmog'ida LSR qurilmalari orasida chegeraviy marshrutizatorPE(Provider Edge) ajratiladi, ular foydalanuvchilar tarmoqlarini MPLS operatorining magistral tarmog'I ulanishiga javob berishadi,

Xulosa. Bugungi kunda MPLS texnologiyasiga telekommunikatsiya operatorlarining magistral tarmoqlari uchun asosiy texnologiya sifatida qaralmoqda. Uning bu tarzda qo`llanishi operator chegaraviy marshrutizatorlari orasida belgilarni kommutatsiyalash yo`lini yaratadi, operator tarmoƒidan tashqarida esa IP paketla xarakati tarmoq satxidagi an`anaviy usulda bajariladi. Magistral tarmoq marshrutizatorlari kombinatsiyalangan murakkab qurilmalardir, chunki ularda IP ni marshrutlash standartnie bloklari, shuningdek mavjuddir, ularni LSRga aylantiriuvchi spetsifik MPLS bloklar mavjuddir.

Quyidagilarni ta'kidlash lozim, VPN ning zamonaviy texnologiyalari avvaldan berilgan zaruriy xususiyatlarga ega qoplama tarmoqlarni tashkil etish imkoniyatini beradi, jumladanm bu tarmoqlar adreslashning mustaqil tizimigaq, berilgan o'tkazuvchanlik qobiliyatga, ishonchlilikka va axborot xavfsizligiga ega keng polosali tarmoqlardir.

TRAFFIC OFFLOAD: HOW IT'S WORK ON FEMTOCELL/LTE NETWORK

Sh.Sh. Karimov (postgraduate student of 2-course, TT faculty, TUIT)
S.A. Sadchikova (Ph.D., docent of TI chair, TUIT)

Small cells create several opportunities to meet the objectives that regulators set out to achieve. Some of these are as follows: improved access, cost effective, visually unobtrusive, spectrum efficiency, innovation and opportunity.

Small cells provide a cost-effective means of improving consumer access to mobile services. They improve coverage in hard-to-reach indoor environments, without the need to deploy large numbers of outdoor base stations. In urban areas, small cells allow for cost-effective deployments, which provide additional capacity and coverage. Equipment costs are generally lower than for macro base station sites and the number of sites can be optimized to provide additional capacity in locations where it is most needed

In the operator's macro-cellular network the operator leases a site, incurs significant civil (site improvements, shelters) and ancillary (antennas, coaxial cable, battery backup, air conditioning) costs, purchases radio infrastructure, and purchases (microwave) or leases (T1/E1) backhaul infrastructure before delivering the first phone call, text message, or e-mail update. Operators may add capacity to existing sites or may build entirely new sites. The architecture of a traditional macro-cellular network is shown in Figure 1.1:

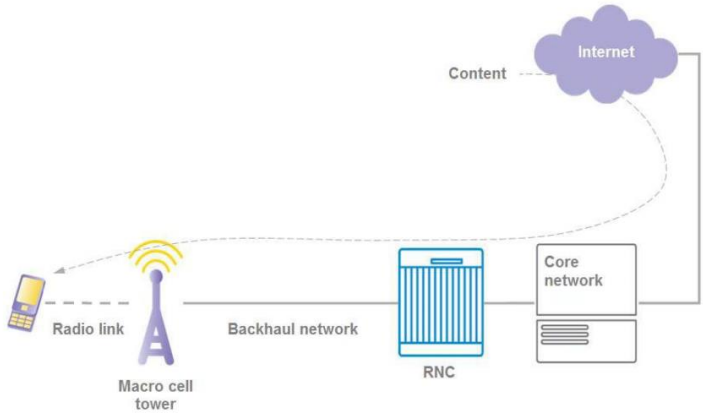


Figure 1.1 Internet Access via a Macro-Cellular Network

In a femtocell environment the operator supplies a femtocell. The consumer attaches it to his or her broadband connection. Traffic then flows over the air to the femtocell then over the internet to the operator's core network, and/or to other internet destinations. In a residential environment a femtocell is likely to supply as much data bandwidth as the subscriber is able to consume. If there is a limitation it is most likely in the speed of the residential or enterprise broadband connection, but this same limitation also applies to wired and Wi-Fi connected devices in the home or office. When a subscriber enters his home or office the devices automatically associate with the femtocell. Traffic that would have flowed between the macro-cellular site and the subscriber's phone/PDA/MID/laptop flows instead through the femtocell and the subscriber's broadband connection.

Studies of measured traffic indicate that mobile broadband usage peaks in the late afternoon, evening, and late evening – the very hours most consumers are at home. Thus, residential femtocells are likely to be highly effective in reducing demand during those periods that matter most to operators. Architecturally, the femtocell also absorbs the RNC, which further lessens the load on the macro-cellular network. Finally, the industry is developing a new standard called Selected IP Traffic Offload (SIPTO).

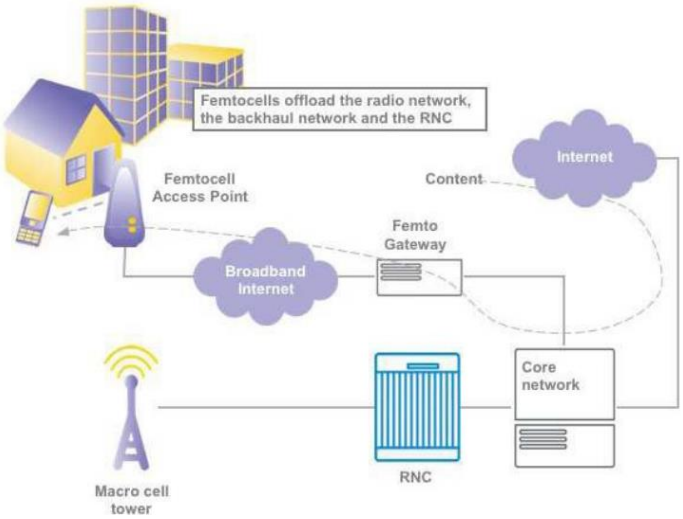


Figure 1.2. Internet Access via a Femtocell

SIPTO allows internet traffic to flow from the femtocell directly to the internet, bypassing the operator's core network, as shown in Figure 1.3.

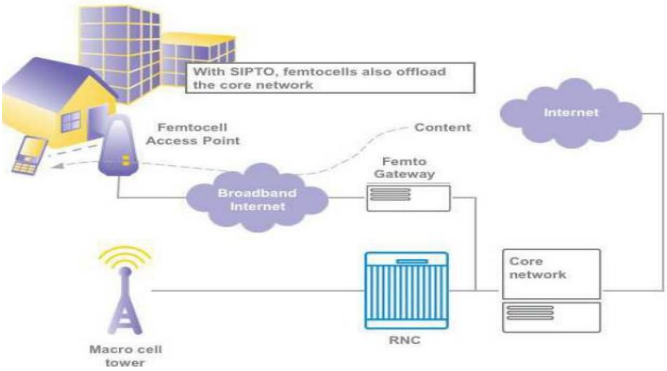


Figure 1.3. Internet Access via a SIPTO-Enabled Femtocell Architecture

OPTIK ABONENT KIRISH TARMOQLARINI KOGERENT VA NOKOGERENT OCDMA ASOSIDA QURISHNI TAHLIL QILISH

I.A.Mirzayeva (TATU, magistrant)

Ushbu ishda yangi avlod optik abonent kirish tarmoqlarini kogerent va nokogerent DS-OCDMA tizimlari asosida qurish imkoniyatini tahlil qilish.

So‘nggi yillarda tezligi oshib borayotgan multiservis xizmatlarni talab darajasida taqdim eta oladigan va xizmat ko‘rsatish sifatini yuqori darajada ta’minlaydigan optik abonent kirish tarmoqlarini yaratish va qurish bo‘yicha ilmiy-amaliy ishlar olib borilmoqda. Kanallar sig‘imini va xizmat ko‘rsatish sifatini oshirish yangi texnologiyalarni yaratishni talab etadi va bu talablar bugungi kunda dolzarb masala bo‘lib qolmoqda. OCDMA asosida, kelajakda, yuqori himoyalangan, ko‘p sonli foydalanuvchilarga bir vaqtda va bir xil tezlikda xizmat ko‘rsata oladigan, kanallarning vaqt va to‘lqin uzunliklari domenlarida o‘zaro ta’sirlashishi kabi muammolar sodir bo‘lmaydigan optik abonent kirish tarmoqlarini qurish mumkin. Tizimda xizmat ko‘rsatish sifati yuqori, bit xatolik koeffitsenti 10^{-9} dan kam va abonent tarmoqlarida xar bir foydalanuvchi Gbit/s tezlikda ishlashi mumkin. OCDMA tizimlarida bitta chastota imkoniyatidan barcha foydalanuvchilar birdek foydalanadi, ya’ni umumiy kanalning o‘tkazuvchanlik qobiliyati foydalanuvchilar soniga nisbatan emas, balki xar bir foydalanuvchi uchun kanalning o‘tkazuvchanlik qobiliyati o‘zgarmas bo‘lib qoladi. Yuqoridagi talablarga javob berishi mumkin bo‘lgan tizimlardan biri bu optik CDMA texnologiyasi bo’lib, bu tizimning turli usullari qurish mumkin masalan DS (Direct Sequence) – to‘g‘ri ketma ketlik usuli, FH

(Frequency Hopping) – chastotalarni o’zgartirib qayta to‘g‘rilash usuli va TM (Time Hopping) – vaqt bo‘yicha psevdo tasoddifiy qayta to‘g‘rilash usuli.

OCDMA texnologiyasi tarmoqqa nisbatan moslashuvchan va boshqa texnologiyalariga qaraganda samaradorligi yuqori. OCDMA texnologiyasi asosida kirish tarmoqlarini qurish orqali ma’lumotlarni asinxron tarzda va yuqori tezlikda uzatish mumkin. Bu tizimning yana bir afzalliklaridan bir fizik pog‘onada turli sifat ko‘rsatgichiga ega va turli sig‘im ma’lumot oqimlarini yuqori pog‘ona protokollaridan foydalanmasdan uzatish imkoniyatini qo‘llab quvvatlashidadir. OCDMA tizimlari ikki xil usulda quriladi: kogerent va nokogerent holda. Bu ikki xil tizimda turli kodlash texnikalari va kodlash usullari ishlab chiqilgan. OCDMA tizimlarini telekommunikatsiya tarmoqlariga kirib kelishi va bu tizimning kirish tarmoqlaridagi o‘rni, imkoniyati va tadbiqi bo‘yicha ko‘pchilik mutaxassislar va olimlar chuqur tahlil qilgan va shu bilan birga kogerent va nokogerent DS-OCDMA tizimlari asosida kirish tarmoqlarini qurish imkoniyatilari xam o’rganilgan.

OCDMA tizimlarini ishlash jarayonini yaxshilash va bu tizimni kirish tarmoqlarida tadbiq qilish bo’yicha ko’pgina sinov testlari o’tkazildi, bu tizimni ishlash jaratonini baxolash uchun turli simulyatsiya modellari yaratildi xamda xatoliklar darajasi o’rganildi va shovqinlarni bartaraf etish uchun turli echimlar taklif qilindi. Natijalar shuni ko’rsatdiki, kogerent tizimlarida optik chastotalarni yuqori aniqlikda nazorat qilish murakkab ekanligi isbot qilindi. Yana bir olib borilgan ilmiy tadqiqot ishida SAC-OCDMA (spectral amplitute coding OCDMA) tizimi manbalari xar tomonlama o’rganilganda, amaliy natijasi shu ko’rsatdiki, nokogerent tizimlarga qaraganda kogerent tizimlarning samaradorligi yuqoriroq bo’lib, bir xil nokogerent manbalardan bir vaqtda foydalanmasdan ko’p lazerli (multi-lazer) manbadan foydalanish OCDMA tizimlarini yuqori aniqlikda ish bajara olishini ko’rsatdi, biroq bu jarayonni amalga oshirish tarmoq qurilishini iqtisodiy juhatdan qimmatlashib ketishiga olib keladi.

Nokogerent tizimlari kogerent tizimlariga qaraganda iqtisosiy jihatdan ancha arzon. Biroq, bu nokogerent OCDMA tizimlarining kamchiligi o’tkazuvchanlik qobiliyatining turlicha bo’lishi kanallarning bir biri bilan ta’sirlashishiga olib keladi. Bu jarayon tizimda optik zarba shovqinini (optical beat noise) yuzaga keltiradi. DS-OCDMA tizimlarini turli usullarda modellashtirish orqali bu tizimlarining bit xatolik darajasi (BER) turlicha aniqlangan. Dastlabgi ilmiy tadqiqot ishlarida Pusson extimolliklaridan foydalanib xatoliklarning extimolliklari xisoblangan. Biroq, bu tahlillar faqatgina ko’p sonli tarmoq foydalanuvchilari bo’lgan xolatlar uchun xaqiqiy xisoblanadi. Quyidagi formula orqali MAI shovqinlari darajasini aniqlash mumkin.

$$\sigma_{MAI}^2 = (k-1)\bar{\sigma}^2$$

bu erda k – interferensiya va $\bar{\sigma}^2$ – turli kod juftliklarining o’rtachasi kros-korrelyatsiyasi. Bu xolatdan kelib chiqib, signal interferensiya nisbati (signal to interference ratio, SIR) quydagicha topiladi.

$$SIR = \frac{p^2}{\sigma_{MAI}^2}$$

bu erda p – kodning og’irligi. Xatoliklarning extimolligi, boshqa shovqin manbalarini xisobga olmagan xolda, quyidagi formula orqali aniqlash mumkin.

$$P_e = Q\left(\sqrt{SIR}\right)$$

Monto-Karlo (MK) usuli orqali DS-OCDMA tizimlari ishlash jarayonini simulyatsiyasi real xolatdagi tizimning ishlashiga ancha aqinlashtirilgan. MK usuli orqali simulyatsiya qilish natijasida bit xatoliklari darajasini xisoblash va real xolatda optik aloqa tizimlarining ishlash jarayonini baxolash mumkin. Biroq tizim mos intervallarda BER darajasini taxmin qilib xisoblash jarayonida katta sonlardan foydalanishni talab qilinadi biroq tizimni murakkab bo’lishiga olib keladi.

OCDMA tizimlarda BER xatolik darakasini yaxshilash va tizimning samaradorligini yaxshilash maqsadida lazer juda katta aniqlikda ishlashi zarur. Shuning uchun xam OCDMA tizimlarida nokogerent manbadan foydalanish maqsadga muvofiqdir, sababi narxi arzon va murakkab qurilishni talab qilmaydi.

PERFORMANCE ANALYSIS OF A NEXT GENERATION CONVERGED NETWORK

F.A.Muzafarov (TUIT,assistant lecturer)

Moving from the existing independent infrastructure to integrate shared environment (converged network) will reduce the infrastructure maintenance cost, which we use for performance analysis. Efficiency metrics, response times, transit time, throughput and transfer delay for different transaction routes in a converged network are evaluated. Various rounds of testing have been conducted using Single User Testing and Load Performance Testing to collect performance metrics to identify architecture bottlenecks. Based on performance analysis, we observed some poor performance as well as more delays in the response times to reach TC servers. We concluded that the response times between a client and TC servers violated the Service Level Agreement. This Paper identifies that most delays were contributed mainly by processing times of TC servers in a converged network.

When a request is sent from the Trusted Zone in an organization, it passes through several layers. One of the problems is to identify where the bottleneck of the performance of the application is. Figure 1 shows the application architecture, which includes vendor, sales client, admin users, differentservers at different tiers, and multiple firewalls to secure the network. Moreover, we show the response times, that will be measured, between the users and different server's zones. The server layer's zones include Mule Servers, TC servers, web servers, and database servers. For sending request transactions from a client to different servers, we use OPNET for modeling the architecture of the network and simulation to calculate different performance metrics, such as transit times, response times, throughput, and others.

With the help of these performance metrics, we can analyze the performance of each transaction and compare the result to identify any performance issues, delay violations, and the Bottleneck in the architecture to be resolved . Two different tests were conducted in this paper: The Load Performance Testing and Single User Testing. Load Performance Testing (LPT)- In this testing, we send multiple requests to the application. Single User Testing (SUT)-SUT determines the most accurate time for the layers in the application.

In sum up,One solution could be replacing the TC server with a faster one. Another solution might be limiting the connections times between the application's units to improve the performance of the applications and reduce the cost of the infrastructure. Using OPNET modeling and simulation, we can collect performance metrics (response times, transit times, throughput, and others) to analyze the performance of the network. We should run two different testing: SUT and LPT, using three different transactions (Dashboard, URL, and Submit Request). After running these tests several times, we may conclude that the architecture bottleneck identifies to be theprocessing time in the TC server layer, which is causing most delays.

REQUIREMENTS OF QUADRUPLE PLAY SERVICES

R.H.Nasimov (TUIT, assistant ofTI department)

Broadband IP is a great leveling ground when it comes to converged services being offered by multiple providers. For example, with the availability of Broadband, companies such as Vonage could offer IP based phone replacement solutions threatening the turf of established phone operators. Similarly, Comcast can now suddenly offer Cable VoIP (phone service) and Verizon can now suddenly offer TV services over IP, thereby threatening each in service areas that were traditionally never their turf. Broadband IP has also enabled 'new kids on the block'

like Skype, Joost and others to offer bundled services that threaten the trillion dollar communications industry as we know it. This is one main reason why carriers are competing to stay alive with “Quadruple Play” blended services that offer Voice, Video, Data and Wireless accessibility into one.

However, providing Quadruple-Play across heterogeneous networks (WiMAX, DSL, Cable, cellular etc.) is a non-trivial task and one needs a robust and well thought out architecture which ensures that services can be provisioned and provided uniformly to subscribers in a way that lends to seamless user experience and operator provisioning/charging and billing.

This thesis describes the merit of IMS (IP Multimedia Subsystem) - an over-arching architecture specification that enables uniformed IP based service delivery over diverse network types (WiFi, DSL, WiMAX, Cellular technologies etc.) as the ideal architecture for Operators to deliver Quadplay services to their users.

Uniformed service delivery is a key requirement for delivering effective Quadruple Play services.

Providing Uniformed Service Delivery architecture can be translated to the following key requirements:

1. Ensure subscribers and devices can be identified uniquely for the purposes of charging and delivery of services across different access mediums;
2. Ensure security, integrity and authentication is maintained;
3. EnsureacommonPolicy (QoS) and charging architecture;
4. Provide call continuity (often referred to as basic service continuity);

The layered 3GPP/IMS architecture attempts to enable all of the above. This thesis will discuss in more detail how IMS enables the above and therefore is ideally suited to a heterogeneous network.

IMS has specified a generic subscriber identity mechanism that is independent of the underlying network. In addition, it is very easy to associate more than one service profile to a single subscriber. This is best described with an example:

Let us suppose that user “Joe” is an IMS subscriber. While he uses a CDMA network to connect to the IMS services, due to the limited bandwidth of the network, he is only allowed to access voice calls at a 5.3kbps codec, and basic email. However, when the same user “Joe” connects via a high speed WIMAX network, he is allowed to use a 64kbps voice codec, make video calls, and access IPTV streaming to his WIMAX device.Thisin herently meansa few different things:

The subscriber identification should be generic so that it can be used across any access network The network needs to correlate all these scenarios to a single user “Joe” The network needs to provide for the fact that user Joe may have one or more service profiles active at any time (for example, Joe may be registered simultaneously with both his WiMAX PDA and CDMA cell phone at the same time).

IMS solves this by introducing the concept of Public, Private URIs and Service Profiles.

All identities in IMS are standardized as SIP URIs. Using the SIP URI addressing scheme ensures that identification is independent of the underlying network. If any mapping is needed to be done, that happens depending upon the network type attached to. For example, when connected to UMTS, the URI may be mapped to an MSISDN or IMSI (for Public and Private URI). In IMS, the Public URI is the ‘public’ address which the entity can be addressed. The Private URI is a network or operator assigned URI that ensures that the user is correctly authenticated and verified by the network (more on this later). A single Private User Identity can have more than one Public User Identity. Finally, each Public URI can be linked to a service profile that describes the available services that are currently active for that profile. It is also possible that a single Service Profile is shared between more than one public URI. Diagrammatically, the relationship between Subscription, Private, Public and Service profile is as below:

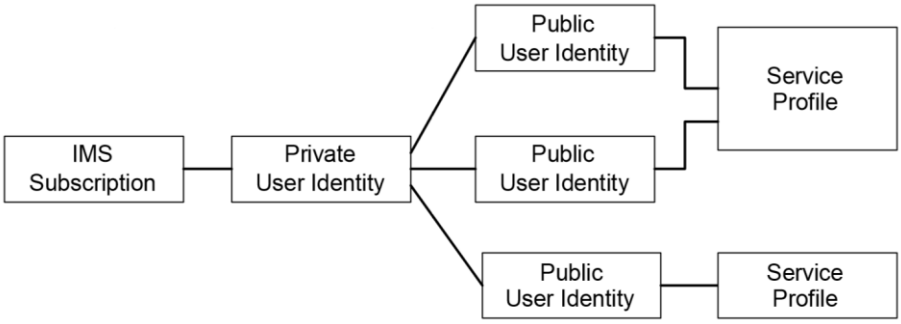


Fig-1.1. Relationship between subscription, private, public and service profile

In this thesis, we have explored how IMS enables key requirements for truly convergent network architecture and further justifies why we believe that as disruptive access technologies such as WiMAX are deployed, IMS will be required as session control architecture to be able to deliver Quadruple Play services across these diverse access technologies.

NETWORK TRANSPARENCY METHODS IN 4G

V.A.Son (postgraduate student of 2-course, TT faculty, TUIT)
S.A.Sadchikova (Ph.D., docent of TI chair, TUIT)

4G wireless systems is foreseen as a globally integrated communication network interconnecting, in a transparent way, a multitude of heterogeneous networks and systems. Optimal allocation of user and system resources may be effectively achieved with the co-operative optimization of communication system components. Innovative schemes enabling joint optimization over wireless links include the development of flexible channel coding and modulation schemes, the adaptation of existing source coding schemes with respect to their ability for Joint Source Channel

Coding/Decoding (JSCC/D) and the specific development of new optimized ones.

Network Transparency is a fundamental aspect that allows an effective realization of the PHOENIX JSCC/D system. It is somehow an abstract idea of making the underlying network infrastructure almost invisible (from which the transparency) to all the entities involved in the jointly optimization of the source and channel (de)coder, as well as of the (de)modulator. Almost transparent is related to the fact that the telecommunication infrastructure by its own, inevitably affects in some extent the overall system, such as introducing delay, loss and various types of errors, but without actually interacting with the control-plane of the concerned deployed devices and providing sufficient delivery guarantees to the video streams in order to accomplish a defined quality of service (QoS) for the end-user. The goal is:

– to realize communication exchanges between entities differently located in the network (including the end-terminals)

– not to interact anyhow with non-JSCC/D aware devices.

The primary goal is referred to the capability of transferring signaling/control data between both different network nodes and link layers as needed, in a transparent manner, in spite of the strict rules of the ISO OSI model, which impose a modular and independent design of each link layer of a network node with well defined interfaces and the delivering through a telecommunication infrastructure that carries data only of a specific format (IP datagram). The second objective aims to ensure as much as possible backward compatibility, not only with the existing standards as also addressed by the first goal, but even with the nowadays telecommunication infrastructure that constitutes the basis for the next generation networks, allowing for a smooth migration to IPv6-enabled devices eventually supporting JSCC/D functionality.

The design of the solution for the Network Transparency must take into account the

deployable security mechanisms, providing authentication and encryption features, even if working at different layers simultaneously, e.g. at both application and data-link layers, as well as compression techniques. Security and header compression facilities can introduce further constraints, not only in terms of additional complexity and hence delay, but also of theoretical and practical feasibility of the available mechanisms to support the Network Transparency. Some mechanisms that could implement the concept of the Network Transparency are: IPv6 data packets and extension headers, ICMPv6 messages, direct socket-to-socket communication, external databases and service profiles stored in shared memory spaces. Other possible methods relies either on the introduction of adaptation layers at the transmitter and receiver side to allow for the exchanges implicated by the joint source and channel (de)coding system, or the exploitation of already existing and deployed ad-hoc signaling protocols.

There are various signaling and control information that need to cross the network from the generation point to the target destination(s), mainly: Source significant information (SSI), Channel state information (CSI), Decision reliability information (DRI), Source a-priori information (SRI), Source a-posteriori information (SAI), Network state information (NSI).

The SSI is generated by the source coder and it represents the information on the sensitivity of source bits to channel errors. The SSI is strictly related to the data stream and needs to be synchronized with it. For this reason, the communication mechanisms that are more suitable to be deployed for the transmission of SSI are: encapsulation inside the IP video packet header, or an ad-hoc signaling protocol. With encapsulation inside the video packet header, SSI is automatically coupled with the data fragment it refers to. More reasonably, this employs the Hop-by-Hop options,

because SSI must be available for different entities of the JSCC/D chain before reaching the destination terminal(s). However, an encapsulation into packet payload could also be appropriate. On the other hand, for an ad-hoc signaling protocol, it is necessary to deal with synchronization to the associated video data stream, which could result in a considerable effort.

It is interesting to evaluate the SSI overhead with different MPEG4 video sources. Simulation results for 4 different cases with the hop-by-hop encapsulation mechanism deployed is shown in Tab.1. Simulation results show that the SSI overhead is proportional to the video codec rate.

Tab.1. SSI overhead for different coding rates

video source	SSI overhead
MP4 370kbps	3 KB/sec
MP4 192kbps	1.5 KB/sec
MP4 125kbps	1 KB/sec
MP4 64kbps	500 B/sec

Obviously, choosing a source with a lower rate means sending lower SSI overhead on the network.

FTTH TEXNOLOGIYASINI TASHKIL QILISHNING AFZALLIK VA KAMCHILIKLARI

A.M. Xidirov (TATU, SF assistenti)
I. Vaydullayev (TATU, SF assistenti)

Yildan yilga istemolchilar yangi turdagi multimediya xizmatidan foydalanish ehtiyoji oshib bormoqda. Yangi turdagi optik tolalarning (siljigan dispersiyasi nolga teng bo'lmagan), keng polosali kvant optik kuchaytirgichlarning yaratilishi to'liq optik tizim va optik traktlarni qurish imkoniyatini yaratmoqda. Bunday texnologiyalardan 100 va 1000 Gbit/s o'tkazish oraliqli tizimlarni yaratishda foydalaniladi.FTTH – uy ichida optik toladan foydalanidigan texnologiyadir. Hozirgi vaqtda abonentlarni asosiy qismi ko'p qavatli uylarda istiqomat

qilishidan kelib chiqan holda, FTTH texnologiyasi FTTB dan farqi shundaki bu texnologiyada optik tola abonentni alohida kvartiralargacha yetkazib beradi.

FTTH - “uygacha optik tola” texnologiyasi haqida gapirilganda optik tola alohida kottedj yoki hovligacha olib borilgan deb tushuniladi. Bunday texnologiyalarni g’arb davlatlarida “oxirgi mil” muammosi emas “oxirgi yuzlik futlar” muammosi deb uqtirishadi.

FTTH - “uygacha optik tola” texnologiyasini afzalliklari:

- Yuqori o’tkazish polosa kengligi.Zamonaviy talablarga ega bo’lgan o’tkazish kengligi -20-50 Mbit/s to’g’ri oqimda va 10 Mbit/s dan yuqori teskari oqimda tezlikga ega bo’lgan talablarga javob beradi. Bunday keng polosali tarqalishda HDTV-uzatish bilan har bir oila praym-taymda bir vaqtda ikkitagacha videooqimni (jami 50 Mbit/s) qabul qilishi mumkin.
- Aloqa liniyasi yashirinligi va sir tutilishi (Konfidensialnost). Ushbu optik tolaga hech kim kichkina elektr probkan “juchok”ni (qo’ng’izcha) qo’ya olmaydi.bundan tashqari optik signal uzatilgan protokollar mustahkam mahkamlangan bo’lsa, masalan GPON standart protokolida eshitish ham mumkin ham bo’lmaydi.
- Liniyani mustahkamligi va ishonchliligi yuqori sifatligi. Misli kabellarga qaraganda optik tolali kabellar kavsharlangan joylarda, kross portlari oksitlanmaydi va bundan tashqari tolali optik kabellarga namlik ham ta’sir etmaydi.
- Aktiv elementlarni soni kamligi.Bunda misli qilib GPON texnologiyasini olishimiz mumkin. Bitta markaziy qurilma PON OLT 20 kilometrli radiusda 1-2 mingtagcha abonentga xizmat qilishi mumkin.
- FTTH –tarmog’ini kamchiliklari esa quyidagilardan iborat:

Yong’in-qo’riqlash signalizatsiya sistemalari.Yong’in-qo’riqlash signalizatsiya sistemalari asosan misli simlar orqali amalga oshiriladi. Bu esa elitali hovli va kottedjlarga qo’shimcha sim shohobchalarini tortishga olib keladi.

Xulosa qilib aytganda, O’zbekistonda ushbu texnologiyani qurish eng yirik shaharlarida va markazlarida amalgam oshirilmoqda. Lekin ushbu tarmoq qurilishida va ulanishida katta miqdordagi sarf xarajatlarini talab qiladi.

РАСЧЁТ ПРОПУСКНОЙ СПОСОБНОСТИ СЕТИ ДОСТУПА НА ОСНОВЕ ПЕРВОЙ ФОРМУЛЫ ЭРЛАНГА

М.Б.Абдужаппарова (старший преподаватель кафедры ТИ, ТУИТ)

Для расчета пропускной способности и объема используемых технологий используются теоретические и инженерные методики. Основные аналитические положения инженерного расчёта позволяют рассчитать необходимое для построения сети доступа количество активного и пассивного оборудования, характеристики сети, а также дать общую оценку капитальных затрат на построение городской оптической сети доступа на этапе предпроектных исследований. Теоретический метод позволяет оперативно оценить сетевые параметры участка доступа, которые подлежат дальнейшему уточнению с помощью детальных инженерных методов. Одним из последних разработанных методов является метод расчёта параметров сетей доступа на основе применение формул Эрланга.

Первая формула Эрланга (ErlangB) представляет зависимость коэффициента потерь вызовов от поступающей нагрузки и числа каналов:

$$B = \frac{\frac{A^N}{N!}}{\sum_{K=0}^{N} \frac{A^k}{k!}} = \frac{A^N}{N!} \cdot \frac{1}{1 + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \ldots + \frac{A^N}{N!}} \qquad (1)$$

где:

B – коэффициент потерь вызовов [%],

A – общая поступающая нагрузка [Ерл.],

N – число каналов (линий связи).

Также первая формула Эрланга может быть выраженная в следующем виде:

$$B = \frac{1}{1 + \sum_{k=1}^{m} \left(\frac{N}{A}\right) \cdot \left(\frac{N-1}{A}\right) \cdots \left(\frac{N-k+1}{A}\right)} \qquad (2)$$

Использование выражения (2) может существенно понизить вычислительные нормы и вычислить нагрузку системы для больших величин.

Для применения первой формулы Эрланга должны быть выполнены следующие условия:

1) Поток запросов (вызовов) состоит из случайных входных запросов с экспоненциальным распределением, что означает более длинные промежутки между запросами для меньшего числа вызовов.

2) Время обслуживания имеет сходное распределение, то есть экспоненциальное понижение числа запросов с более высоким временем обслуживания.

3) Поток запросов стабилен как если бы он исходил от бесконечного числа источников запросов.

4) Полная доступность запросов для всех обслуживаемых каналов.

5) Отклоненные запросы не возвращаются во входящий поток, следовательно нет повторяющихся запросов.

6) Никакие два запроса не создаются одновременно.

IP трафик вносит радикальные изменения в телефонные сети. Условие 2 не удовлетворено. Условие 5 также не может быть удовлетворено из-за того, что трафик из одного источника значительно повышается.

Вычисления по первой формуле Эрланга дали результаты, представленные ниже. Входные параметры задавались следующим порядком:

– Один из параметров был постоянным.

– Другой параметр повышался в заданной шаговой последовательности.

На рис.1 показана зависимость коэффициента потерь от ширины полосы пропускания при постоянном значении параметра использования канала.

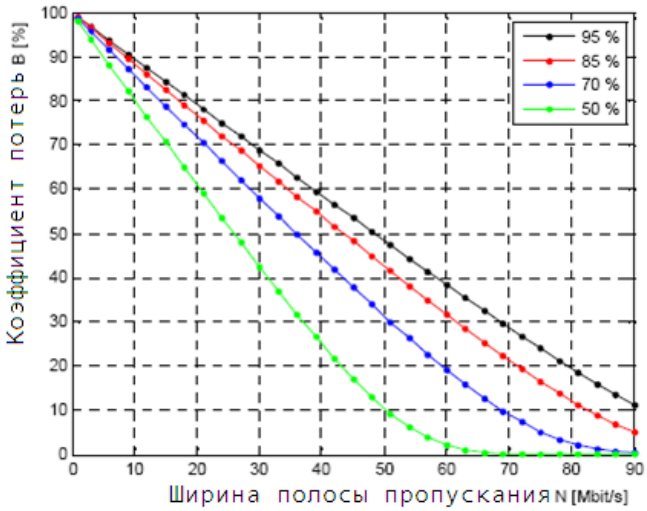


Рис.1. Зависимость коэффициента потерь от ширины полосы пропускания при постоянном значении параметра использования канала

Из графика выявлены следующие тенденции:

– Коэффициент потерь B уменьшается, если параметр ширина полосы пропускания повышается, а параметр использование канала остаётся постоянным.

– Коэффициент потерь B возрастает, если возрастает параметр использование канала.

На рис.2 показана зависимость коэффициента потерь от использование канала при постоянном значении параметра ширина полосы пропускания.

Из графика выявлены следующие тенденции:

–при возрастании параметра использования канала A также повышается коэффициент потерь B, если параметр ширина полосы пропускания N остаётся постоянным.

–при возрастании параметра ширина полосы пропускания N коэффициент потерь B понижается, если параметр использование канала A остаётся постоянным.

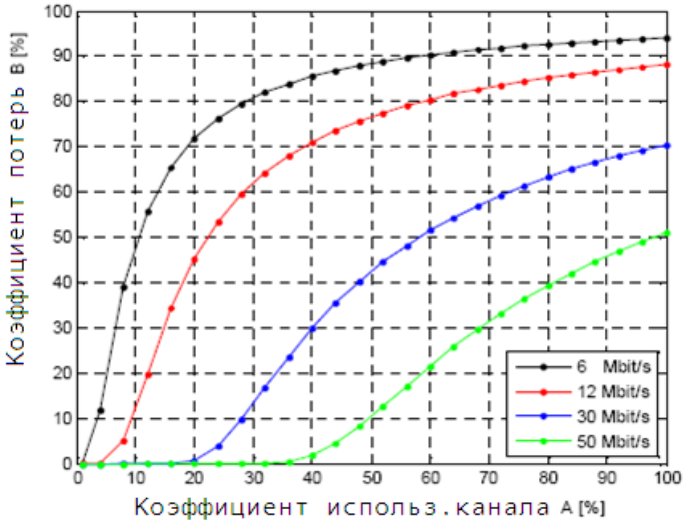


Рис.2. Зависимость коэффициента потерь от использования канала при постоянном значении параметра ширина полосы пропускания

Применение формул Эрланга даёт простой и эффективный способ описания указанных параметров трафика, являющихся основными параметрами QoS в сетях доступа NGN.

МЕТОД РАСЧЁТА ПРОПУСКНОЙ СПОСОБНОСТИ ОПТИЧЕСКОЙ СЕТИ ДОСТУПА ПО ВТОРОЙ ФОРМУЛЕ ЭРЛАНГА

М.Б.Абдужаппарова (старший преподаватель кафедры ТИ, ТУИТ)

Для описания трафика в сетях используются формулы Эрланга. Вторая формула Эрланга допускает бесконечное число источников нагрузки. Эти источники образуют трафик A для N каналов. Если все каналы заняты, то входящие запросы помещаются в очередь ожидания. Очередь ожидания одновременно может вмещать в себя бесконечное число запросов. Вторая формула Эрланга вычисляет вероятность образования очереди ожидания в случае трафика A при допущении, что отклоненные вызова будут оставаться в системе, пока не будут обслужены.

$$C = \frac{\frac{A^N}{N!} \cdot \frac{N}{N-A}}{\sum_{k=0}^{N-1} \frac{A^k}{k!} + \frac{A^N}{N!} \cdot \frac{N}{N-A}}, \text{ где } N > A \qquad (1)$$

где:

A – общая поступающая нагрузка [Ерл],

N – число каналов (линий связи),

C – вероятность ожидания обслуживания.

Вторая формула Эрланга (1) может быть упрощена посредством деления числителя и знаменателя на $\sum_{k=0}^{N} \frac{A^k}{k!}$ и последующим применением первой формулы Эрланга.

Благодаря этим упрощениям мы может представить формулу Эрланга C в виде:

$$C = \frac{N \cdot B}{N - A \cdot (1 - B)} \qquad (2)$$

Уравнения Эрланга изначально были предназначены для описания трафика в синхронных сетях. Для использования этих формул в асинхронных сетях, необходимо определить общие параметры для синхронных и асинхронных сетей, которые приведены в таблице 1.

Вероятность задержки C для асинхронных сетей представляет время ожидания, которое имеет место во время передачи в случае наибольшей нагрузки. Эта задержка проявляется в сетях IP из-за очередей ожидания в буферах узлов сети. Джиттер не может быть подсчитан через формулы Эрланга, т.к. для джиттера в синхронных сетях нет подобного параметра.

Таблица 1.

Общие параметры для синхронных и асинхронных сетей

Синхронная сеть		Асинхронная сеть	
B[%]	Коэффициент потерь вызовов	B[%]	Коэффициент потерь
C	Вероятность ожидания обслуживания	C	Вероятность задержки
A[Erl]	Общая поступающая нагрузка	A[%]	Использование канала
N	Число каналов	N[Mbit/s]	Ширина полосы пропускания

Вычисления по второй формуле Эрланга (2) дали результаты, представленные ниже. Благодаря этому уравнению можно вычислить вероятность задержки C и коэффициент потерь B, если известны два параметра – использование канала A и ширина полосы пропускания N.

На рис.1 приведена зависимость вероятности задержки от параметра использования канала при постоянном значении параметра ширины полосы пропускания

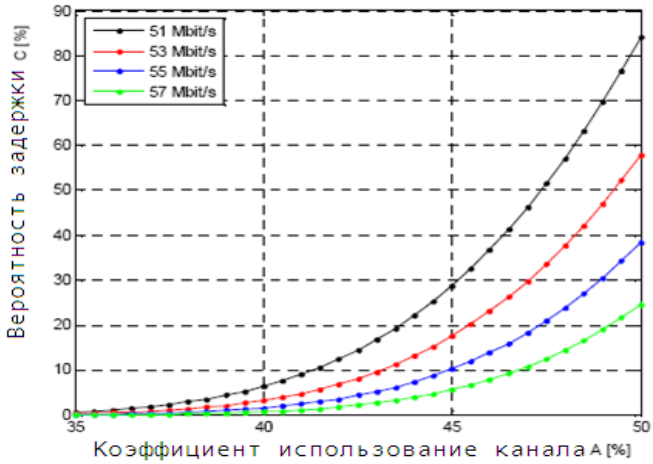


Рис.1. Зависимость вероятности задержки от параметра «использования канала» при постоянном значении параметра «ширина полосы пропускания»

Можно заметить следующие тенденции:

-В случае постоянного значения параметра «вероятность задержки» С при возрастании параметра «ширины полосы пропускания» N возрастает значение параметра «использование канала».

-В случае постоянного значения параметра «использования канала» А при возрастании параметра «ширины полосы пропускания» N значение параметра «вероятность задержки» С уменьшается.

-В случае постоянного значения параметра «ширины полосы пропускания» N при возрастании параметра «использования канала» А возрастает значение параметра «вероятность задержки» С.

На рис.2 приведена зависимость параметра «использование канала» от ширины полосы пропускания при постоянном значении параметра «вероятность задержки».

Можно заметить следующие тенденции:

-В случае постоянного значения параметра «использование канала» А при возрастании параметра «ширины полосы пропускания» N значение параметра «вероятность задержки» С падает.

-В случае постоянного значения параметра «ширины полосы пропускания» N при возрастании параметра «вероятность задержки» С возрастает значение параметра «использование канала» А.

-В случае постоянного значения параметра «вероятности задержки» С с возрастанием значения параметра «ширины полосы пропускания» N возрастает значение параметра «использование канала».

Рис.2. Зависимость параметра «использование канала» от ширины полосы пропускания при постоянном значении параметра «вероятность задержки»

Результаты вычислений показывают, что трафик в асинхронных сетях может быть описан с использованием первой и второй формул Эрланга.

ГЕОИНФОРМАЦИОННАЯ БАЗА ДАННЫХ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ КЕГЕЙЛИЙСКОГО РАЙОНА РЕСПУБЛИКИ КАРАКАЛПАКСТАН

З.Ж.Алламуратова, А.Кутлымуратов, О.И. Абдуганиева
(ТУИТ,с.н.с., магистрант, ассистент)

Рассмотрены вопросы интеграции ГИС для планирования и мониторинга состояния телекоммуникационной сети Кегейлийского района, на основе исходных данных по телекоммуникационной сети Кегейлийского района, характеризуемых прежде всего территориальной распределенностью и получаемых из различных источников. Предполагаемая геоинформационная модель телекоммуникационной сети Кегейлийского

района позволяет оперативно решать задачи, обработки данных и принятия решений на базе удобного и оперативного доступа к базе геоданных.

Геоинформационная модель телекоммуникационной сети Кегейлийского района включает решение следующих взаимосвязанных задач:

1. Разработка структуры геобазы данных;
2. Реализация модели геобазы данных в среде ArcCatalog;
3. Постоянное пополнения или обновления геобазы данных;

Структура базы геоданных проектируется с целью оперативного поиска, подбора и получение исходных данных при решении конкретных задач.На этом этапе предполагается изучение и картирование объектов телекоммуникационной сети Кегейлийского района. С этой целой целью будет произведен сбор и анализ накопленных источников. Источники разделяются накартографические, статистические, атрибутивные;

Подготовка и создание базы геоданных требует тщательного изучения территориальногохарактеры объектов телекоммуникационной сети.

База геоданных является стандартной средой хранения и управления данными в ArcGIS, которая может быть утилизирована в любой нужный момент — на настольных компьютерах, серверах (включая Web) или мобильных устройствах.

При реализации базы геоданных в среде ArcCatalog в начале в системе *ArcCatalog* определяются топологические составляющие ГИС модели телекоммуникационной системы районаКегейли и их типы. Составляющие подразделяются на точечные, линейные и полигональные типы.

Точечными топологическими элементами ГИС модели телекоммуникационной системы являются колодцы, антенны, АТС, столбы, трансформаторы, распределительные коробки линии связи, регенерационные пункты кабельных сооружений, а также то конечные элементы передачи данных - компьютеры, коммутаторы, цифровые модемы-шлюзы.

Линейными топологическими элементами ГИС модели телекоммуникационной системы являютсялинии связи (магистральные, оптически, КСПП, ТПП 600х2).

Площадными топологическими элементами ГИС моделителекоммуникационной системы являются границы территорий города,территории проживания населенияи и тд.

Эти топологические составляющие ГИС модели представим в системе *ArcCatalog* (Рис.1)

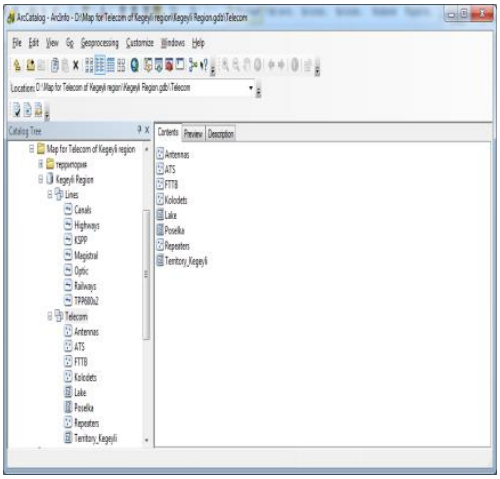


Рис.1. Размешение топологических элементов ГИС модели телекоммуникационной сети района Кегейли в *ArcCatalog*

При создании базы геоданных объектов телекоммуникационной сети необходимо учитывать, что ГИС работает пространственной и атрибутивной информации. Пространственная информация в ГИС находится в цифровой форме и служит для

визуализации изображения в той или мной модели данных. Атрибутивная информация в ГИС - это данные, описывающие параметры пространственно соотнесенных объектов. Например, антенна на дисплее может быть представлена в виде точка, а атрибутивная информация будет содержать сведения об ее высота, мощность, уровень электромагнитной волны и т.д.

Геоинформационная модель телекоммуникационной сетиКегейлийского района позволяет оперативно решать задачи по мониторингу состояния, инвентаризациии планированиясети с учетом различных требований к услугам телекоммуникационной сети. А также позволяет принимать решения, создать целостную территориальную картину состояния и развития структуры телекоммуникационной сети.

К ВОПРОСУ РАЗРАБОТКИ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ

З.Ж. Алламуратова (ТУИТ, снс), А.Кутлымуратов (ТУИТ, магистрант)
М.Нартбаева (ТУИТ, студент)

Поддержка принятия эффективных решений в телекоммуникационной области существенным образом зависит от информатизации данной отрасли, в которой одним основных в решении задач оперативного сбора и анализа информации является геоинформационный подход.

Использования геоинформационных технологий в телекоммуникационной отрасли позволяет решать следующие задачи:

-инвентаризация телекоммуникационных сетей (ТС);

-планирование ТС с учетом повышения роста уровня благосостояния населения;

-прогноз дальнейшего развития ТС;

-изучение и прогнозирование рынка услуг ТС;

-повышение качества принимаемых задач за счет оперативности и актуальности используемой информации.

Система поддержки принятия решений для сферы ТС включает следующие функциональные подсистемы:

-подсистема сбора информации и информационного обмена;

-подсистема анализа, хранения и поддержки принятия решений;

-подсистема визуализации информации

Подсистема сбора информации и информационного обмена включает источники и протоколы передачи информации между системами обработки данных, объектами и пользователями услуг ТС на основе стандартных форматов данных.

Подсистема анализа, хранения и поддержки принятия решений реализуется в виде объектно-реляционной базы данных и принятия решений различного типа (предупредительный, локализационный, восстановительный).

При этом, подсистема поддержки принятия решений включает в себя систему функций, позволяющих в режиме реального времени анализировать данные, прогнозировать состояние ТС и моделировать различные сценарии развития и провести ситуационный анализ состояний ТС.

Весьма важным моментом системы поддержки принятия решений на основе геоинформационной модели ТС является формирование тематических слоев ГИС модели ТС экономического, экологического, социального и др. содержания и формирование корреляционных полей взаимосвязи двух и более тематических слоев геоинформационной модели ТС на основе метода «скользящего окна».

Следует отметить, что ныне в решении задач типа поддержки принятия решений для ТС наблюдается тенденции сближения ГИС с системами DSS

(DecisionSupportSystems), технологиями DataMining и многомерного (OLAP) анализа данных.

Перечисленные парадигмы интеллектуализации являются базисными современных геоинформационных систем поддержки принятия решений SDSS (Spatial Decision Support System).

Разработка системы SDSS направлена на решении следующих классов моделей:

-пространственно-временного прогнозирования изменений состояния ТС;

-интеллектуальной классификации объектов и ситуаций в ТС;

-принятия решений.

Развитие систем поддержки принятия решений на основе интеграции в рамках ГИС систем DSS, DataMining, OLAP и разработка на их основе системы поддержки принятия решений SDSS является перспективной и актуальной проблемой.

SPATIAL ANALYSIS CHARACTERISTICS OF ARCGIS FOR ENVIRONMENTAL MONITORING

Kuchkorov T.A., Allamuratova Z., Ajibayeva K.
senior scientific researcher, TUIT

ArcGIS Spatial Analyst (SA) adds a comprehensive set of advanced spatial modeling and analysis tools to the ArcGIS Desktop. Using ArcGIS Spatial Analyst, you can derive new information from your existing data, analyze spatial relationships, and build spatial models in different kind of purpose, for example environmental monitoring.An extension to ArcGIS for spatial analyst gives you a rich toolset to perform advanced analysis and visualize data. It can track groundwater contaminants, understand watershed flow characteristics, and categorize findings based on threat types.

Using ArcGIS spatial analyst, it can interpolate data values for a study area based on a collection of samples; clean up data to prepare it for further analysis or display; and calculate spatial statistics based on the local environment, small neighborhoods, or predetermined zones. All of these analysis operations will allow you to learn more about your data and help you make better informed decisions (Fig1, Fig2).

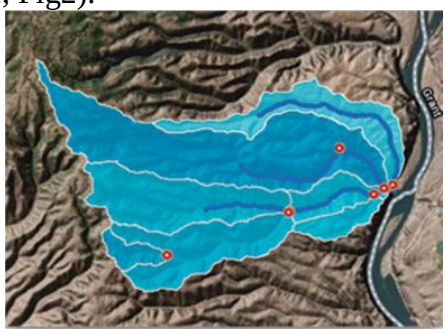


Fig1. The appearance of the movement of groundwater (by spatial analysis)

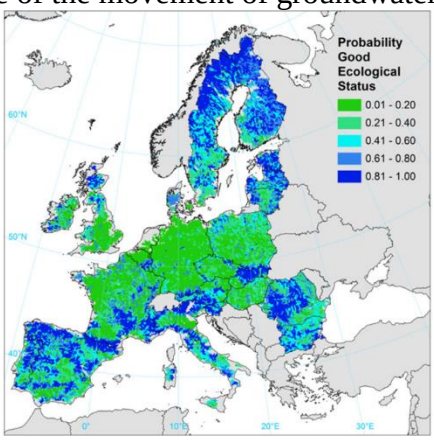


Fig2. The spread of water and trees in main part of Europe (by spatial analysis)

Main characteristics of spatial analyst are:

- find suitable locations;
- find the best path between locations;
- perform integrated raster/vector analysis;
- perform distance and cost-of-travel analyses;
- perform statistical analysis based on the local environment, small neighborhoods, or predetermined zones;
- generate new data using simple image processing tools;
- interpolate data values for a study area based on samples;
- clean up a variety of data for further analysis or display.

To provide ecological monitoring, following functions are necessary for spatial analysis in fixed area:

- perform integrated raster/vector analysis;
- perform statistical analysis based on the local environment, small neighborhoods, or predetermined zones;
- generate new data using simple image processing tools;
- interpolate data values for a study area based on samples.

To research ecological stress area based on ecological factors, we should determine how places are related between each other. For example, how related the amount of salt between districts and regions of Uzbekistan (north side of Uzbekistan), water quality and changes in different places, using and changes underground water trends in special places and so on (Fig3).

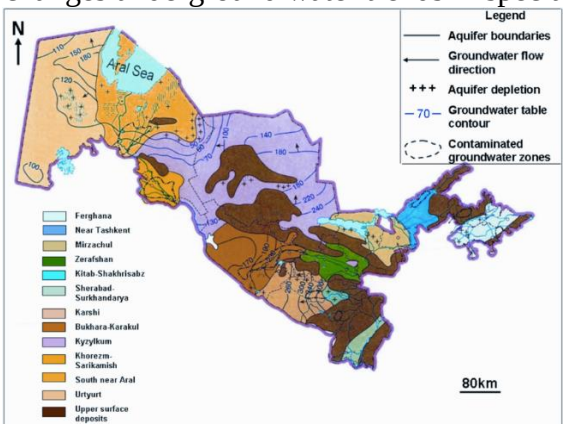


Fig3. Hydrogeological map of Uzbekistan (adapted and modified from [2])

ArcGIS spatial analyst is so strongly integrated with the ArcGIS Desktop geoprocessing environment that is easier than ever to solve complicated analysis problems. Geoprocessing analysis models are not only easy to create and implement, but they are also self-documenting, so anyone can quickly understand your spatial analysis process. Thousands of ArcGIS users are leveraging this modeling environment to take full advantage of their data and make better decisions.

АНЪАНАВИЙ ТАРМОҚДАН ДАСТУРИЙ КОНФИГУРАЦИЯЛАНАДИГАН ТАРМОҚЛАРГА ЎТИШ САБАБЛАРИ

Т.М. Бабажанова (ТАТУ Нукус филиали, ассистент)

Дастурий конфигурацияланадиган тармоқ (ДКТ) – бу компьютер тармоқ архитектурасини қуришга янгича ёндашувдир, бунда бошқарув функциялари контроллер деб номланадиган алоҳида қурилмага ўтказилиши ҳисобига тармоқни бошқариш поғонаси ва маълумотларни узатиш поғонаси ажратилади. Бошқарув функцияларини анъанавий

тармоқларда маршрутизаторлар ва коммутаторларда амалга оширилар эди. ДКТда бу вазифа контроллерга юклатилган. Контроллер эса ўз навбатида дастурий таъминот билан таъминланади ва тармоқни динамик бошқаришда асосий рол ўйнайди. ДКТни ташкил этишда тармоқнинг мантиқий ташкил этилишини инобатга олган ҳолда, трафикни бошқариш поғонаси, трафикни узатиш поғонасида амалга ошириладиган вазифа ва компоненталарнинг ташкил этилиши, функционаллиги ва амалга оширилишини ўрганиш муҳим аҳамиятга эга.

Компьютер тармоқларининг замонавий ҳолати ва ривожланиш тенденциялари, шуни кўрсатдики, анъанавий технологияларга асосланган тармоқларнинг ўтказиш қобилияти, тезкорлигининг ўсиш потенциали амалда ўз чегарасига етган.

Виртуаллаштиш дейилганда умумий тармоқ ресурсларида мустақил хизмат кўрсатиш сифати политикаларига эга бирнечта мантиқий изолцияланган тармоқларни ифодалаш тушунилади.

Юқорида кўрсатилган муаммоларга жавоб сифатида 2006 йили дастурий-конфигурацияланадиган тармоқлар концепцияси юзага келди (шундан буён интенсив ривожланмоқда). Бу концепция тармоқларда маршрутлашни тезлаштириш, конфигурациялаш, виртуаллаштириш, хизмат кўрсатиш сифатини созлаш қулайлигини ошириш имконияти беради, лекин қўшимча тадқиқотлар ва ишланмаларни талаб қилади, хусусан, тармоқ коммутаторлари аппаратурасини ташкил этиш, тармоқни бошқариш учун дастурий иловалар ва уларни бажариш учун платформалар соҳасида ўз ечимини кутаётган муаммолар мавжуд.

Тармоқ коммутаторлар, маршрутизаторлар ва бошқа қурилмаларни фойдаланган ҳолда қурилади ва улар кўп сонли мураккаб тақсимланган протоколларни амалга оширганлиги сабабли ҳаддан ташқари мураккаб бўлиб бормоқда. Бугунги кунда IETF томонидан стандартлаштирилган фаол ишлатилаётган протоколлар ва уларнинг версиялари сони 600 дан ортиқни ташкил этади.

Бундай шароитларда тадқиқотчилар уларга зарур экспериментларни ишлаб турган тармоқларда ўтказа олмайдилар, операторлар ўзларининг фойдаланувчилари учун янги хизматларни тез кирита олмайдилар, тармоқ қурилмалари ишлаб чиқарувчилари эса буюртмачиларнинг талабларини қондириш учун инновацияларни тез жорий эта олмайдилар.

Шундай қилиб, анъанавий тармоқларда ечими мавжуд архитектурага ўзгартириш киритишни талаб қиладиган бир қатор муаммолар тўпланган:

1. Илмий-техник муаммолар – бугун компьютер тармоқлари сингари мураккаб объектларни назорат қилиш ва ҳолатини ишончли олдиндан кўриш мумкин эмас.
2. Ижтимоий – кундалик ҳаётимизда биз барчамиз кўпроқ ва яна кўпроқ Интернетга таянамиз. Лекин, маълумотлар шу билан бирга шахсий маълумотлар ҳавфсизлиги кафолатланмаган, Интернет ташқи ҳужумларга бардош бера олмайди.
3. Иқтисодий – тармоқлар қиммат ва хизмат кўрсатиш мураккаб, юқори квалификацияли мутахассисларни талаб қилади.
4. Ривожланишда муаммолар – замонавий тармоқлар архитектурасида инновациялар киритишга, экспериментлашга, янги сервисларни яратишга барьер мавжуд.

ДКТ ёндашувининг асосий ғояси Стэнфорд ва Беркли университетлари мутахассислари томонидан 2006 йилда таърифланган ва академик муҳитда, етакчи тармоқ қурилмалари ишлаб чиқарувчилари ҳамжамиятида ва йирик IT-компаниялари томонидан кенг қўллаб-қувватланишига эришилган.

ДКТ ёндашувига IT-компаниялари томонидан қизиқиш билдирилишига қуйидагилар сабаб бўлган:

- Тармоқ қурилмалари самарадорлигини 25-30% га ошириш имконияти;
- Тармоқ эксплуатацияси учун ҳаражатларни 30% гача камайтириш;
- Хавфсизликнинг сезиларли ошиши;

Шу билан бирга дастурий конфигурацияланадиган тармоқларнинг камчилиги сифатида қуйидаги жиҳатларни келтириш мумкин:

- Контроллер тармоқ ишлашни рад қилишининг потенциал нуқтасидир;
- Тармоқнинг унумдорлиги тўғридан-тўғри контроллер унумдорлиги ва унинг физик имкониятларига боғлиқ;
- Янги оқимларнинг уланиш вақти тармоқ ўлчами ошиши билан сезиларли ўсиши мумкин.

АЛГОРИТМ ФОРМИРОВАНИЯ ТРАНСПОРТНОЙ СЕТИ

Л.Э.Байжонова (ТУИТ, ассистент)

Последовательность формирования транспортной сети (ТС) как виртуальной сети связи в общем виде включает две основные процедуры синтеза и анализа. Процедура синтеза позволяет определить оптимальную топологическую структуру виртуальной транспортной сети (ВТС) на основании исходных данных о топологии магистральной первичной сети связи общего пользования (ССОП), совокупности конечных точек и трафике конечных точек ВТС. Для расчета кратчайших путей предлагается использовать алгоритм Ярника- Примы-Дейкстры, основанный на применении стратегии поиска минимального остовного дерева.

Алгоритм начинает построение минимального остовного дерева с конкретной вершины графа и постепенно расширяет построенную часть дерева. Алгоритм работает пошагово — на каждом шаге он «посещает» одну вершину и пытается уменьшать метки. Метка произвольной вершины представляет собой число, оценивающее верхнюю границу длины пути от заданной начальной вершины к другой вершине. Алгоритм состоит в изменении меток вершин на каждой итерации по определенному правилу. От итерации к итерации метки уменьшаются либо остаются неизменными. На каждой итерации только одна метка принимает значение, уменьшить которое нельзя. Она считается постоянной и в ходе дальнейшего вычисления не меняется. Эта метка дает точную длину кратчайшего пути от начальной вершины к вершине с этой меткой. Когда все вершины получат постоянные метки, процесс решения заканчивается. Полученные метки дают длины кратчайших путей от заданной начальной вершины до каждой из остальных вершин графа. Данный алгоритм предлагается оптимизировать таким образом, чтобы, во-первых, начинать не с конкретной вершины, а с пустого дерева и в дальнейшем добавлять не вершины, а делать упор на ребра в порядке возрастания их весов; во-вторых, при выборе ребра, ведущего в кайму, необходимо выбирать ребро, являющееся частью кратчайшего пути в целом пути из начальной вершины; в-третьих, при появлении на пути ребер с одинаковыми весами выбор ребра будет осуществляться с учетом минимального вхождения этого ребра в другие пути.

Основное отличие этой математической модели, последовательности и алгоритма формирования ВТС - комплексный учет характеристик как самой ВТС, так и первичной сети связи. Это совместный учет топологической структуры транспортной сети связи, на базе которой реализуется ВТС, и непосредственно топологической структуры ВТС, информации о количестве и распределении трафика конечных точек ВТС, возможных алгоритмах маршрутизации потоков и ограничений на сетевые ресурсы.

ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАРНИ ТАШКИЛ ЭТИШ МУАММОЛАРИ

Л.Э.Байжонова (ТАТУ, ассистент)

Замонавий телекоммуникация технологияларида қабул қилинган атамаларда VPN (Virtual Private Network) аббревиатураси одатда виртуал қоплама тармоқни англатади. IP-тармоқлар ривожланиши глобал қоплама тармоқлар қуриш учун нисбатан арзон ва осон

киришли пакетли тармоқлар транспортидан фойдаланиш имкониятини яратади. Буни амалга ошириш айрим муаммолар билан боғлиқ, яъни VPN ни ташкил этиш усуллари, уни туркумлаш ва транспорт технологиялари таҳлил қилиш лозим бўлди. Яъни VPN технология сифатида умумий фойдаланиш пакетли тармоқларни кафолатланган ўтказиш қобилиятга эга ҳимояланган каналларга айлантириш имкониятига эга бўлиш муаммоси долзарбдир.

VPN асосий ғояси муракаб магистрал ва кириш тармоқларини лойиҳалаштирмасдан ташкилотнинг хусусий телекоммуникация тармоғини яратишдир. Зарурурий параметрларга эга VPN яратиш учун уларни ташкил этиш усулларига эътибор қаратиш лозим.

VPN ўзига хос бошқалардан ажратувчи хусусиятлари унинг бошқа тармоқлардан фарқлари қуйидагича белгиланиши мумкин:

-тармоқ технологияларини мустақил танлаш;

-адреслашнинг мустақил тизими;

-унумдорлик аввалдан белгиланиши;

-ахборот хавфсизлигининг юқори даражалиги.

VPN технологияси хам идоралар, хам хизматлар оператори томонидан ташкил этилиши мумкин. Биринчи холда оператор фақат “оддий” анъанавий хизматларни тақдим этади, идора мутахассислари эса VPN воситаларини мустақил конфигурациялайди в уларни бошқаради.

Иккинчи холда провайдер ўз хусусий тармоғи асосида хар бир идора учун хусусий тармоқни ташкил этади, уни бошқа тармоқлардан ажратади ва химоялайди.

Виртуал хусусий тармоқ қуйидагилар асосида қурилиши мумкин:

-буюртмачи худудида ўрнатилган ускуналар хисобига (Customer Premises Equipment based VPN, CPE-based VPN, ёки Customer Edgebased VPN - CE-based VPN);

-провайдернинг хусусий инфраструктураси хисобига (Network- based VPN, ёки Provider Edge basedVPN - PE-basedVPN).

Шундай қилиб, провайдер қўллаб қувватлайдиган тармоқлар ёки PE-based, ёки CE-based турида бўлиши мумкин. Биринчи вазиятда провайдер унинг тармоғида жойлашган ускуналарни бошқаради. Иккинчи вазииятда- VPN ускуналари мижоз территориясида жойлашади, лекин уни олисдан провайдер бошқаради. Бундаги асосий муаммо, бошқариш буйруқларининг ишончлилиги ва ўз вақтида бажарилишини таъминлашдир.

IP-ТЕЛЕФОНИЯ ДЛЯ ПОВЫШЕНИЯ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ КОРПОРАТИВНЫХ ОРГАНИЗАЦИЙ

Ф.К. Бекмуратов (Ассистент, СФ ТУИТ)
А.М. Хидиров (Ассистент, СФ ТУИТ)

Повышение экономической эффективности корпоративных образований является актуальной проблемой, особенно в условиях после глобального экономического кризиса. Существует масса способов и инструментов для решения выделенной проблемы. В данной статье рассмотрены, на первый взгляд, не столь очевидные, но весьма недооценённые способы и инструменты такой составляющей инфраструктуры предприятия, как телефония.

Корпоративное образование – это распределённая сеть, которая объединяет в себя офисы предприятия, производственные помещения и прочие строения, которые находятся на некотором удалении друг от друга – в разных частях города, разных городах или разных странах. Естественно, руководство компании стремиться объединить локальные АТС в единую телефонную сеть. Что естественно улучшит многие показатели предприятия, так как «живое общение» сотрудников разных офисов, часто находящихся на значительном удалении друг от друга, ускоряет решение многих задач, поставленных

перед предприятием. Именно IP-телефония позволяет выполнить эту функцию наиболее эффективно: экономия при междугородных и международных звонках, достаточно быстрая окупаемость средств, вложенных в создание сети IP-телефонии, в связи с быстрым совершенствованием и удешевлением программного обеспечения для IP-телефонии, в сравнении с ПО для аналоговых АТС, сокращение затрат на обслуживающий персонал для телефонии, нет необходимости содержать сотрудников во всех офисах, достаточно только в головном, из которого и будет проводиться администрирование сети IP-телефонии.

Телефонная связь внутри корпоративных образований является неотъемлемой частью для повышения экономической эффективности. От качества телефонной связи, в конце концов, зависят экономические показатели предприятия. Телефонная связь позволяет быстро передавать информацию внутри компании и, конечно же, позволяет вести конструктивное общение с клиентами корпоративных образований, которые и приносят конечный доход.

От того насколько эффективно будет использоваться телефонная связь корпоративных образований, насколько качественно будет реализован весь потенциал, которого достигла телефония на данный период времени, и будет зависеть благосостояние предприятия как показано на рисунке 1.

В середине первого десятилетия XXI века технический прогресс глубоко проник и в такую услугу, как телефонная связь. На рынок обеспечения телефонной связи корпоративных образований вышла новая, более гибкая, более функциональная, а главное, намного менее затратная технология – IP-телефония.

IP-телефония – это прорыв в области телефонной связи. Впервые телефонная связь внутри компании стала мобильной, легко разворачиваемой с нуля, и наращиваемой без существенных дополнительных финансовых вливаний. Дополнительный функционал, который она предоставляет, включает, в первую очередь, интеграцию телефонного сервиса с существующими информационными системами предприятия, разнообразными базами данных и прочее. Телефонная связь позволяет быстро передавать информацию внутри компании и, конечно же, позволяет вести конструктивное общение с клиентами корпоративных образований, которые и приносят конечный доход. Также возможна рассылка важной информации среди сотрудников компании, например, курса валют, котировки ценных бумаг и др.

Правильное применение новых возможностей, которые даёт IP-телефония, выводит корпоративные образования на новых виток экономической эффективности.

Конечно же, IP-телефония не идеальна. В первую очередь, это надёжность IP-телефонии, которая ниже надёжности аналого-цифровых АТС. В сравнении с первыми версиями разработок IP-телефонии, которые допускали искажение и прерывание речи, качество связи по всем характеристикам значительно улучшилось. Качество работы IP-телефонии можно оценить, используя следующие основные параметры:

– уровень искажения голоса;
– частота "пропадания" голосовых пакетов;
– время задержки.

В аппаратной части проблемы появляются из-за того, что сети IP-телефонии проектировались исходя из требований передачи данных, а отнюдь не для голосового трафика. Для сокращения задержек, до уровня позволяющего получить устойчивый сигнал, приходится дополнять системы специальными средствами обеспечения гарантированного уровня качества обслуживания (QOS – Quality-Of-Service). Однако, при внедрении IP-телефонии на предприятии, часто необходимо проводить модернизацию телекоммуникационной сети с сохранением существующего уровня качества связи.

Но с каждым годом показатели качества небольшими шажками приближаются по значению к эталонным. Безопасность телефонных разговоров тоже не находится на высшем уровне, но как и надёжность, этот показатель растёт из года в год.

Таким образом, можно сделать вывод – корпоративная организация, которые не совершенствуют организацию своей телефонной связи, заведомо оказываются в проигрышной ситуации. И как следствие, с увеличением эффективности и качества услуг IP-телефонии будет расти и экономическая эффективность корпоративных образований.

МОДЕЛЬ ФОРМИРОВАНИЯ ТРАНСПОРТНОЙ СЕТИ

Н.Х.Гультураев (ТУИТ, доцент)

Для создания эффективной и надежной транспортной сети VPNв виде наложенной сети связи необходимо использовать модели и алгоритмы разработанные на основе математического аппарата теории телетрафика, методов теории связи и теории графов. Они позволяют определить необходимую минимальную пропускную способность виртуальной транспортной сети (ВТС), которую требуется выделить из ресурса магистральной первичной сети связи общего пользования (ССОП). Основное отличие предложенной математической модели и алгоритма формирования ВТС: совместный учет топологической структуры первичной сети связи, на базе которой реализуется ВТС, и непосредственно топологической структуры ВТС; учет информации о количестве и распределении трафика конечных точек ВТС, возможных алгоритмов маршрутизации потоков и ограничений на сетевые ресурсы.

Теоретически и практически показана принципиальная возможность создания транспортной сети связи (ТС) организации (ведомства) с заданными параметрами надежности и качества обслуживания в виде виртуальной сети связи (ВСС).

Можно задать магистральную первичную ССОП в виде неориентированного графа *G(MN)* без петель и контуров. Множество вершин $M = \{a_1,a_2,...,a_m\}$ *E G*соответствует узлам сети (маршрутизаторы), где *m*— число вершин в графе *G(\M\).* Множество ребер *N*= { / j , r 2 , с *M* x *M* € *G*соответствует звеньям сети, связывающим узлы а, и a_1 каналами связи между этими узлами. Звеньям сети графа *G(MN)*приписаны веса (длина звена), которые заданы матрицей в направлении от вершины.

Модель ТС как виртуальной сети связи может быть представлена в виде ненаправленного графа G^{BTC}(M'A). В таком варианте ВТС представляет собой не-направленный граф, для которого выполняются следующие условия: в графе нет петель; существует только одна вершина *ie W, WCM'*, не имеющая входящих в нее ребер.

В качестве структурного ограничения принимаем, что ВТС имеет специальную структуру в виде древовидной топологии. Следует отметить, что древовидная топология для соединения конечных точек ВТС легко масштабируема и позволяет достаточно просто реализовать процессы маршрутизации и резервирования. Особенностью графа древо-видной топологии является то, что он может быть разделен на две соединенные компоненты путем удаления любого ребра.

Произведя соответствующие математические преобразования, с учетом принятых допущений и ограничений можно получить математическую модель транспортной сети в виде виртуальной сети.

ПОВЫШЕНИЕ ЖИВУЧЕСТИ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ

Н.Х.Гультураев (ТУИТ, доцент)

Современные условия эксплуатации сетей электросвязи диктуют необходимость повышения устойчивости их работы. На функционирование сетей негативно влияет множество факторов: недостаточная автоматизация технологических процессов, рост числа внешних воздействий (чрезвычайные ситуации, террористические акты), постоянно увеличивающийся парк оборудования и т.д.

В сложившихся условиях необходимо разрабатывать и внедрять мероприятия, позволяющие повысить устойчивость функционирования транспортной сети связи. Один из способов повышения устойчивости направлен на сокращение времени восстановления работоспособности сети в условиях отказов и внешних неблагоприятных воздействий. При этом важно сформировать такую конфигурацию сети и режим работы оборудования, которые обеспечатпереход на резервный маршрут за максимально короткое время.

В настоящее время транспортная сеть на базе технологии SDH позволяет организовать резерв только при кольцевой топологии включения, но такая топология по техническим причинам не всегда возможна. В случае выхода из строя оборудования или линейного тракта, в том числе из-за несанкционированных действий злоумышленников, переход на резерв осуществляется вручную. Как показывает практика, подобные переключения могут занимать значительное время, приводя к довольно длительному перерыву связи или срыву плановых работ из- за неготовности для замены трасс компонентных потоков Е1. Кроме того, эта система не позволяет избирательно переводить компонентные потоки Е1 на другое направление, уменьшая тем самым трафик сети связи на основной трассе.

Во многих существующих транспортных сетях задействовано оборудование разных производителей, причем компонентные информационные потоки жестко привязаны к системе передачи конкретного направления. Из-за этого у администратора сети нет возможности перераспределить нагрузку в автоматическом режиме, что значительно снижает пропускную способность сети в целом.

Для повышения живучести транспортной сети связи необходимо осуществлять проект по внедрению оборудования систем передачи синхронной цифровой иерархии ZTE. В результате реализации проекта вместе с системами DWDMи CWDMбудут необходимо введены в эксплуатацию мультиплексоры уровня STM-16 и STM-4..

При этом наряду с системами синхронной цифровой иерархии ZTEпредлагается использовать мультиплексоры МЦП-155К и СМК-30 в качестве основы сети автоматической коммутации.

Возможность совместной работы мультиплексоров при разных топологиях сети с учетом небольшой реконфигурации первичной сети при ее модернизации была проанализирована в лаборатории связи. Исследования показали, что автоматическая коммутация потоков Е1 на ZTESDH, МЦП-155К и СМК-30 возможна при любой топологии включения при наличии альтернативного маршрута вне зависимости от пути прохождения компонентного потока Е1 или STM-N.

Следует отметить, что данное оборудование имеет возможность использования блока SNC, с помощью которого можно организовать переход на резервное оборудование на уровне контейнера VC-12 (VC-4). В таком случае при нарушении целостности одного из полуколец на резерв перейдут только те потоки, для которых программно указан резерв на случай аварии основной трассы.

Реализация предложенного решения позволила осуществлять автоматическое переключение на резервные потоки при обнаружении неисправности на основном. Перерыв трафика при этом составляет 2-3 с, а обратный переход происходит в течение 60 с без нарушения связи. Алгоритмы работы оперативно-технического персонала при выполнении ручного и автоматического резервирования транспортной сети связи реализуются достаточно просто. При сравнении алгоритмов наглядно видно, что благодаря автоматическому резервированию исключаются несколько организационно-технических процедур и практически не происходит перерыва связи. Итак, в результате анализа работы транспортной сети и ее трафика были сделаны следующие выводы:

-существует техническая возможность организации на SNCрезерва компонентных потоков Е1, причем такой резерв может быть организован избирательно согласно технической необходимости через различные системы передачи;

-время перехода на резерв и обратно задается программно;

-возможна организация совместной работы оборудования SDHразличных производителей.

Для повышения живучести транспортной сети связи необходимо модернизировать существующую схему связи можно путем установления мультиплексоров, позволяющих автоматически переходить на резервные потоки, в том числе потоки STM-Nвне зависимости от топологии сети. Главным преимуществом этой схемы является возможность программного выбора администратором транспортной сети связи различных маршрутов прохождения компонентных потоков как для основного, так и резервного направлений.

Следует отметить при этом, что чем больше будет организовано альтернативных маршрутов, тем оптимальней распределится нагрузка по сети. Это будет содействовать значительному повышению ее живучести.

ОСОБЕННОСТИ ВЗАИМООТНОШЕНИЙ ОПЕРАТОРОВ СВЯЗИ ДЛЯ ПОДДЕРЖКИ QoS

Х.Р. Давлетова (ТУИТ, ассистент)

С широким внедрением мультисервисных сетей преобладающим должен стать подход к нормированию уровня качества обслуживания клиентов на основании требований со стороны самих абонентов к качеству предоставляемых услуг. С учетом требований абонентов оператор может

формировать исходные параметры QoS, которые определяют требуемый уровень качества предоставления услуг. Оператору необходимо иметь возможность гарантировать этот уровень качества. Современный подход к определению гарантированного уровня качества заключается в разработке соглашений о качестве обслуживания (SLA) между оператором связи и теми пользователями (потребителями услуг), которые готовы оплачивать подобные возможности по более высоким тарифам.

Предоставление новых услуг подразумевает создание решений для их поддержки, управление услугами и обеспечение их высокого качества. Одним из главных моментов при этом является техническое обеспечение заданного уровня QoS. Это касается как реализации необходимой скорости передачи данных в сети абонентского доступа, так и обеспечения требуемого качества обслуживания трафика в пределах магистральной сети.

Также важной задачей, от решения которой во многом зависит успешное предоставление услуг, является задача управления. В рамках концепции построения NGN этот компонент сетей также претерпел значительные изменения. Оператору, кроме инфраструктуры самой NGN, Необходимо создавать новую или совершенствовать уже используемую систему управления сетью. Это связано с пересмотром приоритетов среди задач управления. Если раньше для управления сетью было необходимо управлять работой оборудования, то сегодня на первый план выходит управление услугами связи и качеством их предоставления.

Кроме этого, к задачам управления следует отнести поддержку бизнеса оператора –не только обеспечение взаимодействия диспетчера с клиентом (техническая поддержка), но и гибкая тарификация услуг (передача различных видов трафика с учетом требований SLA , поддержание большого количества тарифных планов, скидки т.д.).

Следовательно, с позиций управления услугами можно сформулировать ряд требований, которым должна отвечать сеть оператора связи:

•предоставление абоненту возможности выбора услуг из их широкого набора услуг;

•обеспечение гибкого управления услугами, как со стороны потребителя услуг, так и со стороны провайдера;

•определение перечня параметров SLA , методов и механизмов их контроля;

•гарантирование оператором связи гибкости и точности систем учета и расчетов за услуги.

SLA – наилучшее средство для удовлетворения конкретных требований по QoS при обеспечении оптимального соотношения стоимость/качество, как для пользователя, так и для поставщика услуг. Целью SLA является определение общего качества процесса управления, используемого поставщиком услуг и клиентом, в том числе – управление повреждениями, сбор статистики для проведения профилактики, использование статистики.

Оператор связи, заключающий SLA с потребителем услуг, гарантирует обеспечение определенного уровня качества. Однако, качество предоставления услуги, как правило, зависит от нескольких взаимодействующих друг с другом операторов связи, через сети которых проходит маршрут доставки данных. Следовательно, операторы должны определить такой механизм взаимодействия, при котором обеспечивается гарантируемое качество предоставления услуги. При этом могут применяться разные подходы.

Например, возможно определить равные нормативы для сетей всех операторов, участвующих в предоставлении услуги, которые обеспечивают выполнение норматива по доставке данных из конца в конец.

Однако такой подход не всегда применим. В общем случае, техническое оснащение и возможности сетей связи различных операторов могут быть различны.

Это приводит к тому, что показатели качества обслуживания трафика в сетях разных операторов могут быть не идентичны. Поэтому, уравнительный подход может привести к дополнительным расходам некоторых операторов, которые не будут восполнены доходами от предоставления услуги. В ряде случаев такое распределение нормативов может привести к необоснованно высокому качеству обслуживания, которое не востребовано пользователями, а ряде случаев выполнение норматива может быть вообще невозможно, например, когда маршрут в сети одного из операторов проходит по кабельной линии связи, а в сети другого оператора по спутниковому каналу.

Таким образом, при распределении (декомпозиции) нормативов качества обслуживания нужно допускать возможность достаточно широкого диапазона изменения качества обслуживания в рамках сети каждого из операторов.

При этом норматив качества обслуживания на участке UNI-UNI выполняется при различной степени участия операторов. При этом оператор, в сети которого, норматив не выполняется "заимствует" ресурсы сети другого оператора, в сети которого качество обслуживания выше. При этом декомпозиция показателей качества является не только технической, но и экономической задачей, при решении которой необходимо учитывать расходы и доходы операторов при совместной работе по предоставлению услуг связи.

СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Х.Р. Давлетова (ТУИТ, ассистент)

Облачные вычисления- это модель предоставления вычислительных ресурсов по требованию, охватывающая всё, начиная от приложений до центров обработки данных, через Интернет при условии оплаты за фактическое использование. Такой подход к организации вычислений дает небывалые возможности клиентам, независимо от мощности их компьютеров и при этом обеспечивает доступ к облаку миллионам пользователей в каждый момент. Однако, при такой заманчивости использования облачных платформ, пользователи предъявляют к ним и высокие требования, связанные с сохранностью данных и их защищенностью.

Поставщики облачных решений хранят данные на своих сервисах с использованием избыточности, что само по себе гарантирует надежность.

Дополнительно к этому, на любом из устройств, подключенных к "облаку", хранится, ещё как минимум, еще одна актуальная копия данных.

Лучший способ защиты расположенных в хранилище данных – использование шифрования. С целью предотвращения случаев неправомерного доступа, провайдер должен шифровать хранящуюся на своих серверах информацию клиента, безвозвратно удалять данные, когда они больше не нужны и не потребуются в будущем.

Передаваемые данные должны быть зашифрованы и доступны пользователю только после аутентификации. Это является гарантией того, что эти данные не сможет изменить или прочитать ни одно лицо, даже если оно получит к ним доступ посредством ненадежных узлов сети. Эти технологии давно известны, созданы надежные протоколы и алгоритмы, такие как TLS, IPsec и AES.

Самым распространенным способом аутентификации является защита паролем. Однако некоторые провайдеры, для обеспечения более высокой надежности, прибегают к помощи таких средств, как сертификаты и токены. На сегодняшний день практически каждая крупная IT-компания стала поставщиком облачных услуг.

Облака стали определяющим вектором развития ИТ. Они постоянно развиваются, дополняются новыми сервисами, инструментами развертывания этих сервисов и самой облачной среды, средствами управления, возможностями автоматической миграции виртуальных машин.

Лучший способ защиты расположенных в облачном хранилище данных – использование шифрования. Передаваемые данные должны быть зашифрованы и доступны пользователю только после аутентификации. Это гарантирует эти данные не сможет изменить или прочитать ни одно лицо, оно получит к ним доступ. Примером надежных протоколы и алгоритмов TLS, IPsec и AES.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ОПТИЧЕСКИХ КОММУТАТОРОВ

Н.Н. Зуфарова (ТУИТ, магистрант)

Современные оптические коммутаторы в основном строятся на основе двух структур. Для более простой из них характерно использование координатных (матричных) коммутаторов. Линии входных и выходных оптических каналов образуют прямоугольную сетку. В случае ОЕО коммутаторов эта сеть обычно образована электронными ключами. В полностью оптических коммутаторах вместо электронных ключей применяются оптические ответвители (opticalcouplers). При этом различные порты соединяются между собой путем задания различных положений этих ответвителей.

Оптический коммутатор – один из самых важных волоконно-оптических элементов, который поддерживает сетевую работоспособность и является гибкой платформой для маршрутизации сигнала.

В настоящий момент в стадии разработки находятся два основных типа коммутаторов оптических сигналов: оптические коммутаторы (all-optical switches), которые называют также прозрачными, световыми (photonic) или ООО (optical-optical-optical) коммутаторами, и оптико-электрооптические коммутаторы, называемые также непрозрачными или ОЕО (optical-electrical- optical) коммутаторами. Полностью оптические ООО - коммутаторы принимают оптический сигнал на входе, осуществляют его коммутацию, и направляют через оптический выход далее безпреобразования в электрический сигнал. Оптико-электрооптические ОЕО-коммутаторы принимают оптические сигналы на входе, преобразуют их в электрические сигналы, осуществляют процесс коммутации при помощи электронных компонентов, при этом могут выполнять определенные функции, такие как, например, поиск адресов в базе данных

маршрутизации, после чего вновь преобразуют электрический сигнал в оптические сигналы на выходе.

Оптические коммутаторы преследуют единую цель – увеличение эффективности сетей с помощью гибкой переадресации трафика, разница в их технологических подходах существенна. Каждый из применяемых методов имеет свои достоинства и недостатки, что порождает не только конкуренцию технических решений, но и их технологическую несовместимость. То есть их одновременное внедрение может привести к созданию двух типов оптических сетей, работающих на различных принципах. Именно этот фактор, по нашему мнению, тормозит внедрение новых типов оптических коммутаторов, поскольку ведущие производители сетевого оборудования и сетевые провайдеры до сих пор не пришли к единому мнению, какой из этих двух видов коммутаторов им лучше избрать. Различия в физических принципах действия и в методах управления разными типами коммутаторов, отличия их интерфейсов и отсутствие общепринятых стандартов, и при этом необходимость разработки специализированного программного обеспечения, усложняют выбор. Поэтому в настоящее время мало кто берется предсказать, возможно ли общее решение для всех коммутаторов, применяемых в настоящее время в разнообразных оптических сетях.

В то же время, очевидно, что осуществление коммутации информационных пакетов на фотонном уровне, без промежуточного превращения их в электрические сигналы, позволяет избежать высоких расходов, связанных с преобразованием сигналов, а самое главное, позволяет на несколько порядков увеличить скорость передачи информации.

К сожалению, на сегодняшний день эта идея пока не вышла за пределы исследовательских лабораторий и до ее практической реализации еще весьма далеко. Сегодня еще невозможно обойтись без совместного присутствия в сетях и фотонов, и электронов. Оптико-электрооптические коммутаторы могут извлекать служебную сетевую информацию, например, адресную, и восстанавливать затухающий сигнал. На сегодняшний день ни одна из этих функций не может быть выполнена исключительно оптическими средствами.

И все же, поскольку непрозрачные коммутаторы не в состоянии в полной мере обеспечить те характеристики масштабируемости и независимость протоколов, которые свойственны прозрачным коммутаторам, сосуществование обеих технологий, по всей видимости, будет сохраняться. В то время как непрозрачные коммутаторы применяются для организации доступа к упорядоченному трафику, прозрачные коммутаторы используются в центральной части сети либо для агрегации данных с целью повышения скорости передачи через порт, либо для обеспечения ремаршрутизации трафика в случае отказа одного из сегментов сети без преобразования сигналов в электрическую форму. По мере того как усиливаются возможности оконечных коммутаторов засчет DWDM и интеллектуальной маршрутизации, эти коммутаторы, обладающие улучшенными возможностями упорядочения трафика, могут обрабатывать все большее число каналов. В результате этого создаются благоприятные условия для расширения масштабов применения методов оптической коммутации в сети.

В полностью оптических сетях коммутаторы применяют для того, чтобы при возникновении неисправностей в сети направить сигнал по другому оптическому пути или через другую сеть.

Делая вывод стоит отметить что оптические коммутаторы обеспечивают высокую надежность передачи данных.

ОБЗОР ОСОБЕННОСТЕЙ ОПТИЧЕСКИХ КОММУТАТОРОВ

Н.Н. Зуфарова (ТУИТ, магистрант)

В настоящее время трафик приложений в сети растёт в геометрической прогрессие, а с развитием виртуализации появляются новые решения и сервисы, для которых рекомендуемые скорости интерфейсов на оборудовании уже составляют 10Гбит/с. Для малого и среднего бизнеса на сегодняшний день выгодно использовать технологию Ethernet — как для подключения пользователей, серверов, телефонии и прочего, так и для подключения систем хранения, т.е. организации SAN. Ниже будет рассмотрен коммутатор с 24 10Gb оптическими портами. Коммутатор Dell Power Connect 8132F обладает «джентльменским» набором, который позволяет внедрить большинство современных медиа-услуг: поддержка большинства стандартных L2-протоколов и безопасности (spanning-tree, LACP, VRRP, Dynamic ARP Inspection, 802.1x и т. д.); поддержка маршрутизации — 512 IPv4 / 256 IPv6 статических маршрутовподдержка RIP и OSPF; поддержка мультикаст-протоколов PIM-SM и PIM-DM; поддержка средств QoS и управления;

Одно из многих достоинств коммутатора — возможность увеличения количества портов картами расширения с 24 до 32 портов 10Gbps или добавления карты с 2-мя интерфейсами по 40Gbps QSFP. Можно ё поддержкой функционала DCB (data center bridging), является технология для оптимизации iSCSI, которая автоматически определяет и настраивает коммутатор при подключении систем хранения Dell EqualLogic.Кроме того существует модель с медными 10GbE портами Dell Power Connect 8132. В заключении стоит отметить что, Dell Power Connect 8132 предоставляет большой набор дополнительных функций такие как поддержка большинства стандартных L2-протоколов и безопасности (spanning-tree, LACP, VRRP, Dynamic ARP Inspection, 802.1x и т. д.), поддержка маршрутизации — 512 IPv4 / 256 IPv6 статических маршрутов, поддержка RIP и OSPF, поддержка мультикаст-протоколов PIM-SM и PIM-DM, поддержка средств QoS и управления. Все выше перечисленные дополнительные функции позволяют обеспечить высокую надежность передачи данных а также позволяет сделать систему очень гибкой. более того настройка оборудования происходит в облегченной форме , а это позволяет инжинерам легко эксплуатировать данный коммутатор, техническая поддержка на данный комутатор предоставляется на более 3 года.

ЯНГИ ТЕХНОЛОГИЯ АСОСИДА ШАКЛЛАНГАН ОПТИК ТОЛАЛАР

Д.Х.Ибатова (ТАТУ, ТИ кафедраси катта ўқитувчиси)

Фотон кристалли толалар - Photonic-crystal fiber (PCF), оптик толанинг янги тури бўлиб фотонли кристаллар, яримўтказгичнинг кристалл тузилишини мунтазам умумлаштирилган макромодели хисобланади. Фотон кристалли оптик толалар янги турдаги оптик тўлқин узатгичлар хисобланади.

Толали оптик узатиш тизимлари учун бир модали оптик толанинг ўтказиш қобилияти жуда юқори. Хозирда кенг полосали толали оптик узатиш тизимларида частота оралиғи кенглиги 10 ТГц да (DWDM – зич тўлқин узунлиги бўйича зичлаштирилган тизимларда). Фақатгини бир модали оптик толанинг асосий камчилиги – бу ўзакнинг кўндаланг кесими эффектив майдонининг жуда кичиклигидир. Оптик оқим қуввати зичлигини ортиши оптик толада турли тартибдаги ночизиқли эффектлар сатхини ўсишига олиб келади. Ночизиқли эффектларнинг харакати хатоликлар сонини ошишига, секция узунлигини камайишига, бир каналли тизимларда рухсат этилган узатиш тезлигини камайишига, кўп каналли тизимларда ташувчи частота қадамини ортишига олиб келади.

Юқорида келтирилган муаммоларни ечиш мақсадида фотон кристалл асосидаги толалар ишлаб чиқилган. Фотон кристалли толалар оптик тола қобиғида шаклланадиган “кварцли шиша - хаво” композицияси асосидаги икки ўлчамли фотонли кристалл тузилишини ўзида намоён этади.

Фотон кристалли толалар – (ФКТ) оптик тўлқин узатгичларнинг янги синфидир. Икки ўлчамли фотон кристалли толанинг симметрик текислигини кўндаланг кесими нуқтали камчилик билан қайта ишлаб чиқарилади.

Икки ўлчамли ФКнинг тузилиши, ўзак мухити атрофида симметрик жойлашган олти қиррали ёки доира шаклидаги зич жойлашган диэлектрик найлардан иборат жуда ингичка найчалар ёрдамида қобиқда шаклланади. Бу найчалар доимий панжарали даврий кристалл панжарани хосил қилади. Бундай тузилиш фотон таъқиқланган сохани шакллантириши мумкин.

ФКТнинг иккита асосий тури мавжуд:

- Юқори синдириш кўрсаткичли ўзаги тоза кварц шишадан иборат ва унинг қобиғини атрофи эффектив (қуйи) синдириш кўрсаткичи билан характерланадиган, икки ўлчамли фотон кристалл тузилишли ФКТ. Ушбу ФКТ учун характерли бўлгани бу унинг оддий оптик толага ўхшашлиги, яъни ёруғлик тўлиқ ички қайтиш (ТИҚ) шарти асосида ўзак бўйлаб тарқалади, фотонли таъқиқланган соха хеч қандай таъсир қилмайди. Бу ФКТ – ТИҚ туридир (1 а-расм);
- Паст синдириш кўрсаткичли ўзаги бўшлиқли (хаволи) ва унинг қобиғини атрофи эффектив (ўзакка нисбатан юқори) синдириш кўрсаткичи билан характерланадиган, икки ўлчамли фотон кристалл тузилишли ФКТ. У оддий оптик толага ўхшамайди, унда ТИҚ шарти бажарилмайди. Шаклланган фотонли таъқиқланган соханинг (ФТС) тарқалишни чеклайдиган ва йўналтирувчи каби хусусиятлари туфайли, ёруғлик мода ўзак мухитининг бўшлиғи бўйлаб йўналади. Бу ФКТ – ФТС туридир (1 б-расм).

а) б)

1-расм. Фотон кристалли толанинг тузилиши: а- тўлиқ ички қайтишли ФКТнинг кўндаланг кесими; б- фотон таъқиқланган сохали ФКТнинг кўндаланг кесими.

Тола узунлиги бўйича жойлашган бу каналлар ўзак атрофидаги синдириш кўрсаткичини локал тарзда камайтиради ва шундай қилиб оддий тола қобиғини эффектив тарзда ўзгартиради.

Кичик букилишларда йўқотувчанлиги камайтирилган янги микроструктуралаштирилган HAF (Holed assisted fiber) туридаги оптик толалар жавоб беради. Бу ғояни яратишда икки қатламли ҳимояловчи тўсиқ нанотехнология ёрдамида бажарилган. Унда кварцдан тайёрланган ўзак атрофида иккита олти бурчакли ҳалқа тўлиқ ҳаво тешикларидан иборат бўлиб, у кварц/ҳаво бўлиниш чегарасида тўлиқ ички қайтишни таъминлаб беради. Иккинчи қатлам эса биринчи тўлиқ тузилма чегараси ташқарисидан бир мунча ўтиб нурлантирилган ёруғлик нурларини қайтариш учун қўлланади.

ФКТ катта сонли апертурага эга бўлиши мумкин, бу эса уларга нурланишни киритишни енгиллаштиради. ФКТда ночизиқли оптик эффектлар сўндирилиши ёки кучайтирилиши мумкин. Хозирги вақтда ФКТда йўқотишлар оддий турдаги оптик толаларга қараганда бир мунча ортиқ. Бу эса фотонли кристални тайёрлашнинг технологик жараёни мураккаблиги келтириб чиқарган фотонли кристалл тузилишининг мукаммал эмаслиги билан боғлиқдир. Бўшлиқ ўзакли ФКТлар назарий 0.0005 дБ/км сатхидаги йўқотишга эга бўлиши мумкин. Хозирги вақтда олинган ФКТнинг узунлиги 10-100 м га етади.

Умуман олганда хозирги кунда ФКТ оптик кучайтирувчи қурилмаларда ва лазерли юқори самарали коммутация шнурларини яратиш учун, шунингдек тармоқлагичларда қўлланилади.

ФКТ нинг яна бир керакли қўлланилиш сохаси – бу дисперсияни компенсацияловчи модуллар (DCM). ФКТлар оптик импульсларни кенгайишини компенсациялаш учун кўп каналли толали алоқа линияларида қўлланилиши учун истиқболли хисобланади.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОПТИЧЕСКИХ СИСТЕМ СВЯЗИ

Р.И. Исаев (профессор кафедры ТИ, ТУИТ)
А.А. Абдукадиров (магистрант ТУИТ)

Высокие требования, предъявляемые к современным системам телекоммуникаций (высокая скорость передачи информации, надёжность, защищённость от несанкционированного доступа), привели к осознанию неоспоримого преимущества оптических систем связи. В связи с глобализацией телекоммуникации возникла проблема защиты информации в оптических системах связи. Утечка информации в результате несанкционированного доступа имеет первостепенное значение. Изначально оптические системы связи имеют более высокую степень защищённости информации от несанкционированного доступа, чем какие-либо иные системы связи, что связано с физическими принципами распространения электромагнитной волны в оптическом волокне. В оптическом волокне электромагнитное излучение выходит за пределы волокна на расстояние не более длины волны при отсутствии внешнего воздействия на оптическое волокно. В таблице сравнительный анализ электрических и волоконно-оптической среды передачи информации и возможные виды угроз.

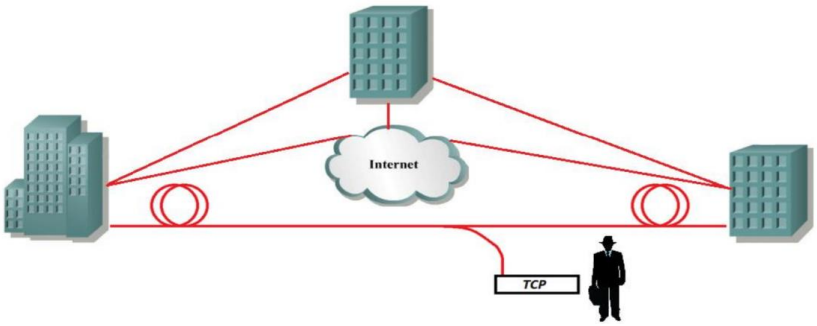
Таблица

Свойство	**Электронный транспорт**	**Фотонный транспорт**
Носитель	Электрон: заряженная частица $e=1{,}6\cdot10^{-19}$ Кл с массой покоя $m_e=9{,}1\cdot10^{-31}$ кг	Фотон: незаряженная частица с нулевой массой покоя
Среда	Проводник: медь, алюминий, сталь	Диэлектрик: плавленый кварц, стекло, оптические пластмассы
Реализация	Медный кабель (коаксиальный кабель, витая пара и тд.)UTP 5 cat: 100 MHz, 100 m, 22dB/100m	Оптический кабель (многомодовое, одномодовое волокно)SMF: 40 GHz, 100 km, 0.2 dB/km, 1550 nmдолговечность, надежность
Угрозы	ПЭМИН, несанкционированный съем информации	ПЭМИН отсутствует, несанкционированный съем информации

Одним из характерных угроз волоконно-оптическим системам связи является угроза безопасности информации - перехват трафика путем несанкционированного доступа к оптической транспортной сети телекоммуникации.

Перехват трафика - получение доступа к информационным потокам, передаваемые через оптическую транспортную сеть телекоммуникации, телефонную сеть, сеть кабельного телевидения, сети систем безопасности, измерительные и другие сети объекта информатизации, которые построены на основе внутренней оптической кабельной

инфраструктуры объекта и с выходом за пределы объекта информатизации и контролируемой зоны.



Сценарий перехвата трафика. Содержит следующие этапы:

I. Выявление топологии кабельной инфраструктуры, определение расположения коммутационных элементов.

II. Определение типа оптического кабеля, волокна и выявление характерных неоднородностей кабельной системы – мест установки оптических муфт, мест сварки и разъемных соединений.

III. Подбор специальных технических средств, подключение к уязвимым местам оптического канала и реализация съема информации.

IV. Проведение мероприятий по повышению эффективности перехвата трафика.

V. Регистрация сигнала утечки информации и перехват трафика.

Нарушители выявляют топологии оптической сети и её особенностей. Например, кабель внешней прокладки (между объектами) имеет следующие особенности:

– в конструкции присутствуют металлические усиливающие и защищающие элементы;

– специальный кабель может быть полностью диэлектрическим;

– прокладка – подземная, подвесная и подводная;

– возможно использование городских и междугородных коммуникаций;

– для соединения используются соединительные муфты, регенераторы и оптические усилители.

Предлагается ряд научно – обоснованных методов защиты трафика оптических транспортных сетей телекоммуникации.

Оптические системы связи, системы передачи данных могут быть подвержены угрозе перехвата передаваемой информации. Технология защиты трафика требует анализа технических возможностей поиска и подсоединения к оптическому каналу, защита трафика зависит от технических и организационных возможностей нарушителя. В перспективе, предполагается использование квантовой криптографии и других методов защиты.

АНАЛИЗ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕМЕЙСТВА ПРОТОКОЛОВ IPV6

Р.И.Исаев (ТУИТ, профессор кафедры ТИ)
Ж.Б.Тлеумуратов (ТУИТ, магистрант 2 – го курса)

Информационные технологии успешно внедряются во все сферы человеческой деятельности. Всемирная сеть Интернет с помощью стека протокола TCP/IP и единого пространства объединяются не только в корпоративные и ведомственные сети, но и в отдельные сети пользователей. Поэтому одной из задач проектирования межсетевого протокола IPv6 было повышение требований к безопасности по сравнению со своим предшественником, протоколом IPv4. На основе протокола IPv6 лежит утверждение, что IPSec должен использоваться в данном протоколе по умолчанию. Однако, в большинстве практических случаев, при использовании IPv6, протокол IPSec не

используется вообще. К тому же в новых протоколах, которые лежат в основе стека протоколов IPv6, найдено множество уязвимостей. С целью устранения таких уязвимостей были разработаны специальные механизмы безопасности:

Протокол CGA (“Cryptographic generated address”), который позволяет генерировать IPv6 адрес на основе криптографических алгоритмов и позволяет предотвратить подмену IPv6 адресов в сети.

Каждый из механизмов безопасности требует более детального анализа, который позволит выявить оставшиеся уязвимые места в семействе протоколов IPv6 и найти возможные векторы атак в самом алгоритме защиты.

В протоколе CGA данный механизм позволяет создать уникальный IPv6 адрес, который считается невозможным подменить за разумное время, не зная всех параметров, на основании которых генерируется CGA. Главная идея протокола CGA состоит в том, чтобы создать идентификатор интерфейса (правые 64 бита) IPv6 адреса при помощи вычисления криптографического хэша публичного ключа устройства. Затем приватный ключ может быть использован для подписи исходящих от устройства сообщений. Для того чтобы проверить подпись получателю необходимо знать: исходный адрес, публичный ключ и значения дополнительных параметров. Данный процесс не связан с глобальной инфраструктуры открытых ключей (“Public Key Infrastructure, PKI”), не требует никаких дополнительных центров сертификации и доверительных сторон.

Рассмотрим протокол IPv6 IPSec в Requestforcomments (RFC) 2460 указано, что безопасность IPv6 рассматривается в стандарте, который посвящен IPsec. В текущем стандарте, посвященном требованиям, которые предъявляются к конечным узлам, указано, что IPsec является лишь рекомендательным средством безопасности, в отличие от старой версии этого же стандарта, где IPsec был обязателен для использования. Главной трудностью реализации IPsec в IPv6 по умолчанию является создание стандартизированной PKI, которая смогла бы обслуживать все устройства в Интернет. Также существуют трудности стандартизации и других областей, таких как, например, создание единой базовой конфигурации на конечных устройствах и устранение терминологической путаницы при создании подобной конфигурации (на данный момент, многие производители сетевого оборудования обладают своей специфической терминологией). Или проблема стандартизации технических моментов, например, какой механизм управления ключами использовать по умолчанию IKEv1 или IKEv2. На данный момент уже создано множество наработок в данной сфере, например, существует ряд RFC публикаций, такие как: описание IPsec PKI профилей IKEv1, IKEv2 и PKIX ; использование IPsec для защиты туннелей IPv6-в-IPv4; мобильные IPv6 и IKEv2. Подобных стандартов, которые относятся к IPsec-v3, можно перечислить целую массу, именно поэтому в 2011 году появилась публикация с дорожной картой, которая содержит краткие выжимки и пояснения множества различных стандартов, относящихся к IPsec и IKE. Следует отметить, что в стандартном RFC, посвященном IPv6, ссылка в разделе о безопасности указывает на устаревшую версию протокола IPsec (RFC 2401). В 2005 году в свет вышел RFC 4301, в котором описан IPsec-v3. Ключевым изменением является то, что в новом стандарте появилось такое понятие как PAD (“PeerAuthenticationDatabase”). Данная база содержит информацию, необходимую для аутентификации узла, чтобы обеспечить связь между протоколом IPsec и протоколом управления ключами (например, IKE). Ведутся работы и в области IKE протокола. На данный момент, выпущен черновой вариант RFC публикации, в котором описан IKEv3.

IPsec предусматривает процедуры аутентификации и шифрования. Формирование и удаления заголовка IPsec может осуществляться в машине клиента или в сетевом шлюзе.

Протокол IPsec предоставляет три вида услуг: аутентификацию (AH), шифрование (ESP) и безопасную пересылку ключей. Первые услуги, так как неавторизованный клиент

не сможет проникнуть в), а шифрование не позволит злоумышленникам прочитать, исказить или подменить сообщения. По этой причине протокол ESP предпочтительнее, так как он позволяет совместить обе эти услуги.

Следует отметить, что, несмотря на то, что IPsec еще не может быть внедрен в IPv6 протокол как стандарт обеспечения безопасности “из коробки”, все же его можно задействовать вручную. Данный протокол позволяет обеспечить две важные составляющие безопасности данных: конфиденциальность и целостность. Однако IPsec не гарантирует доступность информации.

TCP ВА UDP ПРОТОКОЛЛАРИНИНГ ЎТКАЗУВЧАНЛИК ҚОБИЛИЯТИНИ БАҲОЛАШ

Қ.А. Исманов (ТАТУ, ТИ кафедраси ассистенти)

IEEE 802.11n стандарти 2009 йилда пайдо бўлган ва 100 Мбит/секунд тезликка эришишга имкон берган асосий технологиялар OFDM (каналлар ортогонал частота бўйича ажратиладиган мультиплекслаш) ва MIMO (узатиш ва қабуллашга кўплаб антенналарни ишлатилиши) бўлди, бу технологиялар кўриб чиқиладиган Wi-Fi нимстандартининг физик даражасини ташкил этди. Wi-Fi физик даражаси 540 Мбит/секунд маълумотларни максимал узатиш тезлигини таъминлаши мумкин, бунинг учун MCS 64 кодлаш ва MIMO 4x4 (қабуллашга 4 та антенналар ва узатишга 4 та антенналар) схемаси бўйича оқимларни фазовий бўлишдан, шунингдек 40 МГцгача оширилган каналнинг кенглигидан (стандарт 20МГц кенглик ўрнига) фойдаланиш зарур бўлди. MCS 64 64 QAM-модуляциялаш ва 5/6 нисбатдаги кодлаш тезлигили BCC икккилик ўрама коддан фойдаланиш орқали амалга оширилади.

Шунга қарамай, тижорат юқори унумдор 802.11n қурилмалари маълумотларни максимал узатиш тезлиги 450 Мбит/секунддан ошмади. Алоҳида эътиборни шунга қаратиш керак бўладики, кўплаб 802.11n қурилмалари 3 тадан ортиқ бўлмаган антенналардан фойдаланиш билан бажарилган, бу кичиклаштириш ва энергия истеъмолини камайтириш мақсадида қилинган. Шунингдек таъкидлаймизки, 802.11ac стандарти пайдо бўлгунча Wi-Fi тармоқдаги ҳар бир симсиз қурилмага хизмат кўрсатиш бир вақтда эмас, балки навбатма-навбат амалга оширилган.

Бозор талаблари ва Wi-Fi уланиш нуқтасидан ката маълумотлар миқдорини кўп оқимли узатилишини ташкил этилиши заруратига биноан 2010 йилда 802.11n стандартдан «аста-секин ўтиш»ни таъминлаши керак бўлган 802.11ac стандартни ишлаб чиқишга жавоб берадиган ишчи гуруҳ яратилди. Гуруҳнинг ишлари натижаси 2012 йилнинг июнидаMCS9 (256 QAM модуляциялаш ва R=5/6 кодлаш тезлигили BCC) билан ишлашда 6933.3 Мбит/секундгача маълумотларни максимал узатиш тезлигида намойиш этилди, бунда узатиш каналининг узунлиги яна 160 МГцгача оширилди ва ҳимоя интервали 400 наносекундни, MIMO фазовий оқимларининг сони 8 тани ташкил этди.

2015 йилда 802.11ac спецификациясига мувофиқ ишлайдиган тармоқ қурилмаларининг сони бир миллиондан ошди. Бу мақолада биз IPv4 ва IPv6 тармоқларда ишлайдиган 802.11n ва 802.11ac симсиз қурилмаларининг маълумотларни узатиш тезликларини таққослаймиз. Агар сизда нима учун IPv6 тармоқлардаги тезликларни таққослаш керак деган савол туғилса,у ҳолда жавоб қуйидагича бўлади: биринчидан, IP-манзилларнинг етишмаслиги туфайли IPv6 тармоққа ўтиш шарт, иккинчидан, TCP/UDP-трафик учун барча операцион тизимлар учун IPv6 тармоқларга қараганда IPv4-протокол кичик ўтказиш полосасига эга.

Роутер ишлатадиган каналнинг кенглиги абонентлар ишлатадиган кенглик каби бўлиши керак: каналнинг кенглиги қанчалик ката бўлса, ўз-ўзидан каналнинг ўтказиш қобилияти шунчалик юқори ва демак, шунчалик юқори маълумотларни узатиш тезлиги бўлиши керак. Кўриб чиқиладиган тажрибада ҳар бир

тармоқ максимал бўлиши мумкин каналнинг кенглигига созланган, бу қурилмаларга 2.4 ГГц диапазондаги 802.11n учун 20 МГц, 5 ГГц диапазондаги 802.11n учун 40 МГц ва 802.11ac учун 80 МГц канал кенглигини беришга имкон берди.

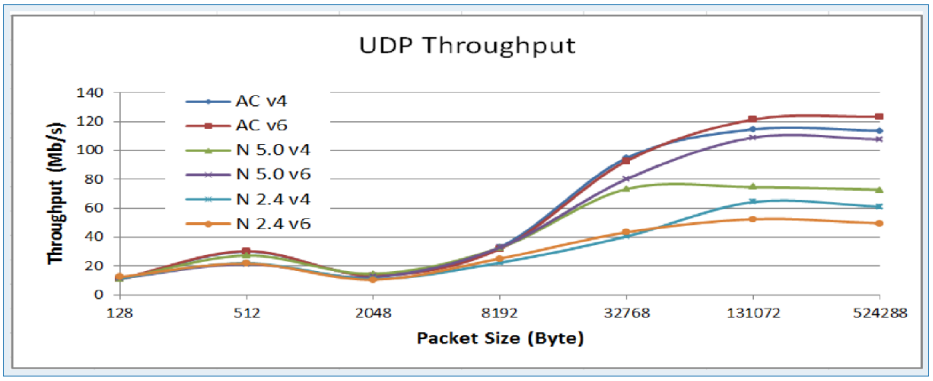
Энди узатиш учун канални танлаш ҳақида тўхталамиз. 2.4 ва 5 ГГц диапазонларда кўп сонли симсиз қурилмалар ва тармоқлар ишлайди, у ҳолда уларнинг тадқиқ қилинадиган тармоққа таъсиридан қочиб бўлмайди. Шу билан бирга, EA6500 уланиш нуқтаси оптимал узатиш каналини танлашнинг яхши (энг кам шовқинли) алгоритмига эга, бу 2.4 ГГц дипазонда 2.412 дан 2.472 ГГцгача частоталар диапазонидаги каналлар ва 5 ГГц дипазонда 5.180 дан 5 .240 ГГцгача частоталар диапазонидаги каналлар ҳисобланади, шунинг учун узатиш канали уланиш нуқтаси орқали автоматик танланади.

Тармоқни лойиҳалаштириш ва узатиш учун энг яхши канални танлашда махсус дастур ёрдамида электромагнит фонни мониторинг қилиш тавсия этилади.

Биринчи тажрибада TCP ва UDP трафикларнинг ўтказиш қобилияти ўлчанди. Иккинчи тажрибада TCP ва UDP трафикларнинг джиттери (jitter – титраш) ўлчанди. Учинчи қадамда тармоқдаги санаб ўтилган протоколларнинг кечикиши ўлчанди. Барча самарадорликни баҳолашга тестлашлар 20 секунд давомида ўтказилди. Ўлчашларнинг зарур аниқлигини таъминлаш учун пакетнинг ҳар бир ўлчами 3 мартадан узатилди, ҳисоботга учта ўлчашлар бўйича ўртача қийматлар кетди.

Назарий жиҳатдан, кўп фойдаланувчили MIMO қўлланадиган кўп сонли MIMO оқимлари, шунингдек каналнинг кенглигини 40МГц дан (N режими) 80 МГц гача (AC режим) оширилиши ҳисобига 802.11ac тармоқ 802.11n тармоққа қараганда ўтказиш қобилиятини кенгайтирди.

1-расмда тасвирланганидек, IPv6 Ac режимига энг юқори 120 Мбит/секунд маълумотларни узатиш тезлигида эришди. Алоҳида таъкидлаймизки, IPv6 N режими (2.4 ГГц) IPv6 AC режимига қараганда 2 марта секинроқ ишлади. Қараладиган графикда IPv6 802.11ac учун энг юқори нуқта ва 2.4 дипазондаги 802.11n учун энгпастки нуқта орасидаги энг ката фарқ 524288 байт пакетда кузатилди,бу ерда IPv6 AC режими 2.4 дипазондаги IPv6 N режимига қараганда 148.8% юқори (73.8 Мбит/секундга фарқ) тезликни таъминлайди.

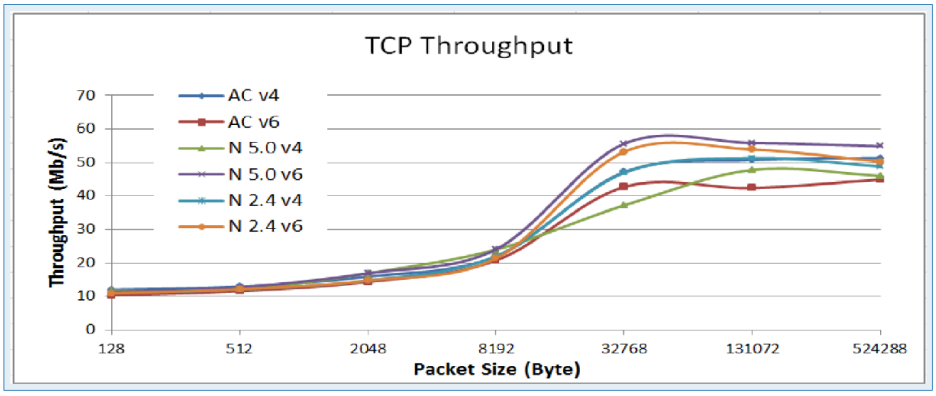


1-расм. UDP-трафикнинг ўтказиш қобилияти

Бу унча ката бўлмаган тажрибада IEEE 802.11ac ва IEEE 802.11n тармоқларнинг унумдорлигини таҳлил қилиш амалга оширилди, тестлаш эмпирик модель асосида ўтказилди.

TCP ва UDP трафикларнинг тезлиги, кечикиши ва джиттери ўлчанди. Тажрибалар натижалари бўйича биз қуйидаги хулосаларни чиқаришимиз мумкин:

Табиийки, 802.11ac стандарт 802.11n стандартга қараганда ҳам IPv4, ҳам IPv6 тармоқларда юқори ўтказиш қобилиятига эга. UDP трафикнинг ўтказиш қобилияти TCP трафикнинг ўтказиш қобилиятидан доимо кичик бўлди. 802.11ac стандартдаги UDP трафикнинг тезлиги 2.4 частотада 802.11n стандартдагига қараганда тахминан 148%га юқори бўлди.



2-расм. TCP трафикнинг ўтказиш қобилияти

Симсиз каналнинг энг юқори ўтказиш қобилияти UDP трафик учун IPv6 IEEE 802.11ac режимида олинди ва 123 Мб/секундни ташкил этди.

IPv6 тармоқ учун 802.11 ac ва 802.11n режимлари IPv4 тармоқдагига қараганда пакетнинг нисбатан паст джиттери қийматига эга бўлди.

ЯНГИ АВЛОДЛАР ХИЗМАТЛАРИ СИФАТИ ПАРАМЕТРЛАРИНИ ТЕСТЛАШ ВА НАЗОРАТ ҚИЛИШ УСУЛЛАРИ

Қ.А. Исманов (ТАТУ, ТИ кафедраси ассистенти)

Алоқа операторлари сифат кўрсаткичларини тестли ўлчаш ва назорат қилишни ҳамўз кучлари билан, ҳам мос келишни баҳолаш бўйича ўрнатилган тартибда аккредитацияланган органларни (синов лабораторияларини) шартнома асосида жалаб қилиш билан ўтказиши мумкин. Янги авлод тармоқларининг хизматлари умумий сифат кўрсаткичлари билан бир қаторда ўлчаш учун махсус техник воситалар зарур бўладиган учта кўрсаткичларни ажратиб кўрсатамиз:

- муваффақиятсиз чақирувлар фоизи (миллий чақирувлар учун);
- боғланиш вақти бўйича меъёрларга мос келадиган чақирувлар фоизи (миллий чақирувлар учун);
- абонентнинг ташаббуси билан бўлмаган боғланишни вақтли узилиши билан тугаган ўрнатилган чақирувлар фоизи (миллий чақирувлар учун).

IMSтармоғида янги хизматларини яратишда ишлатиладиган ресурсларга боғлиқ бўлмаган ҳолда хизматларни тез яратиш ва жорий этиш масаласини сезиларли даражада ечадиган амалдаги интеллектуал платформани сақлаш зарур бўлади. Хизматларнинг интеграцияланишида
3-4G тармоқлардаги хизматлар ва Интернетни IMS (IP-Multimedia Subsystems) платформасидан фойдаланиш асосида созланишини таъминлаш мумкин. IMSплатформаси бу уланиш турига боғлиқ бўлмаган кўп мақсадли ечим симли ва симсиз уланиш доменларини қўллайди, хизматлар брокери эса иловаларнинг ўзаро таъсирлашишини мувофиқлаштиради, мавжуд ва янги хизматларни стандартлаштирилган радиоинтерфейслар ёрдамида комбинациялашга имкон беради (1-расм). Ҳар бир хизмат учун ўтказиш қобилияти максимал эришиладиганга, яъни битта хизмат учун IMS тармоғида олинган ўтказиш қобилияти (BEnetwork) билан таққослашда қуйида берилади.

IMS тармоғидаги трафик моделлари қуйидагиларни ўз ичига олади:

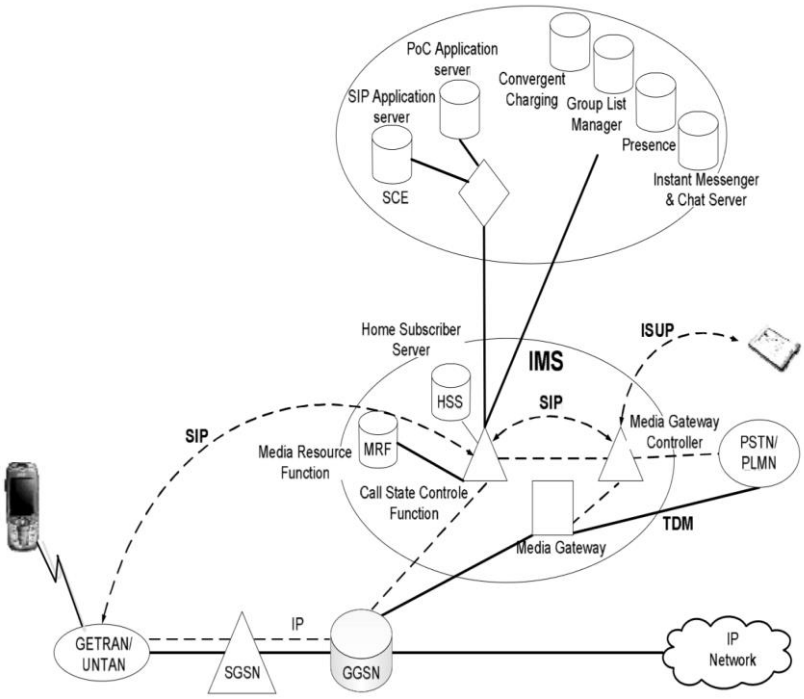
- mix1: VoIP &real-time video;
- mix2: VoIP & mobile TV;
- mix3: VoIP& web surfing.

Ўтказиш қобилияти ҳар бир хизмат учун орасидан 95% хизматнинг сифатидан қониққан ячейкадаги фойдаланувчиларнинг максимал сони сифатида алоҳида аниқланади.

Барча хизматлар учун бир вақтда қониққан фойдаланувчи томонидан талаб қилинадиган комбинацияланган ўтказиш қобилияти ҳисобланади. барча симуляциялар учун ўша бир фойдаланувчилар трафиги ишлатилади. Барча фойдаланувчилар 30секундга тенгсимуляциялаш вақтига тизимда қолади. Таъкидлаймизки, видео ва веб трафикларнинг ўтказиш қобилияти эталон натижаларга яқин. Фарқ мобил ТВ учун катта бўлди. QoS тармоқдаги VoIPнинг ўтказиш қобилияти ҳам эталондан анча паст бўлди.

Хулоса қилиб шуни айтиш мумкункихизматларнинг тўлиқ конвергенцияланиши Triple Playни (видео, нутқ, маълумотларни узатиш) мобиллик ва мультимедиалик функцияларини қўшилиши йўли билан Quad Play (видео, нутқ, маълумотларни узатиш + мобиллик) ва Multimedia Playга айланишини англатади. IMS тизими пакетларни коммутациялаш режимида ишлайди ва IP-технологиялар асосий сигнализация протоколи SIP протоколи ҳисобланади

Хизматлар сифати кўрсаткичларини (QoS) ҳисоблаш, таҳлил қилиш ва баҳолаш фақат махсуслаштирилган қурилмадан фойдаланиш билан ўтказилади ва эталон маълумотларга қараганда чиқиш маълумотларининг (тасвир, овоз, узатиладиган маълумотлар) бузилиши даражасини назорат қилиш йўли билан амалга оширилади.



1-расм. IMS платформаси асосидаги тармоқнинг конвергент архитектураси

Тажриба мисолида бу ишда таъкидлаш керак бўладики, фойдаланувчилар каналлари VoIP трафик бошқа трафик турларига нисбатан устивор бўлганида ўтказиш қобилиятини энг катта ёмонлашганида рухсат этилади. Айрим юкламалар учун йўқотишлар фоизлари 0 дан 15%гача бўлди. QoS максимал юклама учун ўртача ўтказиш қобилиятини камида 10%га пасайтиради.

IP-ТАРМОҚ БЎЙИЧА РЕАЛЬ ВАҚТ ОВОЗЛИ ХАБАРЛАРИНИ УЗАТИШ СИФАТИГА ТАЪСИРЛАРНИ КАМАЙТИРИШ ЧОРАЛАРИ

А.О.Каримова (ТАТУ Нукус филиали, талаба),
Б.М.Сапарова (ТАТУ, талаба).

IP-тармоқ бўйича реаль вақт овозли хабарларини узатиш сифатига бир қанча омиллар таъсир қилиши мумкин. Бунинг оқибатида овозли маълумот ҳар хил узилишлар, кечикишлар ва бузилишларга учрайди. Буларнинг орасида джиттер, яъни қабул қилгичга

пакетларнинг ҳар хил вақт интерваллари да етиб келиши энг кўп учрайдиган ва реал вақт овозли хабарнинг сезиларли бузилишига олиб келадиган сабаб ҳисобланади. Қуйида джиттернинг пайдо бўлиш сабаблари ва уларни бартараф этиш чораларига батафсил тўқталиб ўтамиз.

IP-тармоқ орқали узатиш учун овоз ёки маълумотлар пакетларга тақсимланганда, пакетлер кўпинча белгиланган жойга ҳар ҳил вақтта ва ҳар хил кетма-кетликта келиб тушади. Бу пакетларнинг етказиб берилиш вақтларнинг ҳар ҳиллиги – джиттерни келтириб чиқаради. Джиттер овозни узатишда специфик бузилишларни келтириб чиқаради, бу шавқин ва узилишларни юзага келтиради. Джиттерларни 3 та турга ажратиш мумкин:

1. Маълумотларга боғлиқ бўлган джиттер (DataDependent Jitter - DDJ) – ўтказувчанлик полосаси чегараланган ҳалотта ёки тармоқ компонентларининг бузилиш ҳолатларида содир бўлади.

2. Ишлаш циклининг бўзилиши (DutyCycle Distortion - DCD) – пасттан юқорига ва юқоридан пастка ўзатишлар орасидаги тарқалиш кечикишига боғлиқ.

3. Тасодифий джиттер (Random Jitter - RJ) – актив шовқин натижаси ҳисобланади.

Пайдо бўладиган кечикишларнинг катталиги ва уларнинг юз бериш эҳтимоллиги қайта ишлаш процедураларини ташкиллаштиришда ва қайта ишлаш параметрларини танлашда аҳамият касб этади. Овозли пакет оқимининг вақт бўйича тузилиши ўзгарувчан бўлади. каналда пакетларнинг ностационар кечикишлари ва ўрин алмашишлари сабабли пайдо бўладиган пакетли овоздаги ўзгаришларни филтрлаш учун, реал вақт масштабидаги узлуксиз табийий овозли сигналга буферни қўллаш зарурлиги пайдо бўлади. Буфернинг параметрлари алоқанинг дуплекс режмида телефон сигнали кечикиш катталиги ва йўқотилган пакетларнинг проценти орасидаги компромисс орқали аниқланади. Пакетлар йўқотилиши IP-телефониядаги бошқа жиддий салбий вазият ҳисобланади.

Джиттернинг пайдо бўлишининг асосий сабаблари сифатида қуйидагиларни кўрсатиш мумкин:

1. Тармоқ тасири.
2. Операцион тизимнинг тасири.
3. Джиттер буферининг таъсири.
4. Кодек таъсири ва пакетда узатилувчи кадрлар сони.

Тармоқ тасирида джиттернинг юзага келиши. Биринчидан, тармоқтан пакетнинг тахминий ўтиш вақти турғинмас ва олдиннан аниқлаш қийин. Агар тармоқнинг юклаши нисбатан оз бўлса маршрутизатор ва коммутаторлар пакетларни амалда бир зумда қайта ишлаши мумкин, ҳамда алоқа линиялари ҳар доим очиқ бўлади. Тармоқнинг юкланиши нисбатан кўп бўлса, пакетлар навбатда хизмат кўрсатилишини кўп вақт кутиши мумкин. Пакет узатиладиган йўлда маршрутизаторлар, коммутаторлар ва линийялар канча кўп бўлган сари, унинг кечикиш вақти шунча кўп ва бу вақтнинг вариацияси, яъни джиттер ҳам шунча кўп бўлади.

IP-телефониянинг кўпчилик иловалари (айниқса мижоз иловалари) ўзида Windows ёки Linux каби қандайдир бир операцион тизим муҳитида бажарилувчи оддий дастурларни тақдим этади. Бу дастурлар периферик қурилмаларга (овозли сигналларга ишлов бериш платаси, сигнализация тизимининг иҳтисослаштирилган платаси) бу қурилмаларнинг драйверлари билан ўз-аро мулоқат қилиш учун амалий дастурлар интерфейси орқали мурожат қилади, IP-тармоққа уланиш Socket интерфейси орқали амалга оширилади.

Кўплаб операцион тизимлар марказий процессорнинг бир нечта ўнлаб миллисекундларда ошиб кетувчи ҳар ҳил процесслар орасида вақтни аниқлик билан тақсимлашни назорат қила олмайди, ҳамда бундай вақтда ташқи қурилмадан тушувчи биттадан ортиқ тўқталишни қайта ишлай олмаслиги мумкин. Бу тармоқ интерфейси ва овозни чиқарувчи ташқи қурилмалар орасидаги маълумотларнинг узатилишида, овозни кодлашнинг фойдаланаяткан алгоритмига боғлиқ бўлмаган, кечикишга олиб келади.

Демак, опреацион тизимни тўғри танлаш кечикишнинг умумий ҳажмига таъсир қилувчи омил ҳисобланади. Операцион тизим таъсирини камайттириш учун айрим шлюзлар ва IP-телефонларни ишлаб чиқарувчилар реал вақт операцион тизимларини қўлланишади. Реал вақт операцион тизимлари узилишларга нисбатан тез реакцияни таъминлаш ва процесслар ўртасида маълумотлар оқимларини нисбатан эффектив алмашиш учун процессор вақтини тақсимлашнинг мураккаброқ механизмини ишлатади.

Джиттер муоммаси пакетка йўналтирилган тармоқларда жуда муҳим аҳамиятга эга. Жўнатувчи овозли пакетларни белгиланган вақт оралиқларида жўнатади (масалан, ҳар 20 мс дан), лекин тармоқдан ўтишда пакетларнинг кечикиши бир ҳил эмас, шундай қилиб улар белгиланган пунктга ҳар хил вақт интервалида етиб боради.

Джтернинг таъсирини қоплаш учун терминалларда джиттер-буферлар ишлатилади. Бу буфер белгиланган вақтта етиб келган пакетларни белгиланган ҳажмда хотирада сақлайди. Агар буфер тўлган бўлса жуда кечигип келган пакетлар ташлап юборилади. Пакетлар орасидаги интервал RTP-пакетлар вақт меткалари қиймати орқали қайта тикланади. Джииттер буфери вазифасига одатда агар тармоқ бўйича траспортировка қилишда пакетларнинг жойлашиш тартиби бўзилган бўлса пакетларнинг бошланғич кетма-кетлигини тиклашҳам киради.

ТЎЛҚИН УЗУНЛИГИ БЎЙИЧА ЗИЧЛАШТИРИШЛИ ТИЗИМЛАРДА УЗАТИЛАДИГАН ГУРУҲЛИ СИГНАЛ ҚУВВАТИНИ НАЗОРАТ ҚИЛИШ

Г.Х.Миразимова (*ТАТУ, ТИ каф. катта ўқитувчиси*)

Узатиш тизимининг сиғими ошиши билан сигнал қуввати ортиб боради, бироқ қувват ортиши чегараланган, юқори қувват сигнал/шовқин нисбатини, шунингдек толали оптик узатиш тизим **(**ТОУТ) нинг максимал сиғимини аниқлайди. Бу ўз навбатида оптик қувватнинг юқори чегарасини ўрнатишга олиб келади. Оптик сигнал қуввати ошиши билан оптик сигнал ва толали оптик узатиш муҳити ўртасида ночизиқли ўзаро таъсирлар кузатилади. Оптик сигнал қуввати тўлқинли зичлаштиришли тизимларнинг жиҳозлари, қурилмалари ишлатилганда сигнал таркибига киритиладиган йўқотишларни компенсациялаш ва сигналларни узатиш масофасини узайтириш учун оширилади. Натижада тўлқинли зичлаштиришли тизимларда кучайтиргичли участкаларда ночизиқли эффектлар таъсирини назарда тутиш керак.

Юқоридагилардан келиб чиққан ҳолда мақола мавзуси долзарб ҳисобланади.

Оптик толада юзага келадиган ночизиқли эффектларни ўрганиш ва таҳлил этиш, тўлқинли зичлаштиришли тизимларини лойиҳалаштириш ҳамда фойдаланишдаги муаммоларни ечиш, алоқа сифатини таъминлаш масалаларини ечишга ёрдам беради. Шу сабабли ушбу мақола мавзуси муҳим аҳамиятга эга.

Тўлқинли зичлаштиришли тизимларда оптик сигнал қувватининг назоратини таҳлил этиш мақсад этилган.

Бир тўлқин узунликли синхрон тизимларнинг линия трактида сўниш ва дисперсия сабабли муаммолар юзага келган бўлса, ҳозирги вақтда, тўлқинли зичлаштиришли ТОУТ ларида юқори зич мультиплексорлашда ночизиқли халақитлар каби муаммолар энг асосий ўрин эгаллайди.

Тўлқинли зичлаштиришли тизимларида линия трактида ҳосил бўладиган йўқотишларни компенсациялаш ва алоқа масофасини узайтириш учун +20 ÷ +30 дБқ қувватли сигналларни узатиш даркор. Бундай катта сатҳли оқимларни кичик ўлчамли муҳитга узатишда сигналли оқимларнинг жадаллиги ортади ва бу оптик ночизиқли халақитларга олиб келади.

Узатилаётган сигнал сатҳи катта бўлганда ночизиқли оптик элемент чиқишида асосий сигналдан ташқари сигнал таркибида бўлмаган бир қатор ночизиқлилик гармониклари вужудга келади.

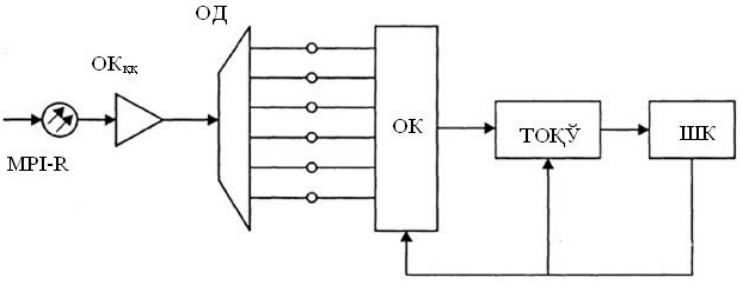
Бундай халақит гармоникалари ишчи оптик каналларнинг гармониклари билан частота бўйича мос тушса, асосий каналларнинг гармоникаларини фильтрлаш муамммоси юзага келади, яъни фильтрлаш ҳам ишчи канал гармоникаларини халақит гармоникаларидан ажратиб ололмайди, натижада ишчи каналларнинг маълумотлари бузилади.

Ночизиқли халақитларни камайтириш мақсадида гуруҳли сигнал оқимининг қуввати 100 мВт - 20 дБқ сатҳдан ошмаслиги талаб этилади. ХЭИ-Т G.662 тавсияси бўйича қувват сатҳи 23 дБ деб қабул қилинган.

Тўлқин узунлиги бўйича зичлаштиришли(ТУБЗ) ТОУТ ларида оптик ўртача қувватни ўлчаш баъзи хусусиятлари билан фарқланади. Бундай тизимларда оптик сигналларнинг икки тури мавжуд: индивидуал сигнал ва гуруҳли оптик сигнал. Гуруҳли оптик сигналнинг қуввати индивидуал оптик канал сигналлари қувватининг йиғиндисига тенг. Каналлари ТУБЗ ТОУТ лари хусусиятларидан бири оптик тракт ўтказиш полосасининг катталигидир. С ва L диапазонлар учун оптик трактнинг ўтказиш полосаси 35 нм га тенг (уларнинг ҳар бири учун). ITU-T тавсиясига кўра тракт амплитуда частота характеристикаси (АЧХ) нинг нотекислиги +/-1 дБ (ёки +/-20 %) дан ошмаслиги керак. Бундан келиб чиқадики, индивидуал каналларда сатҳ бўйича ўртача оптик қувватни ўлчаш хатолиги +/-0,3 дБ дан ёмон бўлмаслиги керак. Бу талабни ўртача оптик қувватни ўлчаш учун ишлатиладиган барча қурилмалар амалда қаноатлантиради. Бу қурилмаларни бу параметрни ўлчаш хатолиги +/-0,2 дБ дан ошмайди, G.692 тавсияси бўйича ТУБЗ ТОУТ нинг индивидуал каналларида ўртача оптик қувват сатҳининг максимал қиймати +17 дБ дан юқори бўлиши керак, қачонки спектрал каналлар сони 20 тадан ошмаса (каналлар сони кўп бўлса, индивидуал каналларнинг қуввати камаяди). Ўртача оптик қувватни ўлчовчи кўпгина қурилмалар бу талабларни ҳам қаноатлантиради.

ТУБЗ ТОУТ спектрал каналларнинг сони кўп бўлганда, яъни 160 та ва ундан ошганда, индивидуал каналларда ўртача оптик қувватни одатий ўлчов қурилмалар ёрдамида ўлчаш соатлаб ўлчанадиган кўп вақтни олади. Бу индивидуал каналларнинг спектрал параметрларини ўлчашга ҳам таъллуқлидир. Шунинг учун индивидуал каналларда ўртача оптик қувватни ўлчаш оперативлигини ошириш учун EXPO компанияси томонидан ўртача оптик қувватни тезкор ўлчагич яратилган. Бу IQ-1613/1623/1643 турдаги асбоблар бўлиб, улар ТУБЗ ТОУТ нинг параметрларини тестлаш учун мўлжалланган IQ-200 ўлчов комплекси таркибига киради. Асбоб 4 кГц гача частота билан 256 нуқтада ўртача оптик қувватни ўлчаш ишларини олиб бориш имконини беради. Ўлчагич шахсий оний ускунага эга эмас. У компьютер билан уланган бўлиб, компьютер дисплейида ўлчов натижалари акс этади. Ўлчов қуйидаги схема бўйича амалга оширилади (1.1-расм).

Келтирилган схемада тезкор бошқарилувчи оптик коммутатор сифатида FTB-9112 OpticalSwitch турдаги оптик коммутатор ишлатилади. Бу оптик коммутатор юқорида айтиб ўтилган IQ-200 ўлчов комплекси таркибига киради. Шахсий компьютер (ШК) ҳам бу комплекс таркибига киради.



1.1-расм. Тўлқинли зичлаштирувчи тизимларнинг индивидуал каналларида оптик қувватнинг ўртача қийматини оператив ўлчаш схемаси:

ОД - оптик демультиплексор; ОК- оптик коммутатор; ТОҚЎ - тезкор оптик қувват ўлчагич; ШК – шахсий копьютер.

MPI-S назорат нуқтада, шунингдек ҳар бир оралиқ кучайтиргич чиқишида гуруҳли оптик сигналнинг ўртача оптик қувватини ўлчаш сатҳ катталигига нисбатан специфик. G.692 (2001 йил) ва РД 45.286.2002 тавсияларига мувофиқ белгиланган нуқталарда гуруҳли оптик сигналнинг максимал сатҳи +27 дБқ (0,5 Ватт) га тенг бўлиши мумкин, алоҳида холларда эса +30 дБқ (1 Ватт).

2002 йилгача ишлаб чиқарилган барча ўлчагичларнинг ўлчайдиган қувватининг энг юқори чегараси +25 дБқ (300 мВт) дан ошмайди. EXPO компанияси ўлчов қурилмалари бозорига қувватнинг юқори чегараси +30 дБқ бўлган FOT 920 турдаги, 2002 йилда қувватнинг юқори чегараси +35 дБқ бўлган FOT 923XP$_2$ турдаги ускуналарни тақдим этди. Бу ускуналар қуйидаги техник параметрларга эга: ўлчанадиган ўртача оптик қувват сатҳининг чегараси -45 - +35 дБқ, ўлчаш хатолиги ±6,5 %, спектрал диапазони 980-1625 нм, рухсат этилиши – 0,01 дБ, чизиқлилиги ±0,1 дБ.

Тўлқинли зичлаштиришли тизимларини лойиҳалаштиришда, фойдаланишда оптик толада юзага келувчи ночизиқли эффектларнинг турлари ва уларни оптик каналларнинг сифатига таъсири масалалари кўриб чиқилиши ва етарли даражада эътиборга олиниши керак. Кўпинча бу омилларни эътиборга олмаслик нотўғри лойиҳалаш, натижада эса қўлланиладиган қиммат қурилмаларнинг имкониятларидан тўлиқ фойдалана олмасликка олиб келади. Оптик нурланишнинг ўртача қуввати оптик тизимларни қуриш, инсталляция ва эксплуатация жараёнларида ўлчашнинг муҳим турларидан бири ҳисобланади, чунки бу ўлчовлар тизимларнинг энергетик параметрларининг давлат стандартларига мослигини аниқлайди, зарарли халақитларни узатиш сифатига таъсирини камайтириш ва сифатли алоқани таъминлайди.

ТЎЛҚИН УЗУНЛИГИ БЎЙИЧА ЗИЧЛАШТИРИШЛИ ТИЗИМЛАРДА УЗАТИЛАДИГАН ГУРУҲЛИ СИГНАЛ ҚУВВАТИГА ҚЎЙИЛАДИГАН ТАЛАБЛАР

Г.Х. Миразимова (*ТАТУ ТИ каф. катта ўқитувчиси*)

Телекоммуникация ва ахборот-коммуникация технологияларининг тезда ривожланиши билан узатилаётган ахборотлар ҳажми ҳам шиддат билан ошмоқда. Узатиладиган ахборотлар ҳажмининг ошиши кўрсатиладиган хизматларга фойдаланувчилар томонидан янги талабларни қўяди. Телекоммуникация операторлари мақбул капитал ва эксплуатацион харажатлар билан талаб этиладиган сифатини таъминлаши керак. Бунда ахборотларни узатиш воситаларининг ўтказиш қобилиятини ошириш ва қабул қилинаётган трафикка сифатли хизмат кўрсатиш керак, бу операторларга телекоммуникация тармоқлари, тизимлари ва элементларининг ҳамма техник характеристикаларини норматив талаб ва халқаро тавсияларга мувофиқлигини таъминлашни юклайди.

Зичлаштириш даражасининг ортишига эътибор бериш керак, чунки бунда каналлараро таъсирлашувларнинг вужудга келиш эҳтимоллиги ортади. Бунга сабаб каналлар сони орган сари гуруҳли оқим қуввати ошади, бу эса ночизиқли халақитларга сабаб бўлади. Шунингдек гуруҳли қувват сатҳини нормада сақланиши ҳар бир каналнинг қувватини пасайишига олиб келади, кучайтириш оралиқлари масофаси камаяди, бу ўз навбатида қурилмаларга харажатларни оширади, тармоқ мураккаблашади.

Бир тўлқин узунлигида ишловчи синхрон рақамли узатиш тизимларида оптик муҳитга узатиладиган гуруҳли оқимларнинг сатҳи +2÷3 дБқ ни ташкил этади, тўлқинли зичлаштиришли тизимларида линия тракти қурилмаларида ҳосил бўладиган йўқотишларни компенсациялаш ва алоқа масофасини узайтириш учун +20 ÷ +30 дБқ қувватли сигналларни узатиш даркор. Бундай катта сатҳли оқимларни кичик ўлчамли муҳитга узатишда сигналли оқимларнинг жадаллиги ортади. Бу юқори жадаллик 1-100 мВт қувватда оптик муҳитда ночизиқли халақитларнинг юзага келишига сабаб бўлади.

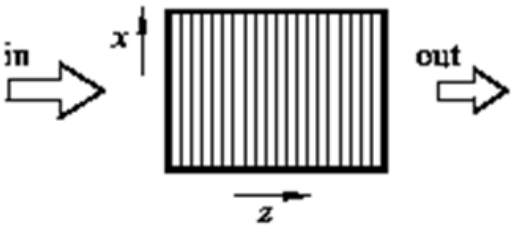
Чунки ўзак кўндаланг кесими майдонининг кичиклиги туфайли сигналнинг жадаллиги жуда катта бўлади хамда нури фокусланмасдан (кесим майдони ўзгармасдан) узоқ масофаларга узатилади.

Сигнал қуввати 10 Вт ва нур узатгич ўзагининг майдони 50 мкм^2 да жадаллик $2\cdot10^7$ Вт/см^2 ни ташкил этади. Бу эса ночизиқли халақитларни юзага келиши учун етарлидир.

Каналлар сони ортиши билан сигнал сатҳи ортиб боради, аммо қувват чексиз ошиши мумкин эмас, чунки сатҳи ошиши билан оптик ночизиқли халақитлар тизим тавсифларини ўзгартиришни бошлайди, тизимнинг имкониятларини - узатиш масофасини, сиғимини, халақитлардан ҳимояланганлигини чегаралайди. Шу сабабли узоқ масофали регенерациялашсиз тўлқинли зичлаштиришли тизимларда ночизиқли халақитлар таъсирини назарда тутиш даркор. Ночизиқлиликлар тизим характеристикаларини нормалардан оғишига олиб келади, оптик каналлар сифатини камайтиради, паразит комбинацион гармоникалар ҳосил қилади ва улар ҳисобига каналлараро ўзаро таъсирларни юзага келтиради.

Оптик муҳит диэлектрикдир, масалан, у ночизиқли элемент (1-расм) сингари кучли электромагнит майдонда ночизиқли тавсифларга эга бўлади. Бу майдонлар нисбатан паст сатҳли лазер диодлардан фойдаланганда ҳам кичик диаметрли ($5*10^{-11}$ м^{2}қийматли) бир модали узатиш муҳитининг кўндаланг кесимининг бирлик майдонига катта зичликли қувватга эга бўлган сигналнинг тушиши натижасида вужудга келади.

Ночизиқли муҳитда тизимнинг параметрлари узатилаётган оқим частотасига боғлиқ бўлади. Оптик кабел толаси ночизиқли муҳитдир, чунки унинг параметрлари узатилаётган сигналнинг қуввати ва жадаллигига боғлиқ.



1-расм. Ночизиқли оптик элемент, in - кириш, out – чиқиш сигналлари, z – бўйлама ва x - кўндаланг координаталар

Узатилаётган сигнал сатҳи катта бўлганда ночизиқли оптик элемент чиқишида асосий сигналдан ташқари сигнал таркибида бўлмаган бир қатор ночизиқлилик гармониклари вужудга келади.

Бундай халақит гармоникалари ишчи оптик каналларнинг гармониклари билан частота бўйича мос тушса, асосий каналларнинг гармоникаларини фильтрлаш муамммоси юзага келади, яъни фильтрлаш ҳам ишчи канал гармоникаларини халақит гармоникаларидан ажратиб ололмайди, натижада ишчи каналларнинг маълумотлари бузилади.

Нурланиш зичлиги - жадаллигининг ошишига бир модали режимнинг бажарилмаслиги ҳам таъсирлашади.

Тўлқинли зичлаштиришли тизимларда бир модали режимни таъминлаш учун $d_ў = \lambda_н$ шарт бажарилиши керак. Лекин, ITU-TG.652 тавсияларида бир модали нур ўтказгич ўзагининг диаметри $d_ў > \lambda_н$ дан бир мунча катта, бу эса бир модали нур ўтказгич орқали битта асосий модадан ташқари бошқа спектрал ташкил этувчиларининг ҳам узатилишига олиб келади. Чунки идеал когерент лазер нурлантиргичлар мавжуд эмас.

Ночизиқлик натижасида муҳитнинг тавсифлари - қутбланганлик, синдириш кўрсаткичи, ютиш коэффициенти нурланиш тўлқинининг электр майдон кучланганлигига боғлиқ бўлишни бошлайди, чунки муҳитнинг қутбланиши майдон кучланганлигига

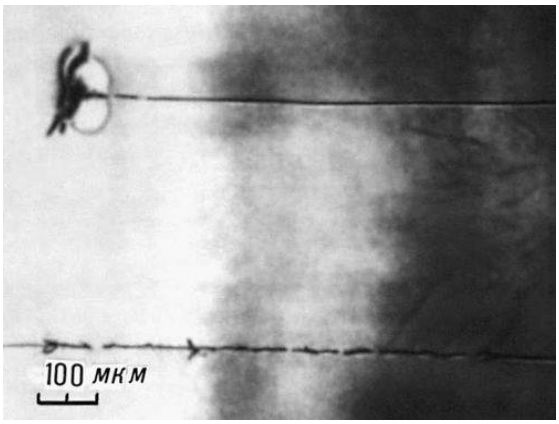
ночизиқли боғлиқ бўлади, турли частотали ва тарқалиш йўналишига эга бўлган тўлқинлар таъсир этади (2-расм).

Оптик нурланишнинг талаб этиладиган нормалардан ошувчи юқори жадаллиги оптик нур узатгич материалини парчалаб сочиши мумкин.

Кварц шишанинг катта сатҳли лазер майдонида ипсимон бузилиши 2-расмда келтирилган ингичка ип – ўз фокусланган ёруғлик оқимининг изи. Натижада сигнални қобиққа чиқиб кетиши ва нурланиши туфайли сигнални узатиб бўлмайди.

Тўлқинли зичлаштиришли тизимларда оптик сигнал сатҳини талаб даражасида сақлаш қуйидагиларга имкон беради:

- ночизиқли халақитларни юзага келмаслиги учун нур ўтказгич толага узатиладиган нурланиш сатҳини талаб даражасида сақлаш керак;
- нур ўтказгич толага узатиладиган гуруҳли оқимнинг йиғинди сатҳи G.662 тавсияси бўйича 23 дБ деб қабул қилинган. Бу ночизиқли халақитларнинг меъёр доирасида сақланишини ва узатиш сифатини таъминлайди.



2-расм. Кварц шишанинг юқори жадалликли нурланиш таъсирида бузилиши

Тўлқинли зичлаштиришли тизимларда оптик қувват қийматини талаб даражасида сақлаш, оптик каналлар сифатини яхшилаш, бунинг якунида эса Тўлқинли зичлаштиришли тизимларни тўғри лойиҳалаштириш, тўлқинли зичлаштиришли тизимларнинг имкониятларидан тўлиқ ва самарали фойдаланиш, тўлқинли зичлаштиришли тизимларнинг қўлланилиши билан юзага келадиган муаммоларни бартараф этиш, талаб этиладиган узатиш сифатини кафолатлаш имконини беради.

МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ ОПТИЧЕСКИХ СЕТЕЙ ДОСТУПА

И.А.Мирзаева (ТУИТ, магистрант)

При проектировании, эксплуатации и исследовании современных структурно-сложных сетей связи возникают задачи оценки эффективности их функционирования, в том числе и по показателю надежности. В настоящее время известен достаточно широкий класс методов анализа структурной надежности сетей. Характерной особенностью этих методов является их высокая вычислительная трудоемкость. Вычисления надежности телекоммуникационной сети можно использовать критерий вероятности связности пар узлов связи.

Фрагменты сети оптического абонентского доступа можно описать используя граф связности, которые последовательно можно привести к нетривиальному (неприводимому) виду, по которому можно вычислить вероятности связности пар узлов связи.

Классификация методов вычисления вероятности связности включает следующие методы: точные аналитические методы, методы Монте-Карло и приближенные аналитические методы. Каждый из этих методов имеют свои особенности. Во всех методах вычисления вероятности связности стохастической двухполюсной сети, является основным показателем оценки структурной надежности сетей связи. К решению некоторых задач, при оперативном управлении предъявляется требование оценки надежности сети в реальном масштабе времени. Известно, что вычисление точных значений вероятности связности двухполюсной сети относится к *NP*-сложной задаче. В силу этого, точные аналитические методы вычисления вероятности связности двухполюсной сети не пригодны для решения в реальном масштабе времени.

Принцип дуальности, позволяющий вычислять двусторонние оценки, монотонно сходящиеся априори к точному значению вероятности связности двухполюсной сети, также малоэффективен. Из консервативных методов быстрого расчета вероятность связности двухполюсной сети, наиболее пригоден - метод экспресс-оценок, но он требует нахождения двух базовых элементарных конструкций-горизонтального и вертикального независимых каркасов двухполюсной сети. Оценки Эзари-Прошана нельзя отнести к быстрым методам, так как являются TVP-сложными. Так называемые оценки Ушакова-Литвака не имеют формальных правил нахождения основных элементарных конструкций.

Для вычисления надежности сети оптического абонентского доступа из множества оценки наиболее приемлем, по нашему мнению, целесообразно использовать метод экспресс-оценки или метод моно-экспресс-оценки вероятности связности.

Рассмотрим метод моно-экспресс-оценки, в котором для вычисления вероятности связности двухполюсной сети требуется найти только одну базовую элементарную конструкцию.

Пусть оптическая сеть доступа с ненадежными линиями связи (для упрощения положим, что узлы связи абсолютно надежны) будет описана случайным перенумерованным графом G{V, L}, где $V=\{v_i\}$ и L = $\{l_{ij}\}$ - множества вершин и ребер графа, на котором выделены s и t . Для юго-западного фрагмента (рис. 1,в) элементы графа перенумерованы, например, так (рис.3,а): $V=\{v_i \,|\, i=1,2,3,...,m_v=|V|\}$ и $\{l_\zeta \,|\, \zeta=m_v+1, m_v+2, m_v+3,..., m_v+m_L\}$, где $m_v=|V|$ и $m_L=|L|$ - мощности множеств вершин и ребер (для данного примера m_v = 5, m_L, = 7).

Обозначим неисправное и исправное состояния ζ-го ребра как $\bar{l}_\zeta$ и $\bar{\bar{l}}_\zeta$ (или просто l_ζ). Предполагается, что отказы ребер наступают независимо друг от друга, при этом $\bar{l}_\zeta+\bar{\bar{l}}_\zeta=I$, где I - полная группа событий. Вероятности этих состояний соответственно равны q_ζ и p_ζ, причем $q\zeta+p\zeta=1$. При рассмотрении численных примеров обозначим состояния ребер с учетом их ζ-х номеров как $\bar{\zeta}$ и $\bar{\bar{\zeta}}$ (или ζ).

В теории графов аспекты связности и несвязности неотделимы от понятий простой цепи и простого разреза. Под простой цепью μ_n понимают последовательность ребер графа без петель и параллелей, соединяющую s и t между собой. Если все ребра n-й простой цепи исправны, то и простая цепь исправна, т. е. $\forall l_\zeta \in \mu_n \left[\bar{\bar{l}}\zeta\right] \Rightarrow \bar{\bar{\mu}}_n$; иначе - простая цепь неисправна, т. е. $\exists l_\zeta \in \mu_n \left[l\zeta\right] \Rightarrow \bar{\mu}_n$. Такие состояния формально запишутся в виде

$$\mu_n \neq \varnothing \Rightarrow \begin{cases} \bar{\bar{\mu}}_n = \prod_{\sigma=1}^{m_n} \bullet l_\zeta \sigma \\ \bar{\mu}_n = \prod_{\sigma=1}^{m_n} \bullet l_\zeta \sigma \end{cases},$$

здесь $\forall$ - квантор общности, $\Rightarrow$ - символ следования "если..., то ...", $\exists$ — квантор существования, $\varnothing$ - пустое множество, Π -конъюнкция, m_n - число ребер n-й простой цепи, σ - номер следования ребра в простой цепи, $\bullet$ - логическое умножение, $\amalg$ - дополнение конъюнкции до полной группы событий.

Под вероятности связности вершин-полюсов двухполюсной сети s и t понимают вероятность $P_{s,t}$ события связности $E_{S,t}$, когда между s и t есть хотя бы одна исправная простая цепь, т. е.

$$P_{s,t} = P\left(E_{s,t} = \exists \mu_n \in M_{s,t}\left[\overline{\overline{\mu_n}}\right]\right),$$

где $M_{s,t} = \left\{\mu_n \middle| n = 1, 2, 3, ..., m_M\right\}$ - множество простой цепи, число которых равно m_M.

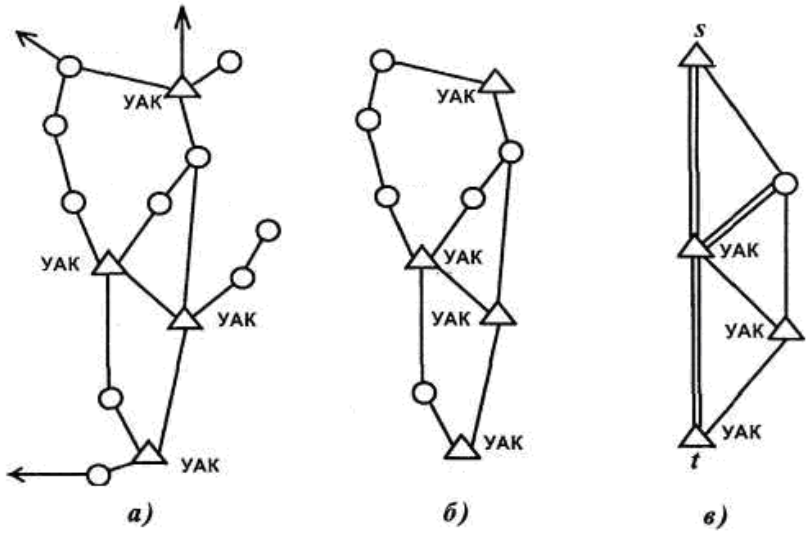


Рис. 1. Фрагмент сети абонентского доступа

Под вероятностью несвязности вершин-полюсов двухполюсной сети s и t понимают вероятность $P_{\overline{s,t}}$ события несвязности $E_{\overline{s,t}}$, когда существует хотя бы один исправный простой разрез, т. е.

$$P_{\overline{s,t}} = P\left(E_{\overline{s,t}} = \exists r_n \in R_{\overline{s,t}}\left[\overline{r_n}\right]\right),$$

где $R_{s,t} = \left\{r_n \middle| n = 1, 2, 3, ..., m_R\right\}$ - множество простого разреза, число которых равно m_R.

При описании $E_{s,t}$ и $E_{\overline{s,t}}$ полностью используются множества $M_{s,t} = \left\{\mu_n\right\}$ и $R_{s,t} = \left\{r_n\right\}$, т. е. на n-х итерационных шагах выполняется: $n = \overline{1, m_M}$ и $n = \overline{1, m_R}$, поэтому $P_{s,t}$ и $P_{\overline{s,t}}$ есть точные значения вероятности связности и вероятность несвязности двухполюсной сети ($P_{s,t} + P_{\overline{s,t}} = 1$). В общем случае расчет этих значений является NP-сложной задачей. Для уменьшения трудоемкости ее решения используют подход к расчету двусторонней оценки, позволяющий вычислять приближенную оценку вероятности связности двухполюсной сети $P_{s,t}$. Такой подход приемлем, если он позволяет оценить погрешность вычислений. Условно в этом подходе различают методы монотонного сближения двусторонней оценки к $P_{s,t}$ и их экспресс-оценки.

Выводы. Для получения двусторонней оценки ВСПУС методом экспресс-оценки необходимо построить две базовые элементарные конструкции. В методе моно-экспресс-оценки,только лишь одной базовой элементарной конструкцией - остаточным подграфом Go. По сравнению с методом экспресс-оценки метод моно-экспресс-оценки по качеству сближения двусторонних оценок ВСПУС несколько проигрывает, но зато существенно снижает трудоемкость вычислений.

КЕЙИНГИ АВЛОД КОНВЕРГЕНТ ТАРМОҚЛАРИДА МАРШРУТЛАШ ТЕХНОЛОГИЯЛАРИНИНГ ҚИЁСИЙ ТАҲЛИЛИ

Ф.А.Музафаров (ТАТУ,ассистент)

Кейинги авлод тармоқ хизматлари, интернет бозорини юқори тезликдаги интернетга уланиш бўсағасига ва телекоммуникация хизматлари интеграллашувига олиб келди. Бу фойдаланувчиларга ушбу хизматлардан фойдаланишдаги харажатларни сезиларли даражада камайтириш имконини беради. Ушбу хизматларга ва иловаларга сўровлар хозирда қўлланилаётган тармоқ технологиялари камчиликларини кўрсатиб беради. NGN IP/MPLS га асосланган интернет технологияси ҳисобланади. Ушбу технология хизматларни тақдим этувчилар (оператор)га турли ҳил хизматларни арзон нархларда юқори тезликда, хизмат кўрсатиш сифати (инг. Quality of Service, QoS) ҳамда оқимларни бошқариш билан фойдаланувчиларга тақдим қилиш имконини беради.

Ҳар бир алоқа тизимида хабарларни узатиш ва қабул қилишда, хабарларни узатишнинг кечикиш вақти асосий параметр сифатида қаралади, сабаби ушбу параметр орқали ўтказиш қобилиятининг қиймати ҳисобланиши мумкин. Шунинг учун, ATM тармоғида IP оқими ATM ячейкалари хажмининг кичиклиги сабабли, сезиларли харажатларни келтириб чиқаради. ATM ячейкаси 53 байтдан ташкил топган,яъни 48 байт фойдали маълумотлар учун ва 5 байт сарлавха қисми учун. IP билан солиштирилганда ATM технологияси улашга йўналтилирган технология ҳисобланади, яъни маълумотни узатишдан аввал охирги қурилмалар ўртасида улашни ўрнатиш талаб этилади. ATM овозли ва видео каби маълум ахборотларни узатишда устунликни тақдим этади ва реал вақт масштабида хизмат кўрсатиш сифатини таъминлайди.

Маршрутлаш технологиялари ATM, IP ва MPLS ларнинг иш қобилиятининг қиёсий таҳлилини амалга оширишда уч турдаги трафик керак бўлади, яъни клиент томонда FTP, овоз ва видео, қабул қилиш томонда эса учта сервер ўрнатилади. ATM ва IP тузилиши жихатдан бир-биридан тубдан фарқ қилади. ATM узатиш бошланишидан аввал маршрутни виртуал тарзда ўрнатади, IP эса маршрутлаш алгоритмлари ёрдамима (Жикста алгоритми, DV алгоритми ва ҳ.к.) пакетларни тасодифан (ёки талабга кўра) узатади. Ушбу фарқ, ATM ва IP протоколлари ўртасида нозик ҳислат саналади. MPLS технологияси операторларга янги хизматларни тақдим этишда ва хизматларни таъминлашнинг соддалаштаришда муҳим омил саналади.

Хулоса қилиб айтганда, ATM нинг интернет ядро қисмида камдан-кам ишлатилишининг сабаби, кенг тарқалган, мавжуд IP инфратузилмасини алмаштиришнинг қийинлиги сабаблидир.Юқорида таъкидлаб ўтилганидек, конвергент тармоқларда MPLS технологиясига асосланган марршрутлаш технологиясини қўллаш операторларга IP трафикдан самарали фойдаланиш, қўшимча хизматларни тақдим этишда учун қулай ечим ҳисобланади.

ОБЕСПЕЧЕНИЕ СЕРВИСА IP QUALITY MANAGER НА УРОВНЕ ПРИЛОЖЕНИЯ ИНФОКОММУНИКАЦИОННОЙ СЕТИ

А.А.Мурадова (ТУИТ, ассистент)

Уровень предоставления услуг инфокоммуникационной сети позволяет предоставлять различные виды услуг с помощью различного программного обеспечения. Также используются различные механизмы обеспечения качества услуг в инфокоммуникационной сети.

IP Quality Manager (IQM) — аппаратно-программный комплекс, он позволяет получать информацию о сквозных параметрах качества с учетом классов сервиса и зональных признаков, поддерживаемых инфокоммуникационной сетью.

Для сбора данных применяется традиционный подход – на узлах сети размещаются специализированные сетевые устройства – пробы. На них запускается программный агент. Агенты в автоматическом режиме периодически осуществляют рассылку тестовых пакетов между собой и измеряют параметры их доставки: потери, задержки, вариации задержек. Полученная информация обрабатывается и собирается в текстовых файлах, а затем передается на более высокий уровень — в систему обработки и анализа статистики. Использование проб на ключевых узлах сети позволит производить измерения не только сквозных параметров, но и на определенных ее участках, что облегчит в дальнейшем процесс локализации проблемы. Таким образом, например, можно осуществить мониторинг и управление качеством на одном из самых проблемных участков сети — на последних милях. В качестве пробы может быть использована любая x86-совместимая платформа под управлением OS Linux, требования к аппаратной платформе – минимальны: память от 512M, свободное дисковое пространство – от 1Г. Это может быть безвентиляторный “тонкий клиент” с флэшовой памятью, настольный PC, возможно использование сетевого сервера совместно с другими сетевыми службами. Несмотря на то, что вполне возможно совместное использование аппаратной платформы как для запуска агентов, проводящих измерения параметров качества, так и для представления других сервисов, следует понимать, что точность измерений на загруженном устройстве, работающем на грани возможностей своих аппаратных ресурсов будет ухудшаться по сравнению с выделенным сервером. Такие измерения могут носить лишь оценочный характер.

Контроль качества включает в себя анализ следующих параметров: потери IP пакетов, круговой задержки IP пакетов, вариации задержки IP пакетов. Измерение этих параметров может производиться в разных классах сервиса, например: standard, premium и real-time. Возможен учет зональной структуры сети, что часто используется операторами при предоставлении услуг IP VPN.

Технически, комплекс IP Quality Manager состоит из следующих базовых элементов: Агенты измерения параметров качества – программно-аппаратные системы, работающие на теневых маршрутизаторах и производящие автоматизированные замеры параметров качества между собой по собственным, либо стандартным протоколам. Агенты могут инициировать тестовые сеансы, а так же принимать запросы от других агентов на произведение замеров. Кроме того, в качестве сопряженного агента возможно использование пассивного устройства с запущенными службами ICMP или UDP/TCP Echo. В роли пассивных агентов могут выступать маршрутизаторы, серверы, специализированные устройства. Агенты не производят сложной обработки измеренных параметров, они передают их в практически исходном виде в ядро IQM — систему анализа статистики.

Система анализа статистики IQM, программная система, расположенная в сетевой инфраструктуре пользователя комплекса, реализует логику обработки и хранения статистических данных. Ядро получает и обрабатывает первичные данные по качеству от агентов, агрегирует их, преобразует в оптимальную для хранения форму, сохраняет в базе данных. Проводит анализ нарушений, в случае их возникновения нарушений возможен вызов внешних сценариев для их выполнения. Это позволяет реализовать функционал отправки сигналов тревоги с информацией о факте нарушения в центральную систему управления посредством SNMP trap либо syslog-сообщений, или отправки сообщений на электронную почту или SMS. Так же возможна реализация автоматической обратной связи с сетевыми устройствами.

Интерфейс статистики IQM – информационная система с графическим интерфейсом, построенным на базе Web, позволяет просматривать полученную и обработанную ядром информацию по параметрам качества. Возможна как автоматизированная генерация отчетов на регулярной основе (например, отчеты за месяц) так и подготовка отчета по требованию. Кроме просмотра статистики посредством

прямых запросов, интерфейс поддерживает функционал «доски здоровья» - это страница, отображающая суммарную информацию о нарушениях. В случае если за определенное временное окно фиксируется факт нарушения — загорается сигнал тревоги, и оператор, увидев его, может перейти на страницу детальной статистики для проведения анализа возникшей проблемы.

Система управления IQM – система конфигурации с графическим интерфейсом, позволяет описать политику качества инфокоммуникационной сети посредством определения классов сервиса, параметров, норм и действий необходимых в случае нарушения норм. Так же позволяет определить список агентов, с которых осуществляется сбор информации, их рабочие параметры и состояние, определить перечень тестов, необходимый для запуска на каждом из агентов. Система в состоянии обслуживать несколько сетей с различными требованиями к параметрам качества.

Следует отметить, что система IQM интегрируется с системами управления и статистики других разработчиков.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА ОБСЛУЖИВАНИЯ ОБОРУДОВАНИЯ СЕТИ ДОСТУПА ИНФОКОММУНИКАЦИОННОЙ СЕТИ

А.А.Мурадова (ТУИТ, ассистент)

Сеть доступа представляет нижний уровень иерархии инфокоммуникационной сети. Основное назначение сети доступа - концентрация в сравнительно небольшом количестве специального аппаратно-программного оборудования информационных потоков, поступающих по многочисленным каналам связи от технических средств пользователей. К этой сети подключаются конечные (терминальные) узлы – оборудование, установленное у пользователей (абонентов, клиентов) сети.

В общем случае уровень доступа ИКС состоит из четырех компонентов: - терминального оборудования, подключаемого в транспортную систему с помощью шлюзов; -терминального оборудования, подключаемого в оборудование транспортного уровня непосредственно, минуя шлюзовое оборудование; - шлюзового оборудования разных типов; -оборудования коммутаторов доступа; -каналов связи с разными пропускными способностями.

Рост требований к качеству со стороны пользователей, обусловленный активным проникновением телекоммуникаций во все сферы жизни, и обострение конкуренции, заставляют операторов все больше заботиться о качестве обслуживания (Quality of Service, QoS). Соглашения об уровне обслуживания (Service Level Agreement, SLA), заключаемые как с конечными пользователями, так и между операторами, становятся важным атрибутом взаимоотношений на современном рынке. А надежность является одним из важнейших факторов, влияющих на QoS, в силу чего требования к надежности (чаще всего к готовности) включаются практически во все SLA.

Высокое качество голоса на шлюзе достигается с помощью передовых методов обработки и обеспечения минимальной задержки. Эти методы сокращают требования к полосе пропускания, снижают расходы и обеспечивают своевременную передачу голосовых пакетов.

Качество голосовой связи во многом зависит от обработки голоса на шлюзе. Шлюз Cisco поддерживает множество средств кодирования и декодирования (CODEC) и имеет следующие возможности обработки голоса: Он поддерживает стандартные средства CODEC G.729 (CS-ACELP), G.729a, G.723.1 и G.711 (PCM), которые позволяют передавать голос с высоким качеством по каналам с низкой пропускной способностью (вплоть до 8 кбит/с). Шлюз выполняет функцию подавления эхо, которая позволяет избавиться от обратных шумов. Для этого используется стандарт подавления эхо E.165. Шлюз генерирует так называемый "комфортный шум". В результате несмотря на

подавление пауз (и, как следствие этого, экономию полосы пропускания) мы избегаем неприятной "мертвой тишины" в трубке, в те периоды, когда по линии не передаются голосовые пакеты.

Некоторые дополнительные параметры VoIP могут настраиваться для достижения более приемлемого качества связи. Среди них усиление и затухание сигнала, глубина подавления эхо, уровень распознавания голосовой активности, соотношение сигнал-шум и степень подавления фоновых шумов.

Задержки являются важнейшим фактором, влияющим на качество голосовой связи. Для приложений, связанных с передачей голоса в реальном времени МСЭ рекомендует задержки в 150 мсек и менее. Работая в сочетании с методами поддержки качества услуг, (QoS) шлюз способен минимизировать задержку по всему каналу за счет нескольких факторов: Большие задержки предотвращаются за счет производительности процессов кодирования/декодирования голоса. Интеллектуальный адаптивный буфер колебаний сглаживает колебания длительности задержек при передаче пакетов. Шлюз может настраиваться на приоритетную передачу IP (IP Precedence), что обеспечивает первоочередность голосовых пакетов в магистральных очередях. Технология многоклассовой и многоканальной фрагментации и встраивания PPP (Multiclass Multilink PPP fragmentation and interleaving; другое название этой технологии - RFC 1990) разбивает объемные пакеты данных, нечувствительные к фактору времени, на более мелкие фрагменты с тем, чтобы в промежутки между ними можно было встроить голосовые пакеты реального времени. Эта технология особенно полезна для низкоскоростных каналов. Она не позволяет большим пакетам данных блокировать голосовые пакеты реального времени. Протокол резервирования ресурсов (Resource Reservation Protocol - RSVP) позволяет шлюзу запрашивать у сети полосу пропускания и резервировать ее.

Для минимизации требований к полосе пропускания шлюзы Cisco VoIP используют следующие средства: Для передачи факсимильных сообщений необходимо только 9,6K полосы пропускания в секунду. Входящие факсимильные сообщения заранее демодулируются, что позволяет снизить требования к полосе пропускания, возникающие из-за использования 64-килобитной импульсно-кодовой модуляции. Шлюз обладает функциями распознавания голосовой активности и подавления пауз. В результате полоса пропускания используется только в те моменты, когда один из абонентов говорит. Во время пауз (на долю которых приходится около половины всего времени разговора) полоса пропускания оказывается доступной для другого трафика. Максимальное время, необходимое для распознавания паузы, составляет 200 мсек. Протокол сжатия для передачи данных в реальном времени (Compressed Real-Time Transfer Protocol - CRTP) сжимает обычный заголовок длиной в 40 байт до 2 - 4 байт. Сокращение длины заголовка пакета на 90 процентов дает очень большую выгоду, особенно в случае обработки голосовых пакетов реального времени, которые отличаются своими малыми размерами. Эта технология рекомендуется для низкоскоростных каналов.

Различные методы, дающие приоритет голосовым пакетам, позволяют стабилизировать качество голосовой связи несмотря на колебания сетевой нагрузки. Приоритетная обработка голосовых пакетов достигается с помощью использования различных стандартов QoS.

Поддерживаются следующие протоколы Cisco IOS QoS:

WFQ - протокол взвешенной справедливой очередности (Weighted Fair Queuing). Это алгоритм очередности потока данных, который одновременно решает две задачи: размещает интерактивный трафик в голове очереди, сокращая тем самым время реагирования, и равномерно распределяет остающуюся полосу пропускания между широкополосными потоками. WFQ обеспечивает предсказуемость услуг. Небольшие потоки данных, составляющие большую часть трафика, обслуживаются на приоритетной основе, что позволяет своевременно передавать всю содержащуюся в них информацию. Большие потоки трафика равномерно делят между собой остающуюся часть полосы

пропускания. Протокол WFQ чувствителен к IP-приоритетности (IP Precedence). Это значит, что он распознает метки высокой приоритетности, которые проставляются на пакетах при передаче данных, и обрабатывает эти пакеты быстрее, чем низкоприоритетные. Тем самым обеспечивается сокращение времени реагирования для приоритетного трафика.

Протокол приоритетной очередности и обычной очередности (Priority Queuing and Custom Queuing). Этот протокол создает гибкие механизмы приоритизации услуг VoIP. Функция приоритетной очередности позволяет сетевым администраторам приоритизировать трафик, создавая фильтры, реагирующие на характеристики пакетов. Эти фильтры разделяют трафик на четыре очереди. Очередь с самым высоким уровнем приоритетности всегда обслуживается первой. Функция обычной очередности (функция распределения полосы пропускания) резервирует часть полосы пропускания для трафика каждого типа. Трафик распределяется по очередям, а затем поочередно передается, так что каждая очередь получает выделенную для нее полосу.

WRED - протокол взвешенного случайного раннего обнаружения (Weighted Random Early Detection). Этот протокол позволяет предвидеть и избегать переполнения сети с помощью первоочередной обработки пакетов приоритетного трафика, распознаваемого по меткам IP Precedence. В моменты, когда на интерфейсе появляются первые признаки переполнения, этот протокол может выборочно отбраковывать пакеты низкой приоритетности. Кроме того, WRED может обеспечивать поддержку разных показателей производительности для разных классов обслуживания.

Коммутация по меткам (Tag Switching) / многопротокольная коммутация по меткам (MPLS) позволяет Интернет-провайдерам дифференцировать тарифы в зависимости от класса обслуживания (CoS). Так, например, абонент может подписаться на обслуживание по первому классу, бизнес-классу или эконом-классу. Трафик этого абонента будет получать метки, соответствующие классу подписки. Gatekeeper может выбирать разные маршруты для передачи трафика с разными классами обслуживания.

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ IMS В СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕРВИСОВ

Х.А.Мухитдинов, (ТУИТ, доцент)
А.А. Абдуллаев (ТУИТ, магистрант)

IMS - это решение для реализации услуг в сетях связи на базе IP, которое представляет собой переход от классических телекоммуникационных технологий к интернет-технологиям.

Иногда этой аббревиатурой именуют сервисную архитектуру подсистемы IP-мультимедиа, которая может стать основой конвергенции сетей, быстрого развертывания новых услуг и сокращения расходов благодаря использованию открытых стандартов. Подсистема IP-мультимедиа (IMS) разработана отраслевым комитетом 3GPP (3G Partnership Project) для использования IP-ядер в сетях 3G и сейчас применяется объединенным техническим комитетом TISPAN в качестве ключевого элемента инфраструктуры Сетей Следующего Поколения (NGN).

Технология IMS, стандарты которой являются базовыми для большинства производителей оборудования, позволяет создать однородную среду предоставления широкого спектра мультимедийных услуг, создавая основу конвергенции фиксированных и мобильных сетей.

IMS позволяет разрабатывать и предоставлять абонентам сетей фиксированной и мобильной связи персонализированные услуги, основанные на различных комбинациях голоса, текста, графики и видео (чат на экране мобильного телефона, электронная почта, игры и многое другое). Решения IMS значительно расширяют возможности конечного

пользователя за счет предоставления расширенного набора услуг, в том числе тех, которые были невозможны или экономически неэффективны в сетях TDM.

Выбор платформы IMS иногда обосновывают тем, что поведение людей в современном мире всё больше и больше определяется такими факторами, как индивидуальность, принадлежность к определенному классу населения (а значит, и сегменту абонентов связи) и мобильность.

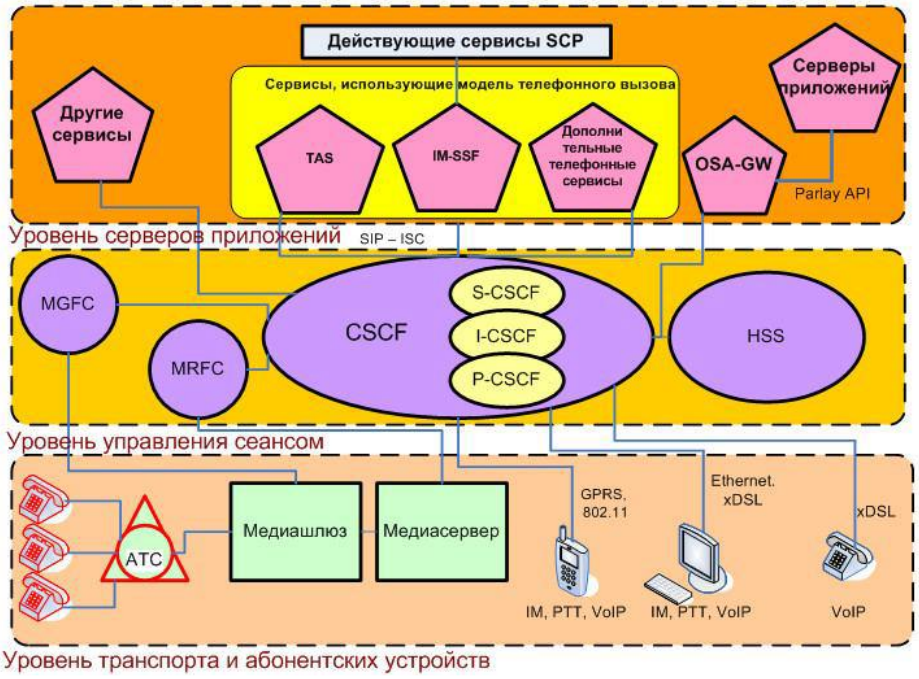


Рис.1. Упрощенный вариант структуры IMS

День за днем постоянно возрастает значимость мобильных мультимедийных услуг, удобных в использовании, позволяющих подчеркнуть индивидуальность пользователя и доступных как для мобильного телефона, так и для PC-терминалов.

Архитектура IMS обычно делится на три горизонтальных уровня: транспорта и абонентских устройств; управления вызовами и сеансами (функция CSCF и сервер абонентских данных); уровень приложений. (рис.1.)Базовые компоненты включают в себя программные коммутаторы, распределенный абонентский регистр (S-DHLR), медиа-шлюзы и серверы SIP. Унифицированная сервисная архитектура IMS поддерживает широкий спектр сервисов, основанных на гибкости протокола SIP (Session Initiation Protocol).

В рамках IMS действует множество серверов приложений, предоставляющих как обычные телефонные услуги, так и новые сервисы (обмен мгновенными сообщениями, мгновенная многоточечная связь, передача видеопотоков, обмен мультимедийными сообщениями и т.д.).

Большинство из ранее сервисов являлись узкополосными сервисами передачи голоса и данных. Однако сигнализация SIP и архитектура IMS поддерживают и широкополосные мультимедийные сервисы, такие как вещательное ТВ с многоадресными (IP multicast) видеопотоками, видео по запросу, видеонаблюдение, видеотелефония, видеоконференцсвязь. Для реализации таких сервисов в сети должны быть установлены дополнительные мультимедийные серверы приложений и абонентские устройства.

Необходимы расширения архитектуры IMS, которые обеспечили бы поддержку расширенного спектра услуг. Многие современные абонентские устройства VoIP, например, IP-УАТС, не поддерживают сигнализацию SIP, используя обычно протокол H.323.

Серьезным фактором, сдерживающим полноценную реализацию архитектуры IMS, является то, что подавляющее большинство телефонных сетей, включая и сети сотовой связи, основываются на коммутации каналов, а “идеология” IMS — пакетная. Причем не просто пакетная: в документах 3GPP прописано использование протокола IP версии 6 (IPv6). Это значит, что для полноценного перехода к IMS операторам связи придется не только выстроить новую схему управления сеансами связи и модернизировать системы поддержки эксплуатации (OSS) и бизнес-операций (BSS), но и существенно поработать над базовой инфраструктурой, обеспечив поддержку маршрутизаторами протокола IPv6. Думается, далеко не все операторы готовы в ближайшее время пойти на такие масштабные инвестиции.

Еще одна большая проблема — отсутствие терминалов, ориентированных на работу в IMS-сетях. Если в традиционных телефонных сетях терминалы (телефоны) — это устройства, обладающие минимумом “интеллектуальных” функций, то технологии IMS требуют достаточно высокого уровня этого самого “интеллекта” для работы со сложными прикладными службами. Когда мы говорим об IMS-совместимых терминалах, то в первую очередь имеем в виду, что мобильная трубка или другое абонентское устройство снабжены клиентом, способным инициировать и обрабатывать IMS-запросы. Кроме того, этот клиент должен поддерживать работу таких приложений, как, например, push-to-talk. Эти приложения могут поставляться с самим терминалом или загружаться из сети. Сегодня ситуация такова, что разработчики терминального оборудования не готовы начать массовое производство IMS-совместимых терминалов по той причине, что самих сетей IMS еще очень и очень мало. Вместе с тем отсутствие терминалов (и новых приложений) серьезно тормозит развертывание новых сетей. Только когда этот замкнутый круг будет разорван, можно будет говорить о начале широкомасштабного развертывания IMS-систем.

Тактическая цель внедрения IMS — реализация новых, интересных пользователям услуг — способна повысить привязанность абонентов к своему сервис-провайдеру.

Однако полный переход к архитектуре IMS может повлечь совсем иной эффект. Как только среда управления предоставляемыми услугами станет стандартной и унифицированной (для сетей и фиксированной и мобильной связи), операторам станет труднее поддерживать строгий контроль над “своими” группами пользователей. Реализация “слоеной” IMS-архитектуры приведет к четкому разделению между поставщиками услуг и сетевыми операторами, и бизнес по предоставлению доступа к сетевым инфраструктурам также будет принципиально отделен от бизнеса по предоставлению коммуникационных и иных услуг.

Как ожидается, внедрение IMS позволит операторам мобильной связи оказывать ряд уникальных услуг, которые не смогут предложить абонентам другие операторы. Это важный фактор для операторов, которые в большинстве своем не желают превращаться в трубу по передаче данных для сервис-провайдеров.

Оценка перспектив внедрения систем IMS весьма реалистична, что даёт надежды на то, что IMS не останется лишь «бумажной концепцией», а станет реальным инструментом, который позволит операторам и сервис-провайдерам при оптимизации затрат предложить новые, действительно интересные пользователям услуги и получить дополнительные источники прибыли.

ОСОБЕННОСТИ ТЕХНОЛОГИИ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ

С.Б. Набиев (магистрант ТУИТ)

В последнее время проблемы “последней мили” становится самой большой преградой для развития телекоммуникационных сетей, технология FSOрешает большую часть возникших проблем в последнее 10 летия. Технология FSO (Free Space Optics,

атмосферная оптическая связь, АОЛС, АОЛП, беспроводный оптический канал связи (БОКС) - это способ беспроводной передачи информации в коротковолновой части электромагнитного спектра. В ее основе лежит принцип передачи цифрового сигнала через атмосферу (или космическое пространство) путем модуляции излучения в нелицензируемом диапазоне длин волн (инфракрасном или видимом) и его последующим детектированием оптическим фотоприемным устройством. Импульс светового излучения при прохождении в атмосфере практически не испытывает дисперсионных искажений фронтов, характерных для любых оптических волокон. Это принципиально позволяет передавать поток данных со скоростями до террабит в секунду. К основным преимуществам такого способа передачи информации можно отнести: высокие скорости передачи (которые невозможно достичь при использовании любых других беспроводных технологий), простота инсталляции, а также отсутствие необходимости платить за использование частотного диапазона. В настоящее время технология обеспечивает передачу цифровых потоков до 10 Гбит/с, что позволяет:

- решать проблемы "последней мили" при высокой защищенности канала связи,
- развивать городские сети передачи данных и голоса (MAN),
- развивать решения WDM (волновое мультиплексирование) для сетей SONET/SDH.

Современное состояние FSO технологии (беспроводной оптической связи) позволяет создавать надежные каналы связи на расстояниях от 100 до 1500-2000 м в условиях атмосферы и до 100 000 км в открытом космосе, например для связи между спутниками. Являясь альтернативным решением по отношению к оптоволокну, атмосферные оптические линии передачи данных (АОЛП) позволяют сверхоперативно сформировать беспроводный оптический канал связи (мобильные системы с автонаведением обеспечивают установление связи за 10-15 минут) при значительно меньших затратах.

Делая вывод можно сказать что, технологииFSO имеет несколько преимуществ и решает ряд проблем, а именно проблемы “последней мили”, обеспечивает высокую защищенность канала связи, развивает городские сети передачи данных а также развивает решения WDM.

ПРАКТИКА ПРИМЕНЕНИЯ ТЕХНОЛОГИИ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ

С.Б. Набиев (магистрант ТУИТ)

Технологию FSO (Free Space Optics, атмосферная оптическая связь) используют многие организации и компании, которым требуется оперативно развернуть надежные, недорогие и безопасные широкополосные линий связи. Два недавних случая демонстрируют уникальное преимущество использования систем FSO в зданиях, которые имеют историческую ценность и являются памятниками архитектуры. В одном случае, потребовалось в недавно отреставрированном историческом здании срочно расширить Gigabit Ethernet сеть с помощью технологии FSO.

В другом случае, не удавалось установить видеокамеры из-за невозможности прокладки кабеля. Препятствием для прокладки кабелей была охраняемая историческая достопримечательность. Только при помощи развертывания системы FSO удалось решить задачу.

Такие физические препятствия как автотранспортные и железнодорожные магистрали, и даже другие здания в промышленной зоне являются основным фактором использования систем беспроводной связи. Один из системных интеграторов использовал систему FSO, когда потребовалось соединить два здания, которые были разделены четырехполосной дорогой.

Управление рисками имеет критическое значение для больниц и оздоровительных центров, которые должны соблюдать федеральное законодательство, требующие от них сохранения конфиденциальности историй болезни пациентов. Вот почему один крупный провайдер установил систему FSO для создания безопасного сетевого соединения между своим медицинским центром и арендованными помещениями в здании, находящемся на расстоянии приблизительно в 300 метрах от медицинского центра. В дополнение к требованиям по безопасности, линию связи необходимо было установить быстро и она должна была пересекать дорогу. Линия FSO отвечала всем этим требованиям, а ее высокие пропускные способности позволяли легко передавать большие файлы с рентгенографическими снимками.

Итак, высокоэффективные беспроводные системы, основанные на использовании технологии FSO, являются реальной альтернативой, если сетевому разработчику необходимо учитывать воздействие обычных в данной местности погодных условий, протяженность линии беспроводной связи, требования к полосе пропускания и потенциальную возможность использования системы FSO в качестве вспомогательных резервных каналов связи.

ИНТЕЛЛЕКТУАЛ УЙЛАР УЧУН АУТЕНТИФИКАЦИЯГА АСОСЛАНГАН ХИМОЯ АЛГОРИТМИНИ ЯРАТИШ

Р.Ҳ.Насимов (ТАТУ, ТИ кафедраси ассисенти)

XX асрнинг ажойиб кашфиётларидан бири бу интернет тармоғининг яратилиши билан боғлиқ бўлса, XXI асрда бу тармоқни барча бизнес ва бошқа соҳаларда кенг фойдаланилиши кўпгина муаммоларни ҳал қилиш учун ечим бўлди. Интернет тармоғи бошқа тармоқларда мавжуд бўлмаган бир қатор афзалликларга эга.Аммо интернет кириб борган барча соҳада ахборотга таҳдид даражаси кун сайин кескин ошиб кетаяпти. Ушбу тесиз мақолада интеллектуал уйлар учун таклиф этилаётган аутентификацияга асосланганҳимоя алгоритми муҳокама қилинди.

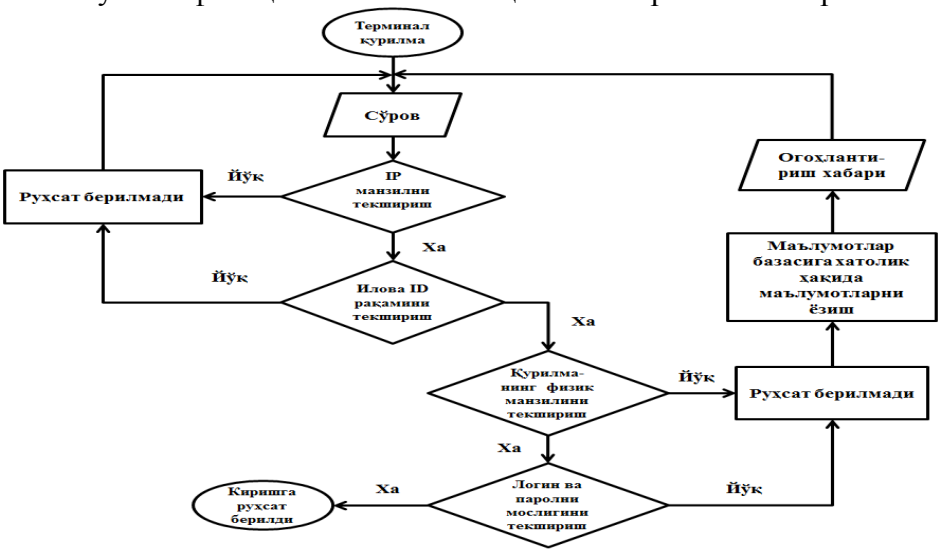
Интеллектуал уй ёки бино деганда одатда махсус структурага эга бўлганайрим қурилма ва жиҳозларга эга, масофадан туриб бошқариш мумкин бўлган автоматлаштирилган объекттушунилади. Бундай уйларни қуришдан асосий мақсад қурилма ва жиҳозларни масофадан туриб бошқариш ва уларни мониторинг қилишдир. Мисол учун, уй эгаси уйдан ташқарида бўлганида ёритиш ва иситиш тизимларини ҳамда бошқа электр жиҳозларини бошқариш ва мониторинг қилиш имкониятига эга бўлади ва шу йўл орқали сарфланаётган ортиқча электр энергия миқдорини тежаши ёки турли қурилмалардан ноўрин фойдаланилган ҳолатда юзага келадиган хавфни масофадан туриб бартараф этиш мумкин бўлади.

Бироқ, турли ташкилотлар томонидан интеллектуал уйлар учун ишлаб чиқарилаётган турли қурилмалар ва дастурий воситалар интернетнинг фаол бўлиши билан асосий хавф манбаи бўлиб хизмат қилмоқда. Бунинг сабаби қурилмалар ва дастурий воситалар танланган ягона стандарт асосида ишлаб чиқилмаган ва шу сабабли ҳам улар ўртасида интеграция жараёни жуда суст. Шунингдек, қурилмалар ва дастурий воситалар ўртасида ўзаро маълумот алмашиш ёки ташқи тармоқ билан боғланиш жараёнларига боғлиқ ахборот хавфсизлиги масалалари талаб даражасида ишлаб чиқилмаган.

Интеллектуал уй эгалари билан олиб борилган сўровномалар натижасида шу нарса маълум бўлдики, кўпчилик уй эгалари ишлаб чиқарилаётган қурилмалар ҳамда операторлар томонидан таклиф этилаётган хизматлар таннархининг қимматлигидан қониқмаётган экан. Кўпгина ривожланган мамлакатларда электр жиҳозлари ва бошқа буюмларни автоматлаштирилган уйларга конвергенция қилиниши даражаси жадал суратларда амалга оширилмоқда, аммо тақдим этилаётган хавфсизлик тизимлари талаб даражасида эмас.

Интеллектуал уйлар учун телекоммуникация технологиялари бозорида таклиф этилаётган аксарият қурилма ва дастурий воситалар фойдаланувчиларнинг эҳтиёжидан келиб чиқиб арзон ва классик хавфсизлик механизмига эга ҳолатда ишлаб чиқарилмоқда. Юқори даражали ҳимоя механизмига эга бўлган қурилма-жиҳозлар ва дастурий воситаларнинг таннархи қиммат ва улар асосан бизнес мақсадларига қаратилган.

Интеллектуал уйларни масофадан туриб бошқариш ва назорат қилишни амалга ошириш учун олиб бориладиган барча жараёнлар хавфсиз бўлишини таъминлаш ва авторизация бўлмаган фойдаланувчилардан тизимни ҳимоя қилиш мақсадида 1-расмда келтирилган аутентификацияга асосланган ҳимоя алгоритми келтирилган.



1-расм. Аутентификацияга асосланганҳимоя алгоритми

Юқорида келтирилган алгоритмга асосланган ҳимоя механизми уй эгаларига интеллектуал уй тизимига кириш, уни бошқариш (масофадан) ва назорат қилиш имкониятини ҳавфсиз бўлишини таъминлайди. Бунда фойдаланувчиларни тизимга кириш жараёни бирнеча босқичларда амалга оширилган ҳолда ҳимоя таъминланади:

*1-босқич.*Уй эгасидан тизимига кириш ҳақидаги сўров қабул қилинганидан кейин, тизим фойдаланувчи терминалининг IP манзилинианиқлайди. Қабул қилинган IP манзили белгиланган чегарасига мос келмаса, тизим зудлик билан киришни бекор қилади.

2-босқич. Агар биринчи босқич мувофаққиятли якунланса, тизим фойдаланувчининг қурилма ID рақамини текширади. Текширишда ID яроқли деб топилса, кейинги босқичга ўтилади ёки кириш жараёни бекор қилинади.

3-босқич. Фойдаланувчининг IP манзили ва қурилма ID рақамиқабул қилинганидан кейин, тизим фойдаланувчининг MAC манзилини аниқлаш учун маълумотлар базасига мурожаат қилади ва кирувчи қурилмани MAC манзили таҳлил қилинади. Натижа ижобий бўлса, фойдаланувчи уй тармоғи тизимига мос логин ва пароли орқаликиради. Агар жараён ижобий бўлмаса, қурилманинг физик манзили маълумотлар базасида ёпиб қўйилади ва кириш бекор қиланади.

4-босқич. Парол ёки логин кетма-кет уч марта хато киритилган ҳолатда, тизим қурилмани ёпиб қўяди ҳамда фойдаланувчи яна тизимга кириши учун унинг терминалини фаоллаштирилиши керак бўлади.

Аутентификация босқичлари мувафаққиятли тугатилганида, фойдаланувчи ўз имтиёзига мувофиқ уй тармоқларининг хизматларидан фойдаланиши мумкин. Акс ҳолда тизим рухсатсиз киришга уринган фойдаланувчининг MAC ва IP манзили бўйича ёпадива уйэгаларига ҳодиса юзасидан маълумот беради.

Фавқулот ҳолати юз берганида, масалан фойдаланувчи мобил телефонини йўқотиб қўйганида, кириш тизими ишдан чиққанида ёки ҳимоя механизмининг ишлаш ҳолати бекор қилинганида, қурилма ва жиҳозлар ўртасида ёки интерфейслар ўртасида ўзаро

алоқа алмашиш йўқолганида, ҳимоя механизми ўзининг ишлаш ҳолатини инкор қилганида, интернет тармоғи узилганида ёки энергия тизимида носозлик бўлганида, телекоммуникация хизматидан фойдаланувчи оператори тармоғига хакерлар томонидан ҳужум уюштирилганида, телекоммуникация хизмати фойдаланувчиси тасодифан йўл қўйган жиддий хатоси натижаси салбий оқибатга сабаб бўладиган жараёнлар юзага келганида, ҳамда файл алмашиш орқали тизимга кирган турли файллар орқали вируслар тизимда фаоллашиб, тизимни ишдан чиқарганда (мобил телефонинг операцион тизимлари орқали вирусларнинг тизимга кириб келиши) таклиф қилинаётган ҳимоя алгоритми (1-расм) олдиндан қарор қабул қилиш ва таҳдидлар таъсирини камайтириш имкониятини қўллаб қувватлайди. Бу алгоритмнинг ҳаётга тадбиқ этиш дастурлари ва уларни баҳолаш усуллари кейинги ишларимизда батафсил муҳокама қилинади.

Юқорида келтирилганларни эътиборга олиб, қуйидагиларни кўрсатиш мумкин:

1. Интеллектуал уйларни қуриш учун махсус қурилмалар ва дастурий воситаларни яратиш имконияти мавжуд бўлган, аммо таннархи қиммат. Шунинг учун ҳам, интеллектуал уйлар учун арзон ва мустаҳкам ҳимоя механизмларини яратиш долзарб масала бўлиб қолмоқда.
2. Таклиф этилаётган ҳимоя алгоритми уй тизимга киришни, хизматларданфойдаланишни, таҳдидлар ва ҳужумларни олдини олиш ва талаб даражасидаги ҳимояни таъминлашни бажаради.
3. Таҳдидлар ва ҳужумлар ўзгариб туриши ҳисобга олинса, алгоритм ҳимоя механизмларини такомиллаштириб боришни таъминлайди.

NGN ТАРМОҒИДА ЧАҚИРУВЛАРГА ИНТЕЛЛЕКТУАЛ ХИЗМАТ КЎРСАТИШ МАРКАЗИНИ МОДЕЛЛАШТИРИШ МАСАЛАЛАРИ

Д.Т. Норматова (ТАТУ катта ўқитувчи)

NGN ва УФТТтармоғида чақирувларга хизмат кўрсатиш маркази эволюция босқичи ва қурилиш принципи таҳлили келтирилган. Бутун тармоқни марказ қурулмаларининг ҳолат башорати ва иш фаолиятини ҳақида ҳисоботни тақдим этиш учун буюртмалар қабул қилиш ҳақидаги статик маълумотларни қабул қилиш, йиғиш ва қайта ишлаш функцияларни бажарувчи NGN тармоғидаги чақирувларга интелектуаль хизмат кўрсатиш структураси келтирилган. Функциональ тизим ости кўрсатилган ҳолда маълумотлар базасининг структураси, NGN тармоғида ишлаб чиқарилган **интеллектуал хизмат кўрсатиш марказини** ишлаш алгоритми ва унинг математик модели ишлаб чиқилган. Ҳар қайси тармоқ сегменти бўйича марказга тушаётган буюртмаларни ҳақидаги маълумотларни йиғиш натижасида реаль сифат кўрсаткичларни, ҳар қайси оператор ишини сифатини ва ҳамма персонал хизмат кўрсатиш баҳолайди. Шу билан бирга тармоқда абонент линиясида узилишни аниқлаш ва мижозларга хизмат кўрсатиш сифатини оширади. Бундан ташқари олдинги марказлардан фарқи кўрилаётган интеллектуал хизмат кўрсатиш марказида буюртмалар автоматик режимда қабул қилинади ва хизмат кўрсатилади. Кенг имкониятли ва аниқ хизматлар тўпламига эга хизмат кўрсатиш марказини тадбиқ қилиш телефон бўйича ҳам, пакетли тармоқ бўйича ҳам юбориладиган чақирувларни қайта ишлашни таъминлайди. Тақдим қилинаётган ахборот хизматлари эхтиёжи доимо ўсиб боради, асосан электрон почта бўйича хизмат кўрсатиш, қўшма веб иловаларни кўриш ва матнли мулоқот каби хизматлар назарда тутилади. Ҳозирги вақтда етарли даражада хизмат кўрсатиш маркази бўйича тадқиқотлар олиб борилган. Аммо умумий хизмат кўрсатиш “классик” назарияси асосида умумий хизмат кўрсатиш тизимига ўхшаб тизимни ишлаши баёнида кўпроқ хизмат кўрсатиш марказининг ишини таҳлил қилишга бағишланган. Абонент линия тармоғида ҳар қайси сегмент бўйича интеллектуал хизмат кўрсатиш марказига тушаётган буюртмалар ҳақидаги статик маълумотларни йиғиш ва қайта ишлаш натижасида NGN тармоғининг

сифат кўрсаткичини, оператор тизим остиларни ишини сифатини реаль баҳолаш, тармоқда абонент линиясининг ҳар хил тавсифда узилишини оператив аниқлаш, мижозларга хизмат кўрсатиш сифат кўрсаткичини оширишига имкон беради. Олдинги хизмат кўрсатиш марказидан фарқи интеллектуал марказдабуюртмаларни қабул қилиш ва хизмат кўрсатиш автоматик равишда бутун сутка давомида дам олишларсиз амалга оширилади.

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА УЗБЕКИСТАНА

Т.Р. Нурмухамедов (ТИИЖТ, профессор)

Внедрение современных информационно-коммуникационных технологий – необходимое условие для развития любого государства, в том числе и Узбекистана, идущего по пути демократических реформ и развития рыночной экономики. Стратегия развития информационно-коммуникационных технологий в стране реализуется в соответствии с Комплексной программой развития Национальной информационно-коммуникационной системы Республики Узбекистан, рассчитанной на 2013–2020 годы, которая утверждена Постановлением Первого Президента Республики Узбекистан Ислама Каримова от 27 июня 2013 года «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан». К настоящему времени осуществлено строительство более 2000 км волоконно-оптических линий связи для широкополосного доступа по современным технологиям на участках «Бузатау-Кунград», «Гузар–Байсун», «Денау–Узун–Шаргун», «Жаслик–Каракалпакстан», «Муйнак–Кибла Устюрт», «Узун–граница Таджикистана» с предоставлением конвергентных услуг, таких как видеотелефония, интернет-телевидение, высокоскоростной Интернет, просмотр HDTV-каналов и другие.

К настоящему времени построены и введены в эксплуатацию несколько железнодорожных линий: Навои-Учкудук-Султанувайс-Нукус; Ташгузар-Бойсун-Кумкурган; Ангрен-Поп. Так, 25 августа 2016 г. сдана в эксплуатацию электрофицированная, высокоскоростная железнодорожная линия Самарканд-Бухара, а с 5 сентября этого же года открыто движение электропоезда “Афросиёб”; 27 августа 2016г. открыто движение пассажирских поездов через перевал Камчик, имеющая протяженность 123,1 км состящей из тонелля протяженностью 19,2 км. Грузооборот и объем пассажирского движения из года в год увеличиваеться, что в свою очередь накладывает более жесткие требования к системам автоматики, блокировки и в целом на автоматизированные системы эксплуатируемые на ж.д.транспорте.

Основная цель создания информационных систем железнодорожного транспорта (ИСЖТ) состоит в полном обеспечении информацией технологических процессов и сфер деятельности ж.-д. транспорта за счет создания информационной основы для достижения максимальной эффективности его работы в условиях рыночной экономики (рис.1). Как видно из рисунка информационная система представлена в виде укрупненной двухуровневой структуры: первый уровень – обеспечивающий, представлен информационной средой и инфраструктурой информатизации, второй уровень – прикладной, реализуется путем формирования новых информационных технологий на базе высокотехнологичных методов управления [2, 3].

Парк технических средств включает в себя вычислительные средства и оргтехнику размещенную в аппарате управления дороги, ИВЦ дороги, а также технические средства опорных станций. В ИВЦ эксплуатируются двухмашинные вычислительные комплексы Z9, мультиплексоры передачи данных выполненные на базе персональных компьютеров, удаленные устройства передачи и приема информации. ИВЦ оснащен новым центральным вычислительным комплексом на платформе трёх серверов – IBM System Z9

ВС XOZ, – на базе которых внедряются современные информационные системы для эффективного управления пассажирскими и грузовыми перевозками, управления финансами и ресурсами компании и другие комплексные задачи [1].

В настоящее время в ИВЦ эксплуатируются автоматизированные системы АСОУП, ДИСКОР, ЕК ИОДВ, АСУ «Экспресс-3» и другие.

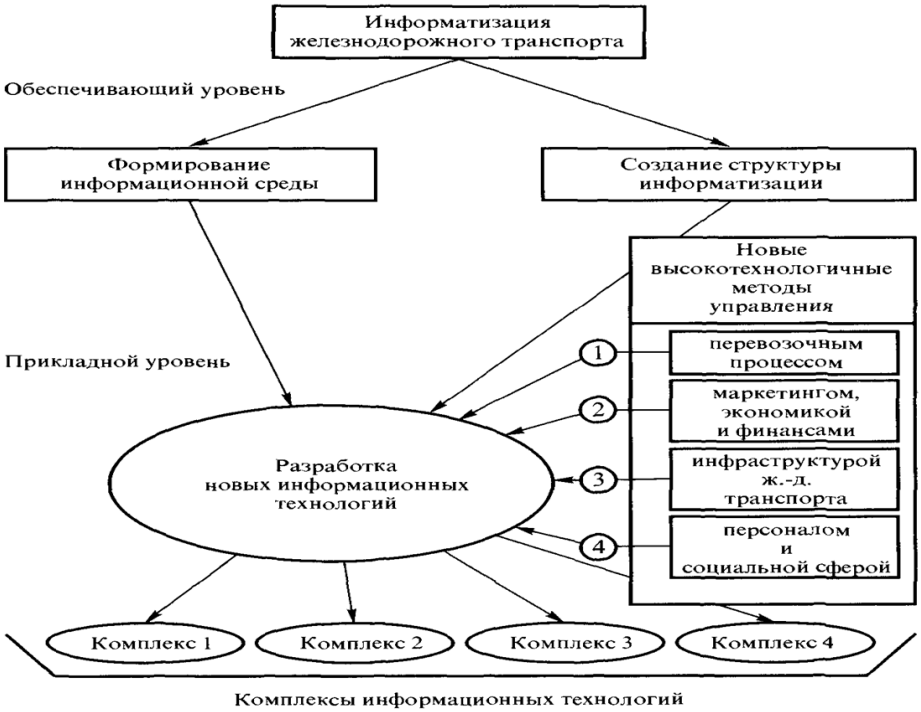


Рис. 1. Структура информационной системы железнодорожного транспорта.

Развивается сеть передачи данных (СПД), местные локальные сети, информационные пункты в линейных подразделениях дороги. Вычислительный центр дороги выполняет поиск и прослеживание вагонов по территории стран СНГ, Латвии, Литвы и Эстонии.

Позитивным является и тот факт, что АО УТЙ активно участвует в «Программе развития межгосударственной информационной сети железных дорог государств – участников СНГ, Латвии, Литвы, Эстонии «Инфосеть-21».

Дальнейший рост объемов перевозок, требования предъявляемые к своевременности доставки грузов до потребителей, бесперебойная работа всех сфер железнодорожного транспорта требует эффективного использования автоматизированных систем оперативного управления перевозками. Разрабатываемые и эксплуатируемые на АО УТЙ автоматизированные системы позволяют эффективно управлять как пассажирскими так и грузовыми перевозками. Кроме этого имеется возможность полного отслеживания подвижного состава по всей территории постсоветского пространства. Созданы все условия для организации автоматизированных рабочих мест сотрудников участвующих в обеспечении бесперебойного движения на дороге.

ПАКЕТЛИ КОММУТАЦИЯГА АСОСЛАНГАН КОРПОРАТИВ ТАРМОҚЛАРДА МУЛЬТИМЕДИАЛИ ТРАФИКЛАР ЎТИШИНИ ОПТИМАЛЛАШТИРИШ

Р.Н. Раджапова (ТАТУ, ТИ кафедраси доценти)

Ҳозирги замон технологияларининг доимий ривожланиши келгусида фойдаланувчиларнинг барча талабларини қондириш имконини беради, янги

технологияларни танлаш эса маълум бир критериялар асосида амалга ошади. Шу нуқтаи назардан корпоратив тармоқларда белгилар бўйича умумлаштирилган кўп протоколли коммутациялаш GMPLS (Generalized MultiProtocolLabel Switching) технологиясини қўллаш долзарблик касб этади.

Ҳозирги пайтда алоқа тармоқларидаги энг муҳим масала Интернет ва мультимедия хизматлари хисобланади. Шу нуқтаи назардан замонавий ахборот технологияларини мувоффақиятли қўллаш фақатгина замонавий дастурий ва техник воситаларга боғлиқ. Шунинг учун ҳам корхона тармоғини ривожлантиришнинг тўғри стратегик йўлини танлаш энг муҳим ҳисобланади.

Юқоридагиларни назарда тутган ҳолда корпоратив тармоқ қуйидаги технологик талабларга жавоб бериши лозим:

- маълумотларни узатишда юқори ишончлилик;
- барча учаскаларда маълумотларни узатиш учун лозим бўлган тезликни таъминлаш;
- тармоқ трафикларининг консолидацияси ҳисобига умумий эксплуатацион харажатларни камайтириш, ўтказувчанлик оралиғини динамик ажратиш, хизмат сифатини дифференциаллаштириш;
- давлатнинг вилоят ва район марказлари билан биргаликда етарли даражадаги зонага эга бўлиши;
- келгусида корхоналар, ташкилотлар, муассасалардан электрон кўринишдаги статистик ахборотларни йиғиш тизимини яратиш, шунингдек электрон кўринишда истемолчига статистик ахборот (маълумот)ларни етказиш;
- ахборот хавфсизлигини таъминлаш.

Бизга маълумки охирги пайтларда пакетли маълумотлар трафигини ҳар қандай сатхда қўллаш мумкин, шу жумладан корпоратив тармоқларда ҳам. Бундай тармоқлардан фойдаланиш учун уни қуйидаги критерияларга асосланган ҳолда оптималлаштириш лозим.

- трафик оқимлари узатиладиган энг қисқа йўлни танлаш;
- узатиладиган ҳар бир ресурсни ўзига мос юклама билан таъминлаш (очиқча бўлмаслиги лозим);
- тармоқнинг барча ресурсларидан имкониятли фойдаланиш;
- кечикишни камайтириш;
- фойдаланувчиларни кўпроқ жалб қилиш.

Юқоридагилардан кўриниб турибдики, тармоқни оптималлаштириш усули стандарт бўлиши ва ишлаб чиқилаётган телекоммуникация қурилмаларида қўлланиши лозим.

Тармоқ бўйлаб ўтадиган трафикларни оптималлаштиришда ва тармоқ ресурсларидан самарали фойдаланишда ХЭАИ-Т G.7713.2 ва G.7713.3 тавсияномаларида назарда тутилган CR-LDP (Constrain-based Routing Label Distribution Protocol) ва RSVP-TE (Resource Reservation Protocol – Traffic Engineering) протоколлар версияларини қўллаш тавсия қилинади. Амалда TE таклифи, фақатгина тармоқ орқали ўтадиган трафиклар оқимини таъқиб қилиш йўли орқали бошқариш усули хисобланади. Бунда IP тармоғида ва трафик оқимларининг йўлларини танлашда асосий қурол метка(сон)ларни коммутациялаш (MPLS) технологияси ҳисобланади.

Бундай MPLS TE технологиялари хозирги пайтда етарли даражада стандартлаштирилган ва IP тармоқлари учун қурилмаларни ишлаб чиқарувчи кўпгина компаниялар томонидан қўллаб қувватланмоқда. MPLS технологиялари асосидаги TE (GMPLS)нинг асосий вазифаси, тармоқ бўйлаб трафиклар ўтадиган тармоқнинг барча ресурслари юкламасини тиклаш ва механизмига эришишдан иборат. Бунинг учун тармоқнинг хизмат сифати катта аҳамиятга эга. Бу биринчи навбатда маршрутизатор ва каналларнинг юкламасига ва тармоқдан самарали фойдаланишга боғлиқ. Худди шу нуқтаи назардан GMPLS технологияси, ҳар қандай умумий фойдаланиш тармоғи орқали территориал тарқалган корхона бўлимларини ёки истемолчиларни, марказлашган

корпоратив тармоққа энг қулай ва самарали улаб бериш усулини амалга оширади. Бундай технологияларда виртуал шахсий тармоқни қўллаш, ахборот алмашишнинг хавфсизлигини таъминлайди, шунингдек алоқанинг шахсий ажратилган каналларига кетадиган харажатни қисқартиради. Истемолчилар орасида узатиладиган барча маълумотлар, ахборот хавфсизлигининг замонавий стандартлари асосидаги ҳимоялаш режимида берилади.Шахсий ёки арендага олинган каналлардан қурилган, умумий фойдаланувчилар тармоғи базаси асосида яратиладиган бундай тармоқ, шартнома асосида ажратилган корпоратив тармоқнинг энг яхши альтернативаси ҳисобланади ва улар қуйидагича афзалликларга эга:

- арендага олинган виртуал каналларнинг нархини пастлиги;
- тармоқ топологиясининг ривожланганлиги (жуда катта географик кенгликга эга);
- ишончлиликнинг юқорилиги;
- локал ҳисоблаш тармоқларининг топологияларига боғлиқ бўлмаган ҳолда, конфигурация ўзгаришининг енгиллиги;
- истемолчиларнинг ҳодиса ва таъсирларини назорат қилиш имкони.

Хулоса: GMPLS технологияси асосида яратиладиган бундай корпоратив тармоқлар, умумий тармоқ ресурсларига эга бўлган ягона ахборотли муҳитда регион бўлимларини марказий аппарат офиси билан бирлаштириш имконини беради ва маълумотларни узатиш, овоз, видеоконференция, мультимедиа иловалари ва шунга ўхшаган телекоммуникация сервисларининг тўлиқ мажмуаси билан таъминлайди.

ТЕЛЕКОММУНИКАЦИЯ ТАРМОҚЛАРИДА MPLS НИ ҚЎЛЛАШ

Р.Н. Раджапова (ТАТУ, ТИ кафедраси доценти)

Бугунги кунда дунёнинг телекоммуникация бўйича етакчи компаниялари томонидан оптик алоқа тизимларини янада такомиллаштириш ва тўлиқ оптик тармоқларни яратиш бўйича кенг кўламли ишлар олиб борилмоқда. Бундай ишларни амалга ошириш учун, трафикни тез ва самарали коммутациялаш талаб этилади. Шу мақсадда жуда катта хажмдаги трафикларни узатишда ва коммутациялашда лямбда коммутациялашни қўллаш долзарб масалалардан бири ҳисобланади.

Бизга маълумки ҳозирги кунда тармоқда қўлланилаётган коммутациялаш қурилмалари тезлигининг чегераланганлиги, сиғими нуқтаи назаридан ўзининг бир қанча камчиликларига эга. Шунинг учун юқори тезикга эришиш ва катта хажмдаги маълумотларни узатишда оптимал вариантли қурилмаларни қўллаш талаб этилади.

Ҳозирги кунда тармоқда тўлқинли зичлаштирувчи технологиялар кенг тарқалган ва ҳар бир тўлқин узунлигида 40 Гбит/с гача маълумотни узатиш имкони мавжуд. Бундай технологиялардан фойдаланган ҳолда лямбда коммутациялаш ўта юқори тезликда катта хажмда маълумотларни узатиш имконини беради. Оптик тармоқ учун яратилган бу протокол MPLS деб аталади. У фотон комутаторларидан, сон бўйича коммутацияловчи (LSR) маршрутизаторлардан, ATM коммутаторларидан ва кириш/чиқиш коммутаторларидан ташкил топган гибрид тармоқларда тармоқни бошқариш учун қўлланилади. MPλS коммутациялаш, оптик сигналларни қайта ишлашга мўлжалланган технология ҳисобланади. MPλS коммутациялашни қўллаш операторларга, тармоқ инфраструктурасини юқори масштабланувчанлик, устма-уст қўйилган хизматлар сонини минималлаштириш, мавжуд ўтказувчанлик полосасини қўллаш самарадорлигини ошириш, асосийси хизмат кўрсатиш ҳисобига қўшимча фойда олиш, алоҳида тўлқин узунликларидан фойдаланиш имконини беради. Бунинг натижасида юзага келган инфраструктура нарх-наво нуқтаи назаридан ҳам анча самарали ҳисобланади ва бунда хар хил турдаги гигант хажмли трафикларни узатиш имкони яратилади. Янги архитектурада тармоқнинг турли элементлари орасидаги ўзаро боғланиш умумий стандартлаштирилган бошқарув платформаси орқали амалга ошади. Айнан шу янги авлоднинг оптик

қурилмаларини интеграллаштириш имконини беради ва ягона гетераген муҳитга бирлаштиради.

Хулоса қилиб шуни айтиш мумкинки, MPLS, жуда катта хажмда оптик трафикларни динамик таъминловчи лойиха учун таклиф қилинган оверлайн тузилишли тармоқ архитектурасини қўллаб қувватлайди. Шунингдек, турли хизматларни қўллашда мустахкамликни таъминлаш, оптик каналларни ҳимоялаш ва хизматларни қайта тиклаш, спектрал ресурслардан самарали фойдаланиш, магистрал тармоқларни ишончлилигини ошириш имконини беради.

NGN ТАРМОҒИДА ИНФОКОММУНИКАЦИЯ ХИЗМАТЛАРИНИ ТАҚДИМ ЭТИШ

С. М. Сайдиакбаров (ТАТУ, магистрант)

Инфокоммуникация тармоғида фойдаланувчиларга хизмат кўрсатиш хизмат ва иловалар тақдим этиш орқали амалга оширилади.

Истеъмолчи тармоғига хизмат унинг коммуникация эҳтиежини қондириш учун тақдим этилади ва у бир маротабалик ишлатилиши билан тавсифланади.

Илова (application), хизматдан фарқли ўлароқ истеъмолчига охирги маҳсулотдан кўп маротабали фойдаланиш мақсадида тақдим этилади.

Хизмат, анъанага асосан, телекоммуникация саноати орқали тақдим этилган, у вақтда ахборот технологияси саноати илова тақдим эта бошлаган эди. Тармоқдан фойдаланувчиларга хизмат кўрсатиш самарадорлиги, тақдим этиладиган хизмат ва иловалар сифатига ва номенклатурасига, шунингдек ахборотга эгалик қилишнинг осонлиги ва тезлиги билан тавсифланади.

Хизмат кўрсатиш учун махсус тармоқ хизмати ташкил этилади. Хизмат еки хизмат турларини амалга оширадиган аппарат, дастур ва ташкилий воситалар комплекси *тармоқ хизмати* деб аталади . Яқин кунларгача аниқ хизматлар тури учун алоҳида махсус тармоқ қурилар эди: УфТТ, умумий фойдаланишдаги телеграф тармоғи, маълумот узатиш тармоғи, телевизион кўрсатувлар тармоғи ва бошқалар.

NGN мавжудлигининг мажбурий шартларидан бири, конвергенция хусусиятидир (мустақил ходисалар белгиларининг бир-бириг ўхшашлиги), хусусан бу хусусият барча холларга мувофиқдир: илова (масалан, нутқ ва маълумот узатиш) конвергенциясидан то инфраструктура (масалан, оптика ва IP) конвергенциясигача.

Анъанавий алоқа тизими хизматларидан фарқли ўлароқ, инфокоммуникация хизматларининг асосий технологик хусусиятларига қуйидагиларни киритиш мумкин:

- инфокоммуникация хизматлари очиқ тизимлар ўзаро боғланиш моделининг юқори поғона даражасида бўлади (аввалги алоқа хизмати тармоқнинг учинчи поғонасида кўрсатилади);
- кўпгина инфокоммуникация хизматлари мижоз ва сервер қисми мавжудлигига мўлжалланган; мижоз қисми фойдаланувчининг жихозида амалга оширилади,сервер қисми эса, хизмат боғламаси деб аталган махсус ажратилган тармоқ боғламасида амалга оширилади;
- одатда инфокоммуникация хизматлари асосан, тезлик билан узатиш ва ахборот оқимларини киришида ва чиқишида носимметрик ҳусусиятга эга бўлган мультимедиа ахборотини узатишга мўлжалланган.

Инфокоммуникация хизматларини тақдим этиш жараени қатнашчиларини ва уларнинг ўзаро муносабатларини белгиловчи бизнес – модель, фақатгина учта, яъни оператор, абонент ва фойдаланувчи каби, асосий қатнашчиси бор бўлган анъанавий электралоқа хизматлари моделидан фарқ қилади.

Инфокоммуникация хизматлари учун қуйидаги талаблар қўйилади:

- хизматларнинг харакатчанлиги (мобиллиги);

- мослашувчан ва тезкор янги хизматларни яратиш имконияти;
- хизматнинг кафолатланган сифати.

NGN тармоғи томонидан кўрсатиладиган инфокоммуникация хизматлари қуйидагиларга бўлинади:

- Мультимедиа хизмати;
- УфТТ/ISDNэмуляция хизмати;
- УфТТ/ISDN симуляция хизмати.

Инфокоммуникация хизматини кўрсатиш жараенида келажак авлод телекоммуникация тармоғида фойдаланувчилар қуйидагиларни таъминлаш ва амал қилиши керак:

- ишончлилик ва хавфсизлик;
- бошқарув, турланувчанлик ва маштаблилик;
- инфокоммуникация хизматининг чегараланмаган турлар тўплами;
- хизмат кўрсатишнинг юқори даражаси ва сифати.

Хулоса қилиб шуни айтишимиз мумкинки, кенг қўламли хизматларга эга бўлиш имконияти NGN доирасида асосий имкониятлардан хисобланади. NGN янги авлод тармоғининг мафкуравий (идеологик) нуқтаи назардан қурилишини, қуйидаги кўринишда белгилашимиз мумкин:

- биринчидан, оралиқдаги тизимдан фойдаланмасдан, тармоққа уланиш жуда осон ва қулай бўлиши керак, шу билан бирга “эски” баеннома ва сервислардан олдинги ҳажмда фойдаланиш мумкин бўлиши керак;

- иккинчидан, олдин пойдевор ўрнини босувчи, яъни компьютер технологиялари асосида керакли сифатни, мустаҳкамлиликни, мослашувчанликни ва кенг кўламлиликни ўз ичига олган базавий пакетли транспорт тармоғи қурилади, сўнг эса ушбу тармоқ устида қудратли телекоммуникация хизматлари комплекси қурилади. Натижада тармоқдаги жами маълумот оқимлари ўзаро боғлиқ ҳолда ривожланади (интеграциялашади).

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ WLAN

Б.М. Сапарова (ТАТУ, студентка 4 курса)

Сети WLAN (WirelessLocalAreaNetworkWLAN)- этобеспроводныесети. С увеличением числа мобильных пользователей возникает острая необходимость в оперативном создании коммуникаций между ними, в обмене данными, в быстром получении информации. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций. Особенно это актуально в отношении беспроводных сетей WLAN. Установка таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно.

Беспроводные сети особенно эффективны на предприятиях, где сотрудники активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации.

- WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорость современных сетей довольно высока (до 108 Мб/с), что позволяет использовать их для решения очень широкого спектра задач;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Безопасности являются аспектом в проектировании и внедрении локальных беспроводных сетей. Особенности реализации, связанные с использованием общей среды передачи, выходящей за контролируемый физический периметр, требует использования

специфического подхода при обеспечении безопасности WLAN. В данной статье рассматриваются основные угрозы и методы защиты, характерные для беспроводных сетей.

В отличие от проводной сети, для подключения к WLAN не требуется получать физической доступ к активному сетевому оборудованию, но достаточно находясь в приделах радиодоступности установить логическую связь с точкой доступа. Если сеть построена с учетом требования минимизации уровня сигнала, использование мощных беспроводных карточек и направленных антенн позволяет злоумышленнику взаимодействовать с точкой доступа на значительном расстоянии.

Специфика беспроводной сети делает ее весьма уязвимой для атак, направленных на отказ в обслуживании. На качестве связи могут сказаться погодные условия, незначительное изменение расположения антенны, использование беспроводной сети в соседнем здании либо офисах. Методов защиты от атак, направленных на отказ в обслуживании, не существует. Эту особенность беспроводной сети надо учитывать при планировании и не использовать WI-FI для передачи трафика с высокими требованиями к доступности.

Поскольку WEP не обеспечивает адекватного уровня безопасности, для защиты беспроводных сетей довольно широко используются средства построения виртуальных частных сетей. В этом случае канальный уровень ISO признается небезопасным, а вся беспроводная сеть приравнивается к сети Интернет, доступ из которой в корпоративную сеть возможен только по каналу, защищенному средствами VPN на основе PPTP, IPSec в туннельном режиме или L2TP+IPSec.

Использование VPN накладывает ряд ограничений на использование беспроводных сетей. Исчезает прозрачность, для работы с сетью требуется активизировать беспроводное подключение. И так достаточно небольшая пропускная способность беспроводного канала дополнительно утилизируется за счет служебного трафика протокола организации виртуальной частной сети. Могут возникать разрывы VPN соединения при интенсивном переключении между точками доступа. Подсистема безопасности семейства стандартов 802.11 представлена двумя спецификациями: WPA и 802.11i.Технология 802.1X служит для аутентификации клиента перед получением доступа к канальному уровню технологии Ethernet даже при наличии физического подключения. Для аутентификации используется протокол EAP и его варианты (PEAP, EAP-TTLS, LEAP). Этот протокол предоставляет механизм безопасной аутентификации и согласование безопасного закрытого ключа, который впоследствии можно использовать для сеанса шифрования беспроводной связи с использованием механизмов шифрования TKIP или AES. В качестве сервера аутентификации может выступать сервер, реализующий необходимые расширения протокола RADIUS. В сетях, к которым предъявляются более строгие требования в отношении безопасности, для предоставления беспроводным клиентам доступа к сети требуется дополнительная аутентификация или вход в систему. Для корпоративного режима безопасности требуется сервер аутентификации, авторизации и учета (AAA) RADIUS. При входе в систему по стандарту 802.1X для обмена данными с точкой доступа и сервером RADIUS используется протокол EAP. Достоинством 802.11X является тот факт, что она может использоваться как в проводной, так и беспроводной сети.Однако при выборе в качестве протокола защиты WPA –PSK следует помнить, что любой протокол аутентификации, основанный на паролях, уязвим для атак восстановления парольной фразы по перехваченной сессии. Для защиты беспроводной сети следует выбирать достаточной устойчивый к подбору пароль.

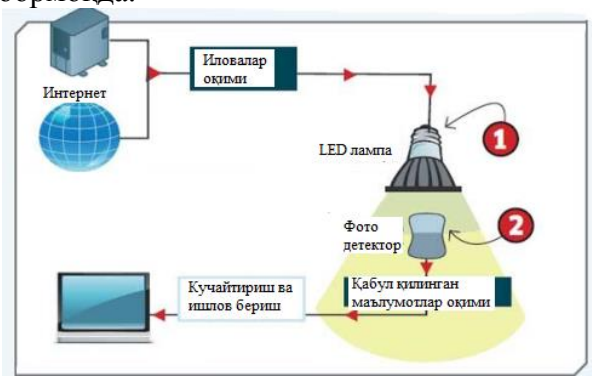
Внедрение IT – технологии, должно сопровождать анализом рисков, разработкой политики безопасности и инструкций администраторов и пользователей по работе с внедряемой технологией. Поскольку требования к безопасности беспроводной сети отличаются от проводной, стоит разделить эти сети с помощью межсетевого экрана.

Желательно контролировать настройки рабочих станций и точек доступа как с помощью активных средств так и с помощью беспроводных систем обнаружения атак.

ЛОКАЛ ТАРМОҚЛАРДА ЗАМОНАВИЙ, ТЕЗКОР ОПТИК ТЕХНОЛОГИЯЛАР

Б.А. Тургунов (ТАТУ, ФФ ассистенти)

Маълумки хозирги глабаллашув жараёнида турмуш тарзида жадаллашиш кузатилар экан, бугунги кунда турмуш тарзимизнинг ажралмас қисмига айланиб улгурган алоқа сохасига, шунингдек алоқа тармоқларидаги маълумотлар алмашиниш тезлигига бўлган талаб тобора ортиб бормоқда.



1-расм. Li-Fiда маълумот узатиши.

Мамлакатимиз алоқа тармоқларининг магистрал қисмлари буткул оптик тармоқлардан иборатлиги сабабли улардаги маълумот узатиш тезлиги етарлича юқори. Шунингдек абонент кириш тармоқларини қуришда ҳам турли замонавий технологияларнинг қўлланилаётганлиги сабабли бундай тормоқларнинг тезликлари ҳам тобора ортиб бормоқда.

Эндиликдаги муаммолардан бири имкон қадар кам харажатли, фойдаланишга қулай, ўтказиш унумдорлиги юқори бўлган локал тармоқларни қуришдир. Бугунги кун тармоқ фойдаланувчилари қурилмалари мобиллашиб бораётганлигини назарда тутган холда шуни такидлаш лозимки, бундай қурилмаларнинг мобил ишлашларини таъминлаш мақсадида мос локал тармоқ технологиясини қўллаш лозим. Хусусан интернет тармоғидан фойдаланиш мақсадида қўлланилаётган телефон аппаратлари, ноутбук ёки стационар компьютерлар. Бундай тармоқ қурилмаларини тармоққа уланишларини таъминлаш учун симсиз технологиялардан фойдаланиш самарали хисобланади. Бу фойдаланишга қулайлик яратишидан ташқари тармоқ қуриш харажатларини янада камайишига олиб келади.

Симсиз локал алоқа тармоқларини қуришнинг энг замонавий технологияларидан бири бу Li-Fi технологиясидир. Ушбу технология алоқа тармоқлари қурилишида яқин унлардагина қўлланилишни бошласада, уни яратиш ишлари Буюк Британиянинг Эдинбург университетида 2010 йилдан бошланган. Локал хисоблаш тармоқлари Li-Fi технологияси асосида қурилганда маълумотлар алмашинуви оқ ёруғлик нури орқали алмашинилади. Секундига милионлаб турли интенсивликка эга бўлган ёруғлик дасталарини узатиш учун бу технолгияда каналларни ортоганал частота бўйлаб зичлаштириш (OFDM) усулидан фойдаланилади.

Ёруғлик манбалари сифатида оддий светодиодлардан фойдаланилади. Маълумотлар узатишда оқ ёруғлик нури таркибидаги қизил, кўк ва яшил ранглардан фойдаланиб узатилади.

Агар бу учта каналдан бирданига фойдаланилса маълумотлар узатиш тезлигини секундига 10 Гб га етказиш мумкин.

-расм. Li-Fi тармоғининг ташкил этилиши.

Ушбу технологиянинг асосида юқори ёрқинликка эга бўлган янги авлод ёруғлик нурлантирувчи диодлардан фойдаланиш ётади. LED лампанинг юқори тезликда ўчиб ёниши хисобига маълумотлар узатишнинг юқори тезлигига эришиш мумкин. Мазкур технологянинг ишлаш принципи шундан иборат: Агар лампа ёниқ бўлса, у холда рақамли сигналнинг 1 импульси, агар LED лампа ўчган холатда бўлса, у холда рақамли сигналнинг 0 импульси узатилади. Бу технолгия умумий холда VLC (Visible light communication) ибораси билан таърифланиб “кўринадиган нурлар ёрдамида алоқа ўрнатиш” каби маънони англатади. VLC алоқаси IEEE 802 алоқа протоколилари гурухида ишлайди (локал ва шахар тармоқлари бўйича умумий стандарт). Бу стандарт алоқа ўрнатилиш физик поғонани белгилайди ва шунингдек мухитга киришни бошқаришни белгилайди. Стандарт аудио, видио ва бошқа мультимедиа маълумотларини узатиш учун етарли тезликни таъминлашга қодир. Бундай тармоқларда маълумот узатиш тезлигининг камайишига таъсир этув-чи омиллардан бири бу ташқи ёритиш тизим-ларидир. Шунингдек хона атмосферасидага нисбий намлик даражасининг ортиб кетиши ҳам маълумотлар узатиш тезлигининг камайишига ва хатолик даража-сининг ортиб кетишига олиб келади. Бу технологиянинг қўлланилиши локал тармоқлардаги мижоз қурилмаларининг юқори тезликда ўзаро маълумот алмашишлари, шунингдек боғланишларни мобил холда амалга оширишлари имконияти пайдо бўлади.

ПРИНЦИПЫ ПОСТРОЕНИЯ ВЫСОКОПРОИЗВОДИТЕЛЬНОГО СТАТИЧЕСКО-ПРОСТРАНСТВЕННОГО МНОГОЗНАЧНОГО ЭЛЕМЕНТА ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Ф.К.Турсунбаев (ТУИТ, профессор)

Представляют интерес и принципы построения многозначных элементов (МЭ) с промежуточными статическими и пространственными признаками представления информации. Наличие в одном элементе двух промежуточных признаков позволило бы существенно повысить многофункциональность элемента.

В МЭ, построенных на статических НЧ наряду со статическим промежуточным признаком возможно также получение и пространственного признака входной информации[1].

Для получения пространственного признака в статических МЭ необходимо:

1) выбрать взаимоисключающие свойства нелинейной функции, являющиеся признаками 0 и 1, определить оператор *D* для дешифрации этих признаков;

2) дешифрировать сформированные характеристики в соответствии с выбранным признаком дешифрации *D* и значением входного сигнала.

Следует отметить, что первая производная от функций Шаудера есть не что иное, как функция Хаара

$$h_{ij}(X) = \frac{\partial \varphi_{ij}(x)}{\partial x}, \qquad (1)$$

которую, так же как и функции Шаудера, можно представить группами функций.

$H_1(x)=h_{11}(x)$;

$H_2(x)=h_{21}(x)+h_{22}(x)$;

…

$H_n(x)=h_{n1}(x)+h_{n2}(x)+\ldots+h_{n2}^{n-1}(x)$;

Взаимоисключающие свойства функции $h_{ij}(x)$, являющиеся признаками 0 и 1, определяется знаками этих функций. Для дешифрации признаков может служить оператор

$$D_{ij}=sign\ h_{ij}\ , \quad (2)$$

где

$$sign h_{ij}(x)=\begin{cases}0 & при \quad h_{ij}(x)\le 0,\\ 1 & при \quad h_{ij}(x)>0.\end{cases} \quad (3)$$

Подставляя функцию Хаара (1) в выражение (2), получаем для треугольной функции выражение оператора дешифрации

$$D_{ij}=sign\left[\frac{\partial\varphi_{ij}(x)}{\partial x}\right]. \quad (4)$$

Точки излома амплитудных характеристик статических МЭ характеризуют символы k-значного алфавита, поэтому применение оператора D_{ij}, несущего в себе цифровую информацию об этой точке, при построении статическо-пространственных элементов вполне оправдано.

Статическо-пространственный МЭ (рис.1) реализован на базе МЭ последовательного типа путем введения дешифраторов знака первой производной (ДЗП), комбинационной схемы (КС) и неоднородного преобразователя $P \to S$. При этом на выходе дешифраторов знака первой производной имеем позиционный двоичный код, который с помощью комбинационной схемы (КС) преобразуется в k-значный пространственный код.

Следует отметить, что осуществляется именно тождественное преобразование статического входного сигнала в пространственный k-значный код, так как преобразование $S \to P$ не зависит от значений базисных сигналов $\vec{V}_f$, поступающих на нелинейные четырехполюсники. Это объясняется и тем, что оператор дешифрации D_{ij}(4) не зависит от значений функции $\varphi_{ij}(x)$, а значит и от значений базисных сигналов, поступающих на НЧ. Тогда можно утверждать, что реализуемые статическо-пространственным МЭ промежуточные признаки-статические и пространственные - взаимонезависимы, а поэтому функции $f_1(x)$ и $f_2(x)$, воспроизводимые элементом, реализуются независимо друг от друга. Это - один из самых важных факторов, позволяющих повысить многофункциональность МЭ. Таким образом, статическо-пространственный МЭ может одновременно воспроизводить две различные взаимонезависимые многозначные функции$f_1(x)$ и $f_2(x)$.

Общим недостатком как универсальных статических, так и универсальных статическо-пространственных МЭ является сложность реализации четырехполюсников с произвольно изменяемой амплитудной характеристикой. По этой причине статические МЭ наиболее эффективно можно использовать для воспроизведения фиксированных многозначных функций. При этом аппаратурные затраты на построение МЭ существенно уменьшаются. Следовательно, воспроизводимая статическо-пространственным элементом функция$f_1(x)$является фиксированной, а функция$f_2(x)$ может иметь различные виды в зависимости от набора базисных сигналов ИБС.

Возможна также реализация более быстродействующих статическо-пространственных МЭ на основе статических МЭ параллельного типа. При этом должны быть дешифрованы взаимоисключающие признаки нелинейных характеристик, формируемых каждым НЧ.

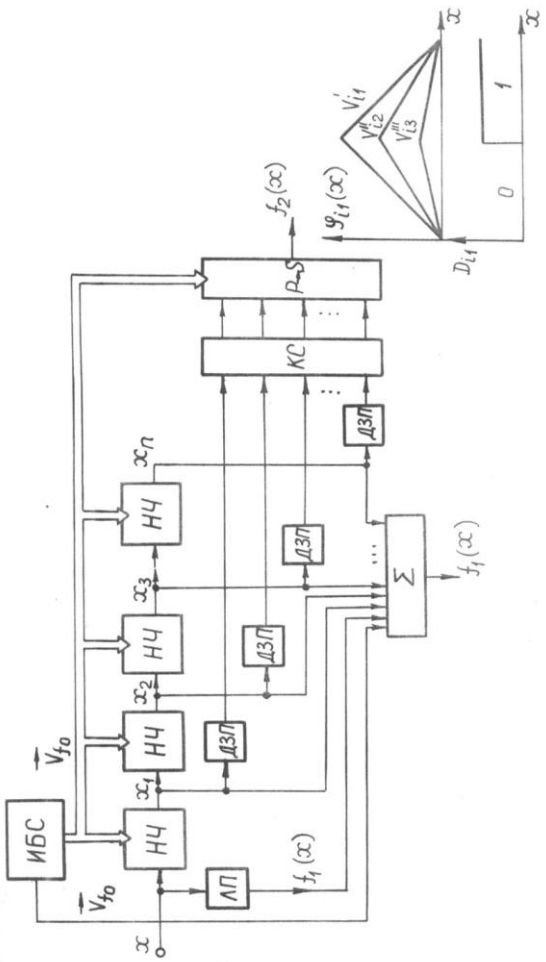


Рис.1. Блок-схема и диаграммы треугольных сигналов статическо-пространственного МЭ последовательного типа

ЮҚОРИ СИФАТЛИ МАЪЛУМОТЛАРНИ РЕАЛ ВАҚТДА УЗАТИШДА SCTP ТРАНСПОРТ ПРОТОКОЛИНИ ҚЎЛЛАШ

Б.К. Турумбетов (ТАТУ Нукус филиали, катта ўқитувчи),
Е.Н. Рейпназаров (ТАТУ, магистрант).

Ушбу мақолада тармоқларда маълумотларни реал вақтда узатишда SCTP протоколини қўллаш билан боғлиқ масалалар тадқиқ этилган.

OSI тармоқ моделининг транспорт сатхи анча мураккаб вазифаларни бажаради. Бу вазифаларга маълумотлар оқимини бошқариш, хатоликларни тўғрилаш ва маълумотларни ишончли етказиб бериш, ўз-аро ҳамкорликдаги иловаларнинг тўғри ишлаши ва зурур самарадорликка эришишини таъминлаш ва шу кабилар киради.

Фойдаланувчиларнинг реал вақт видео маълумотларни олишга бўлган талаби кескин ортмоқда. Шу сабабли юқори сифат ва ишончлиликни таъминлайдиган янги иловалар яратилмоқда. Бу иловалар шундай функционалликни талаб этмоқдаки, бу талабларни TCP ёки UDP протоколлари ёрдамида қониқтириш мумкин эмас. Чунки бу протоколлар икки хил йўналиш учун мўлжалланган бўлиб, бирининг камчилигини иккинчиси тўлдириб туради. Транспорт сатхини функционаллигини кенгайтириш мақсадида оқимларни назорат қилувчи узатиш протоколи SCTP (Stream Control Transmission Protocol) ишлаб чиқилган.

SCTP протоколининг асосий ғояси TCP ва UDP протоколларининг афзалликларини бирлаштириш ва камчиликларини бартараф қилиш ҳисобланади. Протокол пакети икки

таркибий қисм: сарлавҳа ва субпакетлардан тузилади. Ўз навбатида ҳар бир субпакет ўз сарлавҳаси ва маълумотдан таркиб топади [1].

SCTP протоколи TCP протоколига аналог тарзда ишлайди деб қараш мумкин, аммо бу протокол ўзида UDP протоколининг имкониятлари ҳамда бир нечта қўшимча функционал имкониятларни жамлаган. Булар хабарларни чегараларини сақлаш; head-of-line туридаги блокировкаларнинг йўқлиги; етказиб беришнинг бир нечта режими; “multihoming” нинг қўллаб қувватланиши; қўшимча юкланишни назорат қилиш; намуна бўйича тасдиқлаш; фойдаланувчи маълумотларини фрагментациялаш; ишчанлик қобилиятини назорат қилиш механизми; DoS-ҳужумлардан ҳимояланганлик хисобланади.

SCTP протоколи иловаларга ўзининг талаблари бўйича транспорт сатхини созлаш имконини тақдим этади, бу созлаш ҳар бир тизим учун алоҳида бажарилади. Бу эгилувчанлик иловалар учун TCP ёки UDP протоколлари ёрдамида амалга ошириб бўлмайдиган имкониятларни беради.

SCTP протоколининг таъкидлаб ўтилган бу функционал имкониятлари, ушбу протоколга асосланган ҳолда реал вақт телекоммуникация тизимлари ёрдамида фойдаланувчиларга юқори сифатли хизматларни (масалан, HD форматдаги видео, уч ўлчамли 3D телевидение ва шу каби) етказиб бериш имкониятларини тақдим этмоқда.

АТМОСФЕРНАЯ ОПТИЧЕСКАЯ СВЯЗЬ И ЕЁ ПРЕИМУЩЕСТВА

Л.И. Фозилжонова (магистрант ТУИТ)

Атмосферная оптическая связь делает возможной передачу данных (интернет, голос, видео, телефония, телевидение) между объектами в атмосфере, предоставляя оптическое соединение без использования оптоволокна или радио-эфира. В системах FSO для широкополосной передачи данных, голоса и видео от одной точки доступа к другой применяют лазерный луч, распространяемый в зоне прямой видимости по воздуху. Эту технологию можно считать беспроводным эквивалентом проводной оптической связи, осуществляемой по оптическому волокну. Модули FSO подключаются к локальной вычислительной сети с помощью медных или волоконно-оптических кабельных линий, которые отвечают требованиям стандартов TIA и EIA. Любое приложение, данные которого можно передавать через Интернет, а именно речь, данные и видео, может использовать систему FSO. Система FSO имеет следующие преимущества:

- АОЛС не требует получения разрешения на использование частот;
- Работают со скоростью современной кабельной сети до 1 Гбит/с;
- Увеличивают пропускную способность существующих каналов связи (Gigabit Ethernet/Fast Ethernet);
- Соединение «точка-точка» через трудно преодолимые преграды (ж/д пути, шоссе, энергетические объекты создающие сильные; электромагнитные помехи, плотную городскую застройку, промышленные зоны, канализацию, водные преграды, «негостеприимные» земельные участки, горы и т. п.) при прокладке волокна (ВОЛС), WiFi, WiMax;
- Отсутствуют задержки при передаче информации (ping <1ms) как у радиолиний;
- Быстро и просто свертываются – демонтаж несколько часов;
- Создание канала аварийной связи когда необходимо оперативное развертывание;
- АОЛС невосприимчивы к радиопомехам и не создают их сами;
- Отсутствует абонентская плата;
- Большая дистанция и высокая скорость в канале вследствие реализации принципиально нового решения в рамках АОЛС технологии - адаптивно изменяемой скорости и энергетики в зависимости от состояния оптического тракта;
- Соединений базовых станций WiFi, WiMax, UMTS, LTE;

Исходя из этих преимуществ можно сделать вывод, что данная технология отвечает приемлемым требованиям телекоммуникационной сети, а также позволяет моментально развернуть систему FSO.

WDM-PON ТЕХНОЛОГИЯСИ АСОСИДА КЕНГ ПОЛОСАЛИ ТАРМОҚДА ИННОВАЦИОН ЕЧИМЛАРИНИНГ ТАҲЛИЛИ

Л.И Фозилжонова (ТАТУ, магистрант)

Ушбу ишда тўлқин бўйича ажратилган пассив оптик тармоқларни қурилишдаги амалий аспектлар кўрилган. Бу синфдаги тармоқни қуришда янги технология таклиф этилиб унда , ёруғлик оқим тарқалиши йўли бўйича узатиш йўналишини бўлиш ҳисобига оптик толани қўллаш самарадорлигини оширишни таъминлайди. Тақдим қилинаётган технология республикамизда оптик толали элементда электрон компонент базасида амалга оширилиши мумкин. Замонавий телекоммуникациянинг ривожланиш босқичи кейинги авлод тармоғи (NGN- Next Generation Networks) принципида қурилган мультисервис тармоқ инфраструктурасига ўтиши билан характерланади. Бу пакетли тармоқ структурасининг муҳим қисми кенг полосали тармоқ ҳисобланади, унда кириш тугунига фойдаланувчи терминаллар ва локаль абонент тармоқларини уланиши амалга оширилади. Хозирги вақтда фаол қўлланилаётган пассив оптик тармоқ PON (Passive Optical Network) ўзида кенг поласали уланиш технологиясини кенгайтирилган синфини мужассам этади. WDM-PON янги технология базасида FTTB (Fiber To The Building-биногача оптик толани олиб бориш) синфининг аниқ тизимли-тармоқли ечимини қурилишининг амалий аспектлари келтирилган бўлиб унда оптик толали компонентлар асосида амалга оширилади.Тақдим қилинаётган тўлқин бўйича ажратилган WDM-PON пассив оптик тармоғи қуйидаги асосий афзалликларга олиб келади:

1. Ҳар қайси охирги тугун ўзига ажратилган канал тўлқин узунлигида барча канал ресурс ўтказувчанлик қобилияти монополлаштиради, бу эса тақдим қилаётган тармоқда сезиларли даражада трафикга хизмат кўрсатиш кўрсаткичини сифатини оширишга олиб келади.
2. Узатгич йўналишини ажратишда тўлқин узунлиги бўйича эмас ёруғлик оқими тарқалиши йўли бўйича амалга оширилганлигини ҳисобига анъанавий тўлқин бўйича зичлаштирилган технология қўлланилиши билан солиштирганда сиғим икки ҳисса оширишга олиб келади.
3. Ажратилган каналда тўлиқ мантиқий шаффофликни таъминлайди ва прототипга ўхшаб канақадир қўшимча сарлавҳалар каби ахборот пакетларига ўтиш талаб этилмайди.
4. Тўлқин бўйича ажратиш ишлатилади. Бундан ташқари оптик қабул қилгич узатгичлар, мультиплексорлар – демультиплек сорлар, циркуляторлар, ажраткичлар оптик толали алоқа элементлари ўзимизда ишлаб чиқаришни йўлга қўйиш мумкин. Шу билан бирга махсус текширув ва тадқиқотлардан ўтган ва махсус сертификатларга эга ахборот пакетли коммутаторларни ҳам ишлаб чиқаришни йўлга қўйиш мумкин.

ОРГАНИЗАЦИЯ ПРИОРИТЕТОВ ПО ЦЕННОСТИ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЬЯХ И СИСТЕМАХ С РАЗНОТИПНЫМИ КАНАЛАМИ И ИЗМЕНЯЮЩИЙСЯ СТРУКТУРОЙ

И.С. Хайдаров (ТИПСЭАД)

В данной раборте рассматривается организация приоритетов по ценности информации, где общий поток информации характеризуется плотностью распределения ценности информации.

Пусть общий поток информации характеризуется плотностью распределения ценности информации $f(C_0)$. К первому приоритету будем относить информация, имеющие $C_0 \geq C_1$,ко второму- имеющие $C_2 \leq C_0 \leq C_1$ и т.д.Задача заключается в нахождении таких значений $C_к$ (к=1,2….,n) при которых обеспечивается максимум значения показателя эффективности сети, характеризующий ценность передаваемой информации W*. В данном случае удобнее пользоваться несколько другим выражением для W* (без нормировки ценностей информации) :

$$W^* = \sum_{k=1}^{n} P_k M_k(C_0) Q_k \Big/ \sum_{k=1}^{n} P_k M_k(C_0) \quad , \qquad (1)$$

Где. P_k - вероятность своёвременной передачи информации к-го потока;

Q_k - относительная доля к-го потока ;

Легко показать, что

$$P_1 M_1(C_0) = \int_{C_1}^{\infty} C_0 f(C_0) dC_0 \quad , \qquad (2)$$

$$P_k M_k(C_0) = \int_{C_k}^{C_{k-1}} C_0 f(C_0) dC_0 , k = \overline{2,n} \quad , \qquad (3)$$

$$\sum_{k=1}^{n} P_k M_k(C_0) = \int_{0}^{\infty} C_0 f(C_0) dC_0 = M(C_0) , \qquad (4)$$

$$Q_k = Q\infty \frac{1 - \rho^{k+1} Q_m^{k+1}}{1 - \rho^{k+1} \cdot \rho} \quad , \qquad (5)$$

Для нахождения Q_k воспользуемся выражением (5), чтобы исследовать влияние только ценности информаций. Полагая $\mu_k = \mu_1$, $\nu_k = \nu$ (к=1,2,…,n) можно записать

$$Q_k = \frac{1 - \sum_{i=1}^{k} \rho i}{\nu\left[\mu^{-1} + \nu + \delta_{k-1} - \delta_{k-1} \prod_{k-4}(\nu)^{-1}\right] - \rho_k} \quad , \qquad (6)$$

$$\rho_i = \frac{\lambda_i}{\mu} = \frac{\lambda \cdot \rho_i}{\mu} = \rho \cdot \rho_i \quad , \qquad (7)$$

Где :

λ_i - интенсивность i-го потока;

ρ – коэффициент занятости системы;

δ_k -относительная интенсивность старения к-го потока;

$$\delta_{k-1} = \sum_{i=1}^{k-1} \lambda_i = \mu \sum_{i=1}^{k-1} \rho_i = \mu\rho \sum_{i=1}^{k-1} \rho_i \quad , \qquad (8)$$

$$\prod_{k-4}(\nu) = \sum_{i=1}^{k-1} \lambda_i \mu \delta_{k-1}^{-1} (\mu + \delta_{k-1} - \delta_{k-1} \prod_{k-1}(\nu) + \mu)^{-1} , (9)$$

Разрешая (9) относительно $\prod_{k-1}(\nu)$, получаем

$$\prod_{k-1}(\nu) = \frac{\nu + \mu + \delta k - 1}{2\delta_{k-1}} + \sqrt{\left(\frac{\nu + \mu + \delta k - 1}{2\delta_{k-1}}\right)^2} - \frac{\mu}{\delta_{k-1}} \quad , \quad (10)$$

Учитывая , что $П_{к-1}(\nu)$ должно быть меньше единицы, и заменяя $\delta = \nu/\mu$ находим.

$$\prod_{k-1}(\delta) = \frac{1 + \delta + \rho \sum_{i=1}^{k-1} \rho_i}{2\rho \sum_{i=1}^{k-1} \rho_i} - \sqrt{\left(\frac{\nu + \mu + \delta k - 1}{2\delta_{k-1}}\right)^2} - \frac{\mu}{\delta_{k-1}} \quad , \quad (11)$$

$$Q_k = \frac{1-\rho\sum_{i=1}^{k-1}\rho_i}{\delta\left\{1+\left[\delta+\rho\sum_{i=1}^{k-1}\rho_i(1-\prod_{k-1}(\delta))\right]^{-1}-\rho P_k\right.} \quad , \qquad (12)$$

Рассмотрим случая плотности равномерной закона распределения ценности информации :

$$f(C_0) = \begin{cases} \frac{1}{C_{\max}} & 0 \le C_0 \le C_{\max} \\ 0 & C_0 < 0, C_0 > C_{\max} \end{cases} \quad , \qquad (13)$$

В этом случае

$$P_k = \frac{C_{k-1}-C_k}{C_{\max}} = B_{k-1} - B_k \quad , \qquad (14)$$

Где

$$B_k = \frac{C_k}{C_{\max}}, k = \overline{1,n} \quad . \qquad (15)$$

В соответствии с (3)

$$P_k M_k(C_0) = \int_{C_k}^{C_{k-1}} C_0 f(C_0) dC_0 = \frac{1}{C_{\max}} \int_{C_k}^{C_{k-1}} C dC = \frac{C_{k-1}^2 - C_k^2}{2C_{\max}} = \frac{C_{\max}}{2}(B_{k-1}^2 - B_k^2$$

(16)

$$M(C) = \frac{C_{\max}}{2}\sum Q_k(B_{k-1}^2 - B_k^2) \quad , \qquad (17)$$

Где с учетом (12)

$$Q_k = \frac{1-\rho(1-B_k)}{\delta\left\{1+\left[\delta+\rho(1-B_{k-1})(1-\prod_{k-1}(\delta))\right]^{-1}-\rho(B_{k-1}-B_k)\right\}} \quad , \qquad (18)$$

При равномерном законе распределения

$$W^* = \frac{\sum_{k=1}^{n}\left[1-\rho(1-B_k)(B_{k-1}-B_k)\right]}{\delta\left\{1+\left[\delta+\rho(1-B_{k-1})(1-\prod_{k-1}(\delta))\right]^{-1}-\rho(B_{k-1}-B_k)\right\}} \quad , \qquad (19)$$

Очевидно, что максимум достигается при некоторых значениях W*, которые не зависят от абсолютного значения $C_{макс}$. Следовательно, при равномерном законе распределения ценности информаций можно при любом заданном числе n приоритетов определить оптимальные значения обеспечивающие максимум W*.

Экспоненциальный закон распределения ценности информаций :

$$f(C_0) = \frac{1}{C_0} e^{-\frac{C}{C_0}} \quad , \qquad (20)$$

В данном случае

$$P_k M_k(C_0) = \int_{C_k}^{C_{k-1}} C_0 f(C_0) dC_0 = \int_{C_k}^{C_{k-1}} \frac{C_0}{\overline{C_0}} e^{-\frac{C_k}{\overline{C_0}}} dC_0 = C_0 e^{-\frac{C_k}{\overline{C_0}}}\left[1+\frac{C_k}{\overline{C_0}} - e^{\frac{C_{k-1}-C_k}{C_0}}(1+\frac{C_{k-1}}{\overline{C_0}})\right]$$

(21)

$$P_k = \int_{C_k}^{C_{k-1}} \frac{1}{C_0} e^{-\frac{C_k}{\overline{C_0}}} dC_0 = e^{-\frac{C_k}{\overline{C_0}}}(1 - e^{-\frac{C_{k-1}-C_k}{\overline{C_0}}}) \quad , \qquad (22)$$

$$\sum_{i=1}^{k} P_i = e^{-\frac{C_k}{\overline{C_0}}} \quad , \qquad (23)$$

Обозначая $-\frac{C_k}{C_0} = d_k$ получаем

$$Q_k = \frac{1-\rho e^{-d_k}}{\delta\left\{1+\left[\delta+\rho e^{-d_{k-1}}(1-\prod_{k-1}(\delta))\right]^{-1}-\rho e^{-d_k}\left[1-e^{-(d_{k-1}-d_k)}\right]\right\}}$$

(24)

$$W^* = \sum_{k=1}^{n}\frac{e^{-d_k}\left[1+d_k-e^{-(d_{k-1}-d_k)}(1+d_{k-1})\right](1-\rho e^{-d_k})}{\delta\left\{1+\left[\delta+\rho e^{-d_{k-1}}(1-\prod_{k-1}(\delta))\right]^{-1}-\rho e^{-d_k}\left[1-e^{-(d_{k-1}-d_k)}\right]\right\}}$$

Как в предыдущем случае, оптимальные значения обеспечивающие максимум величины W* , не зависят от абсолютного значения ценности информаций.

Отметим, что крайние значения P_1(P_1=0 и P_1=1) соответствуют без приоритетной системе, в которой степень сохранения ценности информации W равна вероятности своё временной передачи Q.

Для оценки выигрыша, получаемого от применения приоритетной системы, рассчитана величина $\eta = \frac{1-Q}{Q}\cdot\frac{W^*}{1-W^*}$ (25)

Результаты проведенного исследования приоритетной системы, основанной на разделении информаций по их ценности , позволяют сделать следующие выводы:

1. Введение приоритетов обеспечивает увеличение ценности потока доставленных информаций.
2. Выигрыш получается при любом делении потока на приоритеты (даже неоптимальном). Когда информациям большой ценности назначаются более высокий приоритет.
3. Выигрыш от введения приоритетной системы увеличивается при увеличении числа приоритетов, повышении загрузки и при более быстром старении информации.
4. Введение приоритетов позволяет избежать блокировки системы даже при больших перегрузках.

ВИРТУАЛ ШАХСИЙ ТАРМОҚ ТРАНСПОРТИНИ ТАШКИЛ ҚИЛИШ УСУЛЛАРИ

А.Ф Хайтбаев (ТАТУ ассистент)

Сўнгги вақтларда телекоммуникациялар дунёсида виртуал хусусий тармоқларга (Virtual Private Network – VPN) оширилган қизиқиш кузатилмоқда. Бу Internet тармоғи орқали олисдаги офисларни ва олисдаги фойдаланувчиларни арзонроқ уланиши ҳисобига корпоратив тармоқларни ишлатишга сарфларни камайтириш зарурати орқали асосланади. Ҳақиқатан, бир неча тармоқларни Internet орқали уланиши бўйича хизматлар нархлари, масалан, Frame Relay тармоқларига таққослаганда нархлардаги сезиларли фарқларни пайқаш мумкин. Лекин, таъкидлаш керакки, Internet орқали тармоқларни бирлаштиришда маълумотларни узатиш хавфсизлиги хақида масала вужудга келади, шунинг учун узатиладиган маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашга имкон берадиган механизмларни яратиш зарурати вужудга келди. Бундай механизмлар асосида қурилган тармоқлар VPN тармоқлар номини олди.

Ушбу ишда хусусий виртуал тармоқларни ишлатиш протоколлари ва усуллари кўриб чиқилган. VPN технологиясининг афзалликлари шундан иборатки, олисдан уланишни ташкил этиш телефон линияси орқали эмас, балки Интернет орқали амалга оширилади, бу анча арзон ва яхши бўлади. VPN технологиясининг камчиликликлари шундан иборатки, VPN ечимни қуриш воситалари ҳужумларни аниқлаш ва тўсиш тўлақонли воситалари ҳисобланмайди. Улар қатор рухсат этилмаган таъсирларни олдини

олиши мумкин, лекин корпоратив тармоққа суқулиб кириш учун ишлатилиши мумкин бўлган барча имкониятларни ҳам олдини ола олмайди. Лекин буларнинг барчасига қарамасдан VPN технологияси кейинги ривожланишга истиқболларга эга.

Келажакда VPN технологияларни ривожланиши режасидани нимани кутиш мумкин? Шубҳасиз, бундай тармоқларни қуришнинг ягона стандарти ишлаб чиқилади ва тасдиқланади. Энг муҳими бу стандартнинг асоси ўзини кўрсатиб бўлган IPSec протоколи бўлади. Кейин ишлаб чиқарувчилар ўз маҳсулотларининг унумдорликларини оширишга ва VPN тармоқни қулай бошқариш воситаларини яратишга эътиборларини қаратишади. Аниқроғи, VPN тармоқни қуриш воситаларининг ривожланиши маршрутизаторлар асосидаги VPN тармоқларни қуриш йўналишида бўлади, чунки бу ечим ўзида етарлича юқори унумдорликни, VPN интеграцияланишни ва битта қурилмада маршрутлаштиришни мужассамлаштиради. Хулоса қилиб айтиш керакки, замонавий VPN технологиялари зарур хусусиятларга эга бўлган устма уст тармоқни ташкил қилиш мумкин.

КИРИШ ТАРМОҒИДА МУЛЬТИСЕРВИС ТРАФИГИНИ ИНТЕРВАЛЛИ УСУЛДА ТАҲЛИЛ ҚИЛИШ

А.Ф. Хайтбаев (ТАТУ ассистент)

Замонавий мультисервис алоқа тармоқлари учун тавсифловчи буюртма оқимларини оммавий хизмат кўрсатиш имкониятли тизими кўрилган. Умумлаштирилган Хинчин-Поллячек формуласи қабул қилинди. Пуассон трафик билан реал трафикни таққослаш келтирилган. Навбатнинг ҳажмида корреляцион оқим хусусиятларига таъсирини аниқловчи омиллар келтирилган.Мультисервис тармоқ трафиги бир неча характерга эга. Айниқса бу кириш тармоғи трафигига амал қилади. Шунинг учун тармоқ чегарасида оператор жуда аниқлик билан трафикдаги нотенгликни назорат қилишга мажбур. Трафикдаги нотенглик коммутаторда нотенгликга олиб келади. Коммутаторларга бир қанча оммавий хизмат кўрсатиш сифатида қаралади. Оммавий хизмат кўрсатишни таҳлилида одатда иккита эҳтимолий тавсифи кўрилади:

1. Қўшни буюртмалар орасида интервал эҳтимолликларини тақсимлаш.
2. Буюртмага хизмат кўрсатишда вақт узунлиги эҳтимоллигини тақсимлаш.

Буюртма сифатида пакетлар оқими тушунилади, хизмат кўрсатиш вақти сифатида эса пакетларни узатиш вақти кўрилади.

Оммавий хизмат кўрсатишда навбатлар хажмини аниқлашда асосий нисбат машҳур Хинчин-Полляч формуласи ҳисобланади, унда ўрта ҳажмли навбат ва тизимда юкланиш коэффициенти орасидаги боғлиқ ўрнатилади. Бу формула фақат Пуассон оқим учун ҳаққонийдир. Шунинг учун умумий кўринишдаги оқимли тизимда навбатдаги ҳажмни аниқлаш учун фойдали бўлган боғликликни топиш зарур. Бундай боғликлик хизмат кўрсатиш интервал мобайнида, буюртмалар сонини аниқлашга асосланган пастда кўрилган интерваль метод ёрдамида қабул қилинган. Олдин қўлланилган икки хилдаги тақсимлаш эҳтимоллиги таҳлили ўрнига тақсимланган юкланиш коэффициенти эҳтимоллигининг битта характеристикаси таҳлили тақдим этилади. Тақдим қилаётган интервал методлари берилган юкланиш коэффициентида каналда берилган ўтказувчанлик қобилиятида юзага келадиган тўғридан тўғри навбатдаги ҳажмлар ва кечикишлар билан алоқадор иккита параметр ёрдамида хоҳлаган турдаги илова трафигини характерлаш мумкин. Келтирилган параметрларнинг афзалликлиги бўлиб чиқиш оқимнинг мос келадиган характеристика суммаси йўли орқали жами трафикларнинг характеристикаларини олиш мумкин. Қабул қилинган умумий аналитик нисбат коммутатор кириш тармоғида кечикиш ва навбатдаги ҳажмларни аниқлашда шундай параметрларни қўллашга имкон беради.

ВОПРОСЫ ПРИМЕНЕНИЯ АОЛС В ТЕЛЕКОММУНИКАЦИИ НА УЧАСТКЕ «ПОСЛЕДНЕЙ МИЛИ»

А.М.Эшмурадов (ТУИТ, зав.кафедрой ТИ)

Высокие затраты при прокладке каналов связи в условиях города, и вводимые в скором времени ограничения на прокладку кабелей, ведут к необходимости появления альтернативных линий связи. Эту проблему можно было бы решить за счет радиочастот, но этот диапазон сильно ограничен нуждами спецслужб и переполнен провайдерами предоставляющие свои услуги на недостаточных скоростях. В цивилизованных странах из пучин проводов города «распутывает» внедрение атмосферные оптические линии связи. Этот способ передачи информации имеет свои значимые плюсы: отсутствие необходимости выделения отдельных частот, очень маленькое время введения линии в эксплуатацию, большой защищенностью информации от перехвата, канал связи не подвержен помехам и наводкам из-за удаленности от радиочастотного спектра, максимально защищен от атмосферного электричества и т.д. В последнее время все большую популярность приобретает применение лазерных каналов при создании охранных периметров и в системах обеспечения безопасности благодаря скрытности канала и возможности передачи качественной видеоинформации от камер наблюдения в режиме реального времени. Основными применениями технологии в настоящее время остаются: доступ на последней миле, преодоление преград, а также связь локальных сетей. Лазерная связь осуществляется путем передачи информации с помощью электромагнитных волн инфракрасного диапазона спектра. Механизмы поглощения света в прозрачной атмосфере во многом аналогичны происходящим в оптоволокне.

В своей работе мы хотим проделать ряд вычислений, для определения реальных характеристик предоставленной нам системы АОЛС. Проверить её надежность от перехвата с помощью системы состоящей из призмы и фо- тодиода. Создать диаграмму направленности АОЛС в зависимости от коэффициента ошибок и определить её форму. С помощью эмитирующих «серых» фильтров(ND) воссоздать различные погодные воздействия, замерить уровень сигнала и посчитать коэффициент ошибок. Для завершения обзора мы сравним цены на построение кабельных и атмосферных линий связи и сравним их окупаемость. Целью работы ставятся три основных задачи: 1. Проверка защищенности сигнала от перехвата и снятия. Диаграмма направленности по коэффициенту ошибки BER. Воздействие погодных условий и их влияние на качество передачи данных и мощность сигнала. 2. Экономическая обоснованность использования. 3. По результатам проделанной работы будут сделаны выводы и внесены предложения по защите сигнала и использованию системы.

АТМОСФЕРАЛИ ОПТИК АЛОҚА ЛИНИЯСИНИНГ САМАРАДОРЛИГИНИ ОШИРИШ УСУЛИ

А.М.Эшмурадов (ТАТУ, ТИ кафедраси мудири)

Замонавий жамиятда ахборот ҳаёт учун энг зарур маълумотлардан ҳисобланади. Шу туфайли ахборотни узатиш жараёни энг муҳим омиллардан саналади. Маълумки ахборотни узатиш жараёни икки усулда олиб борилади: симли ва симсиз. Симли узатиш жараёни оддий бўлиб, кўп меҳнатни талаб қилади. Кабелларни ерга ётқизиш, уларни монтаж қилиш ва ҳ.к. Агарда кабель ётқизиш йўналишида сув тўсиқлари, истироҳат боғлари ва ҳ.к. лар тўғри келиб қолса, бу усул анча қийинчиликларга олиб келади. Албатта бу ҳолатда симсиз узатиш усулини қўллаш ҳар томонлама маъқул ҳисобланади. Бу усул ҳам ишончлилик ва узатиш тезлиги жиҳатидан симли узатиш тизимидан қолишмайди. Симсиз узатиш тизимини ҳам ўз навбатида икки қисмга ажратиш мумкин:

радио ва оптик узатиш тизимларига. Ҳозирги пайтда атмосферали оптик узатиш тизими кенг ривожланмоқда. Албатта бу тушунарли ҳолат бўлиб, бу тизимда алоҳида частота диапозонига лицензия талаб этилмайди ҳамда электромагнит майдони таъсирларига сезувчанлиги мутлақо йўқ деса ҳам бўлади.

Шундай қилиб атмосферали оптик алоқа линияси (АОАЛ) бу алоқа тури ҳисобланиб, маълумотларни икки объектга атмосфера орқали узатиш тушунилади. Бу ҳолатда оптик тола ёки радио эфирдан фойдаланилмайди.

Атмосферали оптик алоқа линиясини ишлатиш жудаям қулай бўлиб, кабелли тизимдагидек мураккаб ва қиммат монтаж тизими талаб этилмайди. Атмосферали оптик алоқа линиясининг яна бир қулайлиги шундан иборатки у симли коммуникациялар ишлатиш таъқиқланган ёки мумкин бўлмаган жойларда, масалан тарихий обидалар жойлашган жойларда ишлатиш мақсадга мувофиқ бўлади. Айниқса, катта шаҳарларда зич жойлашган иморатларга эга бўлган шаҳарларда атмосферали оптик алоқа линиялари тизимларининг қабул қилиш ва узатиш қурилмаларини иморатлар томларига жойлаштириш мумкин. Узатиш ва қабул қилиш қурилмалари орасида бир бирини кўриш имкониятига эга бўлиш лозим. Шу ҳолатда улар орасидаги масофа икки километрни, маълумотларни узатиш тезлиги эса 25 мБ/с дан 1,25 Гб/с гача бўлиши мумкин.

АОАЛ нинг яна авфзалликларидан бири шундаки узатиш ва қабул қилиш қурилмалари ўртасидаги маълумотларни ушлаб олиш эҳтимоли нолга тенг. Шунинг учун ҳам бу тизимни кўпроқ корхоналарда ички алоқани ташкил қилишда кўпроқ ишлатишади. Ҳамма тизимларда камчилик бўлгани сингари АОАЛ да ҳам камчилик учрайди. Жумладан нур тарқатувчи элементлари – лазер диоди ёки ёруғлик диодининг кам бўлса ҳам ишдан чиқиш ҳолати ҳамда ёмон об-ҳаво шароитларида каналнинг ўтказиш қобилиятининг пасайиш ҳолатлари кузатилади.

Кўрсатилган камчиликларни бартараф этиш учун ушбу мақолада лазер нурининг қувватини автомат равишда ўзгартириб туриш таклиф этилмоқда.

МЕТОДЫ СТАБИЛИЗАЦИИ МОЩНОСТИ ИСТОЧНИКА ИЗЛУЧЕНИЯ ПЕРЕДАЮЩЕГО ОПТОЭЛЕКТРОННОГО МОДУЛЯ ВОСС

Н.Юнусов (доцент ТУИТ)

Передающий оптоэлектронный модуль (ПОМ), осуществляющий преобразование входного электрического сигнала в оптический сигнал, вводимый в оптическое волокно линии передачи является одним из важных и неотъемлемых функциональных блоков волоконно-оптических систем связи (ВОСС). В роли основного элемента ПОМ выступает лазерный или светоизлучающий диод - источник оптической несущей, которая модулируется в соответствии с передаваемой информацией. Одно из основных достоинств вышеназванных источников излучения состоит в том, что физические процессы в них, ответственные за электрооптическое преобразование энергии позволяют непосредственную (прямую) модуляцию излучаемой оптической несущей с помощью встроенных к ним электронных устройств.

Исходным моментом в решении такой задачи является необходимость обеспечения стабильного электрического режима, а следовательно, стабильной мощности излучения источника оптической несущей.

Данная работа посвящена вопросам схемотехнической реализации и анализу особенностей функционирования оптоэлектронного устройства стабилизации мощности источника излучения (для определенности, светоизлучающего диода) передающего оптоэлектронного модуля ВОСП.

Принцип стабилизации электрического режима и мощности излучения источника оптической несущей основывается на использовании высоко-омных генераторов тока – так называемых генераторов стабильного тока, схема которого иллюстрируется на рис.1.

Непрерывной и штриховой линиями 1 и 1^1на этом рисунке показаны две неодинаковые вольт-амперные характеристики (ВАХ) светоизлучающего диода. Подобное различие ВАХ может быть связано с температурным или временным дрейфом, а также технологическим разбросом характеристик однотипных светоизлучателей. Рисунок позволяет сравнить два способа возбуждения светодиода от источника постоянного напряжения $E_п$ по цепи с линейным резистором (прямая линия 2) и по цепи с существенно нелинейной ВАХ (кривая 3), обладающей четко выраженным горизонтальным участком.

Как видно из рис.1, сдвиг рабочей точки светодиода по прямой линии 2 относительно низкоомной нагрузки из положения О и O_1 скажется в заметном спаде тока, протекающего через светодиод, что вызывает снижение мощности излучаемого светового потока. В тех же условиях переход рабочей точки О в положение O_2 по горизонтальной линии 3 нагрузки не приводит к заметному снижению тока, протекающего через светодиод и мощности его излучения.

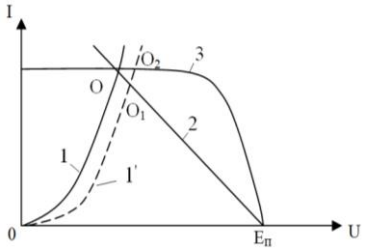


Рис. 1 Возбуждение источника излучения - светоизлучающего диода: по цепи с линейным резистором (прямая линия 2) и по цепи с нелинейной ВАХ, имеющей участок, практически параллельный к оси напряжения U (кривая 3)

Если учесть, что существенно нелинейная ВАХ (2) с участком высокоомного дифференциального сопротивления свойственна коллекторной цепи биполярного транзистора или стоковой цепи полевых транзисторов, то можно прийти к выводу, что использование транзисторных каскадов на биполярных и полевых транзисторах в качестве генераторов стабильного тока, возбуждающего светоизлучатель позволяет в значительной степени устранить влияние нестабильности электрических характеристик излучателя на мощность излучаемого им светового потока.

На рис.2 приведены некоторые примеры схемотехнической реализации выше описанного принципа стабилизации мощности источника излучения на основе биполярных транзисторных каскадов.

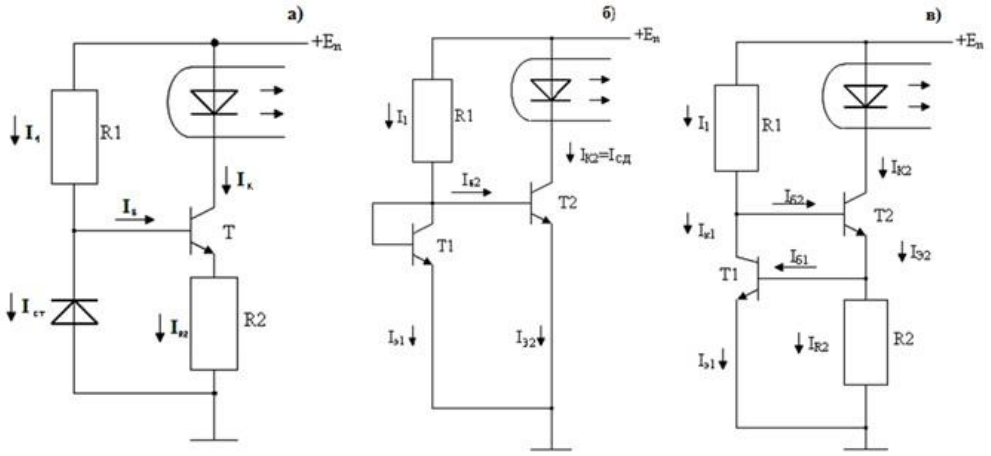


Рис.2. Схемы устройства стабилизации мощности излучения светоизлучающего диода: со стабилитроном (а), биполярным транзистором (б), биполярным транзисторным каскадом с отрицательной обратной связью (в) в управляющей ветви и биполярным транзисторным каскадом в управляемой ветви

Общая особенность приведенных на этом рисунке схем, состоящих из управляющей и управляемой ветвей заключается в том, что выходные характеристики биполярного транзистора, включенного по схеме с общим эмиттером и управляемого потенциалом его базы в активном режиме вклю-чения практически параллельны к оси напряжения $U_{кэ}$ в широком интервале изменений этого напряжения.В результате этого значения тока, соответс-твующие точкам пересечения ВАХ светодиода и биполярного транзистора при различных значениях $U_{бэ}$ окажутся строго фиксированными (рис.3).

В случае схемы, приведенной на рис.2а управление видом ВАХ биполярного транзистора Т осуществляется потенциалом электрода стабилитрона, образующего делитель напряжения с резистором R_1 в управляющей ветви устройства. Величина этого потенциала $U_{ст}= U_{бэ}$ определяется, как напряжение соответствующее точке пересечения ВАХ стабилитрона с линией его нагрузки R1.

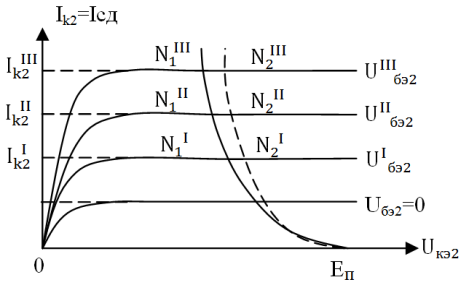


Рис.3. К принципу действия устройства стабилизации мощности излучения светодиода на биполярных транзисторных каскадах

Отличительной особенностью, схемотехнического решения стабиль-ного питания светоизлучателя, показанного на рис.2б состоит в том, что его можно изготовить в интегральном исполнении.Транзистор Т1 здесь включен в диодном режиме (его база коротко замкнута с коллектором) и играет роль генератора напряжения с помощью которого управляется эмиттерный переход транзистора Т2.Недостатком выше рассмотренной схемы является то, что базовый ток $I_{б2}$ транзистора Т2 сильно зависит от температуры (хотя этот ток очень мал по сравнению с токами $I_{э2}$ и $I_{к2}$).

В целях устранения этого недостатка можно использовать моди-фикацию устройства стабилизации мощности излучения светоизлучателя, построенную на основе биполярных транзисторных каскадов, охваченных отрицательной обратной связью, которая играет стабилизирующую роль и ослабляет требования к идентичности транзисторов (рис.2в).

Заключение. В работе рассмотрены схемотехнические решения устрой-ства стабилизации мощности источников излучения, применяемых в приемном модуле ВОСС и их сравнительный анализ относительно влияния таких факторов, как стабильность рабочего режима, температурный дрейф, степень идентичности используемых источников излучения, особенностей конструкции устройства.

ТОАТ ЛАРДА ЁРУҒЛИК МАНБАИ НУРЛАНИШ ИНТЕНСИВЛИГИНИ ТТЛ ИНТЕГРАЛ МАНТИҚ ЭЛЕМЕНТИ ЁРДАМИДА МОДУЛЯЦИЯЛАШ УСУЛЛАРИ

Н.Н. Юнусов (2-босқич магистранти)

Маълумки, бугунги кунда кенг қўлланиладиган толали оптик алоқа тизимлари (ТОАТ) да оптик элтувчи – нурланиш интенсивлигини узатилиши зарур бўлган ахборот сигналига монанд равишда ўзгартиришдан иборат бевосита (тўғридан-тўғри) модуляциялаш жараёни мазкур тизимлар ишини ташкил этишга оид асосий жараёнлардан бири ҳисобланади. Шу муносабат билан ТОАТ ларнинг узатувчи модулини ишлаб чиқарувчи фирмаларнинг ноу-хауси бўлган ва бугунги кунда мавжуд адабиётларда –

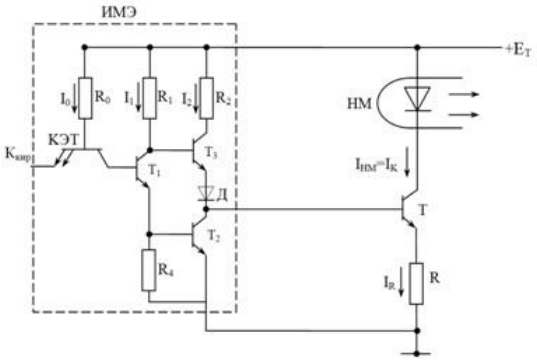
дарслик ва ўқув қўлланмаларида етарли даражада ёритилмаган бу масалани ўрганиш ва тадқиқ этиш долзарб аҳамият касб этади.

Таҳлиллар кўрсатадики, ёруғлик манбаи (лазер диоди ёки ёруғлик диоди) нурланиш интенсивлигини рақамли сигналлар таъсирида модуляциялаш учун ТТЛ туридаги интеграл мантиқ элементи (ИМЭ)ни чиқиш занжиридаги ёруғлик манбаи билан мувофиқлаштириш масаласи мавжуд ва бу масалани бир неча усуллар билан - катта қаршиликли резистор, кремнийдан тайёрланган диод, эмиттер қайтаргичли биполяр транзистордан фойдаланган ҳолда ҳал этиш мумкин. Бироқ бу усулларнинг ҳар бири муайян камчиликларга эга. Интеграл мантиқ элементи ёрдамида бошқарув токи қийматининг нисбатан катталиги, ҳалақитларга бардошлиги-нинг пастлиги, ёруғлик манбаидан оқиб ўтадиган токнинг, демак нурланиш интенсивлигининг нобарқарорлиги шулар жумласидандир.

Ушбу мақола ТТЛ туридаги мантиқ элементини чиқиш занжиридаги ёруғлик манбаи билан юқорида қайд этилган камчиликларни бартараф этиш имконини берадиган мувофиқлаштириш схемасини кўриб чиқишга (қуйидаги 1-расмга қаранг) ва унинг иш хусусиятларини таҳлил этишга бағишланган.

Ёруғлик манбаи нурланиш интенсивлигини рақамли электр сигнали ёрдамида модуляциялаш имконини берадиган ушбу қурилманинг иш принципини қуйидагича тавсифлаш мумкин.

Мантиқ элементининг ишчи киришига мантиқий “0” сатҳига мос келган 0.2 В кучланиш берилса, I_0 токи тегишли эмиттер ўтиши орқали оқади. Тўйиниш улаш режимида ишлаётган бу транзисторнингколлектор ўтиши орқали оқаётган ток бу ҳолда нисбатан кичик қийматга эга бўлиб, у T_1 ва T_2 транзисторлар эмиттер ўтишларининг очиқ ҳолатга ўтказиш учун етарли бўлмайди. Бу транзисторлар берк улаш режимида ишлайди. T_1 транзистор берк ҳолатда бўлгани учун R_1 резистор орқали келаётган I_1 токи T_3 транзисторнинг базаси орқали оқади. Агар R_2 резисторнинг қаршилиги тегишли тарзда танланиб олинса, бу транзистор тўйиниш улаш режимига ўтади. Шундай қилиб, R_2 резистор, T_3 транзисторнинг коллектори ва эмиттери ва очиқ ҳолатдаги Д диоддаги йиғинди кучланиш T_2 транзистор-нинг коллектори ва эмиттери орасидаги кучланиш тушишидан анча кичик бўлади, яъни ИМЭ нинг чиқишида мантиқий “1” га мос келувчи кучланиш ҳосил бўлади.



1-расм. Ёруғлик манбаи нурланиш интенсивлигини ТТЛ интеграл мантиқ элементи ёрдамида модуляциялаш схемаси

Бу ҳолда чиқиш занжиридаги умумий эмиттер схемаси бўйича уланган биполяр транзисторнинг эмиттер ўтиши очиқ ҳолатга, транзистор эса актив улаш режимига ўтади. Натижада бу транзисторнинг катта қаршиликли коллектор занжирида жойлашган ёруғлик манбаи нурланиш тарқатадиган ҳолатга ўтади, яъни чиқишда мантиқий “1” сатҳига мос нурланиш интенсивлиги ҳосил бўлади. Умумий эмиттер схемаси бўйича уланган биполяр транзисторнинг коллектор ўтиши катта дифференциал қаршиликка эга бўлгани учун бу занжирга жойлашган ёруғлик манбаининг электр режими, демак унинг нурланиш интенсивлиги барқарор бўлади.

ТТЛ туридаги ИМЭ нинг киришига мантиқий “1”га мос келган, яъни $E_т$ га яқин кучланиш берилса, R_o резистор орқали оқаётган ток кўп эмиттерли транзисторнинг коллектор ўтиши орқали оқиб ўтади. Бунда T_1 транзистор базасининг потенциали T_1 ва T_2 транзисторлар эмиттер ўтишларининг очиқ ҳолатга ўтиши учун етарли бўлади. R_1 резистор бўйича келаётган I_1 токи T_1 транзистор орқали оқиб ўтади. Бу ҳолда T_3 транзистор базасининг потенциали унинг эмиттер ўтиши ва Д диодни очиқ ҳолатга ўтказиш учун етарли бўлмагани учун бу транзистор берк улаш режимига ўтади. Натижада ИМЭ нинг чиқишида 0.2 В га яқин кучланиш ҳосил бўлади. Бундай кучланиш таъсирида Т транзистор берк улаш режимига ўтади ва ундан кичик қийматли ток оқиб ўтади. Транзисторнинг коллектор занжирида жойлашган ёруғлик манбаи нурланмаган ҳолатга ўтади, бошқача айтганда чиқишда мантиқий “0” сатҳини оламиз.

Шундай қилиб, юқорида кўриб ўтилган қурилма унинг киришига берилган рақамли электр сигнали таъсирида ёруғлик манбаи нурланиш интенсивлигини модуляциялаш ва бу жараённинг барқарорлигини таъминлаш имконини беради.

ПРИНЦИПЫ НАРУШЕНИЯ ДОСТУПНОСТИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ

Д.Б. Абдуллаев (ТУИТ, магистрант)

Необходимо своевременно изучать новые технологии как объекты информационной безопасности, выявлять в них уязвимые места и разрабатывать механизмы и методы обеспечения их информационной безопасности.

Международная практика развитых стран показывает, что одним из важных направлений работ в области информационной безопасности сетей телекоммуникаций является выработка стратегии стандартизации информационной безопасности.

Сейчас все усилия в области информационной безопасности направлены не только на защиту конфиденциальности, но и на другие наиболее важные показатели ИБ, т.е. целостности и доступности содержания информации.

Проблема создания и поддержания защищенной среды информационного обмена, реализующая определенные правила и политику безопасности современной организации, является весьма актуальной.

Одновременно с бурным развитием рынка услуг передачи данных растет и уровень несанкционированного доступа к ним в операторских сетях. Об этом свидетельствуют данные, о зарегистрированных нарушениях по незаконному использованию ресурсов сети передачи данных, несанкционированный доступ к услугам связи остаётся одним из самых больших проблем операторов телекоммуникаций.

Одним из основных факторов обеспечения безопасности от несанкционированного доступа в сетях передачи данных является контроль и управление доступом.

Выбор определенного механизма основывается на анализе СПД, как объекта контроля и управления доступом.

Контроль и управление доступом являются наиболее важными методами защиты сетей передачи данных от воздействий нарушителя. Контроль доступа подразумевает управление идентификацией и аутентификацией пользователей, управление присвоение им прав и привилегий по доступу к ресурсам, контроль доступа и выявление попыток НСД.

Безопасная информационная система — это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надежно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

Конфиденциальность (confidentiality) — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).

Доступность (availability) — гарантия того, что авторизованные пользователи всегда получат доступ к данным.

Целостность (integrity) — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначения системы, характера используемых данных и типа возможных угроз.

Искусственные угрозы, в свою очередь, можно разделить на *умышленные и неумышленные*.

Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности. Кроме того, к такому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы. Так, например, из-за отказа диска, контроллера диска или всего файлового сервера могут оказаться недоступными данные, критически важные для работы предприятия. Поэтому вопросы безопасности так тесно переплетаются с вопросами надежности, отказоустойчивости технических средств. Угрозы безопасности, которые вытекают из ненадежности работы программно-аппаратных средств, предотвращаются путем их совершенствования, использования резервирования на уровне аппаратуры (RAID-массивы, многопроцессорные компьютеры, источники бесперебойного питания, кластерные архитектуры) или на уровне массивов данных (тиражирование файлов, резервное копирование).

Умышленные угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств. Так, умышленные угрозы возникают в результате деятельности хакеров и явно направлены на нанесение ущерба предприятию.

К умышленным угрозам относятся:

- несанкционированный доступ к информации и сетевым ресурсам;
- раскрытие и модификация данных и программ, их копирование;
- раскрытие, модификация или подмена трафика вычислительной сети;
- разработка и распространение компьютерных вирусов, ввод в программное обеспечение логических бомб;
- кража магнитных носителей и расчетных документов;
- разрушение архивной информации или умышленное ее уничтожение;
- фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема;
- перехват и ознакомление с информацией, передаваемой по каналам связи, и т. п.

Незаконное проникновение может быть реализовано через уязвимые места в системе безопасности с использованием недокументированных возможностей операционной системы. Эти возможности могут позволить злоумышленнику «обойти» стандартную процедуру, контролирующую вход в сеть. Уязвимости, угрозы и риски ИБ носят специфический характер, все зависит от среды передачи данных, структуры сети передаваемых данных, назначения сети и т.д.

Методология выявления уязвимости предусматривает проведение исследований в три этапа.

Первый этап состоит в изучении системы, причем особое внимание уделяется принципам функционирования механизмов защиты.

На *втором этапе* происходит выдвижение предположений (гипотез) о потенциально уязвимых компонентах, которые затем тщательно проверяются на основании анализа документации, реальных особенностей телекоммуникационной системы и деталей ее функционирования и с помощью проведения специальных тестов, призванных подтвердить или опровергнуть присутствие предполагаемого изъяна в системе защиты.

Наконец, на *третьем*, заключительном этапе проводится обобщение полученных результатов, и формируются списки (перечни) выявленных ИЗ и успешных атак.

С точки зрения технологии создания защищенных систем, наибольшее значение имеют следующие вопросы:

1. Каким образом уязвимости появляются в системе защиты? (Классификация уязвимости по источнику появления).

2. На каком этапе они вносятся? (Классификация уязвимости по этапу возникновения).

Необходимо ясно осознавать, что потенциальный нарушитель всегда сам определяет правила своих действий, поэтому для разработки эффективной системы защиты СПД от НСД необходимо располагать моделью Потенциального нарушителя.

К множеству НСД к СПД, относительно которых должна быть обеспечена защита, относятся:

- защита от наиболее опасных из известных (обнаруженных и зафиксированных в функционирующих на сети СПД) НСД;
- защита от всех известных (из литературных источников) НСД;
- защита от всех потенциально возможных НСД.

Для каждой СПД необходимо рассматривать относящиеся к ней уязвимые места и соответствующие угрозы. При этом необходимо понимать, что если уязвимость существует, но и связанной с ней угрозы или существует угроза, несвязанная с каким либо уязвимостями, то рисков НСД нет.

ДАСТУРИЙ КОНФИГУРАЦИЯЛАНАДИГАН ТАРМОҚ ТЕХНОЛОГИЯСИ, УНИНГ АФЗАЛЛИК ВА КАМЧИЛИКЛАРИ

М.М. Абдуллаев (ТАТУ, ассистент)
З.Р.Атажанов (ТАТУ, 4 – курс босқич талабаси)

Кўплаб мутахасисларнинг фикрига кўра ўтган асрнинг 80 йилларида яратилган стандарт TCP/IP стек протоколи асосида компютер тармоқларининг бошқарув тизимлари эскирди ва катта трафикларни узатишда паст самародорликка эгалигини кўрсатди. Замонавий компютер тармоқларининг айрим катта ахамиятга эга камчиликлари қуйда келтирилган:

1.Бугунги кунда трафик ҳажми сезиларли даражада ўсиб бориши кузатилмоқда.

2. TCP/IP стек протоколида янги муаммо пайдо бўлганда бу муаммони ечадиган янги протоколни қўшиш орқали ҳал қилинади. Натижада доимий равишда протоколлар ва стандартлар сони ўсиб борди, бугунги кунда уларнинг сони 600 ортиқ .

3. Анъанавий тармоқ архитектураси тадқиқотлар учун ёпиқ ва амалий жиҳатдан ихтиёрий ўзгаришларни амалга ошириб бўлмайди.

4.Трафик геометрик прогрессия асосида ўсиб бормоқда.

Юқорида келтирилган муаммоларни ҳал қилиш мақсадида дастурий конфигурацияланадиган тармоқ(ДКТ) технолгияси ишлаб чиқилди.

ДКТ ишлаб чиқишдан асосий мақсад:

1.Оддий компютерда ишлатиш мумкин бўлган махсус дастурий таъминот яратиш ҳисобига маълумотларни узатишни бошқаришдан тармоқ қурулмаларини бошқаришни ажратиш.

2.Тармоқ бошқарувига, тармоқ қурилмаларининг алоҳида нусҳаларини бошқаришга ўтиш.

ДКТ технологияси компютер тармоғида бошқарув ва маълумотларни узатиш функцияларини ажратишни таклиф қилади. Бу вазифани амалга ошириш мақсадида OpenFlow номли очиқ кодли протоколни ишлаб чиқилган.

ДКТ архитектурасини тармоқ инфраструктураси, бошқарув ва илова поғоналаридан иборат.

ДКТ афзалликлари

1. Тармоқни бошқаришни виртуализациялашга ўхшаб ДКТ хусусиятида тармоқни қуриш ва хизмат кўрсатиш харажатларини пасайтиради.

2. Бошқарув функцияларидан ДКТ нинг коммутаторлари озод этилганлиги боис, уларнинг барча ресурсларидан маълумотлар узатишни тезлигни оширишда фойдаланиш мумкин бўлади.

3. ДКТ дастурий воситалари тармоқ архитектурасида мавжуд бўлган янги функционал имкониятларни қўшишга имкон беради.

4. Тармоқ маъмури марказлашган назорат шароитида тармоқ ишлаши тўғрисида тўлиқ маълумотга эга бўлиши мумкин бўлади.

5. Самарадорлик. Маълумотлар тракти ва бошқарув трактини ажратишда тармоқда маршрутизацияни марказлашган бошқарувга, коммутаторга эса трафикларни тезда узатишда ўзининг барча ресурсларини йўналтиришга имкон беради.

6.Таннарх. OpenFlow технологияси тармоқ бошқарувини виртуализациялаш ҳисобига тармоқни қуриш ва ўтказиш харажатларини камайтиради.

7. Администрлаштирилганлиги. Марказлашган сервердан фойдаланаши ҳисобига администраторга қулайликлар яратилади. Шунингдек, тармоқ физик кўринишини ўзгатирмасдан виртуал локал ва глобал тармоқ қуриш – виртуал тармоқ топологиясини яратиш имкониятини таклиф қилади.

ДКТ Камчиликлар.

1. ДКТ да трафикни бошқарув функцияси контроллерда бўлади, шу сабабли контроллерда юклама сезиларли даражада юқори бўлади, бу эса ўз навбатида сервер платформасига жиддий талаблар қўйишга сабаб бўлади.

2. ДКТ га ўтиш жараёни йирик компаниялар учун қийинлигини кўрсатяпти. Кўплаб замонавий коммутаторларда OpenFlow ни қўллаб қувватлашни амалга ошириш чегараланган, шу сабабли ҳозирги кунда бир вақтнинг ўзида иккита режимни – OpenFlow ва анъанавий коммутацияни қўллаб қувватлайдиган комбинацияланган коммутаторлардан кенг фойдаланилмоқда.

3. Масштаблашиш. Тармоқ бошқаруви барча функциялари битта серверда тўпланади

4. Ҳавфсизлик. OpenFlow да битта серверда бошқарувнинг барча функциялари амалга оширилганлиги туфайли, бундай тармоқни бузғунчилар бузиши осонроқ кечади.

Анъанавий тармоқдан ДКТ фойдаланадиган тармоқга ўтишда қуйдаги талаблар бажарилиши керак.

1) Тармоқ турли хил ишлаб чиқарувчиларнинг кўплаб қурилмаларидан биргаликда фойдаланишни таъминлайдиган гетерогенликни қўллаб қувватлаши керак. Хизматлар миграцияси гетероген инфраструктурада кўриб чиқилиши керак. Тармоқни рад этишга бардошлиликни таъминлаш ва ДТ (дастурий таъминот) ни янгилашни автоматик амалга ошириш учун хизматларни бажаришга йўналтирилган бўлиши керак.

2) Тармоқ керакли ДТ , инструментал воситалар (ИВ) ва симуляторларни қўллаб қувватлаши керак. Мавжуд ИВ бутун тармоқда ишлаш имконияти текширилган бўлиши ёхуд уларнинг функциялар шафофлиги таъминланган бўлиши керак.

3) Миграция босқичлари аниқланган бўлиши керак. Бошланғич тармоқ учун айрим оралиқ холатларни ўзгартириш ва кейинги миграцияларни амалга ошириш талаб қилиниши мумкин.

ДКТ компютер тармоқларида фойдаланилмаган ресурсларнинг юкламаларини ва

тармоқ бошқаруви самародорлигини оширишга ёрдам бериш орқали эксплуатацион харажатларни бир неча баробар пасайтиришга имкон беради.

БУЛУТЛИ ҲИСОБЛАШ ТЕХНОЛОГИЯСИДА АХБОРОТ ХАВФСИЗЛИГИГА ТАХДИДЛАР

М.М. Абдуллаев (ТАТУ, ассистент)
Х.Х. Маликов(ТАТУ, 2 – курс магистранти)

Бугунги кунда булут инфраструктарсини қуриш ва қўллашнинг турли туманлиги қатор муамоларни келтириб чиқармоқда, уларнинг ичида энг муҳими ушбу тармоқни яратиш ва ривожлантириш кординатциясини рўйхатга олишда унинг ахборот хавфсизлигини таъминлаш ҳисобланади.

Бугунги кунга келиб булутли ҳисоблаш янги технология ҳисобланмаяпти, лекин ахборот хавфсизлигини таъминлаш билан боғлиқ саволлар унинг энг заиф жойи бўлиб қолмоқди. Стандарт турдаги тахдидларга булутли структурани қуриш учун фойдаланиладиган технологик ҳусусиятлар билан боғлиқлик кириш ҳуқуқларини чегаралаш ва меҳмон машиналари ўртасидаги трафик, булутли воситаларни виртуализациялаш контроллерлари билан боғлиқ бўлган мураккабликларни юклайдиган физик серверларда жойлаштирилиши сабаб бўлади. Потенциал бузғунчилар учун очиқ нишонга айланишига яна бир сабаб мультидоменли ва кўпфойдаланувчили булутли ҳисоблаш структурасининг очиқлиги ва тақсимланганлигидадир.

Булутли ҳизматларни архитектураси бир бири билан ўзаро боғланган учта поғонага бўлинади: инфраструктура, платформа ва илова. Бу сатҳларнинг ҳар бири фойдаланувчи ва провайдер хизматларининг, дастурий ва конфигурациялаш билан боғлиқ бўлган хатоликларига бўлиши мумкин. Булутли ҳисоблаш тизимига хавфсизликка тахдиднинг бир нечта кўринишлари таълуқли. Булар бутунлилик, махфийлик унинг ресурсларига киришнинг рухсат этилганлиги, шаклнинг бир қисмидан фойдаланиш мумкин бўлган виртуал инфраструктура ва маълумотлар.

Булутда маълумотларни сақлаш бу маълумотларга серверда умумий киришга рухсат этилганлиги билан тушунтирилади. Агар компания тасодифан корпоратив маълумотларни, масалан мижозлар ёки интелектуал маҳсулотлар тўғрисидаги ахборот рўйхатдан ўтказилмаса тахдид бир неча маротаба ортади. Шу боис ахборотларни сақлашнинг юридик жавобгарлиги булут хизматларини тақдим этадиган провайдерга эмас, булутда бу маълумотларни жойлаштирадиган ташкилотга юклатилади. Масалан, агар мижоз ўзининг шахсий маълумотларини суғурта компаниясига тақдим этса компания унинг шахсий маълумотларини химоя қилишини кутади. Мижозга ушбу маълумотлар булут провайдерида ишончли сақланяпганлигини ахамияти йўқ. Мижозга маълумотлари ноқонуний тарқатилиши ва ҳимояланиши муҳим. Булутда маълумотларни сақлаш билан боғлиқ кейинги жиддий муамо бу – хавфсизлик хизмати ёрдамида ҳолатларни назорат қилиш ва аудит ўтказиш имконияти булут технология хизматларининг мижозида деярли мавжуд эмаслигида.

Булутли ҳисоблашда виртуализация технологиясини бажарилиши муҳим ҳисобланади. Виртуализация тамойилларидан бирига булутли ҳисоблашда ахборот хавфсизлигига тахдидлар киради, масалан турли хил виртуал машиналарда (ВМ) умумий ахборотларни сақлаш билан боғлиқ муаммолар. Ҳар бир ВМ образ кўринишида сақланиши мумкин, яъни алоҳида файл кўринишида тақдим этилиши мумкин. Бу файлнинг хажми хизмат фойдаланувчисига боғлиқ ҳолда ўзгариши мумкин. Булутнинг ВМ ларидан бирининг хажмини камайтирилиши ва бошқа бирининг хажмини ортишига олиб келади, бу олисда жойлашган файллар тўғрисидаги ахборотни ўз ичига олган физик секторни битта ВМ дан олиб бошқа бирига ўтказиш орқали ҳал этилади. Иккинчи ВМ фойдаланувчиси натижада аваллари бошқа ташкилотда жойлашган бўлган

маълумотларига кириш ҳуқуқига ва қайта тиклаш имконига эга бўлади. Бўлиши мумкин бўлган ечимлардан бири барча ахборотларни шифрлаш ҳисобланади. Шифрланган ахборотлар ушбу ҳолатда тегишли калитсиз қайта тиклаш имкони йўқ, бироқ шифрлаш қўшимча ҳисоблаш ресурсларини талаб қилиши ва маълумотларни ўқиш, ёзиш жараёнини сезиларли секинлаштириши мумкинлигини ҳам ҳисобга олиш керак.

Агар булут провайдери ўзининг асосий конфигаруция шаблонлари асосида мижозлар учун виртуал машинани заҳираласа, бошқарса ёки манипуляцияласа, у ҳолда кириш назорати ва таянч конфигурацияси ташкилотнинг шахсий маълумотлар маркази билан бир хил бўлмайди.

Динамик виртуал машина. Улар клонлаштириши ва физик серверлар ўртасида жойлаштирилиши мумкин. Хавфсизлик тизимини ишлаб чиқишга таъсири ўзгарувчан. Бироқ виртуал воситаларда иловалар ёки операцион тизим заифликларини назоратсиз қолдириши ва ихтиёрий иккита вақт оралиғидан сўнг пайдо бўлиши мумкин. (масалан, заҳира нусхасини қайта тиклаш). Булутли ҳисоблаш муҳитида ҳимоя тизимини унинг жойлашган жойига боғлиқ бўлмаган ҳолда ҳолатини қайд этишни ишончли бўлиши муҳим ҳисобланади.

Виртуал воситаларнинг ички заифликлари. Локал серверлар ва булутли серверлар бир хил операцион тизим ва иловалардан фойдаланади. Булутли тизим учун тахдид кўп миқдорда зарар келтирадиган дастурлар билан юкланганлиги ёки масофадан туриб бузишга бўлган ҳаракатларни келтириш мумкин. Тизимга бўладиган хужумларни аниқлаш ва олдини олиш тизими виртуал машинанинг булутли воситада жойлашган ўрнига боғлиқ бўлмаган ҳолда виртуал машина даражасида фоал зарар келтирувчиларни аниқлай олиш қобилятига эга бўлиши керак.

Ҳаракатсиз виртуал машиналарни ҳимоялаш. Хато виртуал машина ишламай турган ҳолатда ҳам хавф остида бўлади. Тармоқ орқали виртуал машина образига кириш мумкин, шу боис ишламай турган виртуал машинада ҳимояловчи дастурий таъминотни ишга тушириш имконияти мавжуд эмас. Ушбу ҳолатда фақатгина ҳар бир машина ичида ҳимоялашни жорий қилишдан ташқари гипервизор даражасида ҳам ҳимоялашни амалга ошириш керак бўлади.

МЕТОД БАЛАНСИРОВКИ НАГРУЗКИ В КЛАСТЕРНЫХ ПОДСИСТЕМАХ IMS

У.Б. Амирсаидов (ТУИТ, доцент)
А.З. Таджибаев (ТУИТ, магистрант)

Платформа IMS (Internet Multimedia Subsystem) представляет собой подсистему, поддерживающую мультимедийные сеансы связи с использованием протокола SIP (Session Initiation Protocol). Подсистема IMS является общей базой для мультимедийных услуг, доставляющей их через фиксированные и беспроводные среды доступа. Современные решения IMS позволяют операторам внедрять услуги и развертывать разнообразные решения в условиях необходимости управления множества устройств и обработки большого количества информационных потоков. Разработчики непосредственно сталкиваются с задачами обеспечения эффективного использования ресурсов, максимальной пропускной способности, заданного качества обслуживания. Такие задачи непосредственно имеют место и у отчественных операторов: в Узбекистане полным ходом идет реализация решений на основе IMS в рамках проектов развития национальной сети телекоммуникаций.

Балансировка нагрузки в кластерных подсистемах IMS заключается в распределении входящего потока между локальными серверами на основе имеющихся данных о загрузке ресурсов сервера, тем самым уменьшая вероятность того, что перегрузка произойдет на одном из серверов.

Критерием эффективности методов балансировки нагрузки является среднее квадратичное отклонение (индекс сбалансированности) загруженностей серверов:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(\rho_i - \bar{\rho})^2}{n-1}},$$

где: n – общее количество серверов;

ρ_i- загрузка сервера i и $\bar{\rho} = \frac{1}{n}\sum_{i=1}^{n}\rho_i$– среднее арифметическое загрузки серверов.

Чем меньше индекс сбалансированности, тем эффективнее метод балансировки нагрузки.

Современные алгоритмы распределения потоков с целью балансировки нагрузки можно разделить на два типа: статистические и динамические алгоритмы. Статистические алгоритмы просты в реализации, например, случайное распределение нагрузки Random, круговая балансировка нагрузки Round Robin и взвешенное распределение нагрузки Weighted Round Robin. Динамические алгоритмы используют информацию о текущем состоянии системы или узла на основе различных метрик, чтобы определить способ распределения нагрузки. Информация о состоянии системы является важным элементом работы динамического алгоритма. Существуют различные методы сбора данных о загруженности системы и построения характеристик загруженности. Загруженность сервера может определяться, например, как доля процессорного времени, затраченная на обработку запроса, как количество запросов в очереди сервера, либо как вероятность обнаружить сервер занятым обработкой запроса в какой-либо момент времени.

Известные методы балансировки нагрузки не учитывают особенностей создания сессий по протоколу SIP. В связи с этим, задача выбора оптимального метода балансировки нагрузки между серверами кластера SIP является актуальной.

В данной работе предлагается метод балансировки нагрузки с учетом трудоемкости различных процедур установления соединения. Мерой трудоемкости может служить количество обращений к серверам IMS при установления соединения определенного типа. На основе анализа функционирования сети IMS определены трудоемкости различных процедур установления соединения (таблица 1)

Таблица 1

Трудоемкости запросов на установления соединения

	Процедура установления соединения	Трудоемкость (количество обращений к серверам IMS)
	Перерегистрация (*rereg*)	9
	Регистрация (*reg*)	18
	Установление соединения *sip-sip*	45
	Установление соединения *sip-pstn*	66
	Предоставление услуг *(iptv)*	16

В кластере имеются один сервер балансировки нагрузки и *N* виртуальных серверов (IMS-VM) для обслуживания запросов на установление соединения. В каждом виртуальном сервере IMS-VM имеется счетчик трудоемкости запросов. При поступлении на сервер IMS-VM запроса INVITE, например, на установления соединения *sip-sip* счетчик трудоемкости данного сервера увеличивается на 45. После обслуживания данного запроса счетчик данного сервера уменьшается на 45. Сервер балансировки направляет запросы на виртуальный сервер IMS-VM с наименьшим значением счетчика трудоемкости.

Для оценки индекса сбалансированности серверов проводится имитационное моделирование кластерной системы IMS в среде AnyLogic. Структура имитационной модели приведена на рисунке.

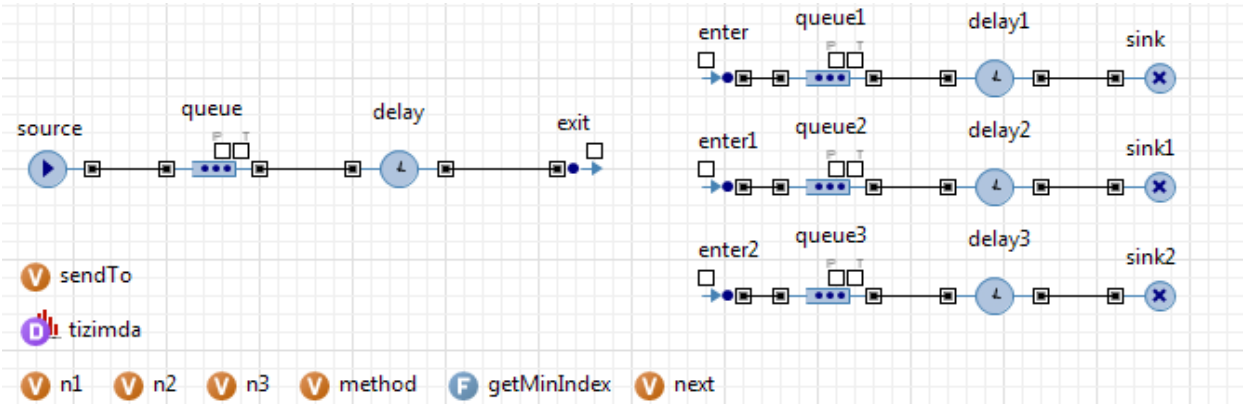


Рис. Структура имитационной модели

Сервер балансировки и виртуальные сервера IMS представлены как системы массового обслуживания. Sourse генерирует пуассоновский поток запросов (заявок).

Поток запросов обслуживается в устройстве delay. Механизм распределения потока запросов по виртуальным серверам реализуется в блоке exit. В модели реализованы три метода распределения потоков. Предложенный метод балансировки нагрузки с учетом трудоемкости запросов обозначен как первый метод (method-1), циклическое распределение запросов – второй метод (method-2) и распределение потоков с учетом длины очереди – третий метод (method-3).

Функция getMinIndex на основе сравнения значений счетчиков трудоемкости запросов трех виртуальных серверов определяет номер сервера с наименьшим значением счетчика трудоемкости. Далее на вход этого сервера направляется очередной запрос.

На основе результатов имитационного моделирования рассчитаны индексы сбалансированности серверов при рассмотренных методах балансировки нагрузки и сведены в таблицу 2.

Таблица 2

Эффективность методов балансировки нагрузки

	Метод балансировки нагрузки	Индекс сбалансированности серверов
	Метод распределения с учетом трудоемкости запросов	0.000969
	Циклический метод распределения	0.0916
	Метод распределения с учетом длины очереди	0.00403

Как видно, предложенный метод балансировки нагрузки с учетом трудоемкости имеет наименьший индекс сбалансированности и поэтому эффективнее по сравнению с широко распространенными методами.

ПРИОРИТЕТНОЕ ОБСЛУЖИВАНИЕ ЗАПРОСОВ НА УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ В СЕТИ IMS

У.Б.Амирсаидов (ТУИТ, доцент)

Изменения, происходящие в последнее время в телекоммуникационной индустрии и сфере услуг инфокоммуникаций, свидетельствуют о дальнейшей мультимедийной конвергенции, когда в качестве конвергентной платформы следующего поколения

используется IMS - IP Multimedia Subsystem - технология передачи мультимедийного содержимого на основе протокола IP.

Функциональная схема сети NGN/IMS включает в себя: транспортный уровень, реализующий функции доступа на различных технологиях; уровень управления сеансами связи, включающий в себя функциональные модули управления вызовами CSCF (Call Session Control Function) и базу данных абонентов HSS (Home Subscriber Server); уровень приложений, включающий в себя серверы приложений AS (Application Server). В состав модуля CSCF включены три уровня (функции):

1. Proxy CSCF (P-CSCF): уровень взаимодействия с сетью – посредник для взаимодействия с абонентскими терминалами. Основные задачи – аутентификация абонента и формирование учетной записи.
2. Interrogating CSCF (I-CSCF): уровень коммутации – посредник для взаимодействия с внешними сетями. Основные задачи–определение привилегий внешнего абонента по доступу к услугам, выбор соответствующего сервера приложений и обеспечение доступа к нему.
3. Serving CSCF (S-CSCF): уровень реализации услуг– центральный элемент сети IMS, обрабатывает все SIP-сообщения, которыми обмениваются оконечные устройства.

Согласно функциональной организации, в процессе установления каждого соединения IMS следит, чтобы пользователям было обеспечено соответствующее качество обслуживания (Quality of Service, QoS). В целом, IMS позволяет оператору более эффективно использовать ресурсы сети, в том числе для различных потоков трафика, что определятся возможностями по использованию различных сервисных алгоритмов. Однако, категоризация услуг и сервисов требует различных характеристик QoS, обеспечиваемых как для различных потребительских групп, так и технологических доменов в функциональной организации сети. Современные подходы обеспечения качества, в том числе с учетом соглашения об уровне услуг SLA-Service Level Agreement, предполагают наличие обоснованных решений по оценке качества, задействующих различные механизмы и методы определения характеристик функционирования IMS базированной сети.

В данной работе с целью повышения качества обслуживания предлагается метод распределения приоритетов между различными процедурами установления соединения в сети IMS.

В теории расписаний доказывается, что минимум среднего времени ответа (задержки) обеспечивается, если работы (обслуживание запроса) выполняются в порядке возрастания их трудоемкости. Обслуживание запросов в порядке увеличения их трудоемкости обеспечивает меньшее среднее время задержки по сравнению со средним временем задержки при обслуживании запросов в порядке их поступления (FIFO). Алгоритм планирования, основанный на использовании этого правила, называют алгоритмом SJF (Shortest Job First, Кратчайшая работа – первой). Это положение может быть использовано для планирования обслуживания различных запросов в серверах IMS.

Трудоемкость запроса отражается на времени обслуживания запроса. С повышением трудоемкости запроса увеличивается время его обслуживания. Из этого следует, что трудоемкость запроса отражается на уровне загрузки сервера. Таким образом, необходимо обслуживать запросы в порядке возрастания уровней загрузки сервера, создаваемые этими запросами.

Пусть в сервер поступает M простейших потоков запросов с интенсивностями $\lambda_1, \lambda_2, \dots, \lambda_M$ и время обслуживания запросов каждого потока запросов имеет математическое ожидание $b_1, b_2, \dots, b_M$. Каждый поток типа i создает для сервера загрузку $\rho_i = \lambda_i b_i$ $(\rho_i < 1)$. Запросам присвоены приоритеты в порядке возрастания

загрузки ρ_i. Среднее время ожидания запросов, имеющих приоритеты $k = 1,2,\dots,M$, определяется значениями

$$W_k = \frac{\sum_{i=1}^{n} \rho_i b_i (1+v_i^2)}{2(1-R_{k-1})(1-R_k)}, \qquad k = 1,2,\dots,M \quad (1)$$

где: $R_{k-1} = \rho_1 + \rho_2 + \dots + \rho_{k-1}$ $(R_{k-1} < 1)$ и $R_k = \rho_1 + \rho_2 + \dots + \rho_k$ $(R_k < 1)$ - загрузки, создаваемые потоками запросов $\lambda_1, \lambda_2, \dots, \lambda_{k-1}$ и $\lambda_1, \lambda_2, \dots, \lambda_k$ соответственно.

Среднее время задержки запросов, имеющих приоритеты $k = 1,2,\dots,M$, определяется значениями

$$\bar{T}_{zk} = W_k + b_k, \qquad k = 1,2,\dots,M \quad (2)$$

Общее среднее время задержки всех запросов определяется в виде

$$\bar{T}_z = \frac{\sum_{k=1}^{M} \bar{T}_{zk}}{M} \quad (3)$$

Для различных нагрузок определены загрузки серверов, создаваемые различными процедурами установления соединения и определены номера приоритетов обслуживания процедур в каждом сервере IMS. Распределение приоритетов обслуживания процедур установления соединения приведено в таблице.

Таблица

Оптимальное распределение приоритетов

Сервера подсистемы IMS	Процедуры установления соединения				
	SIP-SIP	SIP-PSTN	reg	re-reg	IPTV
P-CSCF	4	2	3	5	1
I-CSCF			1	2	
HSS	1		2	3	
S-CSCF	5	2	3	4	1
AS	3	2			1
BGCF		1			
MGCF		1			
MRFC					1

На основе формул (1) и (3) получены графики зависимости общего среднего времени задержки запросов от нагрузки (см. рисунок).

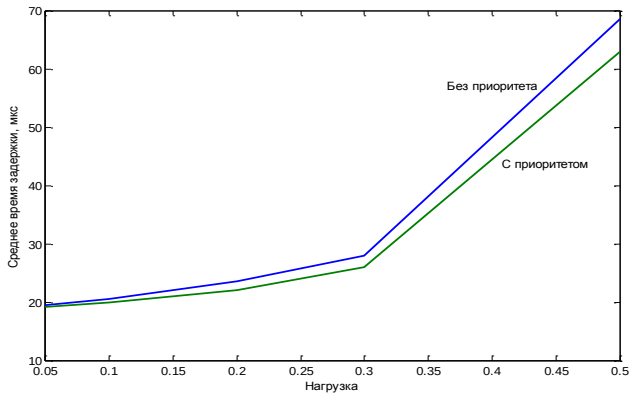


Рис. График зависимости общего среднего времени задержки запросов от нагрузки

Из рисунка 2.7 видно, что приоритетная дисциплина обслуживания запросов в порядке возрастания загрузки серверов снижает общую среднюю задержку запросов до 1.2 раза по сравнению с безприоритетной дисциплиной обслуживания в областях средних и высоких нагрузок.

OPENFLOW ПРОТОКОЛИ АСОСИДА ИШЛАЙДИГАН ДАСТУРИЙ КОНФИГУРАЦИЯЛАНАДИГАН ТАРМОҚ

З.Р. Атажанов (ТАТУ, талаба)

Мобил қурилмаларнинг турли хиллиги, уларнинг кўплиги, ҳамда турли хил симсиз алоқа технологияларининг ривожланиши алоқа тармоқларидан фойдаланувчилар сонининг ортишига олиб келди. Мобил терминалларининг қувватини ошиши иловаларнинг ҳажмини ҳисоблашни оширди, бу ўз навбатида алоқа тармоқларининг ўтказиш қобилятини оширишни талаб қилади. Мобил трафик ҳажми геометрик прогрессияга ўхшаб ўсиб бормоқда, трафикнинг кўриниши эса турли туман бўлиб бормоқда. Тармоқ қурилмаларини ишлаб чиқарувчи етакчи компанияларнинг маълумотларига кўра трафик тахминан ҳар ўн ойда икки маротаба кўпайяпти, бу яқин бир неча йиллар ичида юклама бир неча марта ошишини билдиради. Cisco компаниясининг ҳисоб китобларига кўра трафик ҳажми яқин 5 йил ичида 4 марта ошади, сабаби мобил трафик ҳар йили 2 маротаба кўпаяпди.

ДКТ технолгияси компютер тармоғида бошқарув ва маълумотларни узатиш функцияларини ажратишни таклиф қилади.

ДКТ архитектурасини учта поғонага ажратиш мумкин:

- *Инфраструктура поғонаси*, тармоқ қурилмаларини тақдим этади (коммутатор ва маълумотларни узатиш канали);
- *Бошқарув поғонаси*, тармоқни ва тармоқ қурилмаларини бошқарадиган дастурий интерфейс ва тармоқ хизматлари иловаларини таъминлайдиган ўзининг операцион тизимидан иборат;
- *Тармоқ иловалари поғонаси*, тармоқни самарали бошқаради ва мослашувчан бўлади.

ДКТ тамойили стандарт бошқарув интерфейсларини контроллерга тақдим этадиган коммутация қурилмаларининг ички воситаларини яширувчи махсус тармоқ протоколи асосида коммутатор ва контроллернинг ўзаро биргаликда ишлаши таклиф этади. Бугунги кунда бир бирига ўхшаш бир нечта протоколлар таклиф этилган шулардан кенг тарқалгани OpenFlow протоколи ҳисобланади.

OpenFlow стандарти. SDN технологиясини ривожлантириш йўлида 2011 йилда OpenFlow протоколи ишлаб чиқилган. OpenFlow стандарти SDN тармоғининг маълумотларни узатиш поғонасини масофадан туриб бошқаришга мўлжалланган. OpenFlow спецификацияси коммутатор билан контроллерни биргаликда ишлашини назарда тутади. OpenFlow протоколида ишлайдиган ҳар бир коммутатор олисда жойлашган сервер билан боғлаб турадиган алоқа канали орқали бир ёки бир нечта махсус оқим жадвалларини (flow table), ҳамда гуруҳ жадвалларини (group table) узатади. Коммутаторларнинг ҳар бир оқим жадваллари ўз ичига оқимлар ва уни қайта ишлаш тўғрисидаги маълумотларни олади. Гуруҳ оқими ҳаракатлар тўпламини ўзида тақдим этади, кенг тарқатилиш учун мўлжалланган. Гуруҳ оқими оқимлар учун чиқиш маълумотларини тезда ўзгартиришда фойдаланилади. Контроллерни биз махсус дастурий таъминот ўрнатилган сервер деб ҳисоблаймиз.

OpenFlow интерфейси ҳам физик, ҳам виртуал кўринишда ДКТ архитектурасининг тармоқ инфраструктураси ва бошқарув поғоналарини боғлаш ва киришга рухсат беришни таъминлайди. OpenFlow индивидуал жадвал ечимини изоҳлашда алоҳида ҳар бир маршрутизатор (ДКТ коммуататори) учун ҳимояланган канал буйруқлари асосида узатиладиган бутун бир тармоқ ахборотлари ва умумий конфигурациясига асосланадиган контроллер терминидан фойдаланади. Марказий контроллер тармоқ структураси ва топологияси тўғрисида аниқ ахборотга эга бўлади. Бу маълумотлар пакет ҳаракатини оптималлаштиришда фойдаланилади ва IP-маршрутизацияга ўтмасдан L2 поғонада “ҳар бири ҳар бири билан” боғлашни қисман бажаради.

ДКТ коммутатори фақат маълумотларни узатиш поғонасида OpenFlow ни қўллаб қувватлайди. Ҳар бир коммутатор марказий коммутатордан олинган ахборотлар асосида тўлдирилган ўзининг ноёб жадвалига эга бўлади. Бундай коммутация жадвали FlowTable (оқим жадвали) номи билан аталади, бунда ДКТ – тармоқ алоҳида пакетни эмас (коммутатор тартиб қоидасига кўра фақат биринчи пакетга ўрнатилади, сўнг қолган барча пакетлар ундан фойдаланилади) маълумотлар оқимини узатади. Бундай жадвал ёрдами билан келувчи пакетлар MAC –манзил, IP – манзил, порт ва бошқа воситаларга асосланиб тоифаланади.

Келувчи ҳар бир пакетга маълум бир узунликда бит сатр сарловҳа ажратилади. Оқим жадвалида ушбу бит сатри учун дастлаб қоидалар тўплами изланади, яъни пакет сарловҳасига яқинроқ бўлган белгилар майдони изланади. Қоидалар тўпламида пакет ва унинг сарловҳасига мос келадиган мавжуд бўлса, унинг ичида кўрсатилган йўриқнома тўпламида белгиланган ўзгаришлар бажарилади. Оқим тўғрисидаги ёзувни белгиланган портда пакетни жўнатяпганда ёзиш мумкин (одатда физик порт ёхуд коммутатор вазифасини бажаришга мўжалланган виртуал портлар ёки махсус протокол ўрнатилган заҳираланган виртуал портлар). Заҳираланган виртуал портлар жўнатишда умумий ҳаракатларни белгилайди: контроллерга жўнатиш, кенг миқёсда тарқатиш. Виртуал портлар агрегирланган канал гурухи, туннеллар ёки тескари алоқа интерфейсларини аниқлаштиради.

Агар биринчи жадвалда керакли қоидалар тўплами аниқланмаса, у ҳолда пакет инкапсуляцияланади ва ушбу турдаги пакетга мос келувчи қоидаларни шакллантириш учун контроллерга жўнатилади ва келиб тушган сўров асосида қоида шакллантирилиб коммутаторга ўрнатилади (ёки уни коммутаторни бошқариш тўпламига), ёхуд пакет ўзгартирилиши ёки йўқ қилинади. Қайта ишлаш конвейри йўриқномаси кейинги қайта ишлашлар учун навбатдаги жадвалга пакетни жўнатишда ва жадваллар ўртасида ахборотларни узатишда фойдаланилади. Шунингдек, йўриқнома турли хил статистикаларни тўплашда фойдаланиш мумкин бўлган модификацияланган ҳисоблагич қоидаларини аниқлайди

Анъанавий тармоқ канал тезлиги, яширин ёки заҳира қувватлар асосида машрутни танлаши мумкин, лекин бу унга исталган реал ҳолатларда тезда ўзгартиришни мураккаблаштиради (ҳато MPLS TE - Multiprotocol Label Switching Traffic Engineering фойдаланганда ҳам). OpenFlow ҳар бир оқим асосида турли хил оптимизациялаш учун тармоқни дастурлаштиришга қарши чиқади. Бу шуни билдирадики, трафиклар кечикишига юқори сезувчанлик йўлни тезда топиш имкониятини бериши мумкин, бу вақтда оқимларни алмашиш энг арзон маршрутни танлашдан бошланиши мумкин. Бунда энг охирги нуқта қурилмасига асосланиб OpenFlow ҳар бир охирги нуқтага келиб тушадиган бир бирига яқин трафик кўринишларини кенгроқ синфлашда фойдаланиш имокниятини беради.

OpenFlow протоколи фақат трафик бошқаруви билан чегараланиб қолмайди. Қурилма OpenFlow билан биргаликда NAT ёки AFTR (Address Family Transition Router) каби ишларни пакетга ёзади. Мадомики уни пакетдан олиб ташлаш мумкин экан, қурилма брандмауэр каби ишлайди. Шунингдек у ECMP (equal-cost multi-path) ёки бошқа юкламани баланслаш алгоритмларида амалга оширилиши мумкин. Маршрутизаторлар улар орқали ўтадиган турли хил оқимлар учун турли хил қоидаларга эга бўлиши мумкин. Улар бошқалар учун брандмауэрдан фойдаланиб битта оқимга юкламани тақсимлаши ва учинчи оқим учун пакет сарловҳасини ўзгартириши мумкин. Бундай ҳолатда, тармоқнинг алоҳида элементи анъанавий тармоқ билан солиштириш асосида OpenFlow шартлари нисбатан мослашувчан эканлиги сезилади.

OpenFlow битта ташкил қилиниш чегарасида фойдаланишга мўлжалланган. OpenFlow доменидаги барча маршрутизатор битта мақсадда ҳаракат қилади. Контроллерга ўзи назорат қиляпган барча маршрутизаторлар бўйсунади. Интернет провайдер ўзининг маршуритзаторини назорат қилиш мақсадида OpenFlow дан

фойдаланиши мумкин, лекин мижоз тармоғини назорат қила олмайди. Корхона маълумотларни қайта ишлаш ички тармоғини бошқаришда битта OpenFlow доменидан, бошқа OpenFlow домени эса глобал компютер тармоғига киришни бошқаришда фойдаланиши мумкин.

ДКТ доирасида фоал ривожлантириляпган ғоялардан бири сифатида –тармоқ ресурсларидан самарали фойдаланиш мақсадида виртуал тармоқни ривожлантириш. Тармоқни виртуаллаштириш остида физик тармоқни бошқа мантиқий тармоқ ёки тармоқ кесимига (network slices) ажратиш мумкин бўлган битта тармоқ доирасида турли хил характеристкали бир нечта маълумотлар оқимини гуруҳлаштирадиган – тармоқ трафигини ажратиш тушиналади. Бунда ҳар бир кесим ўзининг манзилланишидан, ўзининг маршуритзация алгоритмидан, хизмат сифатини бошқариш алгоритмидан ва бошқалардан фойдаланиши мумкин бўлади.

Ечиляпган масалага боғлиқ масштабда реал булутни қуришда ДКТ тармоғини кенгайтириш имкониятлари назарий жиҳатдан чегараланмаган. Шу сабабли тармоқ интелектуаллик ҳисобланади.

МЕТОДЫ ДИАГНОСТИКИ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ МНОГОКАНАЛЬНОГО СИГНАТУРНОГО АНАЛИЗАТОРА

Ж.Б. Балтаев (ТУИТ, ассистент)

Проблема анализа многовыходных микропроцессорных схем и процесс их тестирования заключается в определении возникновения неисправности схемы по её выходным реакциям. Отличительной особенностью подобного анализа является необходимость исследования достаточно большого количества выходных реакций схемы (число их может достигать нескольких сотен). Поэтому использование традиционных методов компактного тестирования, применяемых дляодновыходных микропроцессорных схем, в данном случае не позволяет получить желаемого эффекта. Действительно, попытка провести анализ n - выходной цифровой схемы одноканальным сигнатурным анализатор(СА) приводит к увеличению в n раз времени, необходимого для анализа схемы, или оборудования, требуемого для реализации n сигнатурных анализаторов. При этом остаётся открытым вопрос о разрядности сигнатуры, которая также может увеличиться в n раз. Поэтому на практике чаще всего используют специальные методы и приёмы сигнатура многоканального сигнатурного анализатора (МСА), а также размерность сигнатуры S(y) однозначно определяется количеством выходов n исследуемой схемы. Поэтому с увеличением n сложность устройства сжатия и количество бит, используемых для представления сигнатуры S(y), принимает практически недопустимые размеры. Попытка использовать идею каскадирования многоканальных сигнатурных анализаторов позволяет уменьшить размерность результирующей сигнатуры, однако в этом случае оказывается сложным оценить достоверность такого анализатора, которая будет зависеть от организации взаимосвязи МСА и их конкретной реализации.

С помощью многоканальных сигнатурных анализаторов можно существенно ускорить процедуру контроля микропроцессорных схем, которая практически увеличивается в n раз, где n – количество входов применяемого анализатора. В случае совпадения реально полученной сигнатуры с её эталонным значением считается, что с достаточно высокой вероятностью проверяемая цифровая схема находится в исправном состоянии. На этом процедура её исследования оканчивается. В противном случае, когда схема содержит неисправности, реальная сигнатура, как правило, отличается от эталонной, что служит основным аргументом для принятия гипотезы о неисправном состоянии схемы. В тоже время вид полученной сигнатуры не несёт никакой дополнительной информации о характере возникшей неисправности. Более того, остаётся

открытым вопрос о том, какие из n анализируемых последовательностей, инициирующих реальную сигнатуру, содержат ошибки, т.е. возникает задача локализации неисправности с точностью до последовательности, несущей информацию о её присутствии.

Классическая стратегия тестирования цифровых систем, основанная на формировании тестовых последовательностей, требует значительных временных затрат и больших объемов тестовой информации и эталонных выходных реакций, что предполагает наличие сложного оборудования. Наиболее эффективным решением, позволяющим значительно сократить объем хранимой информации об эталонных выходных реакциях, является многоканальный сигнатурный метода диагностики в многовыходный цифровых схемах.

Учитывая эквивалентность функционирования n - канального сигнатурного анализатора и соответствующего ему одноканального анализатора относительно результата сжатия n входных последовательностей $y_v(k) \in \{0,1\},\ v = \overline{1,n},$ логично оценить достоверность МСА, используя результаты, полученные для одноканального сигнатурного анализатора. Действительно, в случае применения примитивного полинома $\varphi(x)$ вероятность необнаружения ошибок в последовательностях $\{y_v(k)\},\ v = \overline{1,n}$ многоканальным сигнатурным анализатором для $nl = 2^m - 1,$ где m – старшая степень порождающего полинома, будет определяться соотношением:

$$P_n = \frac{2^{nl-m} - 1}{2^{nl} - 1} \approx \frac{1}{2^m}$$

Это соотношение справедливо для любого соотношения n и l, произведение которых равно 2^m-1. Приведённая интегральная характеристика эффективности МСА, также как и характеристика одноканального сигнатурного анализатора, является достаточно приближённой оценкой, справедливой для общих допущений. Более полной характеристикой МСА будет распределение вероятностей P_n^{μ} необнаружения возникшей ошибки кратности μ в анализируемых последовательностях $\{y_v(k)\}$. При этом численное значение указанных вероятностей, как и в случае одноканального анализатора, определяется выражениями:

$$P_n^1 = P_n^2 = 0 \quad P_n^{\mu} = \frac{1}{2^m - \mu}\left[1 - P_n^{\mu-1} - (\mu - 1)P_n^{\mu-2}\right],\ \mu = \overline{3, 2^m - 1}$$

Попытка применить это выражение для оценки значений P_n^{μ} при анализе последовательности $\{y_1(k)\},\ k = \overline{1,l}$, когда $l = 2^m - 1$ на n – канальном анализаторе не всегда позволяет получить верные результаты.

Анализ характеристик существующих средств контроля и диагностики показал, что практически единственным для применения в условиях эксплуатации является методы и средства сигнатурного анализа.

Диагностика цифровых устройств с n-выхода одноканальным сигнатурным анализатором (ОСА) приводит к увеличению в n раз времени, необходимого для диагностики устройства С помощью МСА можно уменьшит время диагностики в n раз, где n количество входов анализатора.

АНАЛИЗ ТЕХНОЛОГИЙ КОММУТАЦИИ ДЛЯ СЕТЕЙ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Ж.Б. Балтаев (ТУИТ, ассистент)
Т.Қ. Тоштемиров (ТУИТ, 2-курс магистрант)

Возрастающий спрос на мультимедийные услуги повлек за собой появление различных технологий, и привел к изменению современных телекоммуникационных сетей.

Современные прогнозы указывают на тенденцию превращения всех сетей телекоммуникаций в сети передачи данных, по которым будут передаваться любые виды информации (включая речь и видео), преобразованные в цифровые сигналы.

Современные сети передачи данных можно определить с помощью следующих фундаментальных характеристик;

- базируются на технологии коммутации пакетов IP;
- обеспечивают качество обслуживания;
- обеспечивают предоставление конвергентных услуг и различных мультимедийных услуг, включая вещательные услуги и потоковое видео.

Как показывает международная практика, в настоящее время главной тенденцией на сетях телекоммуникаций является значительный рост *IP*- трафика, поэтому наиболее востребованными являются услуги, которые клиент сети получает от сервис-провайдера. Максимальное же гибкое управление трафиком клиента на уровне приложений обеспечивает IP- протокол. Технология 1P в отличие от других имеет более разработанную систему стандартов и более широкое распространение.

Растущая популярность голосовых и мультимедейных услуг на основе 1P - протокола и вызываемые ими изменения в структуре телекоммуникационных сетей привели к созданию сетей следующего поколения.

Один из ключевых вопросов реализации сетей следующего поколения

— выбор технологии коммутации. Сложность выбора технологии коммутации для сетей следующего поколения чаще всего сводится к оценке эффективности использования транспортных ресурсов и качества обслуживания.

— Исследования и разработки в области сетевых технологий привели к тому, что сегодня наилучший способ передачи информации по транспортным сетям связывается с использованием пакетных технологий.

— На сегодняшний день приоритетным методом коммутации является пакетный (packet switching), обеспечивающий высокие показатели по скорости, экономичности и живучести. Основными методами пакетной коммутации являются дейтаграммный режим и режим создания виртуального канала. Развитие пакетных технологий становится основой для создания сетей следующих поколений.

Для коммутации пакетов классификационным признаком обычно служит название технологии (X.25. Frame Relay, ATM, MPLS и т. д.). Основными преимуществами пакетных сетей является возможность передачи разнотипного трафика, гибкость в построении сетей, масштабируемость, хорошие возможности по взаимодействию с другими сетями и экономичность Каждая технология коммутации пакетов обладает своими особенностями, которые и определяют возможность их использования.

Пакетные технологии являются мощным инструментом существенного повышения эффективности сетей связи. Технология ГР по экономическим показателям не отстает от других технологий даже при передаче речевого трафика и продолжает совершенствоваться в направлении повышения эффективности и повышения качества передачи Исходя из принципа независимости требований по качеству от вида пакетной технологии . общепринятым критерием для оценки применимости технологии является коэффициент эффективности (степень повышения эффективности использования канала). Коэффициент эффективности определяется, исходя из общей длины пакета (кадра): длины информационной (полезной) части пакета(кадра); доли трафика данных .речи и видео в суммарном трафике.

Одна из самых больших проблем при передаче голосовых и видеосообщений по сетям с пакетной коммутацией заключается в обеспечении гарантированного качества обслуживания (QoS) для трафика реального времени. Для этого предложены механизмы и методы обеспечения качества обслуживания разнородного трафика *в IP-сетях,* такие как Best Effort. IntServ, DiffServ. Технология MPLS создана как альтернатива существующим механизмам QOS в современных IP-сетях

Технология MPLS рассматривается как перспективная, хотя и не единственная основа для конвергенции услуг и построения мультисервисных сетей следующего поколения (NGN), в которых станет возможна передача разнородного графика через интегрированную телекоммуникационную инфраструктуру вместо нескольких различных сетей.

Технология многопротокольной коммутации по меткам MPLS в IP- сетях рассматривается специалистами как наиболее эффективная для обеспечения гарантированного качества услуг для мультимедийного трафика.

Сравнительный анализ показывает, что технология MPLS позволяет поддерживать качество обслуживания (QoS) и безопасность, сохраняя гибкость и масштабируемость присущие технологии IP. Появления технологии MPLS определяет направление интеграции маршрутизации и коммутации в общую IP / MPLS сеть. Таким образом технология IP/ MPLS является наиболее эффективной из всех пакетных технологий применительно к передаче смешанное трафика, в котором превалирует доля речевой и видеоинформации.

АНАЛИЗ ВЛИЯНИЯ ПОКАЗАТЕЛЕЙ КОНТРОЛЕПРИГОДНОСТИ НА НАДЕЖНОСТНЫЕ ХАРАКТЕРИСТИКИ СЕТИ ПД

Р.Ж.Бойманов (ТУИТ, магистрант)

Международный опыт развитых стран показывает, что стратегическим направлением работ по технической эксплуатации и обслуживанию сетей передачи данных с КП становится использование системного подхода к самой этой проблеме. Согласно современным представлениям об управлении технической эксплуатацией, формирование её должно осуществляться на этапе проектирования, закладываться при создании, обеспечиваться и поддерживаться в процессе эксплуатации путём систематического контроля на всех этапах и целенаправленного воздействия на условия и влияющие факторы.

Одним из наиболее общих требований, предъявляемых к сети передачи данных с КП является требование по обеспечению эффективного использования технических средств ПД – каналов передачи данных, узлов коммутации и другого оборудования. Так как технические средства, используемые в сетях передачи данных с КП относятся к классу восстанавливаемых систем, надёжность их может быть повышена не только путём использования более совершенных элементов и узлов, то есть увеличением среднего времени наработки на отказ, но также путём сокращения времени простоя, затрачиваемого на поиск и устранение дефекта.

Сокращение времени простоя в сетях телекоммуникации с КП осуществляется путём автоматизации процедур контроля, обеспечения свободного доступа к контролируемым параметрам, а также путём использования специализированного контрольно-диагностического обеспечения. Поэтому решение задачи обеспечения надёжности при эксплуатации технических средств и компонентов непосредственно связано с задачами контроля и состояния сетях передачи данных с КП.

Опыт эксплуатации сетей передачи данных с КП показывает, что при отсутствии специальных средств контроля диагностирования основную долю времени восстановления составляет время, затрачиваемое на установление места неисправности. Для уменьшения времени восстановления, прежде всего, необходимо сократить время контроля и диагностирования, что может быть достигнуто специальными методами и средствами диагностирования.

Однако следует заметить, что применение специальных методов и средств контроля и диагностирования может оказаться не эффективным, если не обеспечена

приспособленность системы к контролю и диагностированию, т.е. сравнительно низкой её контролепригодностью.

Для уменьшения времени восстановления сети передачи данных с КП, прежде всего, необходимо обеспечить требуемый уровень контролепригодности, если система должным образом не приспособлены к техническому диагностированию, то вспомогательные операции составляют 60 – 80% общего времени диагностирования. Под контролепригодностью обычно понимают свойство сети передачи данных с КП, характеризующие её приспособленность к контролю и диагностированию в процессе эксплуатации. Стадия проектирования сети передачи данных с КП является стадией, на которой реализуются требования к приспособленности к техническому диагностированию, оцениваются показатели контролепригодности.

Рассматривая вопрос об уровне контролепригодности, следует отметить, что решение проблем контролепригодности сети передачи данных с КП должно вестись одновременно с разработкой средств её контроля и диагностирования.

Содержание работ по обеспечению контролепригодности сети должно состоять из следующих основных этапов:

– формирование требований контролепригодности сети;

– разработка и анализ модели сети, и выбор параметров контроля и диагностирования;

– определение показателей уровня контролепригодности сети.

– принятие решения по соответствию достигнутого уровня контролепригодности заданным требованиям.

Таким образом, контролепригодность сети передачи данных оценивается рядом показателей, а номенклатура показателей контролепригодности определяется с учётом заданных на систему показателей надёжности, технологичности, эргономичности, массогабаритных характеристик и принятых для этой системы способов обеспечения восстановления, контроля правильности функционирования в процессе эксплуатации.

Основные задачи, решаемые при обеспечении контролепригодности сети передачи данных, могут быть условно разделены на две группы:

Первая группа – обоснование требований по контролепригодности к сети передачи данных.

Эта группа задач решается на ранней стадии проектирования и предусматривает проработку вопросов возможных вариантов диагностирования сети передачи данных.

Вторая группа – проектирование сети передачи данных с требуемым уровнем контролепригодности.

Эта группа задач включает:

– исследование возможных методов обеспечения контролепригодности сети передачи данных;

– выбор наиболее приемлемых методов обеспечения контролепригодности;

– выбор наилучшего варианта сети передачи данных по показателям контролепригодности.

АТМ ТЕХНОЛОГИЯДА IPSec ВА SSL ПРОТОКОЛЛАРИНИНГ ИШЛАТИЛИШИ

Ш.Ю. Джаббаров (ТАТУ, МУТ ва Т кафедраси, доцент)

АТМ технологияда шифрлашни ишлатиш учун IPSec (IP Security Protocol) ва SSL (Secure Socket Layer) каби муҳофаза қилиш протоколлари ишлатилади.

IPSec протоколи иккита Authentication Header (AH) ва Encapsulating Secure Payload (ESP) протоколларига бўлинади. Биринчиси маълумотлар манбаини аутентификация

қилишни, уларнинг яхлитлигини ва такрорий хабарларга боғланиб қолишидан муҳофаза қилинишини таъминлайдиган конвертни яратади.

AH протоколи ўзлари яратадиган конвертда IP-сарлавҳалар ташқарида жойлашганлигига қарамасдан IP-пакетларни аутентификация қилиш имкониятини таъминлайди. AH аутентификация қилиш пакет ўтаётган вақтда IP-сарлавҳалар майдонларини манипуляцияланишини олдини олади. Шу сабабга кўра бу протокол тармоқ манзилларини трансляция қилиш (Network Address Translation, NAT) механизмлари ишлатиладиган мухитда қўллаш мумкин эмас, чунки IP-сарлавҳаларни манипуляциялаш унинг ишлаши учун керак.

ESP протоколи маълумотларни конфиденциаллигини таъминлайди ва аутентификация қилинмаган шифрланган маълумотлар оқимини муҳофаза қилиш бўйича AH протоколининг барча функцияларини бажаради.

IPSec спецификацияси AH функциялари ишлатилишисиз ESP протоколини ишлашига рухсат беради. ESP протоколларида IP-сарлавҳани аутентификация қилишсиз AH протоколни қўлланишига эквивалент бўлган фиктив шифрланиш ишлатилиши мумкин. Бу NAT механизмининг ишлашини қўйилишига имкон беради, чунки бу ҳолда сарлавҳалардаги манзилларни ўзгартириш мумкин.

IPSec бу аутентификация қилиш ва шифрлаш алгоритмлари ишлатиладиган протоколлар тўплами ҳисобланади. Ҳозирги вақтда иккита аутентификация қилиш алгоритми ва еттита шифрлаш алгоритмлари аниқланган. AH ва ESP протоколларида HMAC – MD5 ва HMAC – SHA1 аутентификация қилиш алгоритмлари ишлайди. Уларнинг ишлаши MD5 (Message Digest version 5, RFC 1321 стандарти) холида 128 бит узунликдаги ва SHA1 (Secure Hash Algorithm version 1, FIPS 180-1 стандарти) 160 бит узунликдаги умумий махфий калитни ҳар иккала сеанс иштирокчиларининг қўллашига асосланган. HMAC алгоритми (Keyed-Hashing for Message Authentication Code-хабарларни аутентификациялаш хэш коди) махфий калитли аутентификация қилиш алгоритми ҳисобланади. Маълумотлар манбаини аутентификация қилиш ва уларнинг яхлитлигини таъминлаши билан махфий калитни тарқалиш кўламига боғлиқ.

Агар HMAC калит фақат қабул қилувчи ва узатувчи томонларга маълум бўлса, унда бу ҳар иккала томонлар орасида қайта узатиладиган маълумотлар манбаини аутентификация қилишни таъминлайди. HMAC учун калитлар ISAKMP/Oakley процедураси орқали генерацияланади.

SSL протоколи сервис протоколлари (HTTP, NNTP, FTP ва х.к.) ва транспорт протоколлари (TCP/IP) орасидаги маълумотларни муҳофаза қилинишини таъминлайдиган протокол сифатида Netscape фирмаси томонидан ишлаб чиқилган.

SSL протоколи қуйидаги учта асосий хусусиятларга эга бўлган “хавфсиз канал” ҳисобланади:

– *канал хусусий ҳисобланади.* Шифрлаш махфий калитни аниқлаш учун оддий мулоқотдан кейин барча хабарлар учун ишлатади;

– *канал аутентификация қилинган.* Мулоқотнинг сервер томони доимо аутентификация қилинади, бу вақтда мижоз томони эса опцион аутентификация қилинади;

– *канал ишончли.* Хабарларни ташиш яхлитликни текширишни (MAC жалб этишли) ўз ичига олади.

SSL – протоколнинг бош вазифаси иккита олисдаги ўзаро таъсир этувчи иловалар орасида ахборотларни ишончли алмашинуви усулини таъминлаш ҳисобланади. Протокол махфийлаштирилмаган телекоммуникация каналлари орқали махфий ахборотларни хавфсиз ўтказиш учун махсус мўлжалланган икки қатламли (кўп қатламли) муҳит кўринишида ишлатилади. Бундай муҳитда биринчи қатлам сифатида қандайдир ишончли транспорт канали, масалан, TCP ишлатилади. TCPга юкланадиган иккинчи қатлам SSL Record Protocol ҳисобланади. Бу иккита TCP ва SSL Record Protocol қатламлари биргаликда ўзига хос SSL ядрони шакллантиради. Кейинчалик бу ядро барча кейинги

мураккаброқ протоколли инфратузилмалар учун биринчи герметизацияловчи қобиқ бўлиб қолади. Бундай тузилмалардан бири сифатида SSL Handshake Protocol ишлатилади. У муҳофаза қилинган режимда ахборотлар байтларини узатиш ёки қабул қилишни бошлагунга қадар сервер ва мижоз томонида ишлаётган иловалардан олдин криптографик алгоритмлар, калитларни сервер ва мижозга мувофиқлаштириш, бир-бирларини идентификациялаштиришга имкон беради.

SSL протоколи чидамлилик принципларида ишлаб чиқилган ва унинг қурилиш идеологияси таркибида у ишлатиладиган иловаларга боғлиқ эмас. Бундан ташқари SSL протоколининг устига очиқ бошқа протоколлар ҳам юкланиши мумкин. Бу мақсадли ахборот оқимларини муҳофазаланганлик даражасини янада кўпроқ ошириш ёки қандайдир бошқа маълум вазифа учун SSLнинг криптографик қобилиятларини мослаштириш учун қилинади. SSL назарий жиҳатдан исталган Интернет боғланишни деярли тўлиқ муҳофаза қилишни таъминлайди, лекин унинг муваффақиятли ишлаши ва SSL технологиясини хаётга татбиқ қилиниши учун дастурий воситалар ҳам зарур. SSL протоколларини ишлатадиган дастурлар бу технологиянинг энг заиф жойи ҳисобланади. Айнан бу дастурлардаги хатоликлар SSL ишлатилгандан кейинги барча эришилган тўсиқлар тўла йўқотилиши мумкин.

ОСНОВНЫЕ ПРОБЛЕМЫ, ЗАДАЧИ И ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ В ТЕХНОЛОГИЯХ NGN

Ш.Ю. Джаббаров (ТУИТ, доцент)
Т.Н. Халмурадов (ТУИТ, магистр)

Существует ряд причин, определяющие недостатки решений на основе технологии NGN, затрудняющие их быстрое продвижение на рынке услуг телекоммуникаций. Одной из основных этих причин является критичность к обеспечению надежности и информационной безопасности сети, что потребует разработки системы обеспечения живучести с более жесткими требованиями, чем для классических телефонных сетей.

В обеспечении информационной безопасности NGN заинтересованы абоненты, операторы и пользователи конфиденциальной связи. Абонентам нужна защита передаваемой информации и персональных данных, защита от мошенничества и вирусных атак. Операторам необходимо поддерживать устойчивое функционирование своей инфраструктуры в составе единой сети телекоммуникаций и предотвращать противоправные действия нарушителей, способные нанести финансовый ущерб и подорвать доверие к оператору со стороны абонентов. Большое значение для оператора имеет и защита служебной информации, поскольку это напрямую влияет на работоспособность сети, а значит, и на доходы. Пользователям конфиденциальной связи требуется обеспечение безопасной передачи информации, подлежащей обязательной защите и гарантированное предоставление услуг телекоммуникаций.

Построенной на базе протокола IP, конвергентной и открытой среде сетевая инфраструктура должна быть гибкой и открытой для различных видов услуг: данные, голос или видео. Однако, это делает её значительно более уязвимой для атак по сравнения с традиционной сетевой архитектурой. При интеграции существующих сетей и сетей NGN будут иметь место все специфические угрозы, уязвимости, риски нарушения безопасности, характерные для каждой сети в отдельности.

С учетом возрастания роли протокола IP необходимо быть уверенным в том, что в новой среде будут максимально устранены его уязвимости. Внедрение сетей телекоммуникаций следующего поколения приведет к переносу угроз, существующих в сети Интернет и в сеть мобильной связи. Уровень обеспечения информационной безопасности в NGN должен быть не ниже уровня, достигнутого в сетях предыдущего поколения. Надо учитывать, что NGN ориентированы на

конвергенцию технологий и услуг, это значительно усложняет их топологию и требует от оператора решения вопросов безопасного межсетевого взаимодействия.

Новые технологии и приложения порождают новые угрозы безопасности и уязвимости, а в силу того, что вопрос информационной безопасности является одним из важнейших, то он является наиболее важным критерием для потребителей при принятии решения о выборе поставщика услуг.

Интегрированные сети высокоскоростного доступа, предназначенные для доступа к услугам сети Интернет, телефонии и телевидения, тоже являются лакомым куском для злоумышленников. Проходящий через них трафик сравнительно легко перехватить. Особенно подвержены этому сети, в которых используется принцип разделения среды, такие, например, как HFC, PON, Wi-Fi, Ethernet (в домашних сетях). Анализ трафика от SIP-телефона, передаваемого в сетях доступа, позволяет злоумышленнику узнать логины, пароли, записать телефонные разговоры и пр.

Идеология архитектуры NGN предусматривает создание интегрированных сетей доступа, с помощью которых пользователи получают доступ к услугам сети Интернет, телефонии, телевидения, в том числе к интегрированным услугам, объединяющим функциональность различных сетей. Вследствие этого оператор физически не может отделить инфраструктуру телефонной сети от Интернета. В результате появляются участки пересечения инфраструктур, где возможны злонамеренные действия:

– терминалы пользователя (SIP-телефоны);
– сети высокоскоростного доступа;
– системы доменных имен сети Интернет;
– серверы приложений.

Наличие таких точек соприкосновения различных фрагментов и позволяет злоумышленнику осуществлять неправомерные действия:

– активно влиять на сеть с целью снижения устойчивости сети телекоммуникаций и качества обслуживания (распределенные атаки DDoS, передача «ложных» сообщений);

– выполнять пассивные угрозы по отношению к сети действия (перехват сигнального трафика, декодирование логинов и паролей, перехват разговоров, создание подпольных переговорных пунктов);

– совершать хулиганские поступки (получение контроля над терминалом пользователя, вирусные атаки).

Важными задачами обеспечения информационной безопасности сетей NGN являются: задачи управления безопасностью и борьбы с мошенничеством в этих сетях, включая обеспечение безопасности услуг и сетевой инфраструктуры на основе технологий Softswitch и IMS, управление безопасностью мобильных технологий и минимизация риска при использовании новых технологий и внедрения новых услуг.

Задачи безопасности для сетей NGN состоят в следующем:

–только уполномоченные пользователи должны иметь доступ к сетям NGN и возможность их использования;

–уполномоченные пользователи должны обладать доступом к ресурсам, в отношении которых им предоставлен доступ, и возможностью работать с ними;

–сети NGN должны обеспечивать секретность на уровне, определенном политикой безопасности;

–все пользователи должны нести ответственность за свои и только свои действия в сети;

–в целях обеспечения готовности сети NGN должны быть защищены от несанкционированного доступа или действия;

–следует обеспечить возможность извлечения информации, связанной с безопасностью, из сети NGN (но только уполномоченные пользователи должны иметь возможность извлечения такой информации);

–в случае обнаружения нарушений безопасности они должны обрабатываться управляемым способом, согласно заранее установленному плану, с тем чтобы минимизировать потенциальный ущерб;

–по обнаружении преодоления защиты необходимо иметь возможность восстановления нормальных уровней защиты;

–архитектура безопасности сетей NGN должна обеспечивать определенную гибкость, чтобы поддерживать разные стратегии безопасности, например различную эффективность механизмов защиты.

Можно продемонстрировать, что при осуществлении следующих мер безопасности возможно выполнение первых пяти из вышеуказанных задач безопасности сетей NGN:

–конфиденциальность;

–целостность данных;

–отчетность, включая аутентификацию, сохранность информации и управление доступом;

–готовность.

Подходы к обеспечению информационной безопасности NGN должны определяться следующими характеристиками:

– общими сформированными требованиями к набору, параметрам механизмов и сервисам безопасности;

– реальными механизмами и сервисами безопасности, реализуемыми при обеспечении информационной безопасности;

– анализом существующей статистики угроз информационной безопасности и причин уязвимостей.

Требования к безопасности сетей и услуг NGN должны базироваться преимущественно на согласованных, на международном уровне стандартах безопасности, поскольку выгоднее использовать уже существующие, чем разрабатывать новые. Предоставление и использование услуг и механизмов, обеспечивающих безопасность, может быть довольно дорогим относительно стоимости защищаемых транзакций. Учитывая большое количество возможных сочетаний функций обеспечения безопасности, желательно иметь профили безопасности, охватывающие широкий диапазон сетевых услуг NGN.

Для анализа проблем информационной безопасности сетей NGN необходимо глубоко разобраться в сущности стоящей проблемы, во всех основных и сопутствующих ей аспектах и сформулировать цели, задачи и пути их решения с учетом особенностей, присущих используемым проводным и беспроводным технологиям NGN.

ВЗАИМОСВЯЗЬ ХАРАКТЕРИСТИК КАЧЕСТВА УСЛУГ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Р.Х. Джураев (ТУИТ, старший преподаватель)

Интенсивное внедрение ИКТ в различные сферы деятельности общества приводит к необходимости пересмотра их роля и значения в связи с возрастанием зависимости общества от безопасного функционирования сетей передали данных (СПД). Исследования показывают, что наряду с традиционными угрозами несанкционированного доступа к содержанию информации появились новые угрозы, связанные с нарушениями целостности и доступности информации. Поэтому при создании современных сетей необходимо проводить тщательный анализ последствий в части рисков нарушения целостности и доступности СПД. Ключевыми аспектами при этом становится анализ рисков нарушения целостности и доступности в СПД.

В новых международных стандартах и рекомендациях информационная безопасность рассматривается как один из показателей качества обслуживания в сетях передачи данных. Однако в настоящее время методы количественной оценки

информационной безопасности сетей передачи данных отсутствуют, хотя для большей части других показателей качества обслуживания (достоверность, скорость и надежность) такие методы имеются.

Традиционные методы обеспечения QoS предназначены в основном для работы в условиях случайных отказов и сбоев и не обеспечивают гарантированных качественных характеристик процесса передача информации пользователя в условиях информационных воздействий нарушителя на сети передачи данных.

В этой связи появились принципиально новые задачи, связанные с необходимостью обеспечения гарантированности качественных характеристик процесса передачи информации или качества обслуживания пользователей в условиях возможных преднамеренных воздействий нарушителя на информационную сферу сетей передачи данных.

В области оценки информационной безопасности в настоящее время развиваются два основных методических направления:

первое направление основывается на использовании для оценки ЙБ совокупности строго определенных требований, которым должны удовлетворять сети передачи данных (качественные подходы).

второе направление оценки информационной безопасности сети передачи данных основывается на определении числовых характеристик безопасности используемых в сетях передачи данных (количественные подходы).

Понятие, целостности информации характеризует степень идентичности принятых и переданных сообщений. При этом отличие целостности от достоверности заключается в том, что целостность учитывает, во-первых, как ошибки, так и вегавки и пропадания, а во-вторых, ошибки не только за счет шумов и искажений, но и за счет преднамеренных действий злоумышленников.

Современные технологии передачи данных обладают определенными уязвимостями по отношению к целостности информации и если их не учитывать то могут произойти следующие последствия: непреднамеренные модификация, удаление, задержка или формирование данных.

Рассмотрим уязвимости целостности информации в технологии TCP/IP:

- Искажение поля данных IP-пакета: после получения IP-пакета с нарушенной целостностью терминальное оборудование пользователя осуществит сборку искаженного сообщения и сформирует запрос на повторную передачу этою сообщения:
- Искажение адреса получателя IP-пакета: приведёт к тому, что пакет не дойдет до первоначального адресата и будет передан другому терминальному оборудованию.
- Нарушение целостности на транспортном уровне стека протоколов TCP/IP. приведет к блокированию процесса передачи сообщений, содержащих информацию управления;
- Удаление или искажения TCP-сегментов и UDP-дейтаграмм, посредством которых передаются эти сообщения могут привести к блокированию процесса передачи сообщения. Искажение TCP-сегментов и UDP-дейтаграмм подразумевает внесение в их содержимое обнаруживаемых или не обнаруживаемых средствами IP-сети ошибок;
- Нарушение целостности приводящие к блокированию процесса передачи сообщений, содержащих информацию управления: нарушение целостности пакетов данных может включать в себя: искажение заголовка или поля данных пакета SNMP путём внесения обнаруживаемых и не обнаруживаемых ошибок, а также удаление пакета данных;
- Изменение целостности сообщений приводящее к блокирование процесса передачи сообщений, содержащих информацию управления: блокирование процесса передачи сообщений, содержащих информацию управления, могут быть произойти путем нарушения целостности пакетов данных SNMP, посредством которых передаются эти сообщения.

В связи с этим важной задачей обеспечения качества услуг в сетях передачи данных в условиях возможных преднамеренных и непреднамеренных информационных воздействий на сети уделяется все большее внимание.

В тоже время параметры, характеризующие ИБ, несмотря на всю ее важность, до сих превосходят в число нормированных характеристик качества услуг сетей.

Для поддерживания заданного уровня качества обслуживания в условиях информационных воздействий необходимо производить оценку информационной безопасности сети передачи данных на основе анализа нарушения их целостности информации.

Для угрозы нарушение доступности коэффициент защищенности определяется, учитывая права доступа пользователей к информации и средства резервирования в СПД.

Накладывая коэффициент защищенности на время простоя информации, получим время простоя информации, учитывая средства защиты информации в СПД.

Перемножив итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы отказ в обслуживании для передачи данных «Информация – пользователи»

Для повышения информационной безопасности оператор СПД может задавать контрмеры. Для расчета эффективности введенной контрмеры необходимо выполнить последовательно все шаги алгоритма с учетом заданной контрмеры. В итоге на выходе оператор получит значение двух рисков – риска без учета контрмеры (R_{old}) и риск с учетом заданной контрмеры (R_{new}) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры *E* рассчитывается по следующей формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результате работы алгоритма оператор сети передачи данных получит следующие данные:

- риск реализации суммарно по всем угрозам для ресурса сети передачи данных;
- риск реализации по всем угрозам для СПД;
- риск реализации по «сем угрозам для сети передачи данных после задания контрмер;

Анализ рисков информационной безопасности - процесс получения информации, содержащей определения и анализ потенциальных угроз информационной безопасности сети телекоммуникаций, необходимый для принятия решений, связанных с оптимизацией капиталовложений в обеспечение информационной безопасности сетей телекоммуникаций.

Подсистема анализа и управления рисками становится неотъемлемой составной частью общей системы управления информационной безопасности. Кроме того, должны быть сформированы и установлены современные требования по информационной безопасности сетей передачи данных на основе анализа и управления этих рисков.

Рассмотренная методика анализа рисков нарушения доступности СПД дает оценки возможных потерь при возникновении угроз информационной безопасности. Применение метода количественной оценки риска требует определенных затрат на описание и анализ этих процессов, но неоспоримым преимуществом этого метода является гарантированная полнота определения рисков информационной безопасности.

МОДЕЛЬ И МЕТОДЫ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Р.Х. Джураев (ТУИТ, старший преподаватель)

Несмотря на все возрастающие усилия по использованию различных мер, методов и средств обеспечения информационной безопасности (ИБ) сетей передачи данных их

уязвимость не только не уменьшается, но и постоянно возрастает в условиях внедрения новых технологий ПД, поэтому проблемы ИБ сетей ПД становятся все более важными и актуальными.

Попытки решить проблему информационной безопасности исключительно криптографическими методами не обеспечивает должного результата, поэтому в настоящее время в сфере связи и информатизации встает проблема обеспечения не только конфиденциальности информации, но и обеспечения целостности самой инфраструктуры и информации, а также доступности информационных ресурсов и услуг.

Уязвимости, присущие сетям ПД, обуславливаются недостатками процесса функционирования, свойствами архитектуры сети ПД, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и др.

К числу важнейших задач в области обеспечения ИБ СПД относятся:

- разработка требований, критериев,показателей и методов оценки ИБ;
- разработка методов и методик оценки рисков ИБ;
- сертификация систем обеспечения ИБ и средств защиты информации по требованиям безопасности информации.

Анализ показывает, что ключевым фактором, влияющим на безопасность всей инфраструктуры, является проблема оценки ИБ сетей ПД.

В настоящее время развиваются два основных методических направления, которые могут быть использованы для оценки ИБ сетей ПД:

- первое направление основывается на использовании для оценки ИБ совокупности строго определенных требований и свойств, которым должны удовлетворять сети ПД (качественные критерии).
- второе направление оценки ИБ основывается на определении количественных характеристик ИБ сетей ПД (количественные критерии).

Необходимо отметить, что оценка информационной безопасности сетей ПД должна проводиться в три этапа:

- оценка технологии ПД, внедряемых на сети ПД, с точки зрения информационной безопасности;
- сертификация аппаратно-программного комплекса, внедряемого на сети ПД по требованиям безопасности информации;
- аудит информационной безопасности сетей ПД с целью проверки соответствия достигнутого уровня их информационной безопасности, заданному в техническом задании на их разработку.

Используемые в настоящее время на практике подходы к обеспечению информационной безопасности сетей ПД должны определяться следующими этапами:

- требованиями к информационной безопасности, реализуемыми системами обеспечения информационной безопасности и регламентирующими соответствующими нормативными документами в области информационной безопасности;
- реальными услугами и механизмами защиты, реализуемыми в системах обеспечения информационной безопасности;
- существующей статистикой угроз безопасности для конкретной сети ПД, потенциально возможными угрозами, а также причинами уязвимостей.

Оценка информационной безопасности сетей ПД должна производиться с целью проверки соответствия достигнутого уровня информационной безопасности заданному уровню при проектировании сетей ПД. Оценка информационной безопасности сетей ПД является также важным средством обеспечения гарантированности реализации выбранных механизмов, методов и средств информационной безопасности.

Обеспечение ИБ сетей ПД должно строиться на основе оценки безопасности, которая базируется на анализе рисков ИБ и возможности их количественного определения. В последние годы новое понятие риск ИБ постепенно заменяет

использовавшееся ранее угроза безопасности. Это связано с тем, что уровень риска ИБ зависит от вероятности реализации определенной угрозы в отношении определенного объекта, а также от величины возможного ущерба.

Процесс оценивания рисков может содержать следующие этапы:

- описание объекта и мер защиты;
- идентификация ресурсов и оценивание их количественных показателей;
- анализ угроз ИБ и оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения ИБ;
- оценивание рисков.

Ключевыми аспектами решения проблемы создания и развития безопасных сетей телекоммуникаций являются:

- исследование методов качественной и количественной оценок рисков ИБ;
- разработка методов и механизмов оценки рисков ИБ.
- анализ инструментальных средств оценки рисков ИБ;

Анализ качественных и количественных методов оценки рисков ИБ позволяет разрабатывать ряд методических документов, необходимых для проверки соответствия сетей ПД требованиям по безопасности информации.

В условиях динамичного развития сетей ПД и возникновения новых угроз информационной безопасности важным становится анализ и управление рисками информационной безопасности. Анализ рисков состоит в том, чтобы выявить существующие риски информационной безопасности и оценить их величину (дать им качественную или количественную оценку). Управление рисками информационной безопасности связано с принятием мер обеспечения информационной безопасности, направленных на снижение частоты реализации угроз и размера ущерба в случае их реализации.

Рассмотрим этапы анализа и управления информационными рисками:

- сначала необходимо определить все ценные информационные ресурсы, а также объекты их хранения и обработки;
- далее определяется стоимость информационных ресурсов (или ущерб, который нанесен от нарушения конфиденциальности, целостности или доступности ресурсов);
- кроме того, оценивается вероятность возникновения нарушений информационной безопасности, определяются уязвимости, существующие в сетях ПД и вероятности их реализации;
- на основании полученных данных рассчитывается риск для каждого информационного ресурса, который равен произведению вероятности возникновения нарушений и ущерба, который понесет в случае нарушения информационной безопасности.

Международный опыт развитых стран показывает что объективной и независимой оценкой соответствия систем и средств обеспечения информационной безопасности установленным требованиям безопасности является сертификация систем и средств на соответствие требованиям безопасности информации. Наиболее важными нормативно-правовыми документами при создании и развитии защищенных сетей телекоммуникаций являются документы, стандартизирующие требования, показатели и критерии оценки безопасности. К числу важнейших задач в области обеспечения информационной безопасности сетей телекоммуникаций относятся:

- анализ и разработка требований, показателей, критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности;
- сертификация систем и средств обеспечения информационной безопасности на основе современных требований и подходов.

Для проведения сертификации по требованиям безопасности информации необходимо наличие критериев оценки.

Как показывает международная практика, в ведущих странах мира наметилась

устойчивая тенденция перехода от оценки безопасности информационных технологий по национальным стандартам к их оценке и сертификации на основе международного стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», иначе называемого «Общие Критерии» (ОК).

В целях эффективного решения вышерассмотренных задач сертификации необходимо создание национальной системы сертификации систем и средств обеспечения информационной безопасности по требованиям безопасности информации, разработка методических основ их сертификации на основе Общих критериев.

АНАЛИЗ СРЕДЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ КАК ОБЪЕКТА ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ

Р.М. Ибраимова (ТУИТ, студент)

В среде облачных вычислений одним из актуальных является вопрос обеспечения качества обслуживания, так как облачные технологии могут оказаться не в состоянии полностью гарантировать соответствие уровня обслуживания требованиям производительности. Для решения данной проблемы необходимо исследовать особенности построения механизмов ресурсного обеспечения, исключающих ситуации снижения объемов производительности. В процессе создания и доставки услуг облачных вычислений участвуют сети нескольких типов, такие как внутренняя сеть центра обработки данных (далее ЦОД) и сеть связи между ЦОД, а также базовые сети транспортирования и доступа. Система облачных вычислений делится на две части: внешняя и внутренняя. Они соединяются друг с другом через сеть , как правило, Интернет. Внешняя находится на стороне пользователя компьютера, внутренняя является «облачной» частью системы.

На основе анализа общей модели архитектуры облачных технологий необходимо построить модель облачных вычислений как объекта обеспечения качества обслуживания.

У многоуровневого представления создаваемой модели как объекта качества, используемого в среде облачных вычислений, существуют четыре уровня, а так же ряд функций, которые проходят через эти уровни:

уровень пользователя;
уровень доступа;
уровень службы;
уровень ресурсов.

В созданной модели влияние на качество оказывает каждый из четырех уровней, но особое влияние оказывает уровень ресурсов. На уровне ресурсов находятся ресурсы, включая оборудование, обычно используемое в центре обработки данных, такое как серверы, сетевые коммутаторы и маршрутизаторы, устройства хранения, а также соответствующее программное обеспечение не специфичное для облачных вычислений, которое выполняется на серверах и другом оборудовании, такое как хостинговые операционные системы, гипервизоры, драйверы устройств и общее программное обеспечение управления системами.

В созданной модели участвуют многие элементы такие как: оператор облачных технологий, сеть доступа, транспортная сеть, абонентский терминал. Для того, чтобы анализировать созданную модель как объект качества, стоит дать определение некоторым элементам.

Транспортная сеть – совокупность всех ресурсов, выполняющих функции транспортирования, т. е. переноса информации между разнесенными пунктами. Она включает не только системы передачи информации, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления.

Сеть доступа – сеть связи, обеспечивающая подключение терминальных устройств пользователя к оконечному узлу транспортной сети связи, входящей в состав мультисервисной сети.

Оператор облачных технологий – предприятие (юридическое лицо), оказывающее услуги облачных технологий и имеющее соответствующую лицензию.

Терминал (абонентский терминал)–оконечная часть сети доступа, например, персональный компьютер, карманный персональный компьютер, мобильный телефон.

Важную роль в создаваемой модели играет оценка риска качества обслуживания.

Оценка рисков - это процесс, позволяющий связать воедино информацию о всех ресурсах облачной среды и их инфраструктуре, стоимости и уязвимых местах в системе качества и на основе полученной обобщенной информации.

Для обеспечения требуемого качества услуг (QoS) во время загрузки и преобразования данных в «облаке» необходима реализация требуемого качества на каждом элементе модели облачных вычислений рассмотренной выше. Требования по качеству обслуживания расписываются в соглашение об уровне предоставления услуг (SLA далее) – SLA договоре.

Соглашения об уровне обслуживания - важные компоненты управления облачными вычислениями и представляют согласованные между потребителем служб облачных вычислений и поставщиком служб облачных вычислений измеримые элементы качества обслуживания, которое должны быть гарантированы.

Одну из самых главных ролей в созданной модели играет мониторинг. В среде облачных вычислений важную роль играет мониторинг, особенно для оценки SLA/QoS, поскольку в среде облачных вычислений могут возникнуть проблемы, даже если состояние виртуальной машины или физического сервера, на котором они работают, кажется нормальным.

К мониторингу состояния облачной инфраструктуры относится мониторинг состояния ресурсов, таких как оборудование физических серверов, гипервизор, виртуальные машины, физические и виртуальные сетевые коммутаторы и маршрутизаторы, а также системы хранения данных.

Все технологические компоненты, включая транзакции, приложения, веб-серверы, сетевые коммутаторы, виртуальные компоненты и сторонние облачные услуги, отображаются на карте ресурсов. Наличие такой карты может играть важную роль в эффективном управлении бизнес-услугами, так как в случае возникновения проблемы приложения или транзакции она помогает определить компоненты инфраструктуры, которые могли вызвать нарушение.

XEMMINGNING NEYRON TO'RLARI ASOSIDA TASVIRNI TANISH

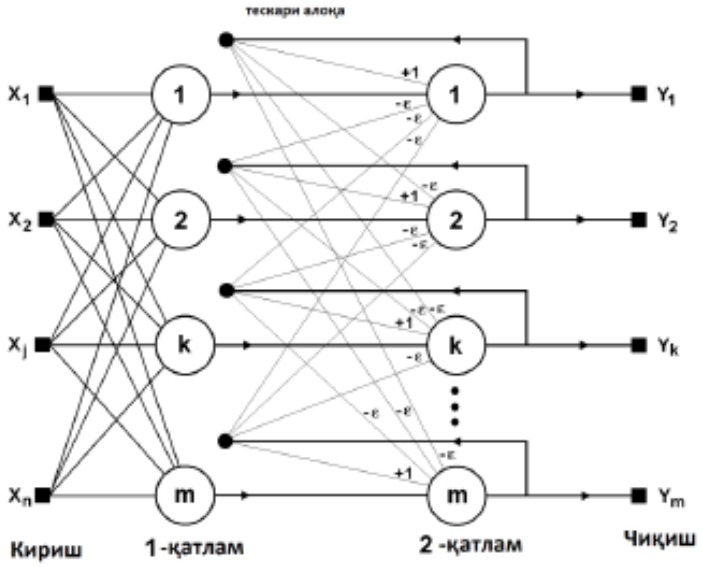
S.N. Iskandarova (TATU Samarqand filiali, assistant)

Ba'zida tarmoq shaklni aniqlay olmaydi va noto'g'ri shaklnng qiymatini chiqaradi. Bu tarmoqning chegaralanganligini bildiradi. Xopfild tarmog'ida saqlanib qoluvchi shakllar soni m, 0.15•n tadan oshib ketmasligi kerak.

Bundan tashqari, agar ikkita A va B shakllar bir biriga juda o'xshash bo'lsa, u holda ular tarmoqda kesishgan assosiasiyalarni tashkil etadi, ya'ni tarmoqqa A ni qiymatlarini berish B ni tarmoqdan chiqaradi, yoki aksincha.

Agar tarmoq shaklning aniq nomerini chiqarsa, u holda assosiativli xotira Ximming tarmog'ini yetarlicha yaxshi qo'llaydi.Tarmoq ikkita qatlamdan iborat bo'lsa, birinchi va ikkinchi qatlamlar m neyronlardan iborat bo'ladi, bu yerda m shakllar soni. Birinchi qatlamdagi neyronlar n ta tarmoq kirishi bilan bog'langan sinapslardan iborat. Ikkinchi qatlamdagi neyronlar teskari aloqa qiluvchi sinapslar bilan bog'langan. Yagona musbat teskari

aloqadagi sinaps o'zining neyronlari bilan bog'langan. Tarmoq ishining maqsadi, barcha tasvirlar bilan testlanayotgan tasvirlar orasidagi masofani topish sanaladi.



1- rasm. Faollashtiruvchi funksiya

Xemming masofasi bu ikkita binar vektorlarning bitlardagi farqi tushiniladi. Tarmoq namuna bilan no'malum tasvirlar orasidagi minimal Xemming masofasini tanlashni amalga oshiradi va natijada bu tasvirga mos bitta neyron faol bo'lib qoladi. Birinchi qatlamga og'irlik koeffisiyentlarini ta'minlashda va faollashtiruvchi funksiyaga qiymat berish qo'yidagicha amalga oshiriladi:

$$w_{ik} = \frac{x_i^k}{2}, i = 0 \dots n-1, k = 0 \dots m-1$$

$$T_{k=\frac{n}{2}, k=0 \dots m-1}$$

Bu yerda x^k_i –k- shaklning i-elementi. Sinapslarni to'xtovchi og'irlik koeffisiyentlari ikkinchi qatlamda qandaydir $0 < \varepsilon < 1/m$ qiymatni qabul qiladi. O'z askoni bilan bog'langan neyron sinapsi +1 og'irlikka ega bo'ladi.

Xemming tarmoqining bajaradigan ishni algoritmi quyidagicha:

1. Tarmoqa birinchi qatlamdagi hisoblangan va uni qiymatini e'tiborga olgan no'malum X = {xi:i=0...n-1}, vektor kiritiladi(yuqori indeks qatlam nomerini bildiradi):

$$y_j^{(1)} = s_j^{(1)} = \sum_{i=0}^{x-1} w_{ij} x_i + T_j, j = 0 \dots m-1$$

Shundan sung olingan qiymatlar asosida ikkinchi qatlamning aksonlari hisoblanadi:

yj(2) = yj(1), j = 0...m-1

2. Ikkinchi qatlamning yangi holati hisoblanadi:

$$s_j^{(2)}(p+1) = y_j(p) - \varepsilon \sum_{i=0}^{n-1} y_k^{(2)}(p), k \neq j, j = 0 \dots m-1$$

va uning aksonlarining qiymati:

$$y_j^{(2)}(p+1) = f\left[s_j^{(2)}(p+1)\right], j = 0 \dots m-1$$

Faollashtiruvchi f funksiyaning qiymati bo'ladi, bu yerda F yetarlicha katta bo'lib, ixtiyoriy argumentning qiymati undan oshib ketmaydi.

3. Oxirgi iterasiyada ikkinchi qatlamning qiymatlari o'zgargan yoki o'zgarmaganligi tekshiriladi, agar ha bo'lsa, u holda 2 qadamga, aks holda esa sikl to'xtatiladi.

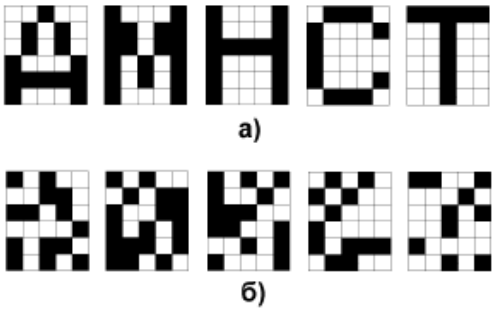
Algoritmni baholashdan ko'rinib turibdiki, birinchi qatlam shartli ahamiyatga ega bo'lib qolmoqda: birinchi qadamda og'irlik koeffisiyentlarining qiymatlarinidan bir marta foydalaniladi, shuning uchun birinchi qatlam qo'yida ko'rsatilganidek tarmoqdan umuman olib tashlandi.

Xemming tarmog'ining dasturiy modeli maxsus sinflarni saralashga asoslangan.
NetHN sinfida qo'yidagi elementlar aniqlangan:

–Nin va Nout – ma'lumotlarga mos ravishda kiruvchi vektorlarning o'lchami va shakllar soni;

–dx va dy – ikkita kordinatalar orqali kiruvchi shakllarning o'lchamlari, dx*dy = Nin, bu funksiyalar LoadNextPattern fayldan ma'lumotlarni kiritish uchun foydalaniladi;

Bu yerda ikkinchi qatlam beshta harfni tanish uchun ishlatilmoqda. Sun'iy neyron to'rlarining rivojlanishida biologiyaning o'rni katta. Izlanuvchilar mavjud tarmoq konfigurasiyasi va algaritmiga mos terminlarni qo'llagan holda aqliy faoliyat tashkilotini tasvirlashadi. Lekin ehtimol shu o'xshashlik bilan tugaydi. Bizni miyaning ishlashi haqidagi bilimlarimiz biroz chegaralangan, oriyentirlab unga taqlid qilganlar kam topilgan. Shuning uchun to'rni ishlab chiquvchilar kerakli funksiyani bajarish qobiliyatiga ega bo'lgan tuzilishni qidirishda zamonaviy biologik bilimlar doirasidan chiqishga majbur bo'lishadi.



2-rasm. Namunaviy va test qilinadigan shakllar.

Shular asosida ko'plab natijalar olinishi mumkin. Neyron to'rlarni o'rganish natijasida ularning bir qancha xususiyatlari ma'lum bo'ldi. Neyron to'rlardan prognozlashda, jarayonlarni boshqarishda, mitatsiya qilish va taxlil qilishda foydalanish yuqori samara beradi. Neyron to'rlarni boshqa usullarni tadbiq qilish qiyin bo'lgan sharoitlarda – muammoni xal qilish algoritmi mavxum bo'lganda, ma'lumotlar noaniqligida, etishmasligida, juda katta yoki juda kichik xajmdaligida, qarama-qarshiliklar mavjud sharoitlarda tadbiq qilish oson va samarali. Neyron to'rlarning afzalliklarini va mavjud kompyuter dastur paketlarining qulaylik va samaradorligini xisobga olib uni innovatsiya jarayonlarida qo'llash istiqbolli ekanligini xulosa qilish qiyin emas.

XOPFILDNING NEYRON TO'RLARI ASOSIDA TASVIRNI TANISH

S.N. Iskandarova (TATU Samarqand filiali, assistent)

Neyron to'rlarini sintez qilishda algoritmlarning nozik tomoni bu qaror qabul qilishni tushuntirish bo'lib hisoblanadi. Bu muammoni yechish bilan ko'pchilik tadqiqotchilar shug'ullanmoqdalar. Bu maqsadda ishlatadigan usullar evristik bo'lganligi uchun ular asosida korrekt qaror qabul qilish foydalanuvchining subektiv mulohazasiga bog'liq bo'ladi.

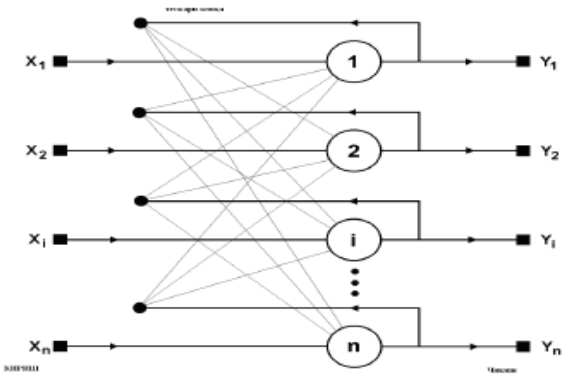
Ko'p o'lchovli chiziqsiz optimizasiyaning an'anaviy iterativ gradiyent

algoritmlari bilan o'rganadigan neyron to'rlari modellarining eng ko'p tarqalgani - bu ko'p qatlamli sun'iy neyron to'rlari sinfidir. Ma'lumki, ko'p qatlamli sun'iy neyron to'rlari o'rganishda iterativ algoritmlar yaqinlashuvi, o'rganiladigan berilganlarning (tanlovning) hajmiga, vaznlarning boshlang'ich qiymatiga, shuningdek, o'rganishdagi maksimal xatolarga

(o'rganishning sifat mezonlariga), o'rganishdagi takrorlanishlar soniga (o'rganish vaqtining uzayishi mezonlariga) bog'liq.

Sunniy neyron to'rlari konfigurasiyalari orasida klassifikasiyalashda o'qitish prinsiplari bo'yicha o'qituvchi yordamida o'rgatish va o'qituvchisiz o'rgatish prinsiplariga to'g'ri kelmaydi. Bunday hollarda og'irlik koeffisiyentlari qayta ishlanayotgan axborotlar yordamida izlab topiladi va barcha o'rgatishlar xuddi shu hisoblashga keltiriladi.

Bir tomondan aprior axborotlarni o'qituvchining yordami sifatida qabul qilish kerak, boshqa tomondan tarmoq tasvirlarni haqiqiy ma'luotlar kelguncha xotirada saqlab qoladi. Bunday mantiqiy bog'lanishli tarmoqlar sifatida Xopfild va Xemming to'rlarini yaxshi tanilgan. Quyida kirishi va chiqishi bitta bo'lgan bir qatlamli Xopfildning neyron tarmog'i keltirilgan.



1-rasm. Xopfild tarmog'ining strukturali sxemasi.

Assosiativ xotira kabi bu tarmoqda yechiladigan masala qo'yidagicha shakllantiriladi. Shakl ko'rinishidagi (tasvir, raqamlashgan ovozlar kabi jaryonlarni yoki ob'yektlarni ifodalovchi) qandaydir ikkilik signallardan tashkil topgan bo'lsin. Tarmoq unga kirib kelayotgan ideal bo'magan mos tasvirli signallarni ajratib saqlab qolsin, yoki kirib kelgan ma'lumotlar birorta ham shaklga mos kelmasligi haqida xabar bersin.

Umumiy holda, ixtiyoriy signalni X = { xi: i=0...n-1} vektor , n – tarmoqdagi neyronlar soni, kiruvchi va chiquvchi vektorlar hajmi. Har bir xi element – 1 yoki -1 ga teng. k – shaklni ifodalovchi vektorni X^k vektor bilan ifodalaymiz va uning kompnentalarini mos holda – x_i^k , k=0...m-1, m – shakllar soni, bilan belgilaymiz.

Tarmoqqa berilgan ma'lumotlar asosida u shaklni tanisa, u holda unga kiruvchi ma'lumot Y = X^k bo'ladi , bu yerda Y tarmoqqa kiruvchi Y = { yi: i=0,...n-1} vektor qiymati. Aks holda, chiquvchi vektor hech qanday namunadagi shakl bilan mos kelmaydi.

Agar, masalan, signallar qandaydir shaklni ifodalasa, u holda u tarmoqqa kirishda uni grafik ko'rinishida ifodalaydi va namunadagi birorta shakl bilan mos kelganligini yoki mos kelmaganligini aniqlaydi.

Tarmoq qiymatlarni qabul qilishda og'irlik koeffisiyenti qo'yidagi shaklda ifodalanadi:

$$W_{ij=\sum_{I=0}^{m-1} x_i^k x_j^k \; agar \; j \neq i \; aks \; holda \; 0;}$$

Bu yerda i, j – indekslar bo'lib, mos holda oldsnaptik va orqsnaptik neyronlar; xik, xjk – i- va j, k- shakl vektorining elementlari.

Tarmoq bajaradigan ishning algoritmi qo'yidagicha (p – iterasiya nomeri):

1. Tarmoqqa kirish uchun no'malum signal beriladi. Unga aksonlarning qiymatlarini beriladi:

yi(0) = xi , i = 0...n-1

shuning uchun tarmoq sxemasida kiruvchi snapslar shartli xarakterda bo'ladi. Nol esa, tarmoqning nolinchi iterasiyasini bildiradi.

2. Neyronlarnng yangi holati hisoblanadi

$$s_j = (p+1) = \sum_{i=0}^{n-1} w_q y_i(p), j = 0 \dots n-1$$

va aksonlarning yangi qiymatlari

$$y_i(p+1) = f[s_i(p+1)]$$

bu yerda f – sakrash ko'rinishidagi faollashtiruvchi funksiya ko'rsatilgan.

3. Oxirgi iterasiyada aksonlarning qiymati tekshiriladi. Agar ha bo'lsa, u holda 2 qadamga o'tiladi, aks holda tamomlanadi. Bu holatda chiquvchi vektor namunadagi shaklga uxshash eng yaxshi shaklga ega bo'ladi.

Maxsus adabiyotlar va Internet resurslarini analiz qilishi natijasida, neyrobiologiya, kibernetika, sunniy intellekt, suniy neyron to'rlari va neyroto'rli o'zi tashkil bo'luvchi, perseptronlar va tasvirlarni mashinada tanish, diskret matematika, ehtimollar nazariyasi va matematik statistika, ob'yektga yo'naltirilgan dasturlash tili C++ o'rganildi.

Muammoni hal etishda har bir belgini xarakteristikalari aniqlandi. Grafik tasvirlarni aniqlashda o'zi tashkil bo'luvchi suniy neyron to'rlari tashkil etildi va parallel hisoblash tashkil etildi. Ishda neyro-matrisali etalon bazasini yaratuvchi va testlanadigan tasvirlarni qayta ishlaydigan Xopfeld to'ri yaratildi. Yaratish belgilar bo'yicha ikki o'lchamli og'irlik koeffisiyentlarini massiv xarakteristikalarini o'zgartirishni amalga oshiriladi.

SNT larida ishlovchi algoritm o'rganildi va uning blok sxemasi, model loyihasi va berilgan usulning talablarini qanoatlantiruvchi dasturiy ilovalari yaratildi. Olib borilgan ish natijasida tasvirlarni tanishdagi usullar o'rganildi, jumladan, raqamlar, lotin va rus grafikasidagi alfavitlar, bundan tashqari barcha xildagi belgilarga qo'llanilishi mumkin. SNT lari modellashtirildi, testlandi va kompyuter dasturi yaratildi.

Yaratilgan dasturiy vositalarni tasvirlarni tanishda va ularga parallel ishlov berish natijasida davturiy vositani ish samaradorligi bir necha marta oshirildi. Xopfeld tarmog'i orqali tasvirlarni tanishning parallel ishlovchi dasturiy vositalari kompyutkrlarni ishlash vaqti tejaladi.

Neyron to'rlarni loyixalash va yaratish borasida ko'plab kompyuter dasturlari ishlab chiqarilgan. Ular orasida MathWorks firmasi tomonidan yaratilgan MatLab kompyuter dasturi paketi ustunliklari bilan aloxida ajralib turadi. Chunki aynan shu dastur matematik yadroga va neyron to'rlar qism paketiga ega. Unda eng sodda neyron modelidan tortib, ixtiyoriy transfer funktsiyali ixtiyoriy arxitekturadagi murakkab neyron to'rlarni oson va tez yaratish mumkin.

Bundan tashqari paket tarkibiga teskari aloqali chiziqli boshqaruvchi, zavod kelajagini prognozlovchi va baxolovchi, funktsiyalarni approksimatsiyalovchi vositalar xam kiradi. Neyron to'rlarni o'rgatishning bir qancha algoritmlari xam paketda amalga oshirilgan.

Bunga asosiy sabab boshqa usullardagi kabi kerakli jarayonni qonuniyatlarini aniqlab, matematik tenglamalar tuzib, echish algoritmlari ishlab chiqishning zaruriyati yo'q. Neyron to'rlar arxitekturasi, transfer funktsiyalar va o'rgatish algoritmlari to'g'ri tanlansa neyron to'rni tayyor ma'lumotlarda o'rgatish natijasida, u foydalanishga tayyor bo'ladi.

GSM SECURITY OVERVIEW

Kh.A. Khamdamova (Student of Master degree of TUIT)

GSM is the biggest wireless network in the world. GSM (Global System for Mobile communication) uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). Infocommunication community is now entering a new stage of development, which can safely be called the era of content when the information is transmitted over the network becomes more valuable than ever before.

Value of the information circulating in communication networks, and makes it necessary to protect it from third parties, the so-called information security violators. In general, the information to be protected, to be split on the accessories, and the level of confidentiality. Accessories - is the actual information of users that an operator provides services, and a service - information service provider. Protection of official information for the operator is of paramount importance, as has a direct impact on network performance, and hence the income from this business. The system establishes a certain basic level of information security, providing technical and organizational security measures. The operator is required to maintain it in their own best interest. This level is defined by the profile of protection and is dependent on a variety of sometimes conflicting factors, as well as the model of action alleged infringer (the attacker), potential attacks and so on. N. In addition, the level of security of the network of information resources is determined by the enterprise security policy, performing the network operator functions, and those financial investments that the organization is ready to allocate the profits for the maintenance and development of information security systems. Given these conditions, and the factor that the attack time, motivation, offender type (internal or external), a model of action of the offender and the potential of his attacks can be known in advance, it becomes clear how difficult it is to ensure a permanent and effective protection of mobile network system information from the attacks.

The advent of GSM cellular network operators allowed to provide a guaranteed privacy for subscribers. This standard uses a quite advanced traffic protection methods and reliable technology solutions. Increasingly, however, there is information about the possibility of interception, hacking and cloning of GSM subscriber terminals operating in these networks.

The GSM standard uses a narrowband multiple access with time division multiplexing (NB TDMA). The TDMA frame structure contains 8 time positions in each of the 124 carriers.

To combat the interference fading of received signals caused by multipath propagation of radio waves in urban environments, communications equipment used by equalizers to ensure alignment of pulsed signals with a standard deviation of up to 16 ms of delay time. Synchronization system is designed to compensate for the absolute time to 233 ms of delay signals corresponding to the maximum communication range or the maximum cell radius (cell) 35 km.

The GSM standard is chosen Gaussian Frequency Shift Keying with a minimum frequency shift (GMSK). Speech processing is performed within the received speech discontinuous transmission system (DTX), which lets the transmitter only when a speech signal transmitter and off at intervals and at the end of the conversation. As speech converting device selected speech codec with regular pulse excitation / long term prediction and linear predicative coding predictive (RPE / LTR-LTP-codec). The total conversion rate of the speech signal - 13 kbit / s.

In the GSM standard, a high degree of safety message transmission; encrypts messages using the algorithm with public key cryptography (RSA).

To guard against errors in the radio channels at transmission of information messages and applies block interleaving to convolutional coding. Improving the efficiency of encoding and interleaving for low velocity of the mobile stations is achieved by slow switching operating frequencies (SFH) in the communication session with the speed 217 hops per second.

Structural construction of the GSM network diagram is shown in Fig. 1. The main elements of this scheme are: MS - Mobile Station; BTS - Base Station; BSC - Base Station Controller; TCE –Transe Coder; BSS - Base Station Subsystem (BSC + TCE + BTS); MSC - Mobile Switching Center; HLR - Home Location Register; VLR –Visitor Location Register; AUC - Authentication Center; EIR – The Equipment Identity Register; OMC - Operation and Maintenance Center; NMC - Network Management Center; ADC - Administrative Center; PSTN - Public Switched Telephone Network; PDN – Packet Data Network; ISDN - Integrated Services Digital Network.

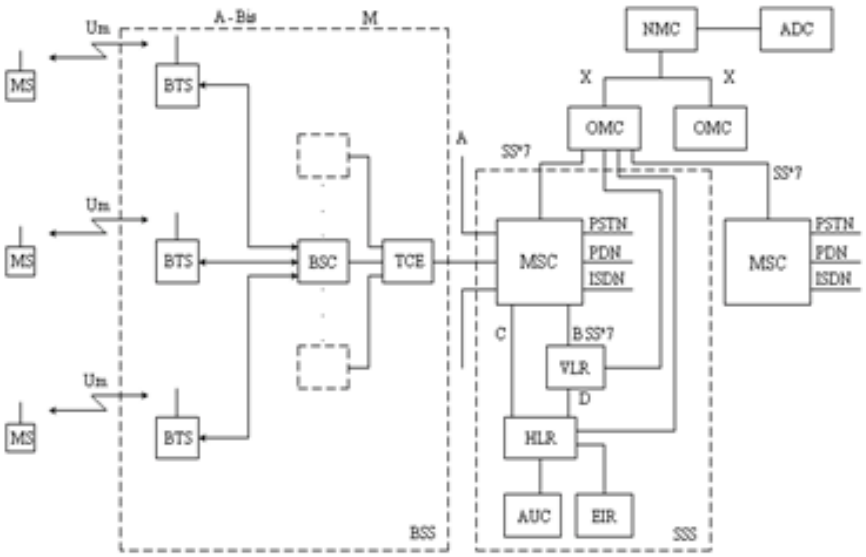


Fig.1. Structural construction of GSM cellular communication network

АНАЛИЗ МОДЕЛИ ТРАФИКА В СЕТЯХ С КОММУТАЦИЕЙ ПАКЕТОВ

И.А. Кадыралиев (ТУИТ, магистрант)

До недавнего времени теоретическую базу для проектирования сетей телекоммуникаций обеспечивала теория телетрафика, которая является одной из ветвей теории массового обслуживания (работы Эрланга и др) .

Классическая теория телетрафика Эрланга и её приложения хорошо описывают процессы, происходящие в телефонных сетях, построенных на принципах коммутации каналов.

Наиболее распространенной моделью потока вызовов в теории телетрафика является простейший поток (стационарный, ординарный без последствия, также называемый стационарным пуассоновским). Исследования телетрафика привели к выводам о пуассоновском потоке телефонных вызовов и экспоненциальном распределении продолжительности телефонных разговоров.

В основе проектирования узлов и сетей для обслуживания речевого трафика , т.е. традиционных услуг телефонной связи, которые составляют основу современных коммутируемых телефонных сетей общего пользования ТФОП принято считать:

-случайный характер потока обычных телефонных вызовов со средним значением 3 вызова в час наибольшей нагрузки от абонента;

-обычные телефонные соединения между абонентами относительно короткие по длительности -в среднем три минуты.

Произведение этих двух величин составляет 0,15 эрланга на абонентскую линию, которая лежит в основе проектирования ТФОП.

В качестве аналитической модели для расчета телефонных сетей с коммутацией каналов используются системы с потерями вызовов.

Развитие сетевых технологий привело к распространению сетей с пакетной коммутацией, которые постепенно стали вытеснять системы с коммутацией каналов, но по-прежнему проектировались на основе традиционных положений теории телетрафика.

В 1993 г. группа ученных (W. Leland, M. Taqqu, W. Willinger, D. Wilson), которая исследовала Ethernet-трафик в сети корпорации Bellcore, обнаружила, что на больших масштабах трафик выглядит качественно одинаково при любых (достаточно больших) масштабах временной оси, т.е. обладает свойством самоподобия. Кроме того, было обнаружено, что в условиях самоподобного трафика методы традиционной теории телетрафика дают неадекватные решения.

Исследования трафика в сетях ПД с коммутацией пакетов показали, что потоки в них имеют совершенно иную структуру, чем принято в классической теории телетрафика. В сетях ПД с коммутацией пакетов трафик обладает так называемым свойством самоподобия, т.е. выглядит качественно одинаково при почти любых масштабах временной оси, имеет память (последствие), а также характеризуется высокой пачечностью.

Однако для потоков с самоподобными свойствами не в полной мере разработаны инженерные методы расчета .Нет единой общепринятой модели самоподобного трафика.Отсутствие общепринятой модели самоподобного трафика и строгих методов расчета затрудняет прогнозирование развития телекоммуникаций.

Для определения самоподобного трафика в работе [3] были введены следующие обозначения:

- стационарный процесс $\boldsymbol{X} = (X_t)$, где, t = (0, 1, 2, …);
- $r(\tau)$ – функция автокорреляции $\boldsymbol{X}$;
- $\boldsymbol{X}^{(m)}$ – агрегированный процесс $\boldsymbol{X}$, т.е. процесс $\boldsymbol{X}$, усредненный по блокам длины m, каждый элемент которого определяется как

$$X_i^{(m)} = \frac{1}{m} \cdot \sum_{t=i\cdot m-m+1}^{i\cdot m} X_t \qquad (1)$$

- $r^{(m)}(\tau)$ – функция автокорреляции агрегированного процесса $\mathbf{X}^{(m)}$.

Для построения модели трафика в конкретных сетях передачи данных необходимо:

-проведение эксперимента по измерению трафика;

-выполнение статистического анализа реализаций трафика.

Одно из направлений решения задачи расчета сетей передачи данных с коммутацией пакетов -оценка параметров качества обслуживания, т.е. анализ вероятностно-временных характеристик сетей. В качестве аналитической модели для расчета сетей передачи с коммутацией пакетов используются системы с очередями.

Для исследования влияния параметров самоподобного трафика была рассмотрена имитационная модель сети IP/MPLS, созданная посредством программного продукта OPNET Modeler. В качестве распределения размеров пакетов было выбрано распределение Парето. В ходе моделирования исследовалась влияние параметров распределения Парето и параметра Хэрста на сетевые характеристики.

По результатам имитационного моделирования должны быть получены следующие выводы:

- влияние параметра *a* распределения Парето на количество отброшенных пакетов,
- влияние параметра Хэрста на размер очередей пакетов в маршрутизаторах.;
- влияние параметра Хэрста на максимальное значение задержки пакетов в очередях маршрутизаторов.;
- влияние параметра Хэрста на среднюю скорость передачи информации в сети:
- влияние параметра Хэрста на задержку передачи пакетов «из конца - в конец».

MAHALIY TELEFON TARMOG'I UCHUN TRIPLE-PLAY XIZMATLARINI TAQDIM ETISH

J.R. Kilichov (TATU SF, assistent)
M.M. Maxammadiyev (TATU,2 – kurs magistranti)

Bugungi kunda integrallashgan multiservis tarmoqlarini qurish tendensiyasi saqlanib qolmoqda. Multiservis tarmoqlarini tadqiq qilish natijalarining ko'rsatishicha, teng imkoniyatli yuklamalarga xizmat ko'rsatishda kanallarning o'tkazuvchanlik qobiliyati cheklanganligini e'tiborga olish zarur.

Multiservisli platforma ulanishlari uchta birlikni (ma'lumotli belgilar/ovoz/video) ushlab turish asosida oriyentatsiya qilib, Triple Play konsepsiyasi talablariga mos keladi. Keng polosali

ulanishlarda raqobatli texnologiyalar bu PON (passiv optik tarmoq) va Ethernet texnologiyalaridir.

Paketli kommutatsiya tarmoqlari signallar kechikishiga kamsezgirli vazifalarni bajarishga mo'ljallangan. Tovush xabarlari va video esa aksincha, axborot uzatish tezligiga juda talabchan, bunda paketlarning 150 ms dan ortiq kechikishi, paket zarur emasligini bildiradi, undagi xabarlar eskirgan bo'ladi. Demak, tovush xabarlari va video ma'lumotlari uchun tarmoqlar, paketlarni real vaqtda o'tishi samaradorligini maksimal oshirish nuqtai nazaridan ishlab chiqilishi, yaratilishi va ekspluatatsiya qilinishi lozim.

Multiservis tarmoqlarining abonent kirishi bosqichida Triple-Play xizmatlarini ko'rsatishda tushayotgan yuklamani axborotlar taqsimoti nazariyasiga binoan ko'p potokolli model deb qarash mumkin. Shunga asosan, abonent kirishi bosqichidagi multiservis yuklamani tasodifiy Markov jarayoni, deb qabul qilamiz. Abonent kirish bosqichida Triple-Play potoklariga xizmat ko'rsatish jarayonining funksional modeli quyidagicha tasvirlanadi:

Triple-Play xizmatlarini taqdim etish funksional modelining sxemasi bo'yicha quyidagilarni ta'kidlash mumkin:

- tovush, video va ma'lumotlar, hamda Internet trafiklari yagona kanal resurisidan foydalaniladi, deb faraz qilish.
- kanalga tushayotgan tovush va video xabarlariga absolyut imtiyozli xizmat ko'rsatish.

Agar tovush va video xabarlariga xizmat ko'rsatishda kanal resurslari bo'sh bo'lmasa, bu xabarlarga xizmat ko'rsatish, ma'lumotlar va Internet xabarlariga xizmat ko'rsatayotgan kanal resursidan foydalana olishlari ko'zda tutiladi.

TriplePlay — marketnigli telekommunikatsiya termini bo'lib, iste'molchiga bitta kabelda keng polosali kirishda bir vatqni o'zida uchta xizmat turi – yuqori tezlikga ega Internet, kabelli televideniya va telefon aloqasini taqdim qiladi.

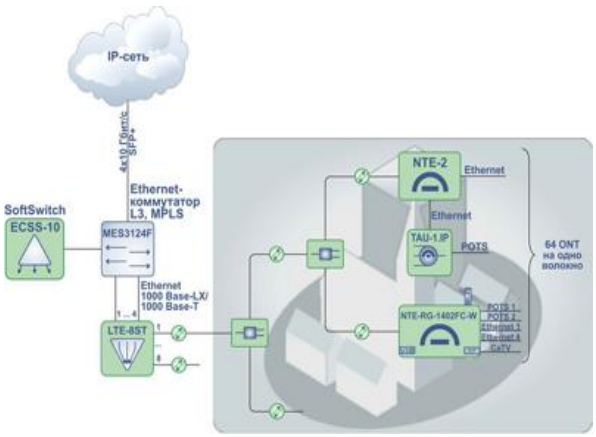
Albatta, o'tkazish polosasini yuklanishida videotrafik muhim rol o'ynaydi. Bugungi kunda bitta televizion kanalini translyatsiyasi yoki VoD 4 Mbit/s uzatish tezligini talab qiladi. Ushbu holat MPEG-4 standartiga o'tsak yaxshilanadi, lekin sifatli tasvirni olish uchun videotrafikda 2 Mbit/s gacha zahira mavjud bo'lishi lozimdir.

Abonent kanalini o'tkazish polosasi nuqtayi nazaridan qarasak yana bir resurslaridan biri bu komyuter o'yinlari servisidir. Tarmoqli komyuter o'yinlari uchun 2 Mbit/s polosa talab qilinadi. Qolgan resurslar esa telefon kanali uchun 64 kbit/s, radio eshttirish va Internet uchun 128 kbit/s yetarlicha bo'ladi. Barcha xizmat turalri uchun 6 Mbit/s minimal o'tkazish polosasi yetarlicha bo'ladi. Ushbu tezlikni ADSL, PON va Ethernet texnologiyalari ham ta'minlab beradi. Ushbu aloqa xizmat turalarini internetdan olingan tahliliy natijalarga asoslanib 300 yirik operatorlari hozirda triple play xizmat turlarini rivojlantrish uchun turli xil qurilma va texnologiyalarni taqdim qilishmoqda.

Yuqoridagilari hisobga olgan holda xorijiy analitiklar triple play xizmatini taqdim qilish uchun abonent kanalini minimal o'tkazish qobiliyati 20 Mbit/s dan kam bo'lmasligini lozimligi ta'kidlashadi. Bunday tezlikni ADSL2+, PON va Ethernet texnologiyalari orqali amalga oshirish mumkin.

Yuqoridagi xizmat turlarini Turbo GEPON texnologiyasi asosida aholi yashash komplekslarida keng polosali kirish tarmoqlari uchun ta'minlab berishi mumkin. Keng polosali kirish tarmoqlari Internet, IP TV, paketli telefoniya xizmat turlari hisoblanadi.

GEPON arxitekturasi asosida **P2MP (point-to-multipoint)** "nuqta-ko'p nuqtalar" logik topologiyasidan foydalanib optik tarmoqlarni tashkillashtirish mumkin. Bitta markaziy tugun portiga butun bir optik-tolali segmentiga ega o'nlab abonentni qamrab oluvchi "daraxt"li arxitekturani ulash mumkin. Bunda passiv optik shahobchalarni (splitterlar) oraliq tugunlarga ulanadi, eng asosiysi ushbu qurilmalar elektr ta'minotini va texnik xizmatni talab qilmaydi.



1- rasm. Turbo GEPON texnologiyasi

VIRTUAL TARMOQLARNI DASTURIY KONFIGURATSIYALANGAN TARMOQLAR (DKT) ASOSIDA TASHKIL ETISH

A.A.Qodirov (TATU, assistent)

Tarmoq virtualizatsiyasi - bu ma’lumot uzatish tarmog‘ining real jismoniy vositalarini mantiqiy tarmoq ko‘rinishida tasvirlash texnologiyasi.

Tarmoq virtualizatsiyasining ikki turi mavjud:

1. Tashqi virtualizatsiya (external) - bitta jismoniy tarmoqni bir nechta mantiqiy tarmoqga bo‘lish yoki aksincha - bir nechta jismoniy tarmoqni bitta mantiqiy tarmoqga birlashtirish.

2. Ichki virtualizatsiya (internal) - jismoniy ma’lumot uzatish tarmog‘i ishtirokisiz bitta jismoniy server kompyuteri ichidagi virtual mashinalar orasida mantiqiy tarmoq yaratish.

Tarmoq virtualizatsiyasi odatda dislokatsiya qilingan, ya’ni har xil “nuqta-larda” joylashgan bir nechta jismoniy lokal kompyuter tarmoqlarini yagona mantiqiy tarmoqga birlashtirish maqsadlarida ishlatiladi.

Ammo bunday usullar negizida mantiqiy tarmoqlarni yaratilishida ikkita muammo kelib chiqishi mumkin.

1- muammo. Bunday tarmoq negizida ma’lumot qayta ishlash markazi yaratilayotganida joriy tarmoqning holatiga qarab mantiqiy tarmoq tarkibidagi virtual mashinalar orasidagi bog‘lanishlar va ular orasidagi tunnellar muntazam ravishda o‘zgartirilishi kerak bo‘ladi. Bunday yangi bog‘lanishlarni ta'minlash uchun tarmoq vositalarini muntazam sozlab turish talab etiladi.

Masalan, yangi mantiqiy tarmoq, yangi virtual mashina yaratilganida, virtual mashinalarni bir serverdan boshqasiga ulash amalga oshirilayotganida tarmoq vositalirining konfiguratsiyasiga ma’lum o‘zgartirishlar kiritilishi kerak bo‘ladi. Virtual tarmoqlarni markazlashgan holda boshqarilishida maxsus interfeyslar talab etiladi. Har xil tarmoq vositalari bog‘lanishi uchun ham interfeyslar talab etiladi.

2- muammo. Mantiqiy tarmoq yaratish texnologiyasida umumiy bir jismoniy vositaning resurslari mantiqiy tarmoqlar orasida bo‘linadi, shu bilan birga tarmoqni boshqarish ham o‘zgaradi, ya'ni marshrutlash va oqimlarni taqsimlash algoritmlari ham o‘zgarishi kerak bo‘ladi. Bir nechta mantiqiy tarmoqlarda har xil boshqarish usullarini qo‘llash kerak bo‘ladi.

Bu muammolarni dasturiy konfiguratsiyalanadigan tarmoqlar (DKT) ni qo‘llash orqali bartaraf etilishi mumkin.

DKT ning asosiy g‘oyasi- tarmoqni boshqarish sathini ma’lumot uzatish sathidan ajratish hisoblanadi.

Ushbu g‘oyani virtual tarmoqlarni boshqarish jarayonlariga qo‘llash butun tarmoq boshqaruvini kontrollerga yuklash va shu yo‘l bilan butun tarmoq tizimining mantiqiy boshqaruvini markazlashtirish va avtomatlashtirish imkonini beradi.

Mantiqiy tarmoqlar boshqaruvini dasturiy konfiguratsiyalanadigan tarmoqlar negizida amalga oshirishda ikkita masalani hal qilish kerak bo‘ladi:

1. Kommutator sozlamalari o‘zgartirilishini avtomatlashtirish;
2. Tarmoqda ma'lumot uzatish jarayonlarini boshqarish.

Kommutator sozlamalari o‘zgartirilishini avtomatlashtirish masalasi.

Buning uchun bitta server doirasidagi virtual mashinalarni serverga ulash va bir nechta serverlar orasida ma’lumot uzatilishi uchun qo‘llaniladigan virtual kommutatorlarga quyidagi o‘zgartirishlar kiritilishi kerak:

- kommutatorda yangi virtual portlarni yaratish va kerakmaslarini yo‘qotish, hamda yangi virtual mashinalarni yaratish, kerakmaslarini olib tashlash yoki boshqa serverga migratsiya qilish negizida virtual portlarning konfiguratsiyasini o‘zgartirish;
- ma'lum bir portga tegishli navbatlar konfiguratsiyani o‘zgartirish, yangisini yaratish, eskisini yo‘qotish. Navbatlar tarmoq resurslarini mantiqiy tarmoqlar orasida bo‘linishini ta'minlaydi va yangi mantiqiy tarmoq yaratilishi yoki eskisini yo‘qotilishi oqibatida tarmoq konfiguratsiyasini o‘zgarishini tashkil etadi.
- portlarni guruhlarga birlashtirilishini boshqarish. Portlar guruhi ma’lum bir mantiqiy tarmoq bilan bog‘lanishi mumkin. Kontroller kommutator orasida bog‘lashni sozlash algoritmlarini aniqlaydi, masalan, kontrollerning IP manzili va TCP portlari.

Ushbu masalalarni yechish uchun OF-Config (OpenFlow Management and Configuration Protocol) protokol va boshqa tarmoq protokollaridan foydalanish mumkin. Undan tashqari OVSDB (Open vSwitch Database Management Protocol) protokoli ham ishlatilishi mumkin. OVSDB - virtual kommutatorni konfiguratsiyalash maqsadida ishlatiladigan protokol.

Tarmoqda ma'lumot uzatish jarayonlarini boshqarish

Virtual va jismoniy kommutatorlarning kommutatsiyalash jadvallarini boshqarish uchun OpenFlow protokoli ishlatilishi mumkin. Protokol har xil klassdagi traffik paketlarini qayta ishlash va marshrutlash qoidalarini taqdim etadi. Protkolning oxirgi variantlari mantiqiy portlar ishlatilishini ta’minlaydi, paketlar moslashuvini (inkapsulyatsiyasini) va tunnellar tashkil etish va ular yordamida mantiqiy tarmoqlarda muloqotlarni amalga oshirish imkoniga ega.

Umuman olganda, virtual tarmoqlarni yaratishda ularni dasturiy konfiguratsiyalangan tarmoq asosida tashkil etish katta samara beradi. Chunki dasturiy konfiguratsiyalangan tarmoq nafaqat yuqoridagi ikki muammolarni bartaraf etishda, balki tarmoqni boshqarishda optimal tamoyillardan foydalanish hamda tarmoq samaradorligini oshirishda qurilmani ayni vaqtdagi to‘liq imkoniyatlarini bilgan holda tarmoqda ma’lumotlarni ishonchli uzatishni ta’minlaydi. Bundan tashqari tarmoqni tashkil etishda hamda ma’lumotlarni uzatishda eng samarali yo‘llarni taklif etuvchi tarmoq sifatida ham hozirgi kunda dasturiy konfiguratsiyalangan tarmoqlar eng ideal tarmoq deb qaralmoqda. Bu tarmoqni an’anaviy tarmoqdan eng katta ustunligi - tarmoqni virtuallashtirishdir. Virtuallashtirish yordamida yaratilayotgan tarmoqni barcha elementlarini birgina tarmoqning kontrolleri yordamida konfiguratsiya qilish hamda nazorat qilish mumkin. Bu jarayonni amalga oshirishda OpenFlow protokolidan foydalaniladi va u tarmoq kontrolleri va tarmoq elementlari o‘rtasida virtual kanal hosil qilish, kontroller tomonidan barcha konfiguratsiyalarni yetkazib berishni ta’minlaydi.

TELEKOMMUNIKATSIYA TARMOG‘IDA IP SLA MONITORINGINI O‘TKAZISH ORQALI HIZMAT KO‘RSATISH SIFATINI BAHOLASH

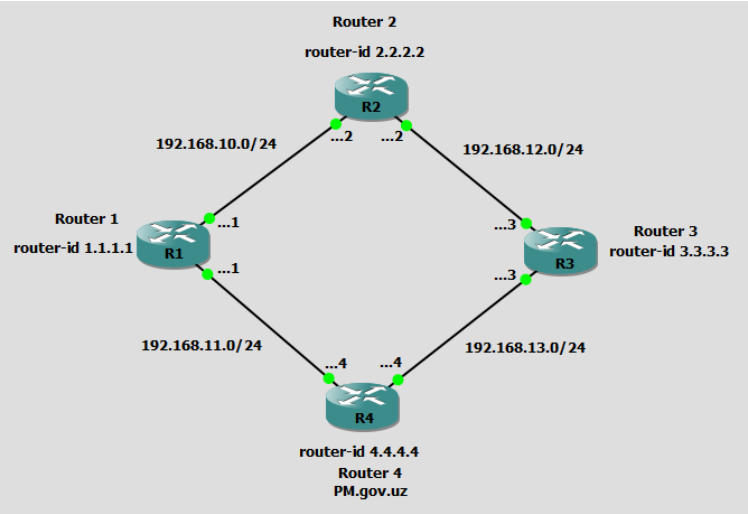
A.A.Qodirov (TATU, assistent)

Hozirgi kunda tarmoqlarni hizmat ko‘rsatish sifati (QoS - Quality of Service) ni monitoring qilishda turli xil yechimlar mavjud. Ammo bu yechimlardan eng optimalini tanlash tarmoqni holatini baholashda va samaradorligini oshirishda muhim o‘rin tutadi.

SLA (Service Level Agreement) – bu hizmat ko‘rsatish darajasidagi shartnoma bo‘lib, u aloqani ta’minlash, ma’lumotni yetkazib berish va hizmat ko‘rsatish sifatini belgilab beruvchi muhim shartnomadir. Bu shartnoma odatda uch xil shaklda namoyon bo‘ladi:

1. Ta’minlovchi va mijoz o‘rtasida (Provider to Customer);
2. Ta’minlovchilar o‘rtasida (Provider to Provider);
3. Mijozlar o‘rtasida (Customer to Customer);

Telekommunikatsiya tarmog‘ida IP SLA monitoringini o‘tkazish orqali hizmat ko‘rsatish sifatini baholash uchun to‘rtta marshrutizatorlardan tashkil topgan tarmoq tanlab olindi (1-rasm). Bu marshrutizatorlar tarmoqdagi to‘rtta turli xil Internet hizmatini ta’minlovchi (Internet Service Provider) larga bog‘lanish uchun hizmat qiladi. Ushbu bog‘lovchi marshrutizatorlarda IP SLA monitoringini GNS3 dasturidan foydalangan holda o‘tkazilib, natijalar olindi:



1-rasm. Turli xil Internet providerlariga ulangan, to‘rtta marshrutizatordan tashkil topgan tarmoq.

Bunda quyidagi monitoring amallari bajarildi:

1. Router 2 nomli marshrutizator qurilmasidan G711 paketlarini *router-id 1.1.1.1* ega bo‘lgan Router 1 nomli marshrutizatorning 16384 porti orqali 160 bayt hajmidagi kodekni 20 ms (millisekund) oralig‘ida doimiy tarzda uzatish orqali ikkita marshrutizatorlarning o‘rtasida hizmat ko‘rsatish sifati (Quality of Service) xarakteristikalari monitoring qilindi.
2. Router 3 nomli marshrutizator qurilmasidan har 9 soniyada doimiy tarzda DNS (Domain name system) so‘rovi router-id 4.4.4.4 ega bo‘lgan Router 4 nomli marshrutizatorga yuborildi va jarayon nazorat qilindi.

Marshrutizatorlar o‘rtasida o‘zaro IP SLA monitoringini o‘tkazish uchun avval barcha marshrutizatorlar konfiguratsiya qilindi hamda marshrutizatsiya protokoli sifatida OSPF (Open Short Path First) protokoli ko‘tarildi.

Konfiguratsiya jarayoni

Router 1:

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 1/0
R1(config-if)#ip address 192.168.11.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback 0
R1(config-if)#ip address 1.1.1.1 255.255.255.255
R1(config-if)#end
R1#configure terminal
```

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.11.0 0.0.0.255 area 0
R1(config-router)#network 1.1.1.1 0.0.0.0 area 0.0.0.0
R1(config-router)#end
R1#configure terminal
R1(config)#ip sla monitor 1
R1(config-sla-monitor)#type jitter dest-ipaddr 2.2.2.2 dest-port 16384  codec g711alaw codec-size 160 codec-interval 20
R1(config-sla-monitor-jitter)#timeout 0
R1(config-sla-monitor-jitter)#frequency 1
R1#configure terminal
R1(config)#ip sla mon schedule 1 start-time now life forever
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip sla monitor respond
R1(config)#ip sla monitor responder
R1(config)#^Z
```

Olingan natija:

```
R1#show ip sla monitor statistics
Round trip time (RTT)   Index 1
        Latest RTT: 1130 ms
Latest operation start time: *00:38:26.095 UTC Fri Mar 3 2017
Latest operation return code: OK
RTT Values
        Number Of RTT: 485
        RTT Min/Avg/Max: 1/1130/5870 ms
Latency one-way time milliseconds
        Number of one-way Samples: 0
        Source to Destination one way Min/Avg/Max: 0/0/0 ms
        Destination to Source one way Min/Avg/Max: 0/0/0 ms
Jitter time milliseconds
        Number of SD Jitter Samples: 480
        Number of DS Jitter Samples: 480
        Source to Destination Jitter Min/Avg/Max: 0/51/5069 ms
        Destination to Source Jitter Min/Avg/Max: 0/18/784 ms
Packet Loss Values
        Loss Source to Destination: 444        Loss Destination to Source: 10
        Out Of Sequence: 0      Tail Drop: 9    Packet Late Arrival: 485
Voice Score Values
        Calculated Planning Impairment Factor (ICPIF): 80
MOS score: 1.41
Number of successes: 3
Number of failures: 5
Operation time to live: Forever
```

Yaratilgan bu model orqali olingan natijadan ko‘rinib turibdiki, IP SLA monitoringi tarmoqdagi har bir qurilmani hizmat ko‘rsatish sifati (Quality of service) parametrlari va xarakteristikalarini baholashi mumkin, jumladan Jitter, paketlar yo‘qolishi qiymatlari va paketlarga hizmat ko‘rsatish davomida kutish vaqti kabilar. Olingan natijalar GNS3 dasturi imkoniyatlari jihatidan kelib chiqqan holda haqiqiy tarmoqdan olinadigan natijalarga deyarli

yaqin hisoblanadi. Shu sababli ushbu natijalarga bemalol tayangan holda, hizmat ko'rsatuvchi providerlar o'rtasida tuziladigan SLA shartnomasini na'munaviy shaklda tuzish hamda tarmoq va uning elementlarini hizmat ko'rsatish sifatini ushbu shartnomada ko'rsatilgan parametrlar asosida doimiy tarzda o'zgarishlarni baholab borish mumkin. Bu baholashlar kelajakda tarmoqda mavjud bo'lgan providerlarni ishlash samaradorligini oshirishda hamda hizmat ko'rsatishga bo'lgan talablarni o'z vaqtida qondirilishga yordam beradi.

ДТS-3100 ТИЗИМНИ УМУМИЙ ТАВСИФИ ВА ТИЗИМНИ БОШҚАРИШ

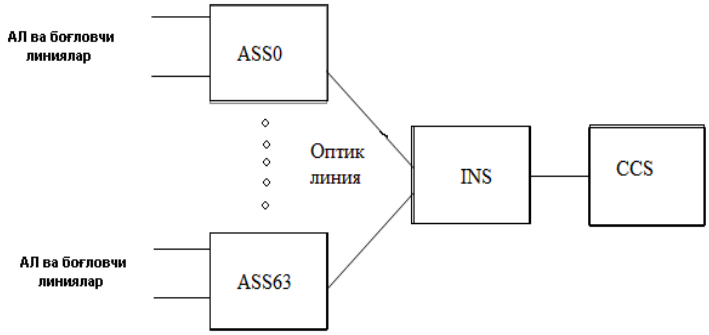
Г.Ю. Қодирова (ТАТУ, ассистент)

ДТS-3100 рақамли коммутация тизими Жанубий Кореяда ишлаб чиқилган. ДТS-3100 тизими ОС, МС, ТС, ШТС ва ШАТС қуришга мўлжалланган. Тизимни бошқаришда марказий ва периферия процессорларидан фойдаланилади. Марказий процессорлар ОМР ва ASP- процессорлари ҳисобланиб улар маълумотларни киритиш ва чиқариш вазифаларини бажаради. Периферия процессорларига INP (Interface Network processor) - маълумотларни тизимлар ўртасида алмашиниш интерфейси процессори, NTP(network transmission processor) - рақамларни тахлиллаш ва узатиш процессори, периферия процессорларига GSP(global service processor), SSP(space switch service processor), NSP(network Synchronization processor). ASP0- 63 (Access Switching Subsystem)тагача марказий процессорлар, периферия процессорларига ASIP(Analog Subscriber interface processor), ASMP(Access Switching processor) ва SP(signaling processor), TLSP(Tine switch Line Service processor) киради ва улардан ҳар хил хизматлар кўрсатишда фойдаланилади.

Марказий процессорлар чақириқларга кўрсатилаётган хизматини назорат қилишда, периферия процессорлари эса алоқа ўрнатишда зарур бўладиган қурилмаларни топишни ва фурилмаларни бошфаришни улар орқали абонентларга мукаммал хизмат кўрсатиш жараёнларни назорат қилиш вазифасини бажаради. ДТS-3100 тизимида улар марказий тизимда ёки қуйи тизимларда жойлашган бўлиши мумкин. ДТS-3100 тизими структурасига кўра 3-та асосий қисмдан ташкил топган. Бу структурага асосан ДТS-3100 тизими қуйидаги қисмлардан иборат:

1. CCS (Central Switching Subsystem) - марказий бошкариш тизими.
2. INS (Interconnection Network Subsystem) - станция қисмлари орасида ўзаро алоқаларни амалга ошириш тизими.
3. ASS (Access Switching Subsystem) - абонент кириш босқичи (бу тизим 0- 63-тагача бўлиши мумкин) тизими.

CCS-(Central Switching Subsystem) марказий бошқариш тизими. CCS- тизимда марказий процессор ОМР жойлашган бўлиб, у тизим ишини назорат қилиши ва керакли маълумотларни ёзиш, ўқиш маълумотларга қайта ишлов бериш, техник хизмат кўрсатиш, тизим холатини статистика қилиш вазифасини бажаради. Маълумотларни киритиш ва чиқаришда махсус портларига уланган CRT –(электрон нурли трубка) қурилмаси ёки ЭХМдан фойдаланилади.



ДТS-3100 тизими структураси

INS (Interconnection Network Subsystem) - станция қисмлари орасида ўзаро алокаларни амалга ошириш тизими. INS-тизими, SWW (Space Switch) (фазовий коммутация) , HIPSU (процессорлараро алоқани таъминловчи), CDL(марказий коммутация блоки), NSS (синхронизация қурилмаси) блокларидан ташкил топган. Марказий коммутация майдони блоки орқали оптик кабелъ билан уланади. Бу қисм INP, NTP марказий процессорлар ва GSP, SSP, NSP, HLIP периферия процессорларидан ташкил топган.

ASS (Access Switching Subsystem) - Абонентлар кириш тизими. ASS-коммутациялашга рухсат берувчи тизим асосан аналог ва рақамли уловчи линияларга хизмат кўрсатиш вазифасини бажаради. Бу тизимда TSW- вақтли коммутатор ва ҳар-хил сигналлар ишлаб беривчи LSI (DTMF,R2MFC,CCT) –қурилмалари вақтли коммутатор билан ташкил топган. Бу қурилмалар хамкорликда ишлайди ва марказий процессор ASP0-63, периферия процессорлари ASIP, ASMP ва SP, TLSP лар ёрдамида бошқарилади. Баъзи бир ASS лар ихтисослаштирилган бўлиши мумкин: файдаланувчилар линиялари учун ASS-S, боғловчи линиялар учун ASS-T, пакетли коммутация учун ASS-P, CCITT №7 умум канал сигналлаш учун ASS-7. Ишлатишни осонлаштириш учун ASS-S ва ASS-T ни боғланган усулда улаш имкони мавжуд.

Ҳар бир ASS ва INS ни ўртасида ўзаро ҳамкорлик юқори тезликдаги оптик-тола линия орқали амалга оширилади. INS ASS лар ва CCS билан ўзаро ҳамкорлик қилади. INS учланган тармоқли синхронлаштирувчи (NEC)га эга, у миллий синхронлаш тармоғига уланган. CCS тизим даражасида хизмат кўрсатиш ва бошқариш функцияларини бажаради. CCS принтерлар, видеотерминаллар, магнит тасмалар ва дисклар кўринишидаги I/O блоклар тизимига эга.

Бошқариш ва техник хизмат кўрсатишнинг фалсафаси бошқариш ишларини мумкин қадар тизимийлаштириш ва автоматлаштириш шунингдек юқори ишончлили тизимни реализациялашдир.

DTS-3100 тизимининг бошқариш ва техник хизмат кўрсатиш ҳарактеристикалар қуйидагилардир:

-тизимнинг юқори ишончлилиги. Юқори ишончлиликнинг ташкил этувчилари, бирлаштирилган дубллашдан фойдаланишда автоматик тизим билан резервлаштириш тизимнинг юқори ишончлилигини таъминлайди;

-бошқариш ва техник хизмат кўрсатишнинг енгиллиги. DTS-3100 тизимининг бошқариш ва техник хизмат кўрсатиши марказий назорат қуйи тизимида концентрацияланганидир. Бу қуйи тизим тестлаш, ўлчаш ва статистика, оммавий хотирани назорат қилиш, тизим даражасида (сатхида) техник хизмат кўрсатишни ва маъмурият ва ташқи звено билан алоқани таъминлайди.

Дисплей блоки орқали одам-машина процессори (ММР) билан боғланган одам-машина интерфейси, хабарларни автоном чиқариш учун кириш ва синтаксис шакли учун менюни танлаш ва шаклни тўлдириш усулини қабул қилади. Шундай қилиб, бошқариш ва техник хизмат кўрсатиш мутахассислар ёрдамисиз техник даражали одам томонидан бажарилиши мумкин

DTS-3100 тизимини бошқариш. Бошқариш маълумотларни қайта ишлаш қуйидаги функциялардан иборат бўлади, масалан, маълумотларни тўплаш, маълумотларни қайта ишлаш, маълумотларни ташқи марказларга юбориш ёки маълумотларни магнит тасмасига ёзиш. Бу операциялар тарификация, ўлчашлар ва тармоқларни бошқаришни қамрайди.

DTS-3100 бошқариш нодир (уникал) ҳарактеристикалари учта асосий функцияларга аниқ ажратилади: маълумотларни тўплаш, маълумотларни қайта ишлаш ва маълумотларни чиқариш. Буни тизим учун бошқаришнинг марказлаштирилган интерфейси таъминлайди. Маълумотларни тўплаш функцияларини ва маълумотларни дастлабки қайта ишлашни коммутацияга (ASS) кириш қуйи тизимида тақсимлаш йўли билан хотирадан самарали фойдаланишга эришилади ва қайта ишлаш реал вақтда бажарилади.

Маълумотларни қайта ишлашни эксплуатациялаш ва техник хизмат кўрсатишнинг процессори бажаради ва маълумотларни киритиш-чиқаришни одам-машинанинг процессори бажаради, иккала процессорлар марказий назорат қуйи тизимига (CCS) киради. Бошқариш CCS ва ASS дан иборатдир. Бошқариш учун ишлаб чиқилган ва ASS таркибида бўлган дастурий таъминот блоки, чақириқлар қайта ишлангандан ва техник хизмат кўрсатилгандан кейин ахборотларни йиғади. CCS даги бошқаришнинг дастурий таъминот блоки ASS даги бошқариш блокидан маълумотларни йиғади, маълумотларни канал орқали қабул қилишни ва узатишни бажаради шунингдек маълумотларни тизим дискларига ва магнит тасмалар блокига ёзади. Одам-машина қуйи тизими (MMS) техник хизмат кўрсатиш ва бошқаришни осонлаштириш учун ишлаб чиқилган. Одам-машина интерфейс кўп турлари ичидан асосий интерфейслари офисдаги ва чиқарилма марказдаги оператор пулътидан таъминланади.

Ушбу мақола мамлакатимиз телекоммуникация соҳасини ривожлантиришда ишлатилаётган тизимларидан DTS-3100 тизими ҳақида маълумотлар келтирилган. DTS-3100 тизимитехник параметрларини ўрганиш, қурилмалар мажмуаси, махаллий, шаҳарлараро, халқаро телекоммуникация тармоқларида ишлаштишда тутган ўрни тўғрисидаги маълумотлар батафсил ёритиб берилган. Ҳамда ушбу тизимда алоқа ўрнатиш тракти жараёнларитушаётган юкламани ҳисоблаш масалалари кўриб чиқилган.

NGN ТАРМОҒИГА ЎТИШДА ТЕЛЕКОММУНИКАЦИЯ ТАРМОГИНИНГ ТЕХНОЛОГИЯСИ, ТОПОЛОГИЯСИ ВА ХИЗМАТЛАРИ

Г.Ю.Қодирова (ТАТУ, ассистенти)

Бугунги кунда NGN тармоғи деганда телекоммуникация хизматларини кўрсатишни таъминлаш имконига эга бўлган ва хизматларни кўрсатиш билан боғлиқ бўлган функциялар транспорт тармоғининг технологиясига боғлиқ бўлмаганда хизмат кўрсатишнинг зарур сифатини таъминлайдиган турли транспортли юқори тезликдаги технологиялардан фойдаланиш учун яроқли бўлган пакетлар технологияси негизидаги телекоммуникация тармоғи тушунилади. NGN фойдаланувчиларни хизматлар билан боғлиқ бўлган функциялар ташишнинг таянч технологиясига боғлиқ бўлмаганда QoS га асосланган ҳолда, жамоа бўлиб кенг полосали тармоқдан фойдаланиш имконига эга хизматлар билан таъминлаш имконига эга тармоқ тузилишининг янги концепциясини ўз ичига олади. Умуман, NGN қуйидаги хусусиятларга эга:

-пакетли коммутацияли технология;

-чақирувларни қайта ишлаш ва иловалархизматларни таъминлаш билан боғлиқ бўлган назорат функцияларга бўлиниши;

-хизматлар, иловалар ва механизмларнинг кенг қаторини таъминлаб туриш, кўрсатиладиган хизматларни берилган QoS сифати билан ва кодлашнинг турли схемаларига нисбатан инвариантлилик билан тўғридан тўғри узатиш билан кенг полосали фойдалана олиш имконияти;

-тармоқлараро алмашинувни таъминлаш ва очиқ интерфейслар ёрдамида ишлаб турган тармоқлар билан ўзаро ишлаш;

-мобил алоқани таъминлаб туриш;

-фойдаланувчиларга хизматларнинг турли провайдерларидан чекланмаган фойдалана олишни тақдим этиш;

-IP тармоқлардаги индентификация схемаларининг турлилиги;

-фойдаланувчилар учун сервис хизматларни унификация қилиш ва уларнинг ташишнинг таянч технологияларга боғлиқ бўлмаслиги.

Тармоқ хавфсизликни ташкил этиш ва рухсат этилмаган тарзда фойдалана олишдан ҳимоя қилишга қўйиладиган талабларни ҳисобга олиши керак.

Ушбу принциплар асосида лойиҳалаштириш асосий мақсад бўлиши керак, ўз навбатида ушбу мақсад даромадларни юзага келтирувчи ва мижозларнинг жорий ва кейинги талабларига жавоб берувчи тармоқларни яратиш имконини берадиган янги авлод –NGN тармоғини режалаштириш ва лойиҳалаштириш методикасини ишлаб чиқишдан иборат бўлади.

NGN тармоғини яратиш учун халқаро нормалар ва стандартларни ҳисобга олганда NGN хизматларни жорий этишни таъминлайдиган норматив базани ишлаб чиқиш зарур. Шунинг учун асосий вазифа бўлиб NGN тармоғига ўтишда тармоқ технологиялари қўлланилишига асосланган ва мувофиқлаштирилган масалаларни белгилайдиган тармоқ норматив базани ишлаб чиқиш ҳисобланади. Қонун ҳужжатлари ва норматив -ҳуқуқий база миллий устуворликларни ҳисобга олган ҳолда телекоммуникация тармоғини ривожлантиришнинг замонавий тенденцияларни ҳисобга олиши керак. Бугунги кунда халқаро даражада NGN тармоғини сандартлаштириш бўйича ишларни амалга оширувчи бир нечта ташкилотлар мавжуд, хусусан:

-Халқаро электралоқа иттифоқи телекоммуникацияни стандартлаштириш сектори (International Telecommunication Union, Telecommunication sector, ITU-T);

-Телекоммуникация соҳасида стандартлаштириш бўйича Европа институти (European Telecommunications Standards Institute, ETSI);

-3G тармоқларни яратиш учун шериклари лойиҳалари (3rd Generation Partnership Project 3GPP и 3GPP2);

-Интернет тармоғини қўллаб-қувватлаш муҳандислик гуруҳи (Internet Engineering Task Force, IETF).

Бугунги кунда NGN тармоқлари учун хизматларнинг умумий таснифи мавжуд эмас. Концепция доирасида NGN хизматларини қуйидагича таснифлаш мумкин:

-иккита охирги терминаллар ўртасида боғланишларни ўрнатишга мўлжалланган таянч хизматлар;

-хизмат кўрсатишнинг қўшимча турлари: имкониятларнинг қўшимча рўйхатини таъминлаб туришга мўлжалланган хизматлар;

-интеллектуал тармоқлар ва маълумотларни узатиш тармоқларининг ресурсларидан фойдалана олишни ташкил этишга мўлжалланган фойдалана олиш хизматлари;

-NGN тузилмасига кирувчи маълумотлар базаларидан ахборотни тақдим этишга мўлжалланган ахборот-маълумотнома хизматлари;

-виртуал хусусий тармоқлар хизматлари;

-NGN томонидан мультимедиа иловаларнинг фаолиятини таъминлаш ва қўллаб-қувватлаш учун мўлжалланган мультимедиа хизматлари.

Юқорида келтирилган тенденциялар асосида NGN тармоқларида кейинги авлод хизматлари (NGS, Next Generation Services) шаклланишини белгилаб ўтиш мумкин. Шунингдек иккита хизматлар тоифаси: паст даражали ва юқори даражалига ажратиш мумкин.

NGN тармоғига ўтишнинг асосий кучли фактори деб фойдаланувчиларни талабларини: терминал қурилмасининг ўзгариши, ҳамда кириш тармоғининг ўзгариши кабиларни ҳисоблаш мумкин;

- NGN тармоғига ўтишнинг қўшимча факторларига, Оператор учун, бир қанча ишлатилаётган қурилмаларнинг улар замондан орқада қолгани ва ёки жисмонан эскиргани туфайли алмаштириш ва янги хизмат турлари бозорида рақобатбардош бўлишига зарурият туғилади ;

- NGS паст даржали хизматлари бир нечта турларга бўлинади: виртуал хусусий тармоқлар VPN хизматлари; контентни тақсимлаш тармоқлари CDN хизматлари;сессия хизматлари;тармоқ иловалари хизматлари масалалари кўриб чиқилган.

ALGORITHM FOR ACCESS NETWORK OPTIMIZATION

D. M. Matkurbonov (TUIT, assistant)
B.I.Rahmanov (TUIT, Student of Master degree of TUIT)

Introduction. The process of optimization of telecommunication network is very important for the creation of a new network or for modification of the resources of an existent network.

The process of network optimization is shown in Fig. 1. The smaller triangle shown in the picture represents the relationship between costs, network resources and quality of the operator network, when it is in the initial stage of operation. The optimization process allows changing the quality of the network when at the same time affecting the costs and resources of network implementation. Although the results obtained in the optimization process often allow to improve the network quality significantly when only insubstantially increasing the costs and resources of the network.

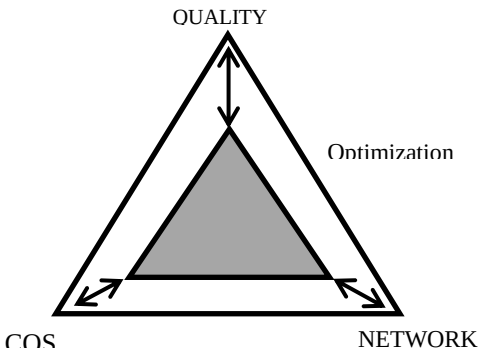


Fig.1. The Effect of Process Optimization

Various methods and programming packages are used for optimization and planning of the network. The supplied methods do optimization according to different criteria of optimization, so they are not universally applicable and can give an optimal solution only in respect to a single criterion. It is possible that when based on a single criterion, say, implementation costs, the result could be optimal regarding the costs but the quality parameters of the network access could be lacking. That's why in practice when solving the tasks of definition of boundary zones and their optimization it is advisable to use several criteria and methodologies. For example having calculated the access ranges according to the minimal costs we could check the technical possibility of user connection by the methods based on the quality criteria.

This optimization task is solved by the aid of the elements of mathematical and telecommunication network optimization :

- multipara metric optimization;
- methodologies of minimal costs and network characteristic's (quality) evaluation.

Currently available methods for calculation of access network optimization are applicable for the search of optimal solutions only by one chosen criterion or a parameter, so using them in solving the tasks of cost and quality becomes rather problematic. The refore we suggest using combined access optimization methods which are obtained combining the methods of minimal costs, quality and multi parametric optimization.

The algorithm for access network optimization is produced using and combining methods of minimal costs and boundary definition by quality parameters. We introduce a multipara metric optimization condition into the goal function i.e. we define n variables, according to which the optimization of access network will be carried out. In this case the access network cost minimization goal function is expressed in the following relationship:

$$C_{min} = f(A,T), \qquad A\epsilon\boldsymbol{A}, T\epsilon\boldsymbol{T}$$

$$A = (B,L), T = (M,R,H,V,W,G) \quad (1)$$

where: C– network implementation costs; A – variables of the access network boundary: B – size of the grid element (area), km^2 ; L– size (area) of boundary zone, km^2 ; T – variables used in the network access technology: M – type of channel/transmission media; R – the speed for the data transmission, kbps; H – discipline for the data package service; V – channel access method; W – type of modulation; G – type of codec. In the expression (1) the variable sets are defined as follows:

$$A = B * L \text{ and } T = M * R * H * V * W * G \qquad (2)$$

We will formulate the optimization task: let's have a function $C = f(A,T)$ and conditions, which are defined by the unknown (A, T), we have to find the values of variables (A*, T*), under which the value of function becomes minimal, i.e. $C_{min} = f(A,T)$. N – dimensional point $C_{ls} = f(A,T)$, that satisfies the boundary system:

$$\begin{aligned} Q_{1\,min} &\le Q_1 \le Q_{1\,max} \\ Q_{2\,min} &\le Q_2 \le Q_{2\,max} \\ Q_{3\,min} &\le Q_3 \le Q_{3\,max} \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ Q_{r\,min} &\le Q_r \le Q_{r\,max} \end{aligned} \qquad (3)$$

we will call permissible solution. Here Q_1 , Q_2 ,..Q_r the r-th quality indicator (factor): Q_{1min} , Q_{2min} ,..Q_{rmin}, Q_{1max} , Q_{2max} ,..$Q_{r\,max}$ – the minimal/maximal value for the r-th quality factor.

Since the quality indicator can be limited from the bottom as well as from the top by the values of Q_{imin} , Q_{imax}, besides their values can be the same as the extreme values of the quality norms, so the restrictions (3) are introduced not with strict equations.

In case the set of permissible (allowed) solutions is not empty, we come to the search of the optimal solution. For the function $C = f(A,T)$ an optimal solution will be a point, for which the variable values belong to the set of permissible solutions and the value of C function is minimal:

$$C_{min} = f(A^*, T^*) = \min \qquad (4)$$

We will build a block diagram for the optimization stages (Fig. 2).

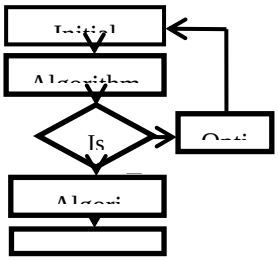


Fig.2. Block diagram of the optimization stages

Conclusions.

There was developed multiparametric access network optimization method with following advantages:

- it allows to perform access network optimization with minimum expenses and at the same time ensures set quality level, according r – number of quality rates;
- access network quality description indexes in model are optional and that allows optimizing access networks with different purpose, oriented to voice, data and other communication services;
- method is for network accesses based on wire, xDSL, fiber optic and radio technologies;
- method can be used to solve some other optimization problem with discrete variables and can be settled in conformity with their influence on objective function and restrictions.

АБОНЕНТ ФОЙДАЛАНА ОЛИШ ТАРМОҚЛАРИДА ОПТИМАЛЛАШТИРИШ МАСАЛАЛАРИ

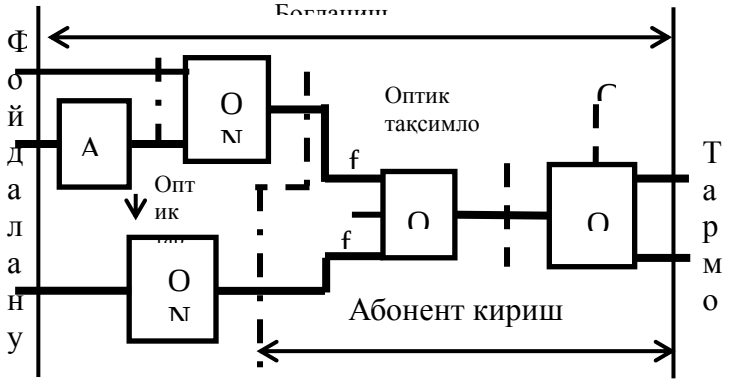
Д.М.Матқурбонов (ТАТУ, ассистент)

Алоқа сохасида асосий талаб ҳар кандай фойдаланадиган тармоқ юкори ўтказувчанлик қобилятига эга бўлиши, турли хизматларни ўз ичига олиши ва уларни вақтида амалга оширилиши, узатиладиган ахборотларни сифатини кафолатланиши, фойдаланадиган тармоқни ишончлилиги, ҳамда хавфсизлик масалалари билан баҳоланади.

Ҳозирги кунда юқорида келтирилган талабларни қондириш мақсадида асосий эътиборни абонент фойдалана оладиган тармоқ тузилишини оптималлаштириш масалаларига қаратилмоқда.

Ушбу мақолада абонент фойдалана олиш тармоғининг тузилиш характеристикалари, тугун кўрсаткичларини оптимал даражада танлаш хамда сарф - харажатларини камайтириш масалаларига қаратилган.

Тадқиқот қилинувчи объектнинг физик структураси 1.1–расмда келтирилган.



1.1–расм. Абонент фойдалана олиш тармоғининг тузилиши:
(OLT (Optical Line Termination- Оптик линия терминали) Optical Network Unit (ONU); Adaptation Unit (AU))

Тармоқ тузилишини кўп вариантларда амалга ошириш имкони мавжуд бўлган ҳолда тармоғининг ўзига хос хусусиятлари ва асосий технологиясини танлашдан келиб чиқиб ўзгартириш ёки кенгайтириш мумкин.

Абонент фойдалана олувчи тармоғини оптималлаштириш масалалари қуйидагиларни эътиборга олган ҳолда амалга оширилади:

а) Тармоқ участкасининг эгаллаган майдонида OLT ва ONU қурилмаларининг жойлашув ўрни;

- ушбу ҳолатда тугунлар орасидаги масофа //C// масофалар матрицаси оркали ифодаланади:

$$|C| = \begin{vmatrix} \infty & C_{12} & & \cdots\cdots & C_{1j} \\ C_{21} & \infty & C_{23} & \cdots\cdots & C_{2j} \\ C_{i1} & C_{i2} & & \cdots\cdots & \infty \end{vmatrix}$$

б) Абонент фойдалана олиш тармоғининг структура векторини f(x) аниқлаш; ушбу ҳолатда максад функцияси аниқланади ва унинг қиймати минималлаштирилади:

$$\Pi(f) \to \min; \qquad (1.1)$$

бу ерда: f ∈ F-тармоғи структурасининг рухсат этилган вариантлар тўплами, чекланмалар аниқланади.

в) Тармоқнинг барча қуйи поғона тугунлари ўртасидаги рухсат этилган линия узунлиги, кабелларни ётқизиш трассаси, тугунларни ҳудудга боғлашни ҳисобга олган ҳолда мумкин бўлган топологик тузилмалари қуйидагиларни ўз ичига олади:

- турли хилдаги ONT ва ONU дан фойдаланган холда регенерация участкалари узунлигининг рухсат этилган киймати:

$$l_{ij} < L; \quad (1.2)$$

бу ерда: l_{ij} - i ва j тугунлари ўртасидаги линия участкаси узунлиги;

- L-тақсимланган тармоқ линиясининг рухсат этилган максимал узунлиги;

- худудий тармоқ инфрастуктураси тармоқнинг келажакдаги эволюциясига бардошлилиги;

г) тармоқни қуриб яратишда тармоқнинг балансланганлиги этиборга олинганлиги; ушбу холатда тармоқлагичнинг тақсимланиш коэффициенти тармоқнинг оптик радиусининг барча холатларида минималлаштирилган холатда бўлишлиги:

$$r_{\text{тармоқ}} = max\,(FL) \quad (1.3)$$

бу ерда: бутун оптик йўл бўйлаб йўқотишлар бир хил бўлган тармоқ $FL_i = FL_j$ барча i ва j абонент тугунлари учун тушинилади ҳамда кейинчалик кенгайишларни ҳисобга олган ҳолда максимал ўзгаришга эга бўлиши ва у оптимал бўлиши зарур.

$$P_{out} = \sum_n P_{n,out} \quad (1.4)$$

бу ерда: p ва P тармоқнинг энергетик потенциалини ёки оптик қувватни англатади ва ифодага мос равишда дБм ва мВт ўлчов бирликларида ўлчанади.

Юқорида келтирилган функцияларни ҳисоблашда эхтимоллар назарияси ва тармоқ тузилишини хисоблашда графлар усули хамда компонентларнинг f векторининг дискретлик хусусияти билан боғлиқ қийматлар соҳаси ушбу масалада кўп турдаги натурал қаторлар оркали амалга оширилади.

Юқоридаги келтирилган шартларни ҳисобга олган ҳолда танланган абонент фойдалана олиш тармоқларида сарф-харажатлар функцияси қуйидагича:

$$\Pi_{(f)} = E_н[C_{(i)} + a_{(i)}(N-1) + b_{(jl)} + V_{(i)}] + Э \quad (1.5)$$

бу ерда: $C_{(i)}$- OLT қурилмасининг нархи ;

$a_{(i)}$- ONU қурилмасининг нархи ;

$b_{(jl)}$-линия қурилмасининг нархи;

$E_н$ - 0,15 алоқа курилмаларига мувофик норматив коэффициент;

$V_{(i)}$ -тизимнинг техник хизмат кўрсатиш нархи;

N – тармоқдаги тугунлар сони;

Э- эксплуатация харажатлари

Қабул қилинган таклиф ва фаразлар:

- Тармоқнинг техник эксплуатация тизимини танлашда кўп вариантли бўлишлилиги;

- OLT ва ONU ёки бошқа танланган тармоқ қурилмалар типини танлашда кўп вариантли бўлишлилиги;

- тармоқ тузилишида ҳалкасимон, юлдузсимон, дарахтсимон топологияси бўйича ёки бошқа принципларда амалга оширилиши;

- линия иншоатлари ва станция қурилмаларининг ишончлилик кўрсаткичи юқори бўлишлилиги;

- қурилмаларнинг барча блоклари назорат тизимига олинган, рад этишларни аниқлаш, авария тўғрисидаги маълумотни тагдим этиш ва тармокнинг ишлаш қобилиятини тиклашда ходимларнинг хизмат кўрсатиш даражалари эътиборга олинган ҳолда амалга оширилади.

Абонент фойдалана олиш тармоғининг бошка вариантларини амалга оширишда бошқа таклифларни қабул қилиши мумкин, аммо мақсад функциясининг (1.1) кўриниши ва параметрлари ўзгармасдан қолади, шундай қилиб тармоқнинг структурасини шакиллантирилаётганда оптимизация масаласига умумий ёндашув хам ўзгармас қолади.

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ IPTV

М.М. Махаммадиев (ТУИТ, 2-курс магистрант)
Н.М. Холматов (ТУИТ 2-курс магистрант)

Рассматривается проблема повышения эффективности предоставления услуги IPTV за счет использования технологии WiMAX. Использование беспроводных технологий позволяет предоставлять услугу не только фиксированным, но и мобильным абонентам. Передача трафика IPTV связана с дополнительными накладными расходами. Кроме того, технология WiMAX

добавляет при передаче трафика свои накладные расходы. Представлены способы снижения накладных расходов при реализации услуги.

Internet Protocol Television (IPTV) становится все более популярным, т. к. позволяет доставить контент пользователям в то время, когда они этого захотят [1]. Следующим шагом является предоставление данного контента в любом месте – там, где это нужно пользователям. Традиционные проводные сети доступа могут предоставить контент только в фиксированных точках. Таким образом, требуется новая технология, которая может доставлять контент подвижным абонентам.

Технология Worldwide Interoperability for Microwave Access (WiMAX), основанная на стандартах IEEE 802.16-2004 и 802.16e-2005, предназначена для организации фиксированного и мобильного беспроводного доступа к городским сетям передачи данных со скоростью до 70 Мбит/с, способна покрывать расстояния свыше 30 км и обеспечивает безопасную доставку контента.

Канальный уровень модели WiMAX поддерживает приоритетное предоставление канала в реальном времени (rtPS), что обеспечивает требуемую полосу пропускания и минимальные задержки для видеоуслуг с поддержкой качества обслуживания (QoS).

В WiMAX используется ортогональное частотное разделение каналов с мультиплексированием (OFDM) и технология OFDMA на физическом уровне, которые устойчивы к затуханиям.

Технология OFDMA принята в качестве предпочтительного решения для стандарта IEEE 802.16a на сетевые средства беспроводного широкополосного доступа, позволяющего операторам предоставлять разнообразные услуги передачи голоса и данных. Кроме того, WiMAX использует адаптивные схемы модуляции и систему исправления ошибок методом упреждения (Forward Error Correction, FEC) для повышения качества сервиса [2].

Поскольку на физическом уровне WiMAX поддерживает различные размеры фреймов и масштабируемую полосу пропускания, данная технология является идеальным выбором для приложений IPTV. На базе WiMAX могут быть построены сети доступа, кроме того, можетбыть реализован принцип прозрачности для опорных сетей. Таким образом, базовые станции WiMAX, абонентские и мобильные станции идеально подходят для доставки IP-услуг (Triple Play): VoIP, IPTV, Интернет-мультимедиа по беспроводным сетям уровня города. Это делает технологию WiMAX лучшим выбором по сравнению с обычным кабелем, технологией DSL и спутниковыми решениями.

Сети доступа на основе WiMAX позволяют предложить повсеместную доставку контента, кроме того, развертывание сетей WiMAX позволит предоставить полный спектр услуг IPTV с высокой степенью качества видео и аудио в сельских и труднодоступных для проводных технологий районах.

Функциональная блок-схема организации услуги IPTV проиллюстрирована на рис. 1.

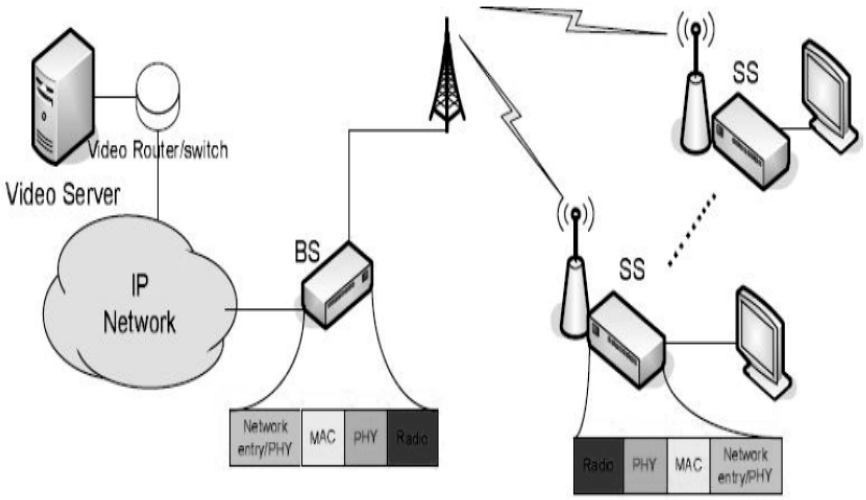


Рис. 1. Модель предоставления IPTV

Передача трафика IPTV ведет к значительному увеличению полезной нагрузки и, следовательно, ставит сложную задачу в обеспечении качественного сервиса. Протоколы UDP, TCP и IP с соответствующими накладными расходами являются частью полезной нагрузки WiMAX.

Кроме того, физический и канальный уровни протокола IEEE 802.16 добавляют свои накладные расходы. Таким образом, необходимо найти методы и выработать рекомендации по снижению вышеупомянутых накладных расходов.

Используемые для предоставления услуг IPTV базовые станции, как и абонентские станции, должны обеспечивать систему доставки типа точка-многоточка для приложений IPTV, которая соответствует стандартам и сертификатам IEEE WiMAX. При этом может быть передан трафик IPTV как стандартной, так и высокой четкости.

Для предоставления услуг потокового видео используются порты UDP, а для услуги «Видео по запросу» – TCP-порты. Поддерживается также одноадресная, многоадресная и широковещательная трансляция. В результате возможно появление нескольких пакетов из различных источников, которые должны быть доставлены заданным пользователям с различными параметрами качества обслуживания. Данная проблема решается на канальном уровне базовых станций WiMAX путем эффективного планирования услуг. По этой причине ожидается, что именно реализация такого планирования на канальном уровне будет ключевым фактором среди конкурирующих продуктов.

Услуга IPTV, которая требует высокой производительности, находится под значительным влиянием этих накладных расходов. Хотя UDP- и TCP-заголовки, а также IP-заголовки остаются в пределах полезной нагрузки и не могут быть доступны в рамках системы WiMAX, накладные расходы, созданные WiMAX, могут быть значительно снижены за счет использования методов подавления заголовка (PHS) и сжатия заголовка (ROHC). Системы WiMAX требуют высокой производительности радиотрансиверов. Основными особенностями приемопередатчиков WiMAX являются: высокий динамический диапазон, низкий уровень фазового шума, высокая стабильность, низкий уровень шума и высокая линейность.

Устройства, которые используются в качестве трансиверов, должны иметь высокий динамический диапазон, свободный от паразитных составляющих, который является одним из важнейших параметров для IPTV. Например, АЦП и ЦАП обеспечивают обычно 86 дБн и 78 дБн соответственно. Кроме того, фазовый шум является еще одной важной характеристикой радиопередатчика, которая может повлиять на качество услуг IPTV.

Низкий уровень шума является еще одним важным критерием производительности для достижения высокого качества услуг IPTV. Компоненты, которые используются в системах, предназначенных для предоставления услуг WiMAX, должны иметь высокое отношение сигнал/шум. Подавление внеполосных сигналов является важным параметром производительности мобильных радиостанций, особенно для услуг IPTV. Это может быть достигнуто за счет подавления гармоник с использованием двухступенчатого преобразования, а также высокопроизводительными фильтрами поверхностных акустических волн.

Таким образом, за счет оптимального использования беспроводных технологий возможно увеличить эффективность предоставления услуги IPTV оператора связи, что позволит добиться повышения конкурентоспособности путем предоставления услуги не только в фиксированной точке, но и в любом месте, находящимся в зоне охвата оператора.

ДАСТУРИЙ КОНФИГУРАЦИЯЛАНАДИГАН ТАРМОҚДА ТАРМОҚ ОҚИМИНИ ЭКСПЕРТ НЕЙРОН ТАРМОҒИ АСОСИДА БОШҚАРИШ

С.О. Махмудов (ТАТУ, катта илмий ходим изланувчи)

Маълумот узатиш тармоғини бугунги кундаги замонавий ҳолати ва ривожланиш тенденция билан тармоқни ишлаш самарадорлиги, ўтказиш қобилятини потенциал равишда ошириш имконини бермайди. Бу ҳолат маршрутлашга кўп вақтни сарфланиши, тармоқни конфигурациялаш ва оқимни бошқаришни қийинлиги, юқори тезликли глобал тармоқда янги хизмат кўрсатиш сифат даражасини зарурлиги ва ресурсларни етишмаслиги билан чамбарчас боғланиб кетган. Ҳозирги кунда ушбу муаммоларни бартараф этишни самарали усули сифатида кўп бора таъкидланаётган дастурий конфигурацияланадиган тармоқ (SDN – software-defined network) технологияси қўл келади.

SDN – бу маълумот узатиш тармоғини қуришга янгича ёндашув бўлиб, тармоқни бошқариш поғонаси (ТБП) маълумот узатиш поғонаси (МУП) дан бошқариш функцияси алоҳида контроллер деб аталувчи қурилмага ўтказилиши ҳисобидан ажратилади. Бундай ажратиш ҳисобига тармоқни бошқариш ва тармоқ ҳолатини назорат қилиш контроллерда мантиқий марказлаштирилган ва шу орқали маълумот узатиш физик поғонасини абстракциялаш имконияти киритилган. ТБП ва МУП ўзаро боғланиши учун ягона унификацияланган очиқ интерфейс яратилган.

SDN тармоғи бир нечта афзаллик ва имкониятларга эга бўлиш билан бир қаторда камчиликларга ҳам эга:

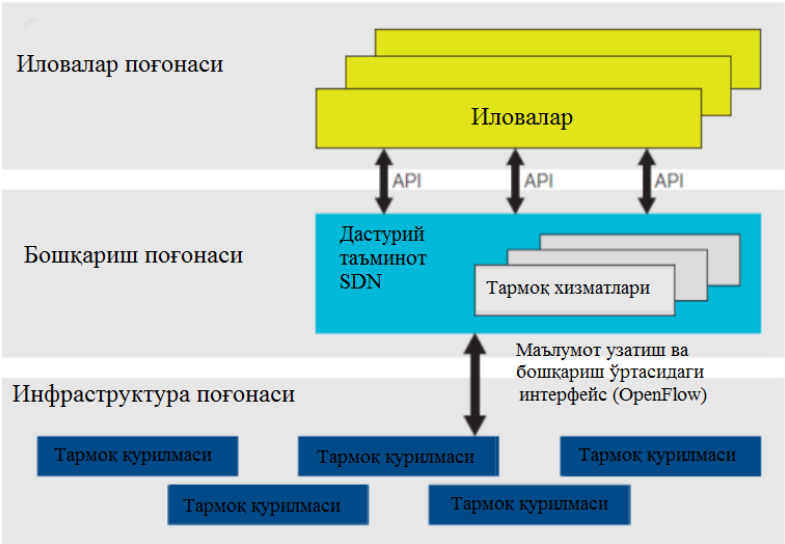
- Ишончлилик: контроллер тармоқдаги асосий ишдан чиқиш нуқтаси ҳисобланади;
- Кенгайтириш муаммоси:

1. Бошқарувчи трафик ҳажми тармоқдаги коммутаторлар сонига пропорционал равишда ошади;
2. Янги оқимни ўрнатиш вақти тармоқ ҳажмини кенгайиши билан ортади;

- Самарадорлик муаммоси: тармоқ самарадорлиги тўғридан-тўғри контроллер самарадорлигига боғлиқ.

SDN тармоғида коммутаторларга қоидалар кириш ва шу орқали маълумотлар оқимини маршрутлашнинг иккита ёндашуви мавжуд:

- Реактив ёндашув – янги оқимни ўрнатиш сўровида контроллер битта қоида ишлаб чиқади ва уни коммутаторга ёзади.
- Проактив ёндашув – янги оқимни ўрнатиш сўровида контроллер оқим учун маршрут ҳисоблайди ва ушбу маршрут бўйича барча коммутаторга мос қоидани ўрнатади.



1-расм. Дастурий конфигурацияланадиган тармоқ архитектураси.

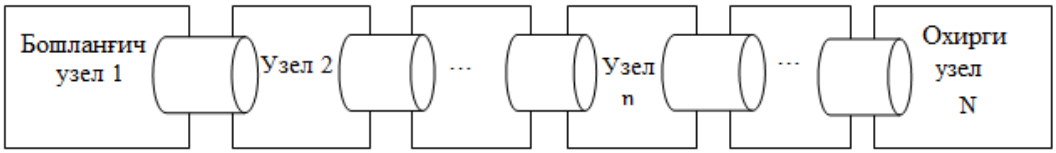
Юқоридаги келтирилган фикрларга кўра таклиф қилинаётган SDN технологиясини ҳам муаммолардан ҳоли деб бўлмайди, сабаби технология ҳали янги уни барча қирралари тўлиқ ишлаб чиқилмаган. SDN тармоғида маршрутлашни амалга ошириш ва трафикни бошқаришда эксперт нейрон тармоғини қўллаш яхши самара беради. Нейрон тармоғи ўзини-ўзи бошқарувчи тизим бўлиб, қадамма-қадам қарор қабул қилиш даражаси оишб боради ва тармоқдаги оқимни тақсимлаш ва канал юкланишини баланслаштиришга ёрдам беради.

Ишдан мақсад SDN тармоғида контроллерга маршрутлаш функциясини бажаришда кўмаклашувчи ўзини-ўзи бошқарувчи тизим нейрон тармоғини ташкил қилишдан иборат. Ишдаги янгилик реал вақтда тармоқ ўтказувчанлигини тақсимлаш ва синфлаш учун тармоқ оқимини таркибини ва ахборот турини аниқлашдан иборат

Техника ва илмий йўналишда сунъий нейрон тармоқ ва нейротармоқ модели аппарат ва назарияси жонли равишда ривожланиб бормоқда. Уларнинг асосий афзаллиги қийин масаларни ечишда қўлланилишидир. Телекомуникация соҳасида улар қуйидаги мухим масалаларда қўлланилади: коммутацияни бошқариш, адавтип маршрутизация, телекоммуникация тармоқлариди трафикни бошқариш, каналларни оптимал тақсимлаш ва бошқа йўналишлар.

Контороллердаги API функцияси орқали нейротармоқ модел киришига фойдаланувчи сўрови киритилади. Сўровлар сонига қараб гексагонал панжара – уларни талаб, имтиёзларига қараб нейронларни шартли тақсимловчи шакллантирилади. Контроллер ва коммутатор ўртасидаги химояланган канал орқали амалга оширилади. Биринчи пакет тузилишига кўра коммутаторларга қоида ёзилади ва шу орқали коммутаторларда туннел ҳосил қилиниб оқим йўналтирилади. Бу ҳолатни математик жиҳатдан оммавий хизмат кўрсатиш тизими ва тармоғи деб олиш мумкин(2-расм).

SDN тармоғида узатувчи ва қабул қилувчи ўртасида бир нечта маршрут йўналиши аниқланади ва улар ўртаси оқим жадаллиги тақсимланиши зарур ва шу ўринда трафикларни турли хил бўлишини ҳам ҳисобга олиб канал ресерслари ҳам тақсимлани зарур бўлади.



2-расм. SDN тармоғида туннеллаштириш ҳолати модели.

SDN тармоғини мустақил ўрганувчи нейрон тармоғи асосида моделлаштирамиз. Нейрон тармоғи ёрдамида маршрутизация масаласи ечилади. Маршрутизация турли йўналишдаги телекоммуникация тармоқлари учун энг муҳим функция ҳисобланади. Асосий вазифамиз белгиланган тизимда маршутни танлашдан иборат, лекин бу вазифани бажаришда тармоқда қурилмалар сони кўпайиши, тармоқ ҳуддуди кенгайишни бошласа аниқ-оптимал танлов даражаси пасаяди. Шунинг учун турли эвристик алгоритм ва жараёнда нейротармоқ модели қўлланилади. Буни натижасида маршрутни танлашга кетадиган вақтни каммйтиришга эришамиз. Нейротармоқ моделини яратишда кўп бора қўлланиладиган Хопфилд нейротармоқ моделидан фойдаланамиз.

Масалани ечиш учун бизга мавжуд тармоқ графи, бир жуфт охирги қурилмалар (ET), яъни узатувчи ва қабул қилувчилар, улар ўртасидаги алоқа линиялари маълум. Энди Хопфилд моделини бир нечта тармоқ линиялари орасида (NL) маршрутни аниқлашда қўллаймиз. Нейронлардаги чиқиш кучланишлари минимал қувватга эга бўлиши тармоқдаги тенглик ҳолатини англатади. і ва j нейронлар ўртасидаги боғланиш $T_{i,j}$ оғирликни англатади. Нейротармоқ моделида ET охирги қурилмалар ўртасидаги ҳар бир маршрут битта нейрон ҳолати билан белгиланади. ij нейрон охирги қурилмалар і ва j орасидаги маршрутни билдиради. Шунга кўра Хопфилд формуласини қуйидаги кўринишда ёзишимиз мумкин:

$$E = -\frac{1}{2}\sum_{i=1}^{N_{ET}}\sum_{k=1}^{N_{ET}}\sum_{j=1}^{N_r(i)}\sum_{i=1}^{N_r(k)} T_{ij,kl}V_{ij}V_{kl} - \sum_{i=1}^{N_{ET}}\sum_{j=1}^{N_r(i)} I_{ij}V_{ij} \qquad (5)$$

бу ерда, $T_{ij,kl}$ *ij* ва *кl* нейронлари ўртасидаги оғирлик;

I_{ij}- *ij* нейрондаги қўзғалиш токи; $N_r(i)$ – маршрутлар сони;

N - нейронлар сони: $\sum_{i=1}^{N_{ET}} N_r(i)$.

Хулоса сифатида шуни айтиш мумкинки, нейротармоқ моделини тўлиқ ҳолатда ишлаб чиқиш ва уни SDN тармоғида қўллаш жараёнини илмий иш йўналиш деб белгилаб оламиз. Модел таҳлили қилиб, нейротармоқ моделини патентлаштирамиз.

ТАРМОҚНИ БОШҚАРИШ МАСАЛАЛАРИДА МАВҲУМ ТЎПЛАМ ВА МАНТИҚНИ ҚЎЛЛАШНИ АҲАМИЯТИ

С.О. Махмудов (ТАТУ, катта илмий ходим изланувчи)

Ҳозирги кунда инфокоммуникация технологиялари ривожланаётган бир пайтда у билан биргаликда бутун бир тармоқдаги ахборотлар оқими ҳажми ҳам жадал равишда ўсиб бормоқда. Бу эса тармоқдаги мавжуд тизимларга катта юкламалар беради. Шу туфайли тармоқ ресурслари борасидаги муаммоларни келтириб чиқаради. Ушбу муаммоларни бартараф этишда иккита усул мавжуд:тармоқ ресурсларини сонини ошириш; оммавий хизмат кўрсатиш тизимларини самарали бошқариш.

Айтиб ўтилган усуллардан иккинчиси энг яхши усул ҳисобланади, сабаби бу усулда тармоқ ресурслари, моддий манбалар тежалади; ортиқча ресурсларни бўш қолиши кузатилмайди. Оммавий хизмат кўрсатиш тизимларини самарали бошқариш усулини ташкиллаштиришда иккита бир-бирига боғлиқ бўлган тартиб-қоидалардан фойдаланилади:хотирани бошқариш; хизмат кўрсатиш.

Буферга келиб тушаётган талабларни бошқаришда хотирани башқариш тартиб-қоидаларидан ташқари мавҳум тизимлар орқали бошқариш мумкин. Мавҳум тизимни ташкил этишда мавҳум тўплам, мавҳум хулосалар фойдаланилади. Мавҳум хулосалар ўзида мавҳум тўпламларни бирлаштириди ва 6 та кетма-келикдаги операциялар бажарилади:қоидалар базасини ҳосил қилиш; фаззификация; бирлаштириш; активлаштириш; аккумуляция; дефаззификация.

Мавҳум тизимли моделни яратишда мавҳум тўплам тушунчасини аниқроқ ёритиб беришни талаб этади, яъни бериладиган жавоблар бир хил бўлиб қолмаслиги зарур.

Мавҳум тўпламни яратишни бир неча хил тартиблари мавжуд ва улар бир-биридан аниқлаб келадиган тавсилотлари бўйича фарқланади.

Мавҳум тўплам *A* аслида тартиблаштирилган жуфтликлардан ташкил топган тўпламдир. Жуфтликлар қуйидаги кўринишда ташкил этилади:

$$<x, \mu_A(x)> \text{ ёки } \mu_A: X \rightarrow [0,1] \qquad (1.1)$$

бу ерда x – унверсал тўплам ёки X универсамнинг элементи;

$\mu_A(x)$ – $x \in X$ эканлигини кўрсатувчи ва [0,1] интервалга тегишлилигини кўрсатувчи тегишлилик функцияси.

Шунга кўра *A* мавҳум тўпламни қуйидаги кўринишда келтиришимиз мумкин:

$$A=\{< x_1, \mu_A(x_1)>, < x_2, \mu_A(x_2)>, < x_3, \mu_A(x_3)>,..., < x_n, \mu_A(x_n)>\},$$

$$\text{ёки умумий ҳолда } A=\{< x, \mu_A(x)> \} \qquad (1.2)$$

Барча мавҳум тўпламда иккита ҳодисани белгилаб кўрсатишимиз мумкин, яъни ўзининг классик аналогига мос тушади ва бошқа мавҳум тушунчаларни агиқлашда қўлланилади.

Қуйидаги кўрсатилган кўришдаги фикрларни мавҳум лингвистик фикрлар деб аталади:

1. “β да α” фикр, бу ерда β – лингвистик ўзгарувчини номи, α – эса унинг қиймати, қайсики Т атама-тўпламдаги β лингвистик ўзгарувчига мос келувчи алоҳида келтирилган лингвистик атамаларга.
2. “β да ∇α” фикр, бу ерда ∇ - модификатор, мана бундай сўзларга ўхшаш: “жуда”, “кўп ёки кам”, “жуда хам кўп” ва бошқалар.
3. Таркибли фикр, бунда 1 ва 2 кўринишдаги фикрлар мантиқий амаллар “ёки”, “ва”, “унда” , “инкор”.

Юқоридагиларга кўра, мавҳум махсулотли қоидалар ёки мавҳум махсулотни қуйидагича кўринишда бериш мумкин:

$$\text{(i): } Q; P; A \rightarrow B; S,F,N, \qquad (1.3)$$

Мавҳум хулосали тизимда жуда кўп ишлатиладиган мавҳум махсулотли қоидаларни оддий холатда қуйидагича келтириш мумкин:

$$\text{ҚОИДА <\#> : АГАР “ } \beta_1 \text{ да } \alpha\text{` ”, унда “ } \beta_2 \text{ да } \alpha\text{``”.} \qquad (1.4)$$

Бу ерда “ β_1 да α` ” мавҳум фикр ўзида мавҳум махсулотли қоидани, “ $\beta_1$ да α` ” мавҳум фикрэса ўзида ўша қоидани мавҳум хулосасини намайиш этади, лекин $\beta_1 \neq \beta_2$.

Мавҳум тўплам ва мавҳум мантиқ ҳақида сўз борганда техник қурилмалар ва жараёнларни бошқаришда кенг қўлланиладиган мавҳум хулосали тизим ҳақидаги тушунчаларга дуч келасиз. Мавҳум хулосали тизимни шакллантириш ва қўллашда биз бир нечта босқичли функцияни бажаришни талаб этади. Бу босқичлар ҳақида қуйида батафсил тўхталиб ўтамиз.

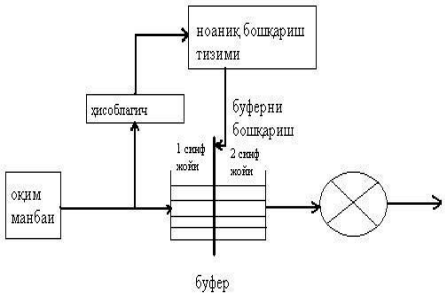
Мавҳум хулосали тизимни киришига келиб тушадиган ахборот кирувчи ўзгарувчини ўлчашлар орқали олинади. Бу ўзгарувчилар бошқарилаётган жараённинг ҳақиқий ўзгарувчисига мос келади. Мавҳум хулосали тизим чиқишидаги шакллантириладиган ўзгарувчи ахборот бошқарилаётган жараённи бошқарувчи ўзгарувчи ҳисобланади.

Операциялар маълум тартибдаги алгоритмлар асосида вужудга келтирилади. Бир нечта алгоритмлар мавжуд: Мамдани, Сугено алгоритмлари. Алгоритмлар операцияларни ташкиллаштириш усуллари билан фарқланади, аммо бир хил натижага эришади.Айтиб ўтилган операциялар кетма-кетлигига амал қилган ҳолда қўйилган масалани ечамиз.

Масала: Оммавий хизмат кўрсатиш тизимига келиб тушаётган талабларни буферга жойлаштиришдан иборат. Жойлаштириш ҳолатини кўрсатиб беришда 2 та турли приоритетли талаблар келиб тушаётган бўлсин. Уларга буферни тенг иккига бўлиш усули билан жой ажратилган. Ҳар бир талаб ўзини белгиланган жойга тушади. Келиб тушаётган талабларни жадаллигига қараб буфердаги жолар кенглигини ўзгартириб турилади. Қўйилган масалани ечиш учун 1-расмдаги схемадан фойдаланамиз. Операцияларни бажариш учун қоидалар базасини ҳосил қиламиз, бунда кирувчи ўзгарувчи сифатида

“оқим жадаллиги”, чиқувчи ўзгарувчи сифатида “буферни бошқариш” параметрларини киритамиз.

Моделда оқимни 2 хил даражадаги синф талаблари ташкил қилади:



Расм-1. Буферни бошқарувчи мавҳум тизим архитектураси.

ҚОИДА-1: АГАР 1 синф-қуйи ва 2 синф-қуйи, унда буфер сатҳи ўзгармасин
ҚОИДА-2: АГАР 1 синф-ўрта ва 2 синф-ўрта,бунда буфер сатҳи ўзгармасин
ҚОИДА-3: АГАР 1 синф-ўрта ва 2 синф-қуйи, унда буфер сатҳи ўзгармасин
ҚОИДА-4: АГАР 1 синф-юқори ва 2 синф-ўрта, унда буфер сатҳи ўнгга кўрроқ сурилсин
ҚОИДА-5: АГАР 1 синф-юқори ва 2 синф-юқори, унда буфер сатҳи ўнгга камроқ сурилсин
ҚОИДА-6: АГАР 1 синф-ўрта ва 2 синф-юқори, унда буфер сатҳи чапга камроқ сурилсин
ҚОИДА-7: АГАР 1 синф-қуйи ва 2 синф-юқори, унда буфер сатҳи ўнгга кўпроқ сурилсин.

Масалани MATLAB дастуридан фойдаланган ҳолда моделлаштириш амалга оширилади.

Сўз сўнги ўрнида шуни таъкидламоқчиманки, мавҳум тизим воситасида оммавий хизмат кўрсатиш тизимида хотирани башқариш тартиб-қоидаларини умумийлаштирган ҳолда самарали бошқариш тартиб-қоидаларини вужудга келтириш мумкин. Бу эса келиб тушаётган талабларга юқори даражадаги сифатли хизмат кўрсатишимизни таъминлайди.

ИНФОКОММУНИКАЦИЯ ТАРМОҒИ РЕСУРСЛАРИНИ СЕРВИСГА ЙЎНАЛТИРИЛГАН АРХИТЕКТУРА УСУЛИ НЕГИЗИДА ТАҚДИМ ЭТИШ АСОСЛАРИ

Т.Н. Нишонбоев (ТАТУ, профессор)
Н.М. Абдулхаев (ТАТУ, 2 – курс магистранти)

Мақолада инфокоммуникация тармоқлари (ИКТ) нинг дислокациялан-ган хизмат ва ресурсларини сервисга йўналтирилган архитектура (СЙА) усули асосида тақдим этиш таклиф этилади.

Инфокоммуникация тармоқларининг дислокацияланган хизмат ва ресурсларини СЙА асосида тақдим этишни қуйидагича ташкил этиш таклиф этилади.

Инфокоммуникация тармоғининг бошқарув сатҳи қурилмасида (яъни, бошқарув маркази вазифасини бажарувчи сервер компьютерида) тармоқ операторлари томонидан тақдим этилган сервисларнинг (хизмат ва ресурс-ларнинг) реестри яратилади, яъни тармоқ доирасида ҳар хил нуқталарда дислокация қилинган тармоқ ресурслари тўғрисидаги ахборотларнинг маълумотлар базаси яратилади.

Маълумотлар базасидаги ахборотлар ресурснинг имконияти, қандай ифодаланганлиги, ресурсни тақдим этишда қўлланиладиган иловалар ёки Web-сервислар (махсус дастурлар) ва ресурсдан фойдаланиш шарти тўғрисидаги аннотациявий маълумотлардан таркиб топади. Улар UDDI (Universal Description, Discovery and Integration) стандартлари асосида шакллантирилади.

Бундай реестр инфокоммуникация тармоғи ресурсларини яратадиган ва тақдим этадиган операторларнинг ахборот муҳити учун ишлаб чиқиладиган сервисга йўналтирилган архитектуранинг интеграллашган таркибий қисми ҳисобланади.

Шу билан бирга, ушбу серверда хавфсизликни таъминлаш нуқтаи наза-ридан фойдаланувчини, ресурсни ҳамда ресурс тўғрисидаги ахборотларни тақдим этадиган тармоқ операторларини аутентификациялаш воситалари ўрнатилади.

Фойдаланувчи сўровига мувофиқ тақдим этиладиган ҳар бир ресурсни амалга ошириш учун керак бўладиган ҳамма воситалар (протокол, интерфейс, иловалар ва бошқа Web-сервислар) танланади ва уларнинг интеграцияси амалга оширилади. Бошқа сўз билан, тармоқ ресурслари тақдим этилишини амалга ошириш учун керак бўладиган воситалар, яъни махсус сервислар танланиб, улар асосида «композит» сервислар шакллантирилади.

ИКТ функцияларини СЙА негизида ташкил этиш унинг сервисларини типларга ажратишни тақозо этади. Сервисларни типларга ажратиш сатҳлари қуйидагиларни ўз ичига олади:

- юқори сатҳ сервислари - ИКТнинг хизматлар сатҳида тақдим этилади-ган ресурслар, иловалар;

- транспорт сатҳ сервислари - маршрутизация, протоколлар боғланиши, ҳар хил типдаги маълумотлар тақсимотини бошқариш, яъни маълумотларни транспортировка қилиш воситалари;

- кириш сатҳ сервислари - ҳар хил типдаги маълумотларни ИКТ транс-порт тизимига боғлаш – тармоқга кириш интерфейслари ва протоколлари.

Композит сервислар тўплами фойдаланувчи томонидан талаб этилган сўровга боғлиқ ҳолда тузилади ва фақат шу сўров учун ишлатилади.

СЙА моделига асосан ИКТ сервисларини икки группага бўлиш мумкин: биринчиси – ресурс ва хизматларларни тақдим этиш сатҳи сервислари ва иккинчиси - маълумотларни транспортировка қилиш сервислари.

СЙА негизидаги ИКТ ресурслари тақдим этилишида иштирок этадиган сервислар сўров бажарилиши давомида бошқарилади.

Шу билан бирга, ҳамма сатҳ жараёнларида ахборот хавфсизлигига алоҳида эътибор бериш керак бўлади.

ИКТ ресурсларини СЙА услублари негизида тақдим этилишида ишти-рок этадиган сервислар (реал вақтда ишлайдиган махсус дастурий таъминот ёки иловалар) қуйидаги талабларга жавоб бериши керак:

1) ИКТ ресурсларининг турлари $[S_i^p]$ ва уларни тақдим этишда қўлланиладиган сервислар ёки композит сервислар тўплами $\{S_i^c\}$ аниқ бўлиши керак, яъни:

$$S^p = \{ S_i^p \} \qquad S^c = \{S_i^c\}.$$

2) СЙА негизидаги инфокоммуникация тармоғи фаолият даврининг ҳар бир вақт оралиғида маълум бир ресурсга сўров келганида, улар ўртасида боғланишни таъминлайдиган композит сервис бўлиши керак;

3) СЙА негизидаги инфокоммуникация тармоғида маълум бир композит сервис асосида бажарилаётган сўровлар бошқарилиши керак;

4) ҳар бир тақдим этилаётган ресурс тури маълум бир даражадаги сифат кўрсаткичига эга бўлиши керак ва б.

Бир хил мазмундаги ресурслар ҳар хил оператор ва провайдерлар томонидан ҳар хил дастурий таъминотлар («композит сервис»лар) ва ҳар хил мезон кўрсаткичи асосида тақдим этилади.

Мақолада мезон кўрсаткичи сифатида «сўровни бажариш вақти» параметрини қўллаш тавсия этилади.

Сўровни бажариш вақти умуман олганда тасодиф қийматга эга, чунки фойдаланувчининг сўровини бажаришда ИКТ нинг деярли ҳамма компоненталари иштирок этади ва сўровни қайта ишлаш учун кетадиган вақт уларнинг ҳолатига боғлиқ.

Интернет тармоғи асосидаги ресурс (яъни, Web-сервис) OSI модели амалий сатҳининг HTTP протоколи ҳамда транспорт сатҳи TCP протоколи негизида тақдим этилади. Ушбу ресурсга сўров амалга оширилишида қуйидаги босқичлар бажарилади:

1) ресурс сақланаётган Web-сервер компьютерининг IP манзилини қидириш. Бу босқичда юзага келадиган кечикиш вақти тармоқда маълумот узатиш тезлигига ва адреслар номи сақланадиган домен сервер (DNS –сервер) ининг ишлаш тезлигига боғлиқ бўлади;

2) сервер билан боғланиш. Бу жараёнда TCP протоколидан фойдала-нилади, дастлаб ресурс сақланаётган сервер билан алоқа ўрнатилади. Кечикиш вақти фойдаланувчи ва сервер оралиғидаги тармоқ характерис-тикаларига боғлиқ бўлади. Боғланиш жараёнида қуйидаги босқичлар бажарилади - фойдаланувчи томонидан боғланиш пакети жўнатилади, сервердан боғланишга розилик пакети қабул қилинади ва қабул қилинганлик тўғрисидаги пакет фойдаланувчи томонидан яна серверга жўнатилади;

3) сўровни жўнатиш. Босқични амалга ошириш учун кетадиган вақт фойдаланувчи томонидан сўровни шакллантириш ва уни жўнатиш учун сарфланадиган вақт билан ўлчанади;

4) жавобни кутиш. Босқич давомида фойдаланувчи сўрови сервер компьютери томонидан қайта ишланади ва жавоб тармоқ орқали узатилади. Кечикиш вақти тармоқдаги кечикиш ва ресурсни қуввати билан ўлчанади;

5) жавобни олиш. Босқичда сўралган ресурс пакет технологияси асосида қабул қилинади. Босқичга кетадиган вақт тармоқ томонидан киритиладиган кечикиш ва ресурснинг ҳажмига боғлиқ бўлади;

6) TCP боғланишнинг ёпилиши - жуда кам вақт талаб этади. HTTP сўрови амалга оширилишида қуйидаги кечикишлар юзага келиши мумкин:

- ҳар хил маълумот узатиш муҳитлари томонидан юзага келадиган кечикишлар - сўров фойдаланувчи компьютеридан, то ресурс сақланадиган сервер компьютерига симсиз, кабел ва оптик толали муҳит орқали узатилиши мумкин;

- фойдаланувчи компьютери ва ресурс сақланадиган сервер компью-тери ҳамда оралиқ коммуникацион марказлар (алоқа тугунлари) орасидаги масофага боғлиқ кечикишлар. Вақт ўтиши билан тармоқ топологияси ўзга-риши натижасида пайдо бўладиган қўшимча факторлар кечикишларнинг ўзгаришига сабаб бўлади.

- тармоқ аппарат-дастур воситалари томонидан юзага келадиган кечикишлар.Сўров сигналини фойдаланувчидан, то ресурс сақланадиган сервер компьютерига узатиш йўлида, у бир неча роутер, коммутатор ва бошқа тармоқ қурилмаларидан ўтиши мумкин. Уларнинг ҳар бири тармоқдаги кечикиш вариациясига ўзининг ҳиссасини қўшади, чунки уларда юкламанинг ҳажми ҳар хил бўлиши ва уларда ҳар хил ёрдамчи қурилмалар ишлатилган бўлиши мумкин.

Бошқа мезон кўрсаткичларини ҳам шундай тасодиф функциялар орқали ифодалаш мумкин.

Хулоса қилиб шуни таъкидлаш жоизки, фойдаланувчи сўрови «композит сервислар» асосида бажарилади, сўровни ҳар хил сифат даражасида амалга ошириш учун ҳар хил турдаги «композит сервислар»ни шакллантириш керак бўлади. Бунда уларнинг сифат кўрсаткичлари танланган мезон кўрсаткичининг қиймати орқали аниқланади.

ФОЙДАЛАНУВЧИ СЎРОВИНИ ИКТ САТҲЛАРИДА БАЖАРИЛИШ ВАҚТИНИНГ ЙИҒИНДИСИНИ ҲИСОБЛАШ АЛГОРИТМИ

Т.Н. Нишонбоев (ТАТУ, профессор)
А.А.Жумабаев (ТАТУ, 2 – курс магистранти)

Мураккаб структурали инфокоммуникация тармоғида мужассамланган ресурслар, жумладан, ҳисоблаш ресурслар бир-бири билан боғланган компьютер тизимларида таркиб топади.

Дислокацияланган компьютер тизимларининг ресурслари кўп ҳолларда ҳар хил дастурий платформаларда тақдим этилади. Тармоқ шароитида уларни бирлаштириб, ягона ресурс шаклида фойдаланувчига тақдим этиш асосий муаммо ҳисобланади.

Муаммо – биринчидан, фойдаланувчи масаласини ечиш учун керак бўладиган ресурсларни кенг доирадаги гетероген муҳит доирасида излаб топиш ва уларни интеграциялаб ягона ресурс шакллантириш, уларни биргаликда қандай кетма-кетликда ишлашларини аниқлаш ва, ниҳоят, сервисларни биргаликдаги фаолиятини ташкил этиш. Бошқа сўз билан, ҳар хил нуқталардаги компьютер тизимларидаги ҳисоблаш ресурслари асосида жорий масала учун керакли ресурсларни излаб топиш ва реал вақтда ўзаро мулоқотларини ташкил этишдаги муаммолар.

Иккинчидан, ТТ таркибидаги ҳар хил нуқталардаги компьютер тизим-лари орасида маълумот узатиш жараёнлари мавжуд транспорт тармоғи асосида бажарилади (етти сатҳли OSI моделининг биринчи тўртта сатҳлари протоколлари асосида). Мавжуд изланишларда транспорт тармоғида ҳал қилинадиган масалалар алоҳида, яъни компьютер тизимлари имкониятларига боғланмаган ҳолда ечилади. Натижада ИКТ доирасида шаклланган виртуал муҳит кўзланган натижага олиб келмайди, чунки транспорт тармоғида маълумот узатишда юзага келадиган кечикишлар миқдори ахборот қайта ишлаш жараёнларининг умумий вақтига катта таъсир кўрсатади.

Мураккаб структурали инфокоммуникация тармоғи шароитида (яъни, мураккаб структурали гетероген муҳит шароитида) унинг таркибига кирувчи тармоқ қурилмалари ва алоқа каналлари ёрдамида ўзаро боғланган ҳар хил аппарат ва дастурий таъминотлар асосидаги ахборот қайта ишлаш воситалари (яъни, серверлар, компьютерлар ва х.к.) негизида ягона ресурс шакллантирилаётганида, албатта, ресурс тақдим этишга мўлжалланган компьютер ва бошқа тармоқ қурилмаларининг ва алоқа каналларининг параметрлари ҳисобга олиниши керак.

Акс ҳолда, гетероген муҳит шароитида яратилган виртуал ресурс-лардан фойдаланиш жараёнлари кўзланган самарани бермай қолиши мумкин.

Шундай қилиб, инфокоммуникация тармоғининг ресурсларидан сама-рали фойдаланиш шароитини яратиш йўлида махсус усул, алгоритмлар ишлаб чиқиш долзарб муаммолардан бири ҳисобланади.

Инфокоммуникация тармоғи йўналишидаги кўп изланишларда ахборот қайта ишлаш воситаларидаги жараёнлар алоҳида, транспорт тармоғидаги ахборот оқимини узатиш жараёнлари алоҳида тадқиқ қилинади. Гетероген тармоқда фойдаланувчининг масаласини қайта ишлаш жараёни ахборот қайта ишлаш тизимидаги ҳолат ва транспорт тармоғидаги жорий ҳолат негизида амалга оширилади, яъни фойдаланувчининг масаласининг ечимида иккала тизим иштирок этади. Транспорт тармоғи воситалари орқали фойдаланувчи ечимидаги маълумотлардан ташқари ҳар хил турдаги маълумотларнинг оқими узатилади.

Бошқа сўз билан, фойдаланувчилар масаласини қайта ишлаш учун кетадиган ўртача вақт иккита ўзгарувчидан функционал боғлиқликда бўлади, яъни

$$\mathbf{T = F\{P, U\},}$$

бунда **P** – ИКТ таркибидаги компьютерларнинг ҳисоблаш қувватини характерлайдиган вектор катталик , ($\mathbf{P = p_1, p_2, \ldots p_n}$);

U – транспорт тармоғининг юкланганлик даражасини характерлай-диган вектор катталик.

Фойдаланувчининг мураккаб масаласи ИКТ муҳитида қайта ишланаётганида компьютер тизимларининг тарқоқ ҳолда (гетероген муҳитда) жойлашганлиги ва маълумот узатиш муҳитининг динамик ҳолда ўзгариши ҳисоблаш ҳамда маълумот алмашиш жараёнларини оптимал ташкил этиш керак, деган масалага олиб келади.

Бу маънода оптималлаштириш масаласи қуйидагича қўйилиши мум-кин:

инфокоммуникация тармоғи таркибида шундай виртуал муҳит тузил-масини шакллантириш керакки, у тармоқ фойдаланувчиларининг сўров-ларини (масалаларини) имкон қадар тез (ёки, қисқа вақт ичида) ва тўлиқ бажариб беришни таъминласин.

Бошқа сўз билан, фойдаланувчи масалаларини қайта ишлашда шундай қувватга эга компьютер тизимлари ва маълумот узатиш тармоқ воситалири топилсинки, бунда оқимларнинг стационарлигига қўйилган чекловлар бажарилган ҳолатда маълумотларни узатиш **[t_1]** ва қайта ишлаш **[t_2]** учун сарфланадиган вақтнинг йиғиндиси минимал қийматга эга бўлсин, яъни

$$\{ [t_1] + [t_2] \} \longrightarrow \min,$$

Бундай натижаларга эришиш учун мавжуд инфокоммуникация тармоғи шароитида яратилиши режалаштирилаётган виртуал муҳит тизимининг ар-хитектурасини маълум даражада такомиллаштириш керак бўлади.

Бугунги кунда инфокоммуникация тармоғининг кириш сатҳида асосан кенг полосали кириш воситалари жорий этилиши сабабли, уларда қўлланиладиган алоқа каналларининг узатиш қобилияти нисбатан юқори (бир неча мегабит) ва бу сатҳда, яъни фойдаланувчи ва кенг полосали киришни таъминлайдиган провайдер орасида маълумот узатиш жараёнида юзага келадиган кечикишлар белгиланган нормада, деса бўлади.

Лекин кейинги транспорт босқичида фойдаланувчи маълумотидан ташқари бир неча ўн, юз ва хатто минг фойдаланувчиларнинг бир неча мегабит тезликдаги маълумотлари узатилиши мумкин. Бунда Гигабит тезликдаги магистрал каналлар талаб этилади. Бу босқичда виртуал ресурсларни тақдим этилишида ва фойдаланувчиларнинг сўровлари ИКТ муҳитида бажарилишида трафик ҳажми кескин кўпайиб кетиши ва кечикишлар нормадан чиқиб кетиши ва бошқа муаммолар юзага келиши мумкин. Бундай муаммолар келиб чиқмаслиги учун виртуал муҳит тузилмаси ва хизматларининг инфраструктураси оптимал шаклантирилиши лозим.

Қисқаси, виртуал муҳит доирасидаги ахборот қайта ишлаш тизимларининг тезлиги улар орасидаги маълумот узатиш воситаларининг тезлиги билан имкон қадар уйғун (имкон қадар бир-бирига тенгроқ) бўлиши керак. Одатда компьютер тизимларининг тезлиги алоқа каналларида маълумот узатиш тезлигидан бир мунча катта бўлади. Бундай ҳолатда виртуал муҳитнингнинг самараси кам бўлади.

ИКТ таркибида виртуал муҳит шакллантирилаётганида қуйидаги маса-лалар ечилиши керак бўлади:

1) компьютерларнинг умумий тўплами характеристикалари ва пара-метрлари бир-бирига яқинлари аниқланади ва улар асосида гуруҳлар (сег-ментлар) шакллантирилади;

2) ҳар бир гуруҳ учун гуруҳ миқёсида “ўртача” характеристакаларга эга бўлган бош компьютер аниқланади;

3) транспорт тармоғи бўйича узатиладиган маълум бир ҳажмдаги гуруҳий ахборот шакллантирилади;

4) гуруҳнинг “жисмоний” ресурслари негизида гуруҳ доирасида вир-туал ресурслар яратилади;

5) бош компьютерда виртуал муҳит доирасида яратилган ҳисоблаш ресурсларнинг реестри шакллантирилади;

6) ИКТ транспорт тармоғида гуруҳ компьютерлари орасида фойда-ланувчи масаласини ечиш даврида юқори тезликда маълумот узатишни таъминлайдиган маршрутлар аниқланади.

Кўп ҳолларда инфокоммуникация тармоғи фойдаланувчилари томони-дан виртуал муҳитга тушган сўровларнинг ҳажми кутилганидан ошиб кетади. Бундай ҳолларда уларни виртуал муҳит компоненталари (ресурслари) орасида тақсимлашни махсус алгоритм асосида амалга ошириш тақозо этилади. “Критик” холатлар учун ишлаб чиқилган алгоритмлар ёрдамида сўровларни нисбатан қисқа вақт ичида бажарилишига эришилади.

Умуман, баён этилган масала қуйидагича қўйилиши мумкин: ИКТ тармоғи доирасида виртуал муҳитининг схемасини белгилайдиган параметрлар берилган бўлса, виртуал муҳитига келиб тушаётган сўровларни шундай тақсимлаш керакки, бунда уларни траспорт тармоғида узатиш ва компьютер тизимларида қайта ишлаш учун кетадиган вақтларнинг йиғиндиси минимал бўлсин, яъни сўровни виртуал муҳитида бажарилиши минимал вақт оралиғида амалга оширилсин.

РОЛЬ ЦИФРОВЫХ ПРОЦЕССОРОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

С.Б. Нурматова (ТУИТ, старший преподаватель)

В статье рассмотрены основные параметры цифровых сигнальных процессоров (DSP) и их влияние на выбор подходящей микросхемы, а также описано текущее состояние рынка DSP. Выбирая цифровой сигнальный процессор, не плохо было бы представлять существующий рынок DSP, знать основных производителей и направления развития создаваемых ими процессоров.

DSP-процессоры предназначены для осуществления цифровой обработки сигнала — математических манипуляций над оцифрованными сигналами. Они широко применяются в беспроводных системах, аудио- и видеообработке, системах управления. С ростом числа приложений, использующих DSP, и сложности алгоритмов обработки увеличивается и требования к ним в плане повышения быстродействия и оснащенности интерфейсными и другими специализированными узлами. К настоящему времени появилось множество типов DSP, как универсальных, так и ориентированных на достаточно узкий круг задач.

Естественно, ни один из процессоров не может подойти для всех приложений. Поэтому первая задача разработчика — выбор процессора, наиболее подходящего по производительности, цене, наличию определенной периферии, потреблению мощности, простоте использования и другим критериям.

Например, для таких портативных устройств, как мобильные телефоны, портативные цифровые плееры, стоимость, степень интеграции и потребляемая мощность являются первостепенными, а максимальная производительность зачастую не нужна (т.к. обычно влечет за собой значительное повышение потребляемой мощности, не давая преимуществ при обработке относительно низкоскоростных аудиоданных).

В то же время для гидроакустических или радиолокационных систем определяющими параметрами являются скорость работы, наличие высокоскоростных интерфейсов и удобная система разработки, а стоимость является второстепенным критерием. Кроме того, во многих случаях имеет смысл учитывать и место на рынке, занимаемое поставщиком процессора, т.к. далеко не все производители могут предоставить в ваше распоряжение спектр процессоров, покрывающих все ваши потребности. Сложившееся к настоящему времени распределение рынка между ведущими поставщиками (см. табл. 1) показывает, что 4 компании, стоящие в начале списка, поставляют более 80% всех используемых в мире DSP. Именно эти компании наиболее известны и на российском рынке, и их продукция часто упоминается.

Таблица 1.

Основные производители DSP и принадлежащие им доли рынка

Компании-лидеры рынка	Company Name	Доля рынка DSP
1	Texas Instruments	54,3%
2	Freescale	14,1%

	Semiconductor	
3	Analog Devices	8,0%
4	Philips Semiconductors	7,5%
5	Agere Systems	7,3%
6	Toshiba	4,9%
7	DSP Group	2,2%
8	NEC Electronics	0,6%
9	Fujitsu	0,4%
10	Intersil	0,3%
	Other Companies	0,5%
	Total	100,0%

В таблице 2 показано позиционирование DSP с точки зрения их создателей.

Таблица 2.

Области применения семейств сигнальных процессоров разных производителей

Обработка видео, видеонаблюдение, цифровые камеры, 3D графика	TMS320DM64x/DaVinci, TMS320C64xx, TMS320C62xx (TI), PNX1300, PNX1500, PNX1700 (Philips) , MPC52xx (Freescale)
Обработка аудио, распознавание речи, синтез звука	TMS320C62xx, TMS320C67xx (TI), SHARC (Analog Devices)
Портативные медиа устройства	TMS320C54xx, TMS320C55xx (TI), Blackfin (Analog Devices)
Беспроводная связь, телекоммуникации, модемы, сетевые устройства	TMS320C64xx, TMS320C54xx, TMS320C55xx (TI), MPC7xxx, MPC86xx, MPC8xx PowerQUICC I, MPC82xx PowerQUICC II, MPC83xx PowerQUICC II Pro, MPC85xx PowerQUICC III (Freescale), Blackfin, TigerSHARC (Analog Devices), PNX1300 (Philips)
Управление приводами, преобразование мощности, автомобильная электроника, предметы домашнего обихода, офисное оборудование	TMS320C28xx, TMS320C24xx (TI), ADSP-21xx (Analog Devices), MPC55xx, MPC55xx (Freescale)
Медицина, биометрия, измерительные системы	TMS320C62xx, TMS320C67xx, TMS320C55xx, TMS320C28xx (TI), TigerSHARC, SHARC (Analog Devices)

Следует помнить, что производители DSP, проектируя новые микросхемы, достаточно четко позиционируют их для использования в тех или иных приложениях. Это оказывает влияние и на их архитектуру, и на быстродействие, и на оснащение процессора тем или иным набором периферийных модулей.

DSP-процессоры широко используются в мобильных устройствах, где потребление мощности является основной характеристикой. Для снижения энергопотребления используется множество методов, в том числе уменьшение напряжения питания и введение функций управления потреблением, например, динамического изменения тактовой частоты, переключения в спящий или дежурный режим или отключения неиспользуемой в данный момент периферии. Следует отметить, что эти меры оказывают значительное воздействие на скорость работы процессора и при некорректном

использовании могут привести к неработоспособности проектируемого устройства (в качестве примера можно привести некоторые сотовые телефоны, которые в результате ошибок в программах управления энергопотреблением иногда переставали включаться) или к ухудшению его эксплуатационных характеристик (например, значительному времени восстановления работоспособности при выходе из спящего режима).

Оценка потребления мощности является не простой задачей, так как эта величина варьируется в зависимости от выполняемых процессором задач. Далее в этой статье будут рассмотрены основные характеристики процессоров, которые должен оценить разработчик для того, чтобы выбрать наиболее подходящий DSP. Правильный выбор DSP сильно зависит от приложения: процессор может хорошо подходить для одних приложений, но абсолютно не подходить для других. При выборе процессора нужно определить самые важные в конкретном случае характеристики и расставить их по степени важности. Затем в соответствии с этими критериями отобрать возможных кандидатов и, наконец, выбрать из подходящих лучший, обращая внимание на дополнительные, не критичные характеристики. При этом целесообразно воспользоваться оценкой характеристик процессоров, производимой какой-либо авторитетной компанией (например, BTDI). Следует помнить, что BTDI производит оценку DSP не только по быстродействию, но и по другим критериям: эффективности памяти, энергопотреблению и т.д.

Не исключена вероятность того, что выбранные процессоры окажутся очень близки по ключевым параметрам. В этом случае выбор будет определяться некритичными характеристиками: доступностью средств отладки, предыдущим опытом разработчика, доступностью компонентов и т.д. Тщательный выбор цифрового сигнального процессора еще на начальном этапе разработки может помочь избавиться от излишних затрат, связанных с выбором неподходящего DSP, и сократить как время разработки в целом, так и время и средства на выявление ошибок.

ТЕЛЕКОММУНИКАЦИЯ ТАРМОКЛАРИДА АХБОРОТНИ КОДЛАШТИРИШНИНГ САМАРАЛИ УСУЛЛАРИ

С.Б. Нурматова (ТАТУ, катта ўқитувчи)

Ахборотни камроқ битларни сарфлаб узатиш ахборотни кодлаштиришнинг самарали усулларининг мақсад ва вазифаси ҳисобланади. Ахборотни кодлаштиришнинг самарали усулларидан фойдаланилганда каналнинг ўтказувчанлик қобилиятидан самарали фойдаланиш мумкин. Ҳозирги кунда ахборотни кодлаштиришнинг самарали усулларининг йўқотишсиз ва йўқотишли турлари мавжуд. Мультимедиа кўринишдаги ахборотларни жўнатиш учун йўқотишли алгоритмлар ишлатилади. Матн кўринишдаги ахборотларни жўнатиш учун йўқотишсиз алгоритмлар ишлатилади. Бундай алгоритмларга

Хаффман ва Шеннона – Фано алгоритмлари мисол бўла олади.

Шеннона Фано коди пайдо бўлгунча алоқа каналлари орқали узатилаётган ахборотлардаги белгилар узунлиги бир хил бўлган битлар ёрдамида кодлаштирилар эди. Шеннона Фано коди пайдо бўлгандан сўнг узатилаётган ахборотдаги ҳар бир белгининг пайдо бўлиш эҳтимоллигига қараб туриб, узунлиги ҳар хил бўлган битлар ёрдамида кодлаш имконияти пайдо бўлди. Ахборотда бирор бир белгининг пайдо бўлиш эҳтимоллиги каттароқ бўлса уни иккилик саноқ тизимидаги кодининг узунлиги кичикроқ бит бўлади. Агар ахборотда бирор бир белгининг пайдо бўлиш эҳтимоллиги кичикроқ бўлса, уни иккилик саноқ тизимидаги кодининг узунлиги каттароқ бит бўлади.

Шеннононинг иши пайдо бўлгунига қадар хабарларни алоқа каналлари бўйлаб узатишда алифбо символарининг кодланиши Хартлининг формуласи бўйича олинадиган битларнинг бир хил миқдори билан амалга оширилган. Мазкур ишнинг пайдо бўлиши билан уларнинг матнда пайдо бўлиш эҳтимоллигига боғлиқ ҳолда битларнинг турли сони

билан символларни кодловчи усуллар пайдо бўла бошлади, яъни эҳтимоллиги юқори бўлган символлар қисқа кодлар билан кодланади, кам учрайдиган символлар эса – узун (ўртачадан узунроқ) кодлар билан кодланади. Ушбу синфнинг ўта машҳур усуллардан Хаффман ва Шенноно-Фанонинг кодлаш усули ҳисобланади. Файлда ҳар бир символнинг пайдо бўлиш эҳтимоллигини белгилаш усули билан фарқланувчи эҳтимолий усулларнинг қуйидаги иккита тури мавжуд:

Биринчиси - кирувчи оқимни кўриш ва тўпланган статистика асосида кодлашни қуриш (бунда файллар бўйича иккита ўтиш талаб этилади – биттаси статистик ахборотни кўриб чиқиш ва тўплаш, иккинчиси – кодлаш учун), бу эса бундай алгоритмлардан фойдаланиш соҳасини бир мунча чеклаб қўяди, шу тарзда телекоммуникация тизимларида қўлланиладиган биттада ўтиладиган кодлаш имконияти йўқолади, бунда маълумотлар ҳажми ҳам номаълум бўлади, уларнинг такрор узатилиши ёки ажратилиш жуда кўп вақтни эгаллайди. Бундай ҳолатда, чиқувчи оқимга фойдаланилган кодлашнинг статистик схемаси ёзиб олинади. Ушбу усул Хаффманнинг статик кодлаши сингари машҳурдир.

Иккинчи усул– адаптив кодлаш усулидир (adaptive coder method). Унинг умумий принципи кирувчи оқимнинг ўзгариш характерига боғлиқ ҳолда кодлаш схемасини ўзгартиришдан иборатдир. Бундай ёндашув биттада ўтиладиган алгоритмга эга ҳамда аниқ кўринишда фойдаланилган кодлаш тўғрисидаги ахборотни сақлаб қолинишини талаб этмайди. Адаптив кодлаш статикга нисбатан юқори сиқиш даражасини бериши мумкин, чунки кирувчи оқим частоталарининг ўзгариши тўлиқ ҳисобга олинади. Ушбу усул Хаффманнинг динамик кодлаши сингари машҳурдир.

Хаффманнинг статик кодлашида кирувчи символларга (турли узунликдаги битларнинг занжирларига) битларнинг занжири, шунингдек, ўзгарувчан узунлигига мувофиқ уларнинг кодлари қўйилади. Ҳар бир символнинг код узунлиги унинг частотасини, тескари белги билан олинган иккиламчи логарифмига пропорционал қилиб олинади. Учраган турли символларнинг барча умумий тўплами эса оқим алифбосини ташкил этади. Ушбу кодлаш префиксли бўлиб ҳисобланади, бу эса унинг натижавий оқимини осон декодлаш имконини беради, яъни, префиксли кодлашда исталган символ коди ҳар қандай бошқа символнинг код префикси бўлиб ҳисобланмайди – бу алифбо ноёбдир.

Ушбу муаммо, одатда, кириш оқими алфавитига 'ab', 'abc',. . . ва ҳоказо турдаги янги символлар оқимини киритиш йўли билан ҳал этилади, бунда a, b, c – бирламчи дастлабки алфавит символлари. Бундай жараён сегментация ёки кириш оқимини блокировка қилиш деб номланади. Бироқ, сегментация сиқишдаги йўқотишлардан тўлиқ ҳалос бўлиш имкониятини беради (улар блокнинг ўлчамига пропорционал равишда кичраяди), бироқ кодлаш дарахти ўлчами ҳамда бунга мувофиқ равишда иккиламчи алифбонинг символлар коди узунлигининг кескин ўсишига олиб келади. Қурилиш техникаси бўйича Хаффман кодига яқинроқ бўлиб ҳисобланадиган кодлар 1948-1949 йилларда бир биридан мустақил равишда Шеннон ва Фано томонидан тақдим этилган Шеннон-Фано кодлари ҳисобланади. Уларнинг қурилиши қуйидаги тарзда амалга оширилган бўлиши мумкин:

Хаффман кодини яратиш алгоритми пастдан-юқорига деб аталади, Шеннон-Фано эса – юқоридан-пастга деб аталади. Ушбу усулларнинг устуворлиги бўлиб уларнинг маълум бўлган амалга ошириш соддалиги ва бунинг натижаси кодлаш/кодни очиш тезлигининг юқорилиги ҳисобланади. Асосий камчилик умумий ҳолатда уларнинг оптимал эмаслиги ҳисобланади. Ахборотни камроқ битларни сарфлаб узатиш ахборотни кодлаштиришнинг самарали усулларининг мақсад ва вазифаси ҳисобланади. Ахборотни кодлаштиришнинг самарали усулларидан фойдаланилганда, ахборотни узатиш тезлигинг оширишга, каналнинг ўтказувчанлик қобилиятидан самарали фойдаланишга эришиш мумкин.

OPENFLOW КОММУТАТОРИ ИШЛАШ ТАМОЙИЛИ ВА УНИНГ ТАРМОҚДАГИ ЎРНИ

К.Е. Садатдийнов (ТАТУ, ассистент)

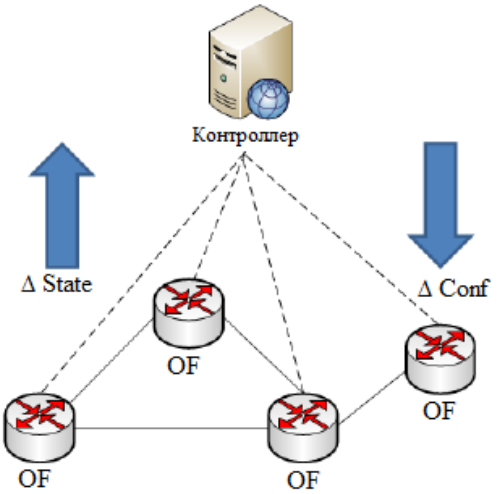
Дастурий конфигурацияланадиган тармоқлар ёндашувининг энг истиқболли ва ривожланаётган реализацияларидан бири OpenFlow технологияси ҳисобланади. Унинг асосий ҳужжати OpenFlow спецификацияси ҳисобланади, унда OpenFlow-тармоқларининг асосий компонентлари, ишлаш тамойиллари ва компонентлар алоқалари ифодаланган (OpenFlow протоколи). Спецификация учун стандартлаштирувчи ташкилот ONF – Open Networking Foundation ҳисобланади.

1-расмда OpenFlow тармоғининг асосий компонентлари кўрсатилган.

Спецификацияга мос, OpenFlow тармоқлари асосий компонентлари қуйидагилар:

- контроллер, ўз ичига олади:

1) тармоқ операцион тизими
2) тармоқ иловалари



1-расм. OpenFlow тармоғининг асосий компонентлари

- OpenFlow коммутатор;
- контроллер ва коммутатор ўртасидаги ҳимояланган канал;
- OpenFlow протоколи.

OpenFlow тармоғи ишлашининг умумий тамойили қуйидагича: ҳар бир OpenFlow коммутатор контроллер билан ҳимояланган канал ўрнатади, унинг ёрдамида контроллер уларни бошқаради. Коммутатор ва контроллер ўртасидаги алоқа OpenFlow протоколи хабарлари ёрдамида амалга оширилади. Контроллер тармоқда элементлар ҳолатининг ўзгариши тўғрисида ахборот олади, унинг асосида а тармоқ қурилмасини конфигурациялайди, тармоқ инфраструктурасини ва тармоқда маълумотлар оқимини бошқаради.

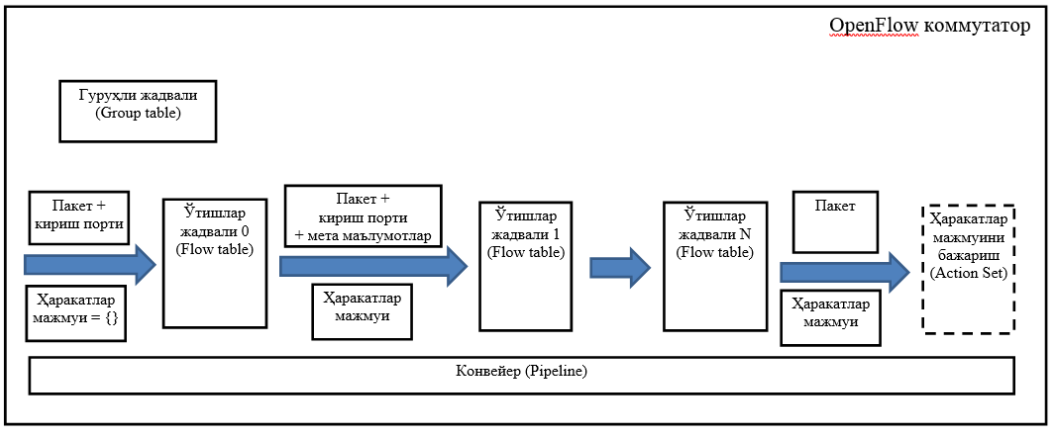
Коммутатор тузилиши. OpenFlow 1.3 версияси спецификациясига кўра коммутатор бир ёки ундан кўп оқимлар жадвали (flow table), гуруҳли жадвал (group table) дан иборат ва масофадаги контроллер билан алоқа учун ҳимояланган канални (Secure channel) қўллаб-қувватлайди.

Коммутатордаги ҳар бир оқимлар жадвали ёзувлар жамланмасидан (flow entries) иборат, уни биз оқимлар ҳақида ёзувлар ёки қоидалар деб атаймиз. Оқим ҳақида ҳар бир ёзув (қоида) белгилар майдони (match fields), ҳисоблагичлар (counters) ва йўриқномалардан (instructions) ташкил топган.

OpenFlow коммутаторининг ишлаш механизми оддий бўлиб, ҳар бир келиб тушган пакет коммутатор конвейерига келиб тушади (2-расм). Ҳар бир пакетда сарлавҳа (маълум

узунликдаги битли қатор) “кесиб олинади”. Бу битли қатор учун оқимлар жадвалидан биринчисидан бошлаб белгилар майдони кўпроқ пакетнинг сарлавҳасига мос келадигани қидирилади. Агар топилса, топилган қоидада кўрсатилган йўриқномалар мажмуи бўйича пакет ва унинг сарлавҳаси устидан ўзгартиришлар амалга оширилади. Ҳар бир жадвал ёзуви билан қўшилган йўриқномалар пакетни узатиш билан боғлиқ, пакетнинг сарлавҳасини ўзгартириш билан боғлиқ, гуруҳли жадвалда ишлов бериш билан боғлиқ, пакетни коммутаторнинг маълум портига узатиш билан боғлиқ ҳаракатларни ифодалайди. Ишлов бериш конвейери йўриқномалари кейинги ишлов бериш учун кейинги жадвалга пакетни узатиш ва жадваллар ўртасида ахборот (метамаълумот кўринишида) узатиш имкониятини беради. Йўриқномалар шунингдек, турли ҳил статистикаларни йиғиб бориш учун ишлатилиши мумкин бўлган ҳисоблагичлар ўзгаришлари қоидасини аниқлаб беради.

Агарда биринчи жадвалда керакли қоида топилмаса пакет инкапсуляцияланади ва контроллерга узатилади, у мазкур турдаги пакетлар учун мос келадиган қоида шакллантиради ва уни коммутаторга (ёки у томонидан бошқариладиган коммутаторларга) ўрнатади ёки пакет (коммутатор конфигурациясига боғлиқ) юқотилиши мумкин.



2-расм. Ишлов бериш конвейеридан ўтаётган пакет оқими

Коммутаторнинг оқимлар жадвалида қоидаларни ўрнатиш, янгилаш ва ўчириш контроллер томонидан амалга оширилади. Қоида реактив (келган пакетга жавоб сифатида) ёки проактив (олдиндан, пакетлар келгунга қадар) ўрнатилиши мумкин.

Маълумотларни бошқариш алоҳида пакетлар даражасида эмас, балки пакетлар оқими даражасида амалга оширилади. OpenFlow коммутаторда қоида контроллер иштирокида фақат биринчи пакет учун ўрнатилади, кейин оқимнинг қолган пакетлари уни фойдаланади.

OpenFlow протоколини қўллаб-қувватлайдиган коммутаторларни ишлаши бўйича икки турга ажратиш мумкин: OpenFlow-only ва OpenFlow-hybrid.

OpenFlow-only – бу фақат OpenFlow операцияларни қўллаб-қувватлайдиган коммутаторлар ҳисобланади. Бундай коммутаторларда барча пакетлар OpenFlow конвейерда ишлов берилади ва бошқа усул билан ишлов берилиши мумкин эмас.

OpenFlow-hybrid – бу коммутаторлар бир вақтнинг ўзида OpenFlow операцияларни ҳам, одатдаги Ethernet-коммутация операцияларини ҳам, яъни анъанавий L2 Ethernet-коммутацияни, VLAN, L3 маршрутлашни, ACL ва QoS ишлов беришни қўллаб-қувватлайди.

Жорий этилиши бўйича дастурий ва аппарат коммутаторларга ажратиш мумкин. Мавжуд коммутаторлар қўллаб-қувватлайдиган OpenFlow протоколи версияси бўйича ҳам ажратилади. Лекин бугунги кундаги барча аппарат коммутаторлар протоколнинг фақат 1.0 версиясини қўллаб-қувватлайди ва фақат битта оқимлар жадвалидан иборат. Дастурий коммутаторлар протоколнинг 1.3 версиясигача қўллаб-қувватлайди ва бирнечта жадваллардан иборат.

OpenFlow коммутаторнинг қуйидаги асосий функцияларини ажратиш мумкин:

1) Контроллер билан ҳимояланган канал ёқиш, ўрнатиш ва қўллаб-қувватлаш;
2) Контроллерга портлар ҳолати ўзгариши ҳақида ахборот бериш;
3) Контроллерга оқим ёзуви ўчирилганлиги ҳақида ахборот бериш;
4) Статус ўзгариши ҳақида огоҳлантириш;
5) Хатолик ҳақида огоҳлантириш;
6) Янги маълумотлар оқими учун қоида ўрнатишга талабнома бериш.

OpenFlow протоколи 3 турдаги хабарларни қўллаб-қувватлайди:

1) Controller-to-switch – контроллер томонидан ишлаб чиқилади ва бевосита коммутатор ҳолатини назорат қилиш ва бошқариш учун ишлатилади.

2) Асинхрон хабарлар коммутатор томонидан ишлаб чиқилади ва тармоқдаги ҳодисалар (хатоликлар, рад этишлар) ҳақида ва коммутатор ҳолати ўзгариши ҳақида огоҳлантириш учун ишлатилади.

3) Симметрик хабарлар коммутатор томонидан ҳам, контроллер томонидан ҳам ишлаб чиқилиши мумкин.

АЛГОРИТМЫ ПОСТРОЕНИЯ ФРАКТАЛЬНЫХ ОБЪЕКТОВ И ВЫЧИСЛЕНИЯ ПОКАЗАТЕЛЯ ХЕРСТА

М. Б. Саитахмадов (ТУИТ, ассистент)

История фракталов началась в конце 19-го века. *Фракталами* называются геометрические объекты: линии, поверхности, пространственные тела, имеющие сильно изрезанную форму и обладающие свойством самоподобия. Слово “фрактал” происходит от латинского слова ***fractus*** (разбитый, сломанный, дробный, состоящий из частей), от этого слова происходят и термины ***fraction, fractional*** - дробь, дробный. Оно было предложено американским математиком Бенуа Мандельбротом в 1975 году для обозначения нерегулярных, самоподобных структур которыми он занимался.

В 1977 году было издано книга Мандельброта «The Fractal Geometry of Nature - Фрактальная геометрия природы», в которой он собрал и систематизировал научные результаты ученых, таких как Жюлиана, Фату, Пуанкаре, Кантора, Хаусдорфа и других, работавших в период 1875–1925 годах, и заложившие теоретические основы фракталов[2].

С развитием теории стохастических фракталов становится актуальной показатель Херста (H). Показатель Херста представляет собой меру персистентности - склонности процесса к трендам. Значение $H > ½$ означает, что направленная в определенную сторону динамика процесса в прошлом, вероятнее всего, повлечет продолжение движения в том же направлении. Если $H < ½$, то прогнозируется, что процесс изменит направленность. $H= ½$ означает неопределенность процесса[3].

Показатель Херста связывают с коэффициентом нормированного размаха (R/S), где R – вычисляемый определенным образом «размах» соответствующего временного ряда, а S – стандартное отклонение.

Показатель Херста вычисляется по следующему алгоритму. Сначала вычисляется среднее значение измеряемой переменной, например, в нашем случае количество сообщений в информационном потоке за N дней:

$$\langle \xi \rangle_N = \frac{1}{N}\sum_{t=1}^{N}\xi(t)$$

Затем рассчитывается накопившееся отклонение ряда измерений $\xi(t)$ от среднего $<\xi>_N$:

$$X(t,N) = \sum_{u=1}^{t}(\xi(u) - \langle \xi \rangle_N)$$

После этого рассчитывается разность максимального и минимального накопившегося отклонения, которая и называется “размахом”:

$$R(N) = \max_{1\le t\le N} X(t,N) - \min_{1\le t\le N} X(t,N)$$

Стандартное отклонение рассчитывается по известной формуле:

$$S = (\frac{1}{N}\sum_{t=1}^{N}(\xi(t) - \langle\xi\rangle_N)^2)^{1/2}$$

В свое время Херст экспериментально обнаружил, что для многих временных рядов справедливо:

$$R / S = (N / 2)^{H}$$

Именно коэффициент H и получил название показателя Херста[1]. Показатель Херста рассчитывается по формуле:

$$H=\log(R/S)/\log(N/2).$$

При изучении фракталов, хаосов, временных рядов, а также обработки сигналов большую роль играет компьютерное моделирование и проведение компьютерных экспериментов.

В качестве примера рассмотрим алгоритмы построения классических фракталов. Все они строились по очень простым правилам с помощью итерационной процедуры и все обладали самоподобием, т.е. на каждом шаге итерации состояли из точных копий самого себя. Одним из таких примеров является ковер Серпинского.

Рассмотрим алгоритм, основанный на использовании рекурсивной функции в построении простого самоподобного фрактала - ковра Серпинского и их программные реализации в среде MatLAB (рис.1). В данном алгоритме используется способ построения, основанный на последовательном удалении из начальной области внутренних подобластей в соответствии с заданными правилами.

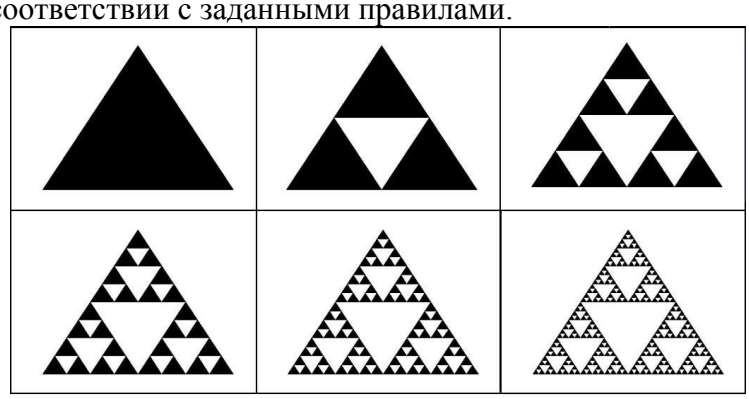


Рис.1. Последовательность построения ковра Серпинского

Выберем в качестве начального множества S_0 равносторонний треугольник вместе с областью, которую он замыкает. Удалим внутренность центральной треугольной области и назовем оставшееся множество S_1. Затем повторим описанный процесс для каждого из трех оставшихся треугольников и получим следующее приближение.

Ковер Серпинского является объединением N=3 непересекающихся уменьшенных в два раза копий треугольника. Множество, которое получается в пределе такой итеративной процедуры, называется ковром Серпинского.

Для построения рассматриваемого фрактала можно использовать следующий алгоритм:

1. Задать порядок ковра N.
2. Задать координаты вершин исходного треугольника ABC: (X_A, Y_A), (X_B, Y_B), (X_C, Y_C).
3. Построить равносторонний треугольник ABC и залить его черным цветом.
4. Вычислить координаты середин сторон треугольника ABC:

$$dx = \frac{X_B - X_A}{2},\ dy = \frac{Y_B - Y_A}{2},\ X_{A'} = X_A + dx,\ Y_{A'} = Y_A + dy,\ X_{B'} = X_B + dx + dx/2$$

$$Y_{B'} = Y_B + dy,\ X_{C'} + X_C + dx/2,\ Y_{C'} = Y_C + dy$$

5.Построить треугольник $A'B'C'$ и залить его белым цветом.

6.Повторить N раз действия, описанные в пунктах 4,5 для треугольников $AA'C'$, $A'BB'$ и $C'B'C$, соответственно [5].

Для реализации алгоритма в MatLAB создадим специальную функцию, возвращающая изображение ковра Серпинского. Для этого используем встроенный текстовый редактор MatLAB и сохраняем текст, например в файле Serpinsky.m[6]. Для вывода результатов в командной строке MatLAB набираем имя функции и указываем порядок фрактального объекта, например:

>> Serpinsky (4)

Результат, возвращаемый функцией Serpinsky(N), представлен на рис.1.

Теперь рассмотрим построение снежинки Коха. Возьмем равносторонний треугольник, будем последовательно заменять каждую линию, составляющую его, на четыре других, как это показано на рисунке 2. Повторяя эту операцию достаточно долго, мы получим фрактальный объект, напоминающий своим внешним видом снежинку, причем с каждым шагом длина кривой, ограничивающей площадь снежинки, увеличивается на одну треть

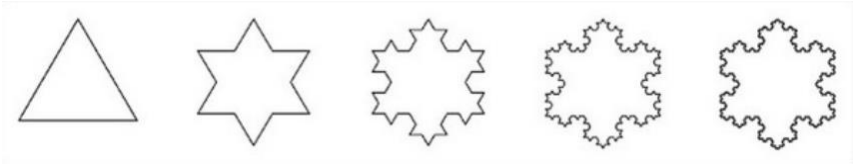


Рис. 2. Построение снежинки Коха.

. Если устремить число итераций к бесконечности, получится объект, конечная площадь которого ограничивается бесконечной кривой[3].

Описанный выше алгоритм легко обобщается для других фрактальных объектов, правила построения которых аналогичны правилам построения треугольного ковра Серпинского. Как видим, среда MatLAB, по сравнению с другими пакетами программ, предоставляет пользователю мощное средство построения фрактальных объектов и их программной реализации и визуализации.

ПРОГРАММНО-КОНФИГУРИРУЕМЫЕ СЕТИ

Н.С. Сайдирасулов (ТУИТ, ассистент)
М.М. Махаммадиев (ТУИТ, магистрант)

Программно – конфигурируемые сети (Software Defined Networks, SDN) — сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно. Одна из форм виртуализации сети. Ключевые принципы программно-определяемых сетей — разделение процессов передачи и управления данными, централизация управления сетью при помощи унифицированных программных средств, виртуализация физических сетевых ресурсов.

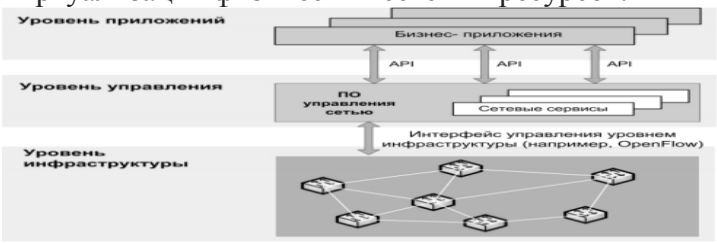


Рис. 1. Архитектура программно-конфигурируемых сетей

В архитектуре SDN можно выделить три уровня (рис. 1):

- *инфраструктурный уровень*, предоставляющий набор сетевых устройств (коммутаторов и каналов передачи данных);

• *уровень управления*, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью;

• *уровень сетевых приложений* для гибкого и эффективного управления сетью.

Наиболее перспективным и активно развивающимся стандартом для SDN является OpenFlow — открытый стандарт, в котором описываются требования, предъявляемые к коммутатору, поддерживающему протокол OpenFlow для удаленного управления. С помощью современных маршрутизаторов обычно решаются две основные задачи: *передача данных* (forwarding) — продвижение пакета от входного порта на определенный выходной порт и *управление данными* — обработка пакета и принятие решения о том, куда его передавать дальше, на основе текущего состояния маршрутизатора. Это соответствует уровню передачи данных, на котором собраны средства передачи (линии связи, каналообразующее оборудование, маршрутизаторы, коммутаторы), и уровню управления состояниями средств передачи данных (рис. 2).

Рис. 2. Традиционные сети и SDN

Ядром уровня управления программно-определяемой сетью является *сетевая операционная система* — программное средство, обеспечивающее, с одной стороны, интерфейс со средствами инфраструктурного уровня (например, динамическое изменение таблиц маршрутизации), и с другой стороны — прикладной программный интерфейс для уровня сетевых приложений, сформулированный в терминах более высокого уровня абстракции (например, «имя узла», «имя пользователя»), нежели используется в параметрах конфигурации сетевых устройств (IP-адрес, маска подсети, MAC-адрес). *Сетевая ОС (СОС)* обеспечивает приложениям доступ к управлению сетью и постоянно отслеживает конфигурацию средств сети. В отличие от традиционного толкования термина ОС, под СОС понимается программная система, обеспечивающая мониторинг, доступ и управление ресурсами всей сети, а не ее конкретного узла.

Одна из идей, активно развиваемая в рамках SDN, — это виртуализация сетей с целью более эффективного использования сетевых ресурсов (рис. 3). Под виртуализацией сети понимается изоляция сетевого трафика — группирование (мультиплексирование) нескольких потоков данных с различными характеристиками в рамках одной логической сети, которая может разделять единую физическую сеть с другими логическими сетями или сетевыми срезами (network slices). Каждый такой срез может использовать свою адресацию, свои алгоритмы маршрутизации, управления качеством сервисов и т. д.

Рис. 3. Виртуализация в SDN

Сегодня на рынке решений SDN заметны две тенденции: наблюдается активное появление перспективных стартапов и происходит ориентация лидеров рынка ИКТ на SDN. Таким образом протокол OpenFlow, реализующий независимый от производителя интерфейс между логическим контроллером сети и сетевым транспортом,

является одной из реализаций концепции программно-определяемой сети и считается движущей силой её распространения и популяризации.

ИНФОКОММУНИКАЦИЯ ТАРМОҒИ КИРИШ САТҲИНИНГ ИШОНЧЛИЛИК КЎРСАТКИЧЛАРИНИ АНИҚЛАШ АЛГОРИТМИ

Ф.А. Сулаймонов (ТАТУ, 2 – курс магистранти)
А.А. Жумабаев (ТАТУ, 2 – курс магистранти)

Мақолада инфокоммуникация тармоғи кириш сатҳининг ишончли-лигини ошириш бўйича алгоритм ишлаб чиқилган. Чунки кириш сатҳининг ишончли фаолияти бутун инфокоммуникация тармоғини ишончли ишлашини таъминлайди.

Инфокоммуникация тармоғи йўналишидаги кўп изланишларда ахборот қайта ишлаш воситаларидаги жараёнлар алоҳида, транспорт тармоғидаги ахборот оқимини узатиш жараёнлари алоҳида тадқиқ қилинади.

Мураккаб структурали инфокоммуникация тармоғи шароитида (яъни, мураккаб структурали гетероген муҳит шароитида) унинг таркибига кирувчи тармоқ қурилмалари ва алоқа каналлари ёрдамида ўзаро боғланган ҳар хил аппарат ва дастурий таъминотлар асосидаги ахборот қайта ишлаш воситалари (яъни, серверлар, компьютерлар ва х.к.) негизида ягона ресурс шакллантирилаётганида, албатта, ресурс тақдим этишга мўлжалланган компьютер ва бошқа тармоқ қурилмаларининг ва алоқа каналларининг параметрлари ҳисобга олиниши керак.

Кириш сатҳи инфокоммуникация тармоғининг энг пастки сатҳи ҳисобланади ва унинг асосий вазифаси – нисбатан тор доирадаги махсус аппарат-дастурий воситаларда кенг миқёсдаги фойдаланувчиларнинг техник воситаларидан келадиган ҳар хил турдаги ва катта ҳажмдаги ахборот оқимлари йиғилади ва қайта ишланиб, IP пакетларига айлантирилади ва транспорт тармоғи воситаларига тақдим этилади.

Кириш сатҳини ўз навбатида инфокоммуникация тармоғига ўхшаб, бир нечта поғоналарга бўлиб таҳлил қилиш мумкин.

Пастки сатҳдага марказларда жойллаштирилган коммутаторлар кўп мингли абонент алоқа каналларидан келаётган ҳар хил маълумотларни мультиплекслайди (яъни, бирлаштиради) ва юқори сатҳ коммутаторларига узатади, улар ўз навбатида маълумотларни қайта ишлаб транспорт сатҳи воситаларига узатади.

Умуман, кириш сатҳи тўртта компонентадан таркиб топади:

- шлюзлар ёрдамида транспорт сатҳига уланадиган терминал восита-лари;
- шлюзларга боғланмасдан, тўғридан – тўғри транспорт воситаларига боғланадиган терминал воситалари;
- ҳар хил турдаги шлюз воситалари;
- кириш коммутаторлари нинг воситалари
- ҳар хил узатиш қобилиятига эга алоқа каналлари.

Терминал воситалар – пакет коммутацияси асосидаги тармоқларда ишлашга мўлжалланган маълумот, товуш ва мультимедиа хизматларидан фойдаланишни таъминлайдиган фойдаланувчи қурилмаси;

Ушбу восита транспорт тармоғи воситаси билан тўғридан-тўғри ёки шлюз қурилмаси орқали мулоқотда бўлиши мумкин (1 - расм).

Шлюз воситалари канал коммутацияси режимидаги сигналларни па-кетли тармоқ ахборотларига ҳамда транспорт тармоғи пакетларини бирламчи сигналларга ўзгартириб беради.

Шлюзлар траспорт тармоғи в воситалари ва терминаллар ўртасида бўлиб, уларнинг ўзаро боғланишларини таъминлайди. Бундай вазифа махсус протокол ва интерфейслар ёрдамида бажарилади.

Кириш тармоғининг битта канали орқали бир неча хил хизматлар тақдим этилиши мумкин: интернетга кириш, электрон почта хизматидан фойдаланиш ва б., виртуал хусусий тармоқ хизматларини ташкил этиш, пакет коммутацияли телефон алоқани тақдим этиш (яъни, IP-телефония), видео сигналларини IP тармоғи орқали узатиш (яъни, IPTV ни ташкил этиш), тақсимланган компьютер тармоқлари ресурсларига кириш)ва б.

Шундай қилиб, битта канал орқали ҳар хил турдаги ахборот оқимлари ўтиши мумкин.Шундай қилиб, инфокоммуникация тармоғида сифатли маълумот узатиш ва қайта ишлаш жараёнларини ташкил этиш кириш сатҳи терминал қурилмаси, шлюз воситалари ва алоқа каналларининг ишончли фаолиятига боғлиқ бўлади. Кириш сатҳида маълумот узатилишининг умумлаштирилган схемаси 14 расмда келтирилган.

Кириш сатҳининг ишончлилик даражаси ундаги воситаларининг ишончлилик коэффициентларини кўпайтмасига тенг, яъни

$$K_{т}^{кс} = \prod_{j=1}^{4} K_{т}^{j} . \quad (1)$$

Тайёргарлик коэффициенти статистик маълумотлар асосида қуйидаги формула негизида ҳисобланади

$$K_{г}=T_0/(T_0+T_{т}) , \quad (2)$$

бунда T_o- маълум бир вақт оралиғида воситанинг ўртача тўғри ишлаган вақти оралиғи; $T_{т}$ - маълум бир вақт оралиғида воситани ишга яроқсиз бўлган вақтининг ўртача қиймати.

Маълум бир вақт оралиғида воситанинг ўртача тўғри ишлаган вақти оралиғи қуйидаги формула асосида ҳисобланади:

$$T_o = \sum_{i=1}^{N} t_i / N , \quad (3)$$

Маълум бир вақт оралиғида воситани ишга яроқсиз бўлган вақтининг ўртача қиймати қуйидаги формула асосида ҳисобланади,

$$T_{т} = \sum_{i=1}^{N} t_{iпр} / N , \quad (4)$$

$t_{iпр}$ – i турдаги носозлик туфайли воситани ишламай турган вақти;

N – носозликлар сони.

Қуйида инфокоммуникация тармоғи кириш сатҳи воситаларининг ишончлилик даражасини ҳисоблаш алгоритми ишлаб чиқилган. Алгоритм ишлаши учун қуйидаги маълумотлар берилган бўлиши керак:

- кириш сатҳининг топологик схемаси, яъни ундаги терминал ва шлюзлар сони, уларни координаталари (яъни жойлаштирилган нуқталари), алоқа каналлари ва уларнинг узатиш қобилиятини белгилайдиган параметрлар;
- маълум бир вақт оралиғидаги носозликлар сони ва уларнинг вақтлари;
- воситаларнинг маълум бир вақт оралиғида ишонли ишлаган даврлари;
- ишончлиликни ошириш учун ажратилган маблағлар.

Масаланинг қўйилиши: кириш сатҳи носоз ишлаётган участкаларни аниқлаш ва берилган маблағни уларнинг ишончлилигини ошириш йўлида ишлатиб, кириш сатҳининг ишончлилигини ошириш талаб этилади.

Маслани ечимини амалга ошириш қуйидаги кетма-кетликда бажарилади.

Берилган маълумотларга асосан (3), (4) формулалар асосида берилган вақт оралиғида воситаларнинг (терминал, шлюз ва бошқа воситаларининг) ишончли ишлаш ва носозликларининг ўртача вақтлари ҳисобланади.

Олинган натижалар негизида (2) формула асосида ҳар бир восита учун тайёргарлик коэффициентининг қиймати ҳисобланади.

(1) формула билан кириш сатҳининг умумий ишончлилик даражаси аниқланади.Ишончлилиги паст восита аниқланади ва унинг параметрлари ажра-тилган маблағ ёрдамида яхшиланади.

Алгоритм берилган статистик маълумотлар негизида топологик схеманинг ишонлилигини ошириш мақсадида ишлатилган.

АНАЛИЗ КОМПОНЕНТОВ СЕТИ И УСЛУГ IPTV

Ғ.А. Тангриберганов (ТУИТ, магистрант)

Интерактивное телевидение IPTV является наиболее сложным и интересным из всех новых видов вещания. Оно предоставляет телезрителю самые невероятные возможности активного участия в телепередачах — от ответов на вопросы в режиме онлайн до участия в шоу с помощью своего виртуального образа. Характерной особенностью цифрового IPTV является, наряду с предоставлением абоненту интерактивного видеоконтента, высокое качество изображения (т. е. телевидение высокой четкости - HDTV) и дополнительные услуги для зрителя, позволяющие ему через обратный канал связи активно взаимодействовать с системой IPTV и оказывать влияние на то, что происходит на экране. Функции интерактивности реализуются с помощью пульта дистанционного управления или интерактивной клавиатуры через клиентский терминал STB.

Известные услуги IPTV можно разделить на 3 большие группы: Телевизионные сервисы и PVR сервисы; 2. Услуги VoD; 3. Интерактивные сервисы. К первой группе относятся такие услуги как: BTV, EPG, SO, NPVR, PLTV, Instant PVR, TSTV. Они включают в себя как классическую услуги вещания телевизионных каналов, так и реализуемые только в IPTV услуги записи и повторного просмотра понравившейся телепередачи.

BTV – Broadcast Television – вещание телевизионных каналов по IP сети. EPG – Electronic Program Guide – электронная программа передач. NPVR – Network Personal Video Recorder – сетевой видеомагнитофон – заказ «записи» будущих программ через EPG. SO – Start Over – перезапуск программ – возможность просмотра текущей телепередачи сначала. PLTV – Pause Live TV - пауза прямого эфира. TSTV – Time-shift TV – телевидение со сдвигом во времени.

К услугам «Видео по требованию» можно отнести: VOD, SVOD, NVOD. Базовой услугой является VOD – Video on Demand – Видео по запросу. Пользователь может выбрать любой фильм, имеющийся в видеотеке и купить его на определенный период времени. SVOD – Subscription Video on Demand – видео по запросу по подписке. Позволяет оплатить абоненту неограниченный доступ к определенной категории VOD контента. NVOD – Near Video on Demand – виртуальный кинозал, трансляция видеоконтента по расписанию в широковещательном режиме (multicast).

Multicast трафик (групповая передача пакетов) используется для передачи потокового видео, когда необходимо доставить видео-контент неограниченному числу абонентов, не перегружая сеть. Это наиболее часто используемый тип передачи данных в IP-TV сетях, когда одну и ту же программу смотрят большое число абонентов.

На сегодняшний день на рынке телекоммуникаций ведущими компаниями производителями и разработчиками оборудования и ПО представлен ряд решений IPTV, отвечающий всем заявленным требованиям со стороны операторов связи. Несмотря на многообразие предлагаемых решений можно однозначно выделить ряд компонентов, составляющих типовой комплекс IPTV. Основными компонентами комплекса IPTV являются:

Сеть передачи можно построить разными способами, базовые требования можно сформулировать следующим образом:

- достаточная полоса пропускания — это от 4 Mbps для MPEG2 и от 2,5 Mbps для MPEG4. Для получения приемлемого качества изображения на среднестатистическом телевизоре.
- поддержка Multicast во всей сети, обязательное условие для реализации услуг IPTV.

- сквозная поддержка механизмов QoS. Для расчета ресурсов полосы пропускания. Если используется достаточная полоса пропускания, услуга работает, но необходимо учитывать приоритетный трафик.

Головная станция и узел кодированияДля удобства головная станция и узел кодирования территориально находятся на одной площадке и осуществляют прием, преобразование сигналов от различных источников и формирование потоков IP-multicast / IP-unicast.

Компоненты Головной станции:

- Антенный пост – обеспечивает прием сигналов от эфирных станций и спутников;
- Цифровые спутниковые приемники – дескрипторы – обеспечивают раскодирование цифровых сигналов, полученных с Антенного поста и передачу материалов Стримеру / мультиплексору;
- Узел цифрового кодирования – обеспечивает MPEG-кодирование аналоговых и цифровых сигналов и передачу материалов Стримеру / мультиплексору;
- Стример / мультиплексор - ключевой элемент Головной станции, обеспечивает мультиплексирование материалов и IP-вещание таким образом, что каждый канал имеет свой уникальный адрес и порт IP вещания.

Подсистема Видео по требованиюВ задачу подсистемы VOD входит запись и проигрывание по запросу пользователя видеоматериалов. Основными компонентами системы VoD являются:

- Центральный узел – аппаратно-программный комплекс, расположенный, как правило, в «центре» сети в непосредственной логической близости к системе условного доступа и головной станции.
- Система управления контентом – программное обеспечение, управляющее видеосерверами и распределением контента.
- Видеосервер – аппаратно-программный комплекс, устанавливаемый для обслуживания групп пользователей в определенной территории, например, в пределах одного узла агрегации.

Сервисная платформа Middleware Главную роль в реализации управления услугами и сервисами IPTV выполняет подсистема управления комплексом и услугами Middleware. Как правило, типовые Middleware реализуют два способа управления услугами и сервисами: непосредственно пользователем (абонентом), либо оператором услуг (администратором).

В первом случае абонент с помощью интерфейса пользователя, выводимого на экран телевизора через абонентский приемник, может изменять перечень услуг. Интерфейс управления услугами для абонента позволяет выбирать услуги из перечня, заранее заданного в системе IP-телевидения. Как правило, такая возможность находится в разделе Middleware «Личный кабинет» и защищена паролем. Абоненту предлагается весь перечень услуг и прайс-лист на них.

После внесения изменений в перечень услуг абонент получает вновь заказанные услуги либо сразу, либо через промежуток времени, необходимый на обновление ключей при использовании систем условного доступа. Информация об изменении перечня услуг будет доступна в детализированном счете абонента. Кроме того, биллинговая система может списывать некоторую сумму за подключение и отключение услуг, если это предусмотрено договором оказания услуг абоненту. Middleware – программно-аппаратный комплекс, который обеспечивает управление всеми компонентами решения IPTV, а также служит для упрощения задач администрирования и управления предоставляемыми услугами. Middleware позволяет осуществлять:

- Авторизацию абонента;
- Формирование программы передач EPG;
- Формирование интерфейса и инструментов управления решением IPTV;

- Взаимодействие с системами CAS, VOD, головной станцией, STB- устройствами;
- Взаимодействие с биллинговыми системами и системами поддержки бизнеса оператора связи.

STB (Set-top-Box) - абонентское устройство, является связующим звеном между системами формирования, доставки аудио- и видеоматериалов, и телевизором абонента. STB – это миникомпьютер с операционной системой, web-браузером, Mpeg декодером. Устройство должно быть интегрировано под конкретный проект, для взаимодействия со всеми компонентами системы.

Подсистема условного доступа (Conditional Assess System) Система условного доступа - техническое средство защиты аудиовизуальных и других сообщений и материалов, распространяемых в составе ТВ программы по эфирным, кабельным и спутниковым сетям связи. Также CAS позволяет разграничивать доступ пользователя к мультимедийным услугам, соблюдать авторские права, обеспечивать защиту контента от несанкционированного доступа/копирования.

КАЧЕСТВО ВОСПРИЯТИЯ В IPTV

Ғ.А. Тангриберганов (ТУИТ, магистрант)

На данный момент научно-исследовательские группы ITU-T определяют качество восприятия QoE (Quality of Experience) основным фактором, влияющим на выбор абонента. IPTV QoE представляет собой степень удовлетворённости пользователей от предоставляемых им видео сервисов. Восприятие абонентами качества систем IPTV должно быть равноценным или даже превосходить современные кабельные или спутниковые ТВ сервисы, в противном же случае Провайдеры Услуг подвергаются риску сокращения своей абонентской базы. Данный фактор определяется не только параметрами сети или качеством предоставляемого контента, но также удобством использования системы и ожиданиям пользователя. Для использования в системах мониторинга параметр QoE должен вычисляться с использованием измеряемых параметров, однако на данный момент не существует математической модели, которая бы учитывала субъективные параметры, влияющие на QoE в системе IPTV.

Качество восприятия (QoE) – это общий показатель качества приложения или сервиса, воспринимаемый субъективно конечным пользователем. Это означает, что QoE является более сложным понятием по сравнению с качеством обслуживания QoS (Quality of Service). QoE включает влияние всех возможных факторов от источника до конечного пользователя. Кроме того, на данный параметр также влияют время ожидания каждого пользователя и содержание контента.

В организациях стандартизации (ETSI, ITU) рассматриваются следующие факторы, влияющие на качество восприятия:

1. Качество передачи данных (минимальная скорость передачи данных, максимальный уровень потери пакетов);
2. Функции интерактивного контроля (время переключения, возможность выбора метаданных, электронное телевизионный гид, время отклика, доступность);
3. Оступность для восприятия (дактилология, чтение по губам, качество контента, такие как качество видео и звука).

Так как качество восприятия определяется «субъективно конечным пользователем», различия в личностном восприятии и предпочтении приведут к тому, что параметры качества восприятия, полученные от разных людей, могут отличаться. Таким образом, измерения QoE, как правило, проводятся с использованием данных группы пользователей. QoE требования для видео и аудио контента, первоначально могут быть определены при помощи субъективной шкалы абонентского обслуживания, таких как MOS (Mean Opinion Score) или DSCQS (The Double – Stimulus Continuous Quality-Scale

method). Поскольку такие исследования субъективных показателей качества восприятия являются трудоемким и дорогостоящим процессом, то необходимо на основании исследований, проведенных для калибровки шкалы QoE, найти способ оценки QoE при использовании объективных измерений.

Большинство характеристик сети передачи данных влияет на QoE. Например, используемый кодек и скорость передачи данных, разрешение видеоданных источника, потеря или искажение информации, задержки. Взаимовлияние между качеством видео контента, используемого кодека и скорости передачи, повреждением определенных битов и/или потерянных пакетов способствуют высокой изменчивости качества восприятия видео на стороне конечного пользователя.

Существуют и другие факторы, которые могут влиять на оценку зрителя. Некоторые из них влияют на восприятие качества, такие как культурный фон, мотивация, внимание, эмоциональное состояние и так далее. Прямая оценки QoE будет исключать эти факторы, так как они обычно не могут контролироваться оператором сотовой сети и не влияют на требования к оборудованию.

Существуют также факторы, влияющие на решение зрителя о приемлемости изображения. Они включают такие вещи, как опыт работы с конкретной системой и ее уровнем качества, стоимость услуги и предоставляемых особых преимуществ для пользователя. Приемлемость не эквивалентна QoE. Изображение с низким разрешением будет иметь более низкий показатель QoE, чем изображение с высоким разрешением, но это может быть вполне приемлемым для некоторых приложений и услуг, в зависимости от конечного устройства, физического размера дисплея, и целей, для которых оно используется.

Согласно рекомендации ITU-TG.1080, на QoE влияют следующие параметры (рис.1): объективные (параметры качества обслуживания QoS); субъективные (человеческий фактор).

Отношение между QoE и QoS может быть оценено эмпирически. После нахождение такого соответствия, эти результаты могут быть использованы следующим образом.

По заданному QoS можно принципиально оценить ожидаемое QoE и, наоборот, при необходимости обеспечить определенное QoE, можно принципиально оценить требуемые сетевые характеристики. Чтобы обеспечить надлежащее качество полученной абонентом услуги, QoE параметры необходимо рассматривать для каждого из сервисов. Эти параметры необходимо учитывать на стадии проектирования системы на каждом уровне модели OSI.

Качество восприятия станет важным фактором успеха на рынке широкополосных услуг и, как ожидается, будет ключевым параметром для сравнения различных сервисов, так как для пользователя важно, насколько сервис отвечает его требованиям. Также данный параметр будет использоваться и на этапе эксплуатации сети для сравнения результирующих показателей при развертывании систем различных производителей и для оптимизации существующей сети.

ПОСТРОЕНИЕ ДИАГНОСТИЧЕСКОЙ ЭКСПЕРТНОЙ СИСТЕМЫ НА ОСНОВЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

Т.Қ. Тоштемиров (ТУИТ, 2-курс магистрант)

Рассмотрим подход построения модели процесса диагностирования СПД в условиях частичной неопределенности. В таких случаях целесообразным является использование теории нечетких множеств и ЭС (экспертных систем).

Для построения искомой модели диагностирования следует сформировать минимальное (необходимое и достаточное) признаковое пространство симптомов и

диагнозов (в том числе на основе эвристических знаний экспертов). Это позволит упорядочить построение БЗ (базы знаний) диагностической ЭС, избегая введения мало информативных правил, которые устанавливают связи, совпадающие с вычисленными правилами на основе модели, т.е. избежать неэффективного разрастания БЗ.

В качестве БЗ можно рассматривать правила продукции, которые устанавливают связи между получаемыми симптомами (или их комбинаций в случае композиционного элемента) и предполагаемым /диагнозом В случае нечеткой модели ОД (объекта диагностики) предполагается использование экспертной информации с вычисляемыми значениями функций принадлежности элементов правил продукций При диагностике для каждой комбинации симптомов вычисляются нечеткие функции принадлежности неисправностей (на любую глубину композиции) и ищется комбинация исходов тестирования с наиболее вероятным исходом неисправности.

Методология эффективного построения экспертных систем включает *в* себя совокупность способов представления и использования знаний, а также перенос образа действий эксперта *я* систему'.

Достоинство теории нечетких множеств в аспекте создания экспертных систем заключается в неопределенности (нечеткости) сущности языка, так как при построении модели мышления эксперта нельзя абстрагироваться от роли и сущности языка его мыслей. Благодаря оперированию с лингвистическими переменными теория нечетких множеств позволяет создавать достаточно точные модели мышления человека. Реальным подтверждением эффективности создания и внедрения систем на основе теории нечетких множеств служат многочисленные уже работающие системы. Рассмотрим некоторые из них.

Система DART оказывает помощь при диагностировании неисправностей компьютерных систем, используя информацию о конструкции диагностируемого устройства. Система работает непосредственно с информацией о структуре и предполагаемом поведении устройства и оказывает помощь при поиске проектных недочетов в заново создаваемых устройствах,

Система CRIB предназначена для оказание помощи разработчикам и обслуживающему персоналу компьютеров при обнаружении неисправностей в аппарату ре и программном обеспечении компьютера. CRIB сопоставляет это описание с базой данных об известных неисправностях. Последовательно сопоставляя всё большие группы симптомов с вводимым описанием: CRIB выявляет блок, который подлежит ремонту или замене. Если после ремонта или замены неисправность не устранена, система автоматически возвращается к точке принятия последнего решения я пытается найти другое решение, В системе CRIB знания и эвристики по диагностике неисправностей аппарату ры и программного обеспечения представлены в виде набора пар «симптом - действие», где действие направлено на устранение симптома. CRIB моделирует диагностируемую машину в виде простой иерархии блоков в семантической сети,

Система COMPASS анализирует сообщения о состоянии телефонных коммутаторов GTE No.2 EAX Switch и предлагает, какой вид технического обслуживания нужно провести. Система рассматривает сообщения о состоянии, описывающие сбои, которые возникают 8 коммутаторе при операциях вызова абонентов. Затем она выделяет группу сообщений, которые, скорее всего, вызваны общей неисправностью, определяет возможные конкретные неисправности коммутатора и предлагает мероприятия но техническому обслуживанию для подтверждения и устранения неисправностей Система воплощает знания и эвристики лучшего знатока коммутаторов и объединяет знания об устройстве конкретных коммутаторов, их неисправностях, сообщениях о состоянии и возможном техническом обслуживании.

Система FOREST локализует и диагностирует неисправности я электронном оборудовании. Система дополняет возможности обнаружения и локализации неисправностей, которыми обладают применяемые ныне диагностические программы для

автоматизированного тестирующего оборудования. Знания FOREST включают эмпирические правила, заимствованные у инженеров-экспертов , а также общие принципы отладки электронных схем. Эти знания кодируются в виде правил с коэффициентами уверенности и со средствами объяснения.

Система BDS оказывает помощь при выявлении неисправных модулей в большой сети. Эта система использует показания испытательной аппаратуры, чтобы обнаружить неисправные печатные платы или другие детали, смонтированные в стойках, из-за которых могла возникнуть неисправность. BDS основывает свой диагноз как на стратегиях зксперта-диагноста, так и на знаниях о структуре, функциях и причинных связях компонентов электронного устройства. BDS реализована ка языке LES и использует представление знаний, основанное на правилах, и управление посредством обратной цепочки рассуждений.

На основании приведенных примеров применения теории нечетких множеств можно утверждать, что использование данной теории может упростить создание эффективной системы диагностики сетей передачи данных.

АНАЛИЗ МЕТОДОВ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

А.А. Турдахматов (ТУИТ, магистрант)

Как известно основными целями маршрутизации в сетях передачи данных являются**:**

- минимальная задержки пакета при его передаче от отправителя к получателю;
- максимальная пропускная способностиьсети;
- надежность доставки пакета адресату;
- минимальная стоимость передачи пакета адресату.

Задача маршрутизации в сетях решается при условии, что кратчайший маршрут, обеспечивающий передачу пакета за минимальное время, зависит от топологии сети, пропускной способности линий связи, нагрузки на линии связи. Топология сети изменяется в результате отказов узлов и линий связи и при развитии (подключении новых узлов и линий связи). Для выбора оптимального маршрута каждый узел связи должен располагать информацией о состоянии сети в целом - всех остальных узлов и линий связи.

При решении задачи маршрутизации могут использоваться данные о состоянии нагрузки, запаздывающие (из-за конечной скорости передачи информации) по отношению к моменту принятия решения о направлении передачи пакетов.

Следовательно, во всех случаях алгоритмы маршрутизации выполняются в условиях неопределенности текущего и будущего состояний сети.

Алгоритмы маршрутизации могут быть классифицированы по типам:

- Статистическими или динамическими
- Одномаршрутными или многомаршрутными
- Одноуровными или иерархическими
- С интеллектом в главной вычислительной машине или в роутере
- Внутридоменными и междоменными
- Алгоритмами состояния канала или вектора расстояний

Распределение статических таблиц маршрутизации устанавливается администратором сети до начала маршрутизации. Оно не меняется, если только администратор сети не изменит его. Алгоритмы, использующие статические маршруты, просты для разработки и хорошо работают в окружениях, где трафик сети относительно предсказуем, а схема сети относительно проста.

Так как статические системы маршрутизации не могут реагировать на изменения в сети, они, как правило, считаются непригодными для современных крупных, постоянно изменяющихся сетей.

Динамические алгоритмы маршрутизации подстраиваются к изменяющимся обстоятельствам сети в масштабе реального времени. Они выполняют это путем анализа поступающих сообщений об обновлении маршрутизации. Если в сообщении указывается, что имело место изменение сети, программы маршрутизации пересчитывают маршруты и рассылают новые сообщения о корректировке маршрутизации. Такие сообщения пронизывают сеть, стимулируя роутеры заново прогонять свои алгоритмы и соответствующим образом изменять таблицы маршрутизации. Динамические алгоритмы маршрутизации могут дополнять статические маршруты там, где это уместно. Например, можно разработать "роутер последнего обращения" (т.е. роутер, в который отсылаются все не отправленные по определенному маршруту пакеты). Такой роутер выполняет роль хранилища не отправленных пакетов, гарантируя, что все сообщения будут хотя бы определенным образом обработаны.

Некоторые сложные протоколы маршрутизации обеспечивают множество маршрутов к одному и тому же пункту назначения. Такие многомаршрутные алгоритмы делают возможной мультиплексную передачу трафика по многочисленным линиям; одно-маршрутные алгоритмы не могут делать этого. Преимущества многомаршрутных алгоритмов очевидны - они могут обеспечить значительно большую пропускную способность и надежность.

Некоторые алгоритмы маршрутизации оперируют в плоском пространстве, в то время как другие используют иерархии маршрутизации. В одноуровневой системе маршрутизации все роутеры равны по отношению друг к другу. В иерархической системе маршрутизации некоторые роутеры формируют то, что составляет основу (*backbone* - базу) маршрутизации. Пакеты из не базовых роутеров перемещаются к базовым роутерам и пропускаются через них до тех пор, пока не достигнут общей области пункта назначения. Начиная с этого момента, они перемещаются от последнего базового роутера через один или несколько не базовых роутеров до конечного пункта назначения.

Системы маршрутизации часто устанавливают логические группы узлов, называемых доменами, или автономными системами (AS), или областями. В иерархических системах одни роутеры какого-либо домена могут сообщаться с роутерами других доменов, в то время как другие роутеры этого домена могут поддерживать связь с роутеры только в пределах своего домена. В очень крупных сетях могут существовать дополнительные иерархические уровни. Роутеры наивысшего иерархического уровня образуют базу маршрутизации.

Основным преимуществом иерархической маршрутизации является то, что она имитирует организацию большинства компаний и, следовательно, очень хорошо поддерживает их схемы трафика. Большая часть сетевой связи имеет место в пределах групп небольших компаний (доменов). Внутри доменным роутерам необходимо знать только о других роутерах в пределах своего домена, поэтому их алгоритмы маршрутизации могут быть упрощенными. Соответственно может быть уменьшен и трафик обновления маршрутизации, зависящий от используемого алгоритма маршрутизации.

Некоторые алгоритмы маршрутизации предполагают, что конечный узел источника определяет весь маршрут. Обычно это называют маршрутизацией от источника. В системах маршрутизации от источника роутеры действуют просто как устройства хранения и пересылки пакета, без всякий раздумий отсылая его к следующей остановке.

Другие алгоритмы предполагают, что главные вычислительные машины ничего не знают о маршрутах. При использовании этих алгоритмов роутеры определяют маршрут через объединенную сеть, базируясь на своих собственных расчетах. В первой системе, рассмотренной выше, интеллект маршрутизации находится в главной вычислительной машине. В системе, рассмотренной во втором случае, интеллектом маршрутизации наделены роутеры.

Компромисс между маршрутизацией с интеллектом в главной вычислительной машине и маршрутизацией с интеллектом в роутере достигается путем сопоставления оптимальности маршрута с непроизводительными затратами трафика. Системы с интеллектом в главной вычислительной машине чаще выбирают наилучшие маршруты, т.к. они, как правило, находят все возможные маршруты к пункту назначения, прежде чем пакет будет действительно отослан. Затем они выбирают наилучший маршрут, основываясь на определении оптимальности данной конкретной системы. Однако акт определения всех маршрутов часто требует значительного трафика поиска и большого объема времени. Внутри доменные или междоменные алгоритмы**.** Некоторые алгоритмы маршрутизации действуют только в пределах доменов; другие - как в пределах доменов, так и между ними. Природа этих двух типов алгоритмов различная. Поэтому понятно, что оптимальный алгоритм внутри доменной маршрутизации не обязательно будет оптимальным алгоритмом меж доменной маршрутизации.

Алгоритмы состояния канала или вектора расстояния. Алгоритмы состояния канала (известные также как алгоритмы "первоочередности наикратчайшего маршрута") направляют потоки маршрутной информации во все узлы объединенной сети. Однако каждый роутер посылает только ту часть маршрутной таблицы, которая описывает состояние его собственных каналов. Алгоритмы вектора расстояния (известные также как алгоритмы Бэлмана-Форда) требуют от каждого роутера посылки всей или части своей маршрутной таблицы, но только своим соседям. Алгоритмы состояния каналов фактически направляют небольшие корректировки по всем направлениям, в то время как алгоритмы вектора расстояний отсылают более крупные корректировки только в соседние роутеры.

ТАРМОҚ ХАВФСИЗЛИГИНИ МИҚДОРИЙ БАҲОЛАШ

Б.М. Умирзаков (ТАТУ, ассистент)

Халқаро электроалоқа иттифоқи (ХЭАИ)ни тадқиқот комиссияси ИК 17 (Хавфсизлик, тиллар ва электралока дастурий таъминоти) ҳозирги кунда учта ўзаро кам даражада боғлиқ бўлган соҳаларда изланишлар олиб бормокда:

1) Электралока тизимларида хавфсизлик;
2) Маълумот тизимлари ва очиқ тизимлар ўзаро алоқасининг бошқа аспектлари, j
3) Формал (формал) тиллар ва электралоқа учун дастурий таъминот.

Ўрганишнинг биринчи соҳасини асосий деб ҳисоблаш мумкин.

Хавфсизлик ҳақида ХЭАИ нинг юздан ортиқ тавсияномаси мавжуд. Бироқ электралоқа тармоқларининг ва ахборот тармоқларнинг янги муҳитида пайдо бўлган долзарб масалалар ўрганиш ҳамда ечимини топишни талаб қилади.

Электралоқа тармоқларининг ва узатилаётган маълумотларнинг хавфсизлигини таъминлаш алоқа операторлари учун муҳим масалалардан бири бўлиб қолмоқда. Бу фойдаланувчиларнинг талаблари ошиб бориши билан боғлиқ, айниқса янги иловаларни қўлловчилар учун, масалан телесавдо, телебанкинг, телебизнес, телетиббиёт.

Учта йўналишдаги ҳимояни мисол сифатида кўриб ўтамиз:

1. Алоқа тармоқларини фроддан ҳимоялаш

Фрод (электралоқа хизматларидан фирибгарлик йўли билан фойдаланиш) алоқа операторларига иқтисодий зарар келтиради. Фроднинг жуда кўп турлари мавжуд. Унинг янги турлари пайдо бўлмоқда. Операторлар учун зиён етказувчилар (фрод манбалари) фақат фойдаланувчилар эмас, балки қўшни алоқа операторлари ҳам бўлиши мумкин. Фрод билан курашиш воситалари бозорда турли туман бўлгани билан улар ёки мураккаб, ёки самарадор эмас.

Зарур халқаро Тавсиялар фроднинг ўзига хос томонларини ҳисобга олган тармоқ хавфсизлигини таъминловчи мавжуд умумий тамойилларни аниқлаштиради, бу

электралоқа хавфсизлиги учун махсус хавф келтириб чиқаради.

2. Кенг тарқалган сенсор тармоқлари хавфсизлиги

Кенг тарқалган сенсор тармоқлари (Ubiquitous Sensor Network, USN) кейинги авлод тармоқлари (NGN) дан кейинги электралоқа тармоқлари ривожининг кейинги босқичи сифатида қаралади. Асосий янги омил сифатида «машина-машина» (M2M) алоқасининг кескин кўпайиши эътиборга олинади. Сенсорлар ва бошқа датчиклар, ишловчи механизмлар, қайта ишлашнинг автоматик воситалари, маълумотларни сақлаш ва бошқа «машиналар» электралоқа тармоқлари учун «инсон трафиклари» дан ўзиб кетувчи янги трафикларни яратади.

Изланишларнинг бу янги йўналиши уч асосий қисмга эга:

-тармоқ масалалари;

-алоқанинг мультимедия ва мономедия хизматлари, улар базасида иловалар ва терминаллар;

-кенг тарқалган сенсор тармоқлари хавфсизлиги.

Кенг тарқалган сенсор тармоқларига биринчи қадам сифатида идентифицирланган радиобелги (радиобирка) лар маълумотларини узатиш (радиоинтерфейсли биркалар-белгилар)ни кўриб чиқишимиз мумкин, масалан «радиочастотали идентификация» (Radio-Frequency Identification, RFID) белгилари тизими. Бу ишлардаги хавфсизлик масалаларини ИК 17 га топшириш мақсадга мувофиқ.

3. IP-телевидение (IPTV) тизимларида хавфсизлик

Ҳозирги вақтда МСЭ-Т да глобал стандартларни яратиш мақсадида IP-телевидениени (IPTV) тезкор ўрганиш бошланди. Телевизион кўрсатувлардан ташқари бошқа видеохизматлар ҳам эътиборга олинади (масалан, талаб бўйича кинофильмлар ва видеоўйинлар). Изланишларни бу истиқболли йўналиши бир қанча асосий қисмларни ўз ичига олади:

-тармоқ масалалари (кейинги авлод тармоқлари, кабель телевидение тармоқлари ва бошқа тармоқлар учун);

-тармоқда хизмат кўрсатиш сифати ;

-хизматлар характеристикаси, фойдаланувчилар учун хизмат кўрсатиш сифати ва терминаллар масаласи;

-маълумотлар учун хавфсизлик.

IP тизимларида хавфсизлик масалалари-телевидениями ИК 17 га топшириш мақсадга мувофиқ.

Ҳозирги пайтгача хавфсизлик миқдорий баҳога эга эмас, аммо хизмат кўрсатиш сифати мезонларининг катта қисми (QoS) миқдорий баҳолаш усулларидан иборат. Масалан, бу тезликка, тўғриликка ва тайёрлигига боғлиқ.

Бир қатор ХЭАИ тавсияларида хавфсизликнинг турли даражаларини амалга ошириш кўзда тутилган. Масалан, аутентификация абонентлик рақами, пароли ёки криптографик ҳимояга эга рақамли имзо базасида амалга оширилиши мумкин. Натижада учта турли даражадаги аутентификация ҳосил бўлади, уларни шартли равишда «оддий», «ўртача» ва «юқори» деб номлаш мумкин. Лекин уларнинг миқдорий баҳоси йўқ.

ХЭАИ Е.408 тавсияномасида қўшимча II) хавфсизлик чораларининг учта тури таклиф қилинган. Функционал синфлари хавфсизлик чоралари йиғиндиси билан фарқланади. Бу функционал синфлар хавфсизликнинг турли даражасини таъминлайди, улар «минимал», «базавий» ва «такомиллашган» деб номланади. Аммо уларнинг миқдорий баҳоси йўқ.

2007 йил ноябрь ойида тасдиқланган ХЭАИ Х.1123 тавсияномасида хавфсизликнинг уч сиёсати ва ҳаракатланувчи алоқадаги хавфсизликнинг беш даражасидан бирини танлаш имкониятлари таклиф қилинган. Аммо уларнинг миқдорий баҳоси йўқ.

Электралоқада ахборот хавфсизлигини миқдорий баҳоси масаласи долзарб бўлиб

турибди. Миқдорий баҳолаш усулларининг мавжудлиги қуйидаги имкониятларни бериши мумкин :

-ишлаб чиқаришда таклиф қилинган хавфсизликни таъминлаш воситаларини объектив қиёслаш ;

-хавфсизликнинг таъминланганлик даражаси бўйича кўрсатилаётган электралоқа хизматлари хизмат кўрсатиш сифати синфларини миқдорий аниқлаш (QoS) ;

-хавфсизликни ҳисобга олган ҳолда QoS синфларини нормага солиш;

-тармоқни лойиҳалаштиришда хавфсизликни таъминлаш воситаларини асосли танлаш;

- оператор томонидан амалга оширилгандан кейин ва эксплуатация шароитида хавфсизлик тизимини миқдорий текширувларини ўтказиш.

Алоқа тармоқларини вируслардан ҳимоя қилиш. Аввалам бор, агар ахборот ҳимоя қилинса, алоқа тармоқларини вируслардан ҳимоя қилишни нима кераги бор деган саволга жавоб берамиз.бу саволга жавоб ойдин.

Ҳозирги пайтда алоқа тармоқларининг барча асбоб-ускуналари (мультиплексорлар, демультиплексорлар, коммутаторлар, маршрутизаторлар, усилителлар, регенераторлар, бошқарув қурилмалари, сигнализация умумий канали тизимлари ва б.)ҳисоблаш техникаси асосида яратилган, шунинг учун уларга ҳам тармоқдан узатилаётган маълумотларга ўхшаб тармоққа кириб олган вируслар таъсир қилади.

Вируслар алоқа тармоқларига ахборотларга нисбатан кучлироқ таъсир кўрсатади, вируслар юқорида кўрсатилган қурилмалар гуруҳи операцион тизимини зарарлайди, бу кўп каналларнинг издан чиқишига олиб келади, бунинг оқибатида тармоқларнинг ҳимояси ахборотни ҳимоя қилишга нисбатан анча мураккаб бўлиб қолади.

Хавфсизлик тизимининг мураккаб архитектураси ҳамда хавфларнинг турли туманлигини эътиборга олган ҳолда хавфсизликни миқдорий баҳолашни ўрганиш мураккаб ва узоқ давом этувчи жараёндир. Бошланғич босқичида услубий (методик) масалалар ва вазифалар декомпозициясига фикрни жамлаш мақсадга мувофиқ бўлади .

Бу масалани ўрганишда манба материаллари сифатида В.О. Шварцманнинг «Методика количественной оценки защищенности информации от вирусов» (Электросвязь, 2007, № 9) номли мақоласини таклиф қилиш мумкин. Ушбу мақолада вируснинг таъсири фойдали маълумотларда хатоларнинг пайдо бўлиши сифатида қаралади. Миқдорий баҳолашни эса хатолар коэффициентини ўлчаш йўли билан ўтказиш таклиф қилинади .

Замонавий ахборот- коммуникацион муҳитни ҳисобга олган ҳолда санаб ўтилган йўналишлар бўйича ХЭАИ тавсияномаларини ишлаб чиқиш алоқа операторларига фойдали бўлади.

ТАРМОҚ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА ХИЗМАТ КЎРСАТИШ СИФАТИ МОНИТОРИНГИ

Б.М. Умирзаков (ТАТУ, ассистент)

Маълумот узатиш тармоқларини ишончли ва хавфсизлигини таъминлашнинг комплекс усуллари таклиф қилинади. ХЭАИ Х.805 тавсияномасида хавфсизликнинг 3 босқичидан фойдаланишни кўзда тутади:

- ўз таркибига ахборот узатиш қурилмаларини олувчи инфратаркиб хавфсизлик даражаси (маршрутизаторлар, коммутаторлар, серверлар), шунингдек улар орасидаги алоқа линиялари;
- сервис-провайдер мижозларга таклиф қилувчи хизматларни ҳимоялаш

принципларини ёритиб берувчи сервислар хавфсизлиги даражаси , масалан Интернетга кириш имконияти, сервис freephone, QoS, VPN ва ҳ.к;

- иловалар хавфсизлиги даражаси,сервис-провайдерлар, иловалар провайдерлари ёки алоқа операторлари томонидан мижозларга иловалар ҳимояланганлигини аниқлайди (FTP,web-сервислар томонидан, IP-телефония, электрон почта, электрон коммерция иловалари ва ҳ.к.). Бу босқичда ҳужумларнинг тўрт нишони ҳимояланганлигини таъминлаш кўриб чиқилади: илова фойдаланувчиси, илова провайдери, интегратор ва сервис-провайдер.

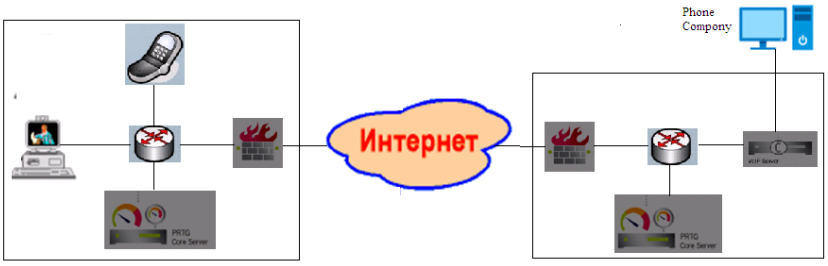
Тармоқни ишончлилигини таъминлашда мониторинг дастурлари муҳим ахамиятга эга. PRTG хизмат кўрсатиш сифати мониторингини ҳам амалга ошириш учун ўзининг QoS сенсорига эга. Шу жумладан Cisco IP Service Level Agreement (SLA) ҳам. Тармоқ параметрларини ўзгариши джиттер, пакетларни йўқолиши ёки пакетлар етиб келишининг кечикиши (PDV) одатда TCP(HTTP, SMTP) сервис баъзасида бироз кичик натижаларни кўрсатади. Бироқ UDP сервер базасида Voice over IP (VoIP) ва видео тасвирларни узатишда маьлумот пакетлари аниқлиги катта. VoIP алоқасида овоз сифати, қачонки UDP пакетлари вақтида етиб бормаса ёки пакетлари йўқотилса кескин тушиб кетади. Қоидага кўра хизмат кўрсатиш сифатини яхшилашда (VoIP да) джиттер ва пакетлар кечикишида кичик ўлчамлар ва пакетлар йўқолиши, иккиланган пакетлар ёки хато пакетлар нольга тенг бўлиши назарда тутилади. Хизмат кўрсатиш сифатини аниқлашда иккита сенсор ишлатилиши мумкин:

- QoS (Quality of Service) Sensor VoIP тармоқ параметрлари мониторинги тармоқ орасидаги боғланиш сифати натижалари билан мос келиши керак.
- QoS (Quality of Service) Round Trip Sensor VoIP тармоқ параметрлари мониторинги тармоқ орасидаги боғланиш сифати натижалари билан мос келиши керак. Трафиклар аниқ ўлчов асосида ўлчанади.
- Cisco IP SLA Sensor- VoIP тармоқ параметрлари мониторинги Cisco қурилмаларининг (viaSNMP) IPSLA натижалари билан мос келиши керак.

QoS (Quality of Service) Sensor - QoS Sensor тармоқ алоқаси сифатини монитор қилишда фойдаланиладиган қуйидаги ўлчов бирликларига эга:

- Джиттер RFC 3550 кўра: мс
- Пакетлар кечикишини ўзгариши RFC 3393 кўра: мс
- Пакетлар йўқотилиши: %
- Тартибдан ташқари пакетлар: %
- Иккиланган пакетлар: %

Ҳар қандай тармоқ боғланишини бошқарув қурилмаси орқали осонгина ҳар бир алоқанинг якунида алоқа сифатини текшириши мумкин. Бу мукаммал қурилма тармоқдаги VoIP овоз сифати ёки видео оқимидаги узилишни топади. Иккита қурилма яқинида ёки узоқда жойлашган ПКлар ўртасидаги алоқани хоҳлагандек монитор қилиш мумкин. Танланган локал тармоқда ПК қурилмалари PRTG асосида ишлаши бир томон оҳирида ишлатилиши мумкин. Ҳар қандай тармоқлараро экран пакет фильтрлари ёки Network Address Translation (NAT) тизимлар маршрути созланади, чунки UDP пакетлар аралаш қурилмаларда қўлланиши мумкин.



1 –расм. PRTG орқали хизмат кўрсатиш сифати мониторинги

Хизмат кўрсатиш сифатини функцияларини аниқлаб, хизмат кўрсатиш сифати даражаси тўғрисидаги (SLA) битимлар билан фойдаланувчининг истакларини ҳисобга олиш зарур. Хизмат кўрсатиш сифатини баҳолашда RSVP протаколи муҳим роль ўйнайди. Бу протакол асосий модуллардан бири ҳисобланади.Тармоқ ресурсларини бошқариш тизимини яратишда телекоммуникацион хизматларнинг интегралли (Int Serv) ва диффернциаллашган (Diffi Serv) турларини қўллаб, олиб борилган лойиҳа кутилган натижалар беради. IP да трафик оқимини категорияларига биноан уларга хизмат кўрсатишни расмийлаштирилиши ва компанияларни шу борадаги ишларидан фойдаланиб тармоқ ресурсларини бошқариш тизимини яратиш мумкин. Ҳар қандай тармоқ боғланишини бошқарув қурилмаси орқали осонгина ҳар бир алоқанинг якунида алоқа сифатини текшириши мумкин.

CHALLENGING ISSUES OF FOG COMPUTING IN BIG DATA PROCESSING IN TANDEM INTERNET OF THINGS

N.B. Usmanova (Phd of DCN and S)
A.X. Suyunov (TUIT, undergraduate student)

Cloud computing provides many benefits to clients in comparison with conventional purchase based own and run computing systems model. The major benefits of cloud computing over the traditional computing paradigm are the economic advantages and the absence of computer systems administrative tasks and associated costs. Users access the cloud services and pay for only the services accessed on a utility costing basis. Likewise, Cloud computing services are priced on a per unit time basis irrespective of how much of resources had been utilized. As all the hardware and software of computers are hosted in a remote data centre, which is owned and run by a service provider, customers could concentrate exclusively on their core business functions. Even the customers involved in computing related businesses such as software development, need not worry about purchasing their own hardware and software such as development platform or project management tools or maintaining them in a house or an office. Notwithstanding Cloud computing's advantages, it suffers from certain shortcomings as well. These shortcomings include the requirement of high bandwidth client access link, high latency, and security. These constraints have a significant effect on certain kinds of computing needs such as sensor networks and especially the Internet of Things (IoT) paradigm which envisages to have every device on the Internet. With the purpose of overcoming the limitations of Cloud computing mentioned above, new kind of cloud computing model has been proposed by researchers. In accordance with the model, devices which respond and process the client requests are hosted either at the edge of the local network or adjacent to it as opposed to being far away in a remote location in the middle of the Internet cloud. This kind of cloud computing model has been named as "Fog Computing".

The state-of-the-art cloud computing model "Fog Computing", which is introduced by the Cisco systems, is distinct from conventional Cloud Computing by a number of facets, namely, latency, jitter, the position of server nodes, the average distance between client and server, the security level, the type of connection, the extent of mobility, and conscience about location of a device. For instance, whilst the location of server nodes of Cloud computing located within the Internet, nodes of Fog Computing reside at the edge of the local network. Evidently, this allows shaving off the latency and achieving very low level of delay jitter in Fog Computing which, in turn, improves QoS because a tremendous number of server nodes are positioned within the local network with high bandwidth. Another noteworthy feature could be the support of mobility, in other words, the nodes of IoT along with other Fog Computing elements are aware of their position and due to their miniature dimensions can be moved easily. Besides, whilst Cloud computing uses several servers in a centralized area, Fog Computing implies a vast number of Fog Computing nodes distributed geographically in various locations. A further

distinctive features of Fog Computing are the operation on a network edge consuming less time and energy, less demand of throughput as every bit of data is aggregated at certain access point rather than transmitting through cloud, and the elimination of response time in tandem scalability issues owing to setting small servers called edge servers in the visible area to potential consumers. The emerging high quality multimedia service applications including distributed interactive games, video on demand, and streaming demand large data transfer rates with low delay, delay jitter and packet loss. So as to achieve this processing these applications closer to the end users is vital. Since cloud data centres are generally located within the Internet, it is difficult to manage these factors. Hence fog computing is the practical solution for this kind of performance sensitive applications.

Having taken the outstanding features of Fog Computing into consideration, a few prerequisites can be made so as to implement them. The first requirement could be a platform of Fog Computing maintaining IoT has to support rapid mobility patterns which might even require high throughput on demand over short period of time. Another requirement might be the support of systems requiring reliable sensing, analysis, control, and actuation, in scenarios subject to poor or unreliable connectivity to a remote network requiring very low latency. Finally, a Fog Computing platform designed for IoT should be able to manage a large amount of geographically distributed objects, which may generate abundant amount of data, which is also known as Big Data, requiring various levels of real-time analytics and data aggregation.

The provision of appropriate Quality of Service is metric of high importance for fog service and could be divided into four constituents, namely, connectivity, reliability, capacity, and delay. In a heterogeneous fog network, network relaying, partitioning and clustering provide new opportunities for reducing cost, trimming data and expanding connectivity. For example, an ad-hoc wireless sensor network can be partitioned into several clusters due to the coverage of rich-resource fog nodes. Xu, et al. (2010) propose an online association strategy which not only achieves a minimal bandwith, but efficiency in computational overhead. Likewise, the selection of fog node from end user will heavily affect the performance. A subset of fog nodes could be selected dynamically as relay nodes for optimization goals of maximal availability of fog services for a particular domain or a single user, with constraints such as delay, throughput, connectivity, and energy consumption. The reliability might be improved through periodical check-pointing to resume after failure, rescheduling of failed tasks or replication to exploit executing concurrently but check-pointing and rescheduling may not fit the hectic environment of fog computing since there will be latency, and cannot adapt to changes. Replication tends to be promising, though it relies on multiple fog nodes to work together. In order to achieve high bandwidth and efficient storage utilization, it is important to scrutinize how data are located in fog network since data locality for computation is essential. Albeit there are some research papers on cloud and sensor network, the problem poses new challenges in fog computing. For example, a fog node may need to compute on data which is distributed in several adjacent nodes. The computation cannot start before the finish of data aggregation, which definitely adds extra delay to services provided. In order to solve this, user mobility pattern and service request pattern can be used to place data on suitable fog nodes to either minimize operational expenses, the latency or to maximize the throughput. Big Data placement in fog and cloud also needs to be pondered over. The challenges posed by the idea of interplaying between fog and cloud to accommodate different workloads. Owing to the dynamic data placement and large overall capacity volume in fog computing, search engine might be also redesigned which can process search query of content scattered in fog nodes according to Wang et al. (2008, 2010). It is also engaging to redesign cache on fog node to utilize temporal locality and broader coverage to save network bandwidth and reduce delay, while there is existing work of cache on end device and cache on edge servers. Latency-sensitive applications, such as streaming mining or complex event processing, are typical applications which need fog computing to provide real-time streaming processing rather than batch processing. Hong, et al. (2013) suggest a fog-based opportunistic spatio-temporal event processing system to meet the latency requirement. Their

system predicts future query region for moving consumers and starts the event processing early to make timely information available when consumers reaches the future locations. The proposal of Ottenwälder, et al. (2014), which exploits overlapping interests in data and acceptable inaccurate results to reuse computation and reduce resource requirement, increases the scalability and amortizes the delay of systems.

With the basic Fog Computing architecture, requirements for Fog Computing along with issues of QoS in mind, the assessment of capabilities of Fog Computing for Big Data provisioning can be conducted. The evaluation process itself could be divided into several stages such as setting up the experimental Fog Computing network composed of edge servers either virtual or physical, the accumulation of data generated by Fog Computing nodes, to put it differently, sensor data measured and transmitted to the edge gateways by various IoT devices. As Big Data processing software, several open-source solutions are proposed, namely, Apache Hadoop as a distributed file system amongst participants of Fog Computing, cluster-computing framework Apache Spark which is a fast and general engine for big data processing, scalable and high available database Apache Cassandra for storing real-time data, and a distributed streaming platform Apache Kafka used for interaction with IoT devices. Following this, experiments on evaluation of Fog Computing performance can be carried out. These include simple Big Data processing tasks such as the most prominent example of word count, the estimation of Pi using Quazi Monte Carlo method, data visualisation involving various internal processes, and, finally, the measurement of average latency, jitter, and the identifying and approximation of their trends. Apart from them, the capabilities of Fog Computing in machine learning and predictive analysis contributing a vast number of areas of domains, such as healthcare, economic policy development and its analysis, might also be tested, though this is somewhat inclined to be a topic for further research studies.

ТЕЛЕКОММУНИКАЦИЯ ТАРМОҚЛАРИДА QoS НИ ТАЪМИНЛАШ МЕХАНИЗМЛАРИГА ОИД

Н.Б. Усманова (ТАТУ, доцент)
Г.М. Жамолова (ТАТУ, 2 – курс магистранти)

Бугунги ҳаётда мамалакатлар иқтисодиётига ва миллионлаб кишиларнинг яшаш шароитларига телекоммуникация технологиялари ва ахборотлаштиришнинг ривожланиш даражаси таъсири кундан кунга ошиб бормоқда.

Телекоммуникация соҳасининг мутахассислари қуйидаги муаммоларни еча билишлари лозим: ахборотларни етказиш бўйича ошиб бораётган талабларни қондириш учун мамлакатда телекоммуникация тармоқлари қайси йўналишда ривожланиши керак; қанча ва қандай алоқа воситаларини яратиш ҳамда жорий етиш лозим; узатилаётган хабарларни ўз вақтида етказиш ва аниқлилигини таъминлаш, минимал харажатлардан зарурий самара олиш, шунингдек, ускуналар ва алоқа каналларидан максимал фойдаланиш учун телекоммуникация тармоқларини қандай оптимал ривожлантиришни билишлари керак.

Замонавий ахборот узатиш тизимлари мураккаб телекоммуникация мажмуаси ҳисобланади. Сифатли хизмат истеъмолчилар сонининг ошиши ва доимий мижозга айланишида асос эканлиги ҳаммага маълум. Фойдали ва кафолатланган хизматлардан олинаётган даромад эса соҳа ривожининг пойдевори ҳисобланади.

Сифат тушунчасининг умумий тавсифи 1994 йил ҳалқаро ISO 8402 стандартида келтирилган : “белгиланган ва кўзланган эхтиёжни қондирадиган объект характеристикаларининг мажмуи”. 2000 йилда ISO 8402 стандарти ISO 9000 стандарти билан алмаштирилган, унда “сифат” тушунчасига ўзининг талаб характеристикаларига мос келиш даражаси сифатида тавсиф берилган. Тавсияномаларида келтирилган, алоқа хизматлари сифати соҳасидаги асосий терминлари белгиланган (Quality of Service, QoS).

ITU-T E.800 Тавсияномаларида QoS га куйидагича таъриф берилган: “фойдаланувчининг хизматдан қониққанлик даражасини белгиловчи, хизматнинг фойдаланишга оид характеристикаларининг умумий кўрсаткичи” деб. Кўпчилик стандартларда, ҳисоботларда ва таснифларда QoS тушунчасидан фойдаланилганда ITU-T E.800-Тавсияномасига таянадилар.

Бундан ташқари “идроқ қилиш сифати” тушунчаси (Quality Of Experience, QoE) ҳам қўлланилади, уни баҳолаш методологияси ва параметрларининг асосий кўрсаткичлари G.1011-Тавсияномасида белгиланган.

Тармоқ хизматини сифатли таъминлашни муҳим вазифалардан бири трафикни бошқариш ҳисобланади. Бу билан биз алгоритмик воситалар мажмуини куйидагича тушунамиз, тармоқни сифатли хизмат кўрсатиш фаолиятини таъминлаш учун аппарат ва дастурий таъминотлардан фойдаланиб, ресурсларидан самарали фойдаланишга, қаратилган. QoSни таъминлаш учун қуйидаги вазифаларни бажариш зарур бўлади:

-Трафик классификацияси(Classification)

-Трафикни белгилаш (Coloring)

-Рухсат этилган уланишни бошқариш (Connection Admission Control)

-Режалаштирилган хизмат кўрсатиш ва тартибни бошқариш (Scheduling and queue management)

-Ўта юкланишни бошқариш (Congestion Management)

-Юкламанни бошқариш (Congestion Avoidance)

Хизматларни режалаштириш:

1. Хизматни устворлиги: Трафик синфларининг турли устворликлари бор ва у ҳам трафикни белгилашга боғлиқ, биринчи трафик синфини юқори ахамиятга эга бўлга қисми, қолганлари навбама навбат узатилади.

2. Пакетларга хизмат кўрсатиш навбатма-навбат амалга оширилади.

3. Даврий хизмат кўрсатиш (Round Robin). Ҳар бир пакет хизмати учун белгиланган вақт навбатма-навбат берилади.

4.Асосан тўғри буферлаш (Weighted Fair Queueing, WFQ). Турли пакет синфларига хизмат кўрсатишини қанча вақти ўтганлиги ва қанчаси ўтаётганлигига боғлиқ.

Юкламани назорат қилиш ва бошқариш:

1. Token Bucket - чегараланган юкламалар сонига хизмат кўрсатишда берилган вақт оралиғи давомида, ўртача оқим тезлигини чеклаш, аниқ параметрли келаётган ва келмайдиган пакетларни таъминлаш

2. Leaky Bucket – кираётган юкламани ўлчаш ва бошқариш.

Пакетларни бошқариш тартибининг пассив алгоритми (TailDrop, DropFrontonFull, RandomDroponFull) қуйидагилардан иборат:

• пакетларни бошқариш тартибини энг оддий алгоритмлари;

• пакетлар узатиш тартибидаги битта оқимини “ушлаб қолиш” имконияти йўқ;

• ўта юкланишни моментини олдиндан аниқлаш ҳолати таъминланмаган.

Пакетиларни бошқариш тартибининг актив алгоритми (RED, ARED) таъминланган

• пакетлар узатиш тартибида бир ёки бир неча оқимларни тутиб қолиш имконияти олдини олиш муаммоси

• ортиқча юкламани олдиндан топиш имкониятлари муаммосини ҳал қилиш

• пакетларни узатиш вақтида кечикишни таъминлаш

Шу каби механизмларни амалга ошириш ва оператор ёки провайдер томонидан йўлга қўйиш масалалари алоқа хизматлар сифати мониторингини ўтказиш, статистик маълумотлар ёки назорат ўлчовларни олиш, алоқа хизматларидан фойдаланувчиларнинг сўровлар ва улар томонидан берилган шикоятларни таҳлил этиш каби омилларга боғлиқ. Шунингдек, турли шароитларда муқобил механизмни қўллаш мақсадида керакли моделлаштириш ишлари ва кўрсатмалар хам қўл келади.

ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОСОБЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ СЕТЕЙ NGN

Т.Н. Халмурадов (ТУИТ, магистр)

Для обеспечения необходимого уровня защиты необходимо определить характеристики информационной безопасности. Основными характеристиками информационной безопасности сети NGN являются, характеристики, показанные на рисунке 1.1.

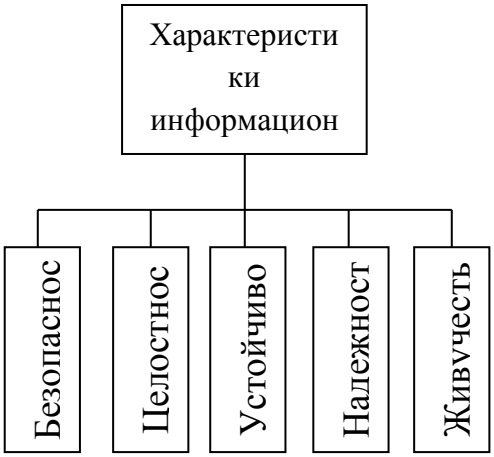


Рис.1.1. Характеристики информационной безопасности

Безопасность NGN: Способность сети противодействовать возможным угрозам и воздействиям дестабилизирующих, факторов, источниками которых являются физический или технологический процесс внутреннего или внешнего, по отношению к NGN, характера, приводящие к отказу элементов сети.

Устойчивость NGN: Способность сети выполнять свои функции при отказе части элементов в результате воздействия дестабилизирующих факторов.

Целостность NGN: Способность сети выполнять предназначенные ее функции в рамках установленных параметров, независимо от преднамеренного или случайного несанкционированного воздействия нарушителя.

Надежность NGN: Способность сети выполнять свои функции при отказе части элементов в результате внутренних воздействий дестабилизирующих факторов.

Живучесть NGN: Способность сети выполнять свои функции при отказе части элементов в результате воздействия внешних дестабилизирующих факторов.

Не секрет, что безопасность сегодня становится одной из главных проблем управления услугами в сетях связи, а к сетям следующего поколения необходим особый подход к обеспечению информационной безопасности.

Поэтому необходимо выполнение требований выработанных специально для сетей следующего поколения. Эти требования отражают основные положения безопасности, изложенные в Рекомендации X.805:

- управление доступом;
- аутентификация;
- фиксация авторства;
- конфиденциальность данных;
- безопасность связи;
- целостность данных;
- готовность (доступность);
- секретность (приватность).

Рассмотрим более детально требования по обеспечению информационной безопасности сетей следующего поколения.

Во-первых, требуется поддержка совместимости для различных элементов сети, в частности для различных механизмов безопасности. Минимальный набор особенностей безопасности должен поддерживаться во всем мире. Аутентификация и авторизация должны проводится на всех слоях от пользователя к сети, от сети к пользователю и от сети к сети.

Во-вторых, в сети NGN должна обеспечиваться безопасность сетевых элементов, связанных с ресурсами менеджмента и ресурсами услуг. Элемент должен принимать определенные меры против несанкционированного доступа к сетевым ресурсам, оборудованию услугам или персональным данным, например, блокировать неавторизованный трафик, также в сети должна быть возможность обнаруживать, сигнализировать и подавлять эпизоды аномальных событий в сети. Функциональность защиты должна быть усилена на приграничных элементах сети, что включает в себя контроль доступа для пакетов данных и сигнальной информации согласно определенным политикам безопасности, например, запрет трафика определенных пользователей или приложений.

Необходимо создание целой инфраструктуры NGN. С точки зрения инфраструктуры NGN операторы сети могут ограничивать прозрачность топологии и ресурсов для авторизованных объектов. Согласно инфраструктуре NGN должна быть гарантирована конфиденциальность и целостность транспортируемых потоков сигнализации, управления и менеджмента, к тому же согласно инфраструктуре NGN должна быть гарантирована конфиденциальность и целостность передаваемых медиапотоков. Инфраструктурой NGN поддерживается создание множества зон безопасности. Между различными зонами может быть применена изоляция в терминологии безопасности.

В сети NGN должно быть безопасное хранилище данных, связанных с защитой. Такое хранилище должно быть отделено от информации об услугах абонентов. Необходима возможность поддержки мониторинга сетевого трафика и установки базового уровня для определения событий сети.

В виду обширности сетей NGN и сложности обеспечения информационной безопасности в сетях NGN важно выполнение так же дополнительных требований, каждый элемент должен поддерживать возможность ограничения собственных ресурсов для обработки запросов. Все элементы сети должны иметь возможность создания журнала аудита, куда заносятся записи событий, связанных с обеспечением защиты.

При обеспечении информационной безопасности в сетях следующего поколения особым требованием является управление информационной безопасностью. Данный процесс предназначен для защиты сетевой инфраструктуры от несанкционированного использования, оценку рисков возникновения подобного события, управления рисками и противодействия им.

Одной из важнейших задач управления информационной безопасностью в сетях связи является обеспечение сохранности информации. Это означает ее защищенность от известных рисков и по возможности уклонение от неизвестных рисков, а также соблюдение определенного уровня конфиденциальности (то есть защищенности от несанкционированного доступа и использования), целостности (то есть точности, полноты и своевременности) и доступности. Кроме того, определенное внимание следует уделять возможностям проверки правильного использования информации и эффективности мер безопасности.

Процесс управления информационной безопасностью также получает информацию, относящуюся к проблемам безопасности, из других процессов (например, об инцидентах, связанных с безопасностью).

В настоящее время многие компании связи имеют дело с информационной безопасностью на стратегическом уровне (в информационной политике и информационном планировании) и на операционном уровне (в частности, при закупке средств обеспечения безопасности). Отметим, что проблемой многих компаний является разрыв между операционным и стратегическим уровнями управления безопасностью, проявляющийся в том, что значительные средства вкладываются в уже неактуальные меры безопасности. В то время как должны быть приняты новые, более эффективные меры, поскольку в отношении сетей следующего поколения выполнение данного требования необычайно важно из-за очень быстрых темпов развитий сетевых технологий.

ОРГАНИЗАЦИЯ WI-FI СЕТИ В ПОДВИЖНОМ СОСТАВЕ

С.С.Холиқов (ТТЙМИ кафедраси катта ўқитувчиси)
Б.Б.Назаров (ТТЙМИ, 2-курс магистранти)

Мир телекоммуникаций и передачи данных сталкивается с динамично растущим спросом на частотные ресурсы. Эта тенденция в основном связана с увеличением числа пользователей Internet и также с растущим взаимодействием международных операторов и увеличением объемов передаваемой информации. Полоса пропускания в расчете на одного пользователя стремительно увеличивается. Поэтому поставщики средств связи при построении современных информационных сетей используют волоконно-оптические кабельные системы наиболее часто. Это касается как построения протяженных телекоммуникационных магистралей, так и локальных вычислительных сетей.

Современные телекоммуникационные технологии активно применяются и будут применяться по мере их совершенствования для решения вышеперечисленных задач. Уровень безопасности движения повышается за счет непрерывного технического контроля и диагностики транспортных средств и магистралей; автоматизации систем управления; цифрового качества связи Железнодорожные поездки достаточно длительные и часто проходят в областях, где покрытие сотовой сети либо недостаточно хорошее, либо отсутствует вообще. Решить проблему доступа к сети Интернет для пассажиров мог бы спутниковый канал связи, но оборудование для него достаточно дорогое и установка его отдельно на каждый вагон избыточна. Правильным решением в данном случае является установка спутникового оборудования в центральном (штабном) вагоне, и организация локальной сети во всем составе.

Использование физических кабелей для создания связей между вагонами влечет за собой определенные проблемы. Основная проблема в том, что порядок вагонов в составе не является постоянным и может меняться со временем. Во время следования вагоны соединяются и разъединяются, что приводит к износу кабельных связей, а также усложняет работу персонала.

Для решения данной задачи используются беспроводные соединения между вагонами на основе самоорганизующейся беспроводной сети Mesh на базе оборудования Motorola.

В основе работы комбинированного комплекса реализован принцип рационального использования ресурсов сетей сотовой и спутниковой связи – на всем пути следования поезда система отслеживает наилучший уровень принятия сигнала и в автоматическом режиме переключается со спутника на 3G- связь и наоборот, что позволяет обеспечивать подключение к Интернет-сети на скорости до 4 Мбит/с. Использование сетей WiMAX и Wi-Fi для мониторинга и удалённой диспетчеризации подвижного состава позволяет:

- осуществлять регулярный мониторинг технического состояния подвижного состава, процессов организации движения электропоездов;
- организовать автоматический обмен информацией между подвижными объектами и

базовыми станциями с минимальной задержкой по времени;
- осуществлять обеспечение безопасности перевозок и контроля качества услуг;

Точки Доступа подвижного состава должны:

-поддерживать стандарт беспроводной связи IEEE 802.11b/g/n, поддержка также стандарта IEEE 802.11ac предпочтительна;

- иметь минимум 4 интегрированные антенны с круговой диаграммой направленности и поддерживать передачу данных не менее, чем по трем пространственным потокам с максимальной суммарной пропускной способностью от 450 Мбит/с;

-поддерживать одновременное подключение до 200 абонентских устройств;

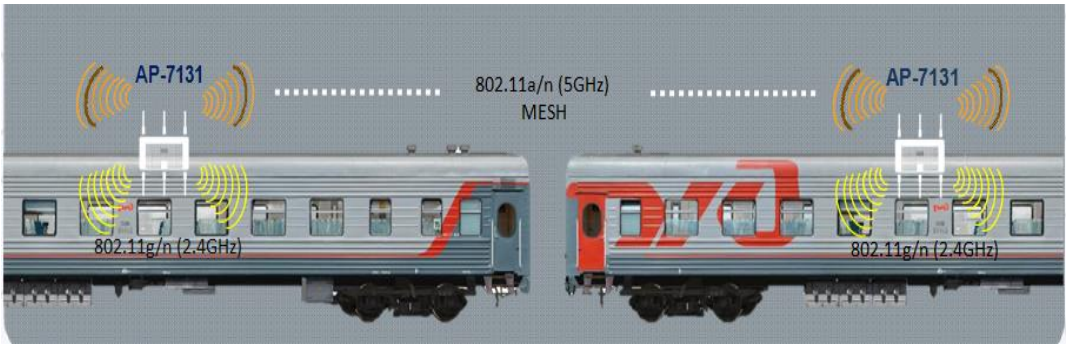
- входное напряжение питания для оборудования установленного на станции от 100 до 240 В переменного тока;

- входное напряжение электропитания 50-100 В постоянного тока для оборудования, устанавливаемого на составе типа Ем и 81серии;

Контроллеры беспроводной сети должны обеспечивать:

- централизованное управление точками беспроводного доступа;
- динамическое выделение радиоканалов Точек Доступа;
- централизованный мониторинг и обнаружение помех радио среды;
динамическое управление мощностью передатчиков Точек Доступа;
- входное напряжение 12 В, 24 В, 48 В или 50-100 В постоянного тока для оборудования подвижного состава и 110-240 В для оборудования станций;
- рабочий температурный диапазон от 0°С до +40°С;

Wi-Fi сеть позволила обеспечить стабильный доступ в **Интернет** пассажирам поезда на протяжении всей поездки. Помимо доступа в глобальную сеть, решение позволяет организовать быстрый доступ к локальным полезным ресурсам во время поездки: видео- и аудио- контенту (например, фильмы или аудиокниги), справочной информации о точке назначения (например, расписания и часы работы организаций) для всех пассажиров поезда. В дальнейшем планируется тиражирование решения на другие железнодорожные маршруты.



CLOUD COMPUTING, CONSEPTS AND MILESTONES

I.T.Xolliyev (Student of Master degree of TUIT)

The idea that computation may be organized as a public utility, like water and electricity, was formulated in 1960s by John McCarthy, a visionary computer scientist who championed mathematical logic in artificial intelligence. Four decades later, utility computing was embraced by major IT companies such as Amazon, Apple, Google, HP, IBM, Microsoft, and Oracle.

Cloud computing is a computing paradigm in which different computing resources, including infrastructure, hardware platforms, and software applications, are made accessible to remote users as services. Successful provision of infrastructure-as-a-service (IaaS) and, consequently, widespread adoption of cloud computing necessitates accurate performance evaluation that allows service providers to dimension their resources in order to full the service level agreements with their customers. In this chapter, we describe an analytical model for

performance evaluation of cloud server farms, and demonstrate the manner in which important performance indicators such as request waiting time and server utilization may be assessed with sufficient accuracy.

Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet, have accelerated interest in cloud computing. A cloud service differs from traditional hosting in three principal aspects. First, it is provided on demand, typically by the minute or the hour; second, it is elastic since the user can have as much or as little of a service as they want at any given time; and third, the service is fully managed by the provider user needs little more than computer and Internet access. Cloud customers pay only for the services they use by means of a customized service level agreement (SLA), which is a contract negotiated and agreed between a customer and a service provider: the service provider is required to execute service requests from a customer within negotiated quality of service(QoS) requirements for a given price.

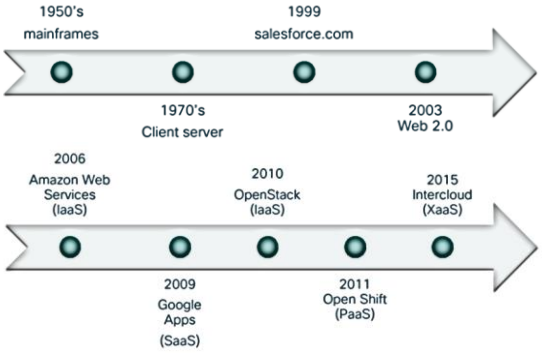


Figure 1. Cloud computing milestones.

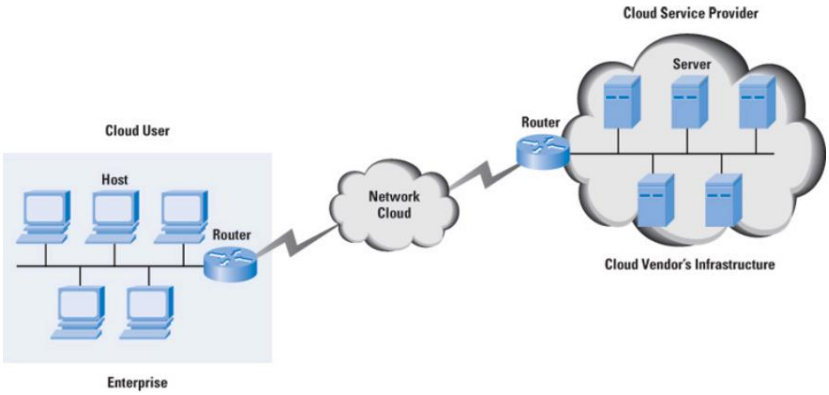


Figure 2. Cloud computing.

Cloud computing - an old idea whose time has come Once the technological elements were in place it was only a matter of time until the economical advantages of cloud computing became apparent. Due to the economy of scale large data centers, centers with more than 50 000 systems, are more economical to operate than medium size centers which have around 1 000 systems. Large data centers equipped with commodity computers experience a 5 to 7 times decrease of resource consumption, including energy, compared to medium size centers. The networking costs, in dollars per Mbit/sec/month, are 95/13 = 7.1 larger and the storage costs, in dollars per Gbyte/month, are 2.2/0.4 = 5.7 larger for medium size centers. Medium size centers have a larger administrative overhead, one system administrator for 140 systems versus one for 1 000 systems for large centers.

Data centers are very large consumers of electric energy to keep the servers and the networking infrastructure running and for cooling. For example, there are 6 000 data centers in the U.S and in 2006 they reportedly consumed 61 billion KWh, 1.5% of all electric energy in the U.S., at a cost of $4.5 billion. The power demanded by data centers was predicted to double from 2006 to 2011. Peak instantaneous demand was predicted to increase from 7 GW in 2006 to 12 GW in 2011, requiring the construction of 10 new power plants. In the US the energy costs differ

from state to state, e.g., 1 KWh costs 3.6 cents in Idaho, 10 cents in California, and 18 cents in Hawaii thus, data centers should be placed at sites with low energy cost.

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture. The services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service), which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud.

Infrastructure-as-a-service (IaaS) refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access.

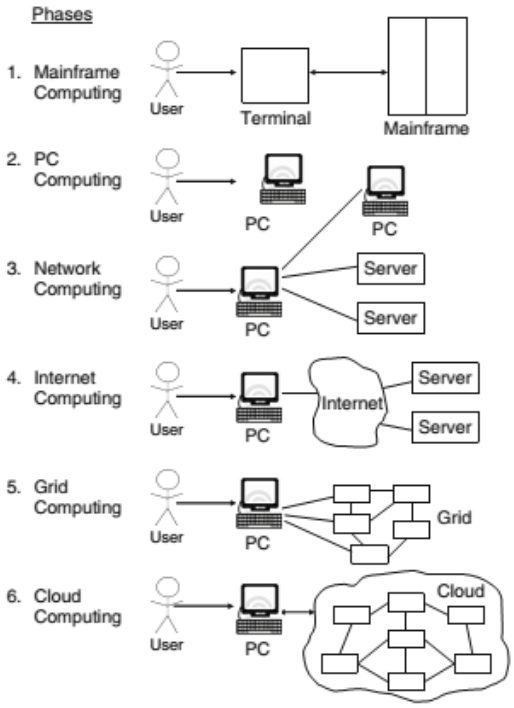


Figure 3. Six computing paradigms – from mainframe computing to Internet computing, to grid computing (adapted from Voas and Zhang (2009)).

Platform-as-a-Service (PaaS) is similar to IaaS, but also includes operating systems and required services for a particular application. In other words, PaaS is IaaS with a custom software stack for the given application.

The data-Storage-as-a-Service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

In this article we discussed the consideration for cloud service providers to build the cloud service. To the cloud service provider, designing, building, implementing, and commissioning underlying technology infrastructure translates to creating the foundation to produce the service that is ready for consumption. This chapter provides clarity on what are the elements that are required to be assessed, evaluated, tested, and accepted prior to classifying a produced service is ready for consumption. These foundation elements will be used to produce the cloud service that will be ready for consumption.

TELEKOMMUNIKATSIYA TARMOQ TRAFIGINI KLASSIFIKATSIYALASH USULLARI

S.A.Abdullayev (TATU, 1-bosqich magistranti)

Tarmoq trafigini klassifikatsiya qilish tushunchasi nafaqat oddiy foydalanuvchi balki tarmoq operatorlari, tarmoq administratorlari va Internet xizmati provayderlari uchun ham muhim tushuncha bo’lib xizmat qiladi. Tarmoq administratorlari trafikni klassifikatsiya qilish

orqali biror xizmat turiga yuqori imtiyoz berishi yoki xizmat turini butunlay cheklab qo'yish imkoniyatiga ega bo'ladilar. Internet xizmat provayderlari uchun trafikni klassifikatsiyalash QoS (Quality of Service, Xizmat ko'rsatish sifati) ni ta'minlashda muhim ahamiyat kasb etadi. Bundan tashqari billing tizimini yangi imkoniyatlarga olib chiqish imkonini beradi.

Trafikni klassifikatsiyalash uchun bir qancha yondashuvlar mavjud bo'lib, ular ichida dastlabkisi port asosidagi yondashuvdir. Bilamizki har bir xizmat turi belgilangan portlar orqali taqdim etiladi. Misol sifatida HTTP 80-port, Telnet 23-port, POP3 110-port, FTP 20-port va boshqalarni misol keltirishimiz mumkin. Tarmoq xizmatlariga portlarni Internet Assigned Numbers Authority (IANA) tashkiloti ro'yhatga oladi. Bugungi kunda ushbu usul deyarli qo'llanilmaydi. Chunki zamoniy xizmatlarni taqdim etish dinamik portlar orqali amalga oshirilayotganligi sababli port asosidagi yondashuv aniqligi kamayadi.

Port asosidagi yondashuv kamchiliklarini bartaraf qilgan alternative klassifikatsiyalash yondashuvlaridan biri foydali ma'lumot tekshiruviga asoslangan yondashuvdir. Ushbu yondashuv odatda paketni chuqur tekshirish (DPI – Deep Packet Inspection) texnologiyasi deb ham ataladi. Ushbu yondashuv asosan P2P ilovalari bilan ishlashga asoslangan bo'lib, ushbu ilovalar xizmatlari niqoblab uzatilishi tufayli ularni portga asoslangan yondashuv orqali aniqlashning iloji yo'q. Bilamizki P2P protokoli asosida taqdim etiladigan xizmatlarda uzatiladigan paketlarning foydali ma'lumot qismi Karagiannis aniqlamalari bilan boshlanadi. Misol uchun eDonkey 2000 trafigi 0xe319010000, Fasttrack trafigi 0x2700000002980 va BitTorrent trafigi esa "0x13Bit" qatorlari bilan boshlanadi. Ushbu yondashuvning ishlash prinsipi aynan shu Karagiannis aniqlamalarini o'qib olish orqali trafikni klassifikatsiyalashga asoslangan.

Foydali ma'lumot qismini tekshirishga asoslangan yondashuv yuqori aniqlikga ega bo'lishi bilan bir qatorda uchta asosiy kamchiliklarga ega. Birinchidan har bir paketdan aniqlanmalarni qidirish juda katta resurs iste'mol qiladi bu esa qurilma narxini ortishiga olib keladi. Ikkinchidan , P2P ilovalari orasidagi shifrlangan trafik bilan ishlay olmaydi. Uchinchidan yangi ilovalarni doimiy yaratilishi va yangilanib borishi tufayli klassifikatsiyala qiluvchi dasturiy ta'minotni doimiy yangilab borish zaruriyati tug'iladi.

Yuqoridagi kamchiliklarga qaramasdan ushbu jarayonni yengillashtirshga bir qancha takliflar mavjud. Bu takliflar trafikni shifrlashni cheklash va ilovalarni yangilanib borishini ma'lum standart asosida amalga oshirishga qaratilgan chora tadbirlarni o'z ichiga qamrab oladi.

Yana bir klassifikatsiyalashga yondashuv usullaridan bir oqim hususiyatiga asoslangan yondashuvdir. Ushbu yondashuv mashina o'rganish (machine learning ML) texnologiyasiga asoslangan. Bu usul turli ilovalarning harakteristikalari bir biridan farqlanishi hisobiga amalga oshadi. ML yondashuvi trafikni klassifikatsiya qilishda yig'ib olingan hususiyatlar to'plamidan tashkil topgan ma'lumotlar yig'indisidan foydalanishni nazarda tutadi. ML yondashuvi ikki usuldan tashkil topadi: Oldindan belgilangan va oldindan belgilanmagan.

Oldindan belgilangan usulda barcha oqim hususiyatlari oldindan ma'lumotlar klassi kiritiladi va trafikni tekshirishda aynan shu ma'lumotlardan foydalaniladi. Ma'lumotlar klassi TS = $<x_1,y_1>,<x_2,y_2>\ldots<x_n,y_n>$ ko'rinishda bo'ladi. Bu yerda x_i i-oqimning hususiyati, y_i i- oqim hususiyatining chiqish qiymati. Ushbu klass oqim hususiyati va chiqish qiymati orasidagi bog'lanishni ifoda etadi.

Oldindan belgilanmagan usulda ma'lumotlar bazasi oldindan shakllantirilmaydi. Bu usul o'zining algoritmiga ega bo'lib, u oqimlar harakteristikalarini o'zi aniqlaydi va guruhlar tuzadi. Trafikni klassifikatsiyalash hosil qilingan guruhlar orqali amalga oshiriladi.

ML yondashuvi texnik jihatdan foydali deb hisoblanadi. Lekin shunga qaramasdan ML asosidagi yondashuv yangi ilovalarga moslashtirish uchun doimiy yangilanib borishini talab qiladi. Bu jarayon qiyin va inson tomonidan nazorat qilishni talab qiladi. Host harakteristikasiga asoslangan yondashuvda trafikni klassifikatsiyalash hostlarning darajalariga qarab amalga oshiriladi. Ushbu yondashuvda hostlarni uchta darajaga ajratish ko'zda tutilgan. Ijtimoiy darajadagi hostlar qiymati unga bog'langan turli hostlar soniga bog'liq bo'ladi. Funksional darajadagi hostlar qiymati uning tarmoqdagi roliga qarab aniqlanadi. Misol uchun host

provayder yoki iste'molchi bo'lishi mumkin. Ilova darajasidagi hostlar qiymati transport pog'onasidagi ilovalar bilan o'zaro aloqalari bilan bog'liq. Host harakteristikasiga asoslangan yondashuvda trafikni klassifikatsiyalash hostlarni qiymatlari orqali amalga oshiriladi. Trafikni klassifikatsiyalashga yondashuvlarning so'ngisi IP addres bo'yicha klassifikatsiyalashdir. IP addreslar trafikga aloqador ma'lumotlarni tashish imkoniyatiga ega. Portga asoslangan yondashuvga o'xshash ravishda ushbu yondashuvda trafikni klassifikatsiyalash uchun IP addreslardan foydalaniladi. IP addres bo'yicha klassifikatsiyalashning ikkita texnologiyasi mavjud. Birinchi texnologiyada xizmatlarni klassifikatsiya qilishda ularning IP addresi asosiy omil hisoblanadi. Bunda trafikni hosil qiluvchi IP addres trafik turini belgilaydi. Ya'ni 31.13.86.16 addresi Facebook ga tegishli bo'lib, aynan shu addresda tarqalayotgan paketlar Facebookga tegishli bo'lib hisoblanadi. Ushbu uchlik offline rejimida ma'lumotlar bazasiga yoziladi.

Ikkinchi texnologiya xizmatga asoslangan usul hisoblanadi. Xizmat turini klassifikatsiyalashda uchta kattlik <IP,Port,Protokol> muhim hisoblanadi. Aynan shu kattaliklar har bir xizmat turi uchun alohida o'rnatiladi.

IP addres bo'yicha yondashuv boshqa yondashuvlar singari doimiy yangilab borishni talab qilasada, u boshqa yondashuvlarga nisbatan yuqori aniqlikga ega.

TELEKOMMUNIKATSIYA TARMOQ TRAFIGINI BOSHQARISHDA PACKETC DASTURLASH TILI IMKONIYATLARI

R.P. Abduraxmonov (TATU, dotsent)
S.A. Abdullayev (TATU 1-kurs magistranti)

Bugungi kunda telekomunikatsiya tarmog'ida ma'lumotlarni paketli ko'rinishda uzatish texnologiyalari joriy etilib kelinmoqda. Tarmoqda audio va video ma'lumotlarni ulushi ko'payishi paketlar sonini oshishiga va yangi uzatish muhiti va texnologiyalarini joriy etilishi esa paketlar jadalligini oshishiga sabab bo'lmoqda. Bu esa DPI (Deep Packet Inspection) texnologiyasida ishlatiladigan dasturlarni yuqori tezkorlikga ega bo'lishini talab qiladi. Ushbu omilni hisobga olgan holda asosan paket jarayonlari bilan ishlovchi packetC dasturlash tili yaratildi. PacketC dasturlash tili CloudShield Technologies Inc. korporatsiyasida faoliyat olib boruvchi Peder Jungck, Ralph Duncan va Dwight Mulcahylar tomonidan ishlab chiqilgan. PacketC dasturlash tilidan bevosita tarmoq trafigi bilan ishlovchi ilovalarini yaratish va umumiy standartlarni rivojlantirish uchun foydalanish mumkin.

Boshqa dasturlash tillari singari packetC dasturlash tili ham Windows va Linux operatsion tizimlari asosida ishlay oladi. Dasturlar yaratish uchun Eclipse Open IDE muhitidan foydalanish mumkin.

PacketC dasturlash tilini asosiy hususiyatlari sifatida quyidagilarni ko'rsatish mumkin: packetC parallel jarayonlarni taminlovchi muhitdan foydalanishga mo'ljallangan; packetC parallel dasturlash qiyinchiliklaridan dasturlovchini ozod qiladi; Kompilyatsiya vaqtini taqsimlanganligi va tizim darajasidagi ma'lumotlar strukturasining yaxlitligi ilovani xavfsizligini ta'minlaydi; packetC xavfsizlik maqsadida ko'rsatkichlarni olib tashlagan.

PacketC dasturlash tili C tili asosida yaratilgan bo'lib, lekin packetC dasturlash tili toifa modellari va semantikasi bilan C dasturlash tilidan farq qiladi. Bundan tashqari C umumfoydalanish dasturlash tili hisoblanadi. PacketC esa tarmoq jarayonlariga yo'naltirilgan;C tilida xotiraga kirish imkoniyati cheklanmagan. PacketC da ilova ishonchililigi va tizim xavfsizligini oshirish maqsadida bunday kirishlar cheklangan

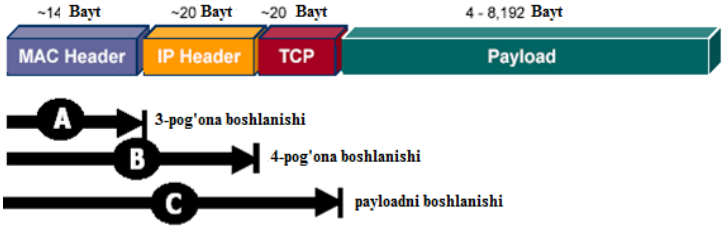
PacketC da C dan farqli ravishda tarmoq o'zgaruvchilarini e'lon qilish imkoniyati mavjud. Bu esa tarmoq muhim hususiyatlarini ifodalovchi IP address, tarmoq maskasi, host addresi va boshqa shu kabi kattaliklarni ifodalashda qulayliklar tug'diradi. Masalan:

int myIP = 162.150.1.1 //myIP ga IP addresni o'rnatadi. 162 asosiy bit sifatida saqlanadi.

int myIP = 256.168.2.3// Xato chunki IP addres 0 – 255 oraliqda bo'ladi

int myNetMask = 255.255.0.0 // tarmoq maskasini o'rnatish
int myNetMask = 0b11111111111111111110000000000000 //Maska ikkilik ko'rinishida
int myHost = 0.0.31.255

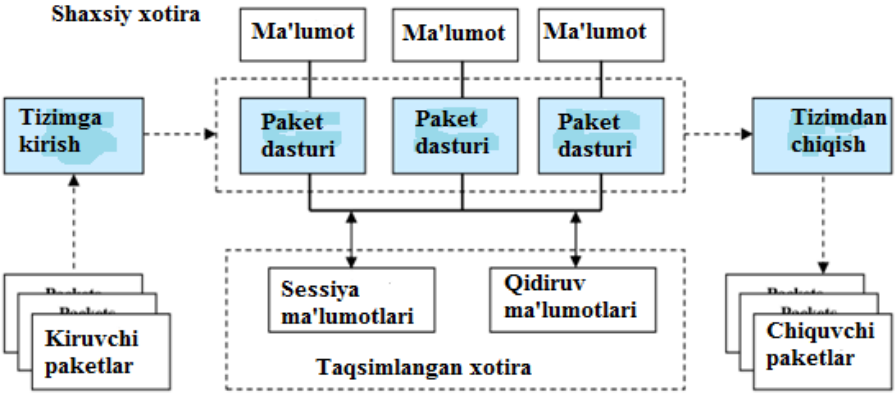
PacketC da mahsus Packet Information Block $PIB funksiyasi mavjud bo'lib u joriy paket haqida ma'lumot olishga imkon beradi. PIBning asosiy hususiyati uning paketga OSI modeli pog'onalari tomonidanqo'shilgan qo'shimcha xizmat ma'lumotlarni o'qiy olishidir.



1-rasm. Ethernet LAN paketi ko'rinishi

PIB paketni dekodlash amalini bajaradi. Paketni istalgan qatlalarigacha yetib bora oladi. 1-rasmdan ko'rinib turibdiki A qism pib.l3Offset ni, B qism pib.l4Offset va C qism pib.payloadOffset ni ifodalaydi.

PacketC parallel paket jarayoni modeliga asoslangan bo'lib, ushbu jarayon mustaqil ravishda hosil qilinadi. Bu esa dasturchiga qulaylik yaratdi. Har bir tushayotgan parallel so'rov uchun xotiradan joy ajratiladi. 2-rasmda parallel paket jarayoni keltirilgan



2-rasm. Parallel paket jarayoni modeli

Ushbu modelni struktural komponentalari quyidagicha: Parallel so'rovlar kichik dastur jarayonlari ko'rinishida ifodalanadi; Global xotira barcha paket dasturlari uchun taqsimlangan xotira va har bir dastur nusxalarini saqlash shaxsiy xotiralardan iborat; Taqsimlangan xotirada protokol , seans va qidiruv haqidagi axborotlar saqlanadi; Host tizimi dastur nusxalarini boshqaradi va paketdagi headerlar joylashuvini qayta hisoblaydi.

PacketC va uning modeli paket jarayoni tizimlarining dinamik istiqbolini ko'rsatadi. Chunki tizim yuqori darajada ixtisoslashtirilgan qurilmadan tashkil topgan. Ushbu qurilma istalgan vaqtda o'z joyini o'zgartirishi mumkin. Ushbu yondashishning asosiy afzalligi bu yuqori sifatni ta'minlash va real vaqt paket ilovalarini yaratishda qulayligidir.

МЕТОДЫ ПАКЕТНОЙ СИНХРОНИЗАЦИИ СРЕДСТВ ЭЛЕКТРОСВЯЗИ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ

Ш.З. Алламуратов, В.Н. Мамутова (ТУИТ НФ)

Развитие мультисервисных сетей приводит к увеличению доли конвергентных архитектур в общей массе средств электросвязи. Основным отличием таких архитектур является одновременная передача данных, видео- и голосовых сообщений через различные сети: с коммутацией каналов (Time Division Multiplexing – TDM) и

коммутацией пакетов (Packet switched network – PSN). При этом особое внимание уделяется процессу синхронизации, обеспечивающему безошибочную передачу данных, голоса и видеоизображения в реальном времени и с постоянной скоростью (Constant Bit Rate – CDR). Передача сигналов сети TDM через сети PSN осуществляется с использованием услуги эмуляции каналов (Circuit emulation service – CES). Требования синхронизации при реализации такой услуги относятся к интерфейсам средств электросвязи в части джиттера и вандера, долговременной частотной точности и полной задержки (является критической для передачи голоса и изображения в реальном времени). Поскольку синхронный поток приложений сети TDM передается через сети PSN асинхронно, решение задачи обеспечения качественных услуг сводится к решению вопросов синхронизации между асинхронным и синхронным оборудованием.

Известны два класса методов пакетной синхронизации: методы синхронизации сетей плезиохронных и синхронных иерархий и методы синхронизации, основанные на пакетной технологии. Первый класс относится к методам, осуществляющим распределение радиосигнала PRC (Primary Reference Clock) при трансляции от источника GPS или на физическом уровне (например, STM-N). Для этого эталонный сигнал синхронизации, транслируемый от PRC, вводится в коммутатор Ethernet через внешний порт генератора. При этом синхронизация узлов сети производится на физическом уровне сети Ethernet по принципу ведущий-ведомый. Такая сеть получила название «синхронная Ethernet» (SyncE), а генераторы синхронных сетей Ethernet называют EEC (Synchronous Ethernet Equipment Clock).

Особенность второго класса методов заключается в передаче пакетов, содержащих синхронизационную информацию в виде меток времени (timestamp). Существуют несколько протоколов, использующих в своих алгоритмах синхронизации метки времени. Наиболее известны NTP (Network Time Protocol), SNTP (Simple Network Time Protocol) и PTP (Precision Time Protocol). Протокол PTP предназначен для синхронизации часов в сети по принципу ведущий-ведомый. Протоколы NTP и SNTP традиционно используются для распределения информации о времени дня. Те же пакеты могут использоваться и для распределения информации о частоте.

Методы синхронные сетей Ethernet применяют для передачи потоков канальных сигналов сетей плезиохронной (PDH) и синхронной (SDH) иерархии через сеть пакетной коммутации.

В зависимости от возможностей в синхронной сети Ethernet выделены четыре основных метода синхронизации:

- синхронно-сетевая работа (Network synchronous operation) – синхронизация блоков от независимых сигналов синхронизации, транслируемых по радио, проводных или оптических линий, от первичных эталонных генераторов;
- адаптивные методы (Adaptive methods) – синхронизация от первичного генератора TSC сети TDM (TDM ServiceClock), сигнал которого транслируется через виртуальный канал сети PSN;
- дифференциальные методы (Differential methods) – синхронизация от двух первичных генераторов TSC и PRC 3, сигналы которых транслируются через виртуальные каналы;
- использование первичных генераторов, размещенных возле оконечных систем TDM - синхронизация от первичных генераторов, сигналы которых транслируются через оконечное оборудование сети TDM.

Реализация методов синхронных сетей Ethernet для гибридных сетей позволяет добиться такого же качества услуг, как при синхронизации отдельной сети TDM.

Для мультисервисных сетей, использующих два типа сетей (TDM и PSN), наиболее эффективным протоколом синхронизации является SyncE. Он реализован на физическом уровне сети Ethernet и имеет различные варианты сопряжения с эталонным источником. Но на качество синхронизации устройств влияет также топология сети и неравномерность

трафика. В сети с большим числом устройств и высокой загрузкой каналов передачи данных точность синхронизации будет хуже.

Исходя из вышеизложенного можно сказать, что особое внимание уделяется процессу синхронизации, обеспечивающему безошибочную передачу данных, голоса и видеоизображения в реальном времени для обеспечения высококачественных услуг пользователям телекоммуникационной сети.

IP TARMOQ TRAFIGINI BOSHQARISHDA DPI TEXNOLOGIYASINING O'RNI

F. I. Axunov (TATU, dotsent)
E.B. Normurodov (TATU, magistranti)

Telekommunikatsiya sohasida abonentlardan tushayotgan talablarning keskin oshishi va ularga javoban sohaning yangi tarmoq xizmatlarini yaratishi hamda taqdim qilishi kundan kunga ortib bormoqda. Global IP tarmoqlar hozirgi kunda foydalanuvchilar uchun bir qancha katta imkoniyatlar yaratibgina qolmay ularning talab va istaklarini chuqur tahlil qilib, shunga yarasha xizmatlar taqdim etib kelmoqda.

Tarmoqda foydalanuvchilar sonining ko'payishi hamda ularning keng polosali xizmatlarga bo'lgan talablarining ortishi IP tarmoq bo'ylab uzatilayotgan ma'lumotlar oqimi hajmining yuqori sur'atda o'sishiga olib keldi. Shu bilan birgalikda tarmoqda uzatilayotgan ma'lumotlar oqimining xavfsizligini ta'minlash muhim ahamiyatga ega bo'lib qoldi. Buning natijasida tarmoqda yuqori darajadagi yuklanishlar va tarmoqqa bo'ladigan tashqi tahdidlarning soni oshmoqda. Bu holat tarmoq operatorlari oldiga ma'lumotlar oqimini intelektual nazorat qilish muommosini qo'ymoqda.

Internet servis provayderlari (ISP) va tarmoq administratorlari uchun doimo tarmoqlaridan qanday turdagi trafik o'tayotganini bilish muhim ahamiyatga ega bo'lib kelgan. Shuning uchun, tarmoq administratorlari va menejerlar doimo tarmoq monitoringi va trafik analizini olib borishlari kerak. Bunday ishlarni bajarish bilan tarmoq haqida quyidagi axborotlarga va statistikalarga ega bo'lish mumkin: tarmoq muommolari, foydalanuvchilar foydalanayotgan protokollar va dasturlar, hamda boshqa tarmoq infrastrukturasi haqidagi ma'lumotlar.

Tarmoq monitoringi texnologiyasining eng ko'p foydalaniladigan turlaridan biri bu trafik klassifikatsiya texnologiyasidir. Trafik sinfini bilgan holda ISPlar ularga mos xizmatlar ko'rsata oladilar. Masalan ma'lum oqimlar uchun xizmat ko'rsatish sifatini oshirishi yoki kamaytirishi va xavfli ma'lumotlar oqimini bloklab qo'yishi mumkin.

Trafik klassifikatsiya texnologiyasining ikki xil usuli mavjud bo'lib, ular online va offline trafik klassifikatsiyalardir. ISP lar asosan Online trafik klassifikatsiya texnikasiga tayangan holda ishlaydi. Chunki real vaqtda trafik sinfini aniqlab ular ustida mos qaror qabul qilish kerak. Shu bilan birga online trafik klassifikatsiya usuli DPI(Deep Packet Inspection) texnologiyasiga asoslanadi. Avvalgi texnologiyalar faqatgina paketning sarlavha qismini tekshirish bilan cheklangan bo'lsa DPI texnologiyasi esa paketning foydali yuklama qismini ham tekshira oladi. 4 pog'ona sarlavha qismidagi port raqamlarini bilish orqali paketning amaliy pog'onadagi qaysi protokolga tegishli ekanligini bilish mumkin, ya'ni qaysi sinifga tegishli ekanligini aniqlash mumkin. Agar amaliy pog'ona protokollari shifrlangan yoki o'zini yashirgan bo'lsa, masalan boshqa protokol port raqamini ko'rsatish yo'li bilan, bu holda 4 pog'anadagi port raqamlari orqali paketning qaysi sinfga tegishliligini aniqlab bo'lmaydi. DPI texnologiyasi paketning foydali va yuklama qismini tekshirishi orqali aniq yechimga kela oladi. DPI tizimlari butun paketni tutadi va paketning foydali yukalama qismi va dastur signaturalari o'rtasida moslashuvchanligini aniqlashga harakat qiladi.

Asosan DPI texnologiyalari amaliy pog'ona protokolini aniqlashi va farqlashi uchun signaturali analizdan foydalanadi. Signaturalar har bir amaliy pog'ona protokollariga mos keluvchi yagona shablonlardir. Boshqacha qilib aytganda, har bir amaliy pog'ona protokoli xarakteristikalari o'rganiladi va ularni ifodalovchi ma'lumotlar bazasi yaratiladi. Keyin klassifikatsiya mashinasi tarmoqdan o'tayotgan trafikni ana shu ma'lumotlar bazasi bilan taqqoslash orqali paketning amaliy pog'ona protokolini to'g'ri aniqlay oladi.

Shuningdek, ma'lumotlar bazasini davriy ravishda yangi amaliy pog'ona protokollari bilan to'ldirib turish lozim. DPI tizimlari trafik klassifikatsiyasini to'g'ri va aniq amalga oshirishi uchun turli internet dasturlarini aks ettiruvchi katta hajmdagi signaturalar bazasi bilan ta'minlanishi lozim. DPI tizimiga qo'yiladigan muhim talablardan yana biri, u paketni ma'lumot uzatish kanali tezligida tekshirishi kerak.

Ma'lumotlar oqimi va paketlar sinfi aniqlanishi bilan, ularga belgi qo'yish (ya'ni imtiyoz berish) kerak. Ana shu holda ularga mos xizmat ko'rsatish mumkin bo'ladi. Belgilar yoki bayroqlar bir necha yo'llar bilan o'rnatilishi mumkin. IP paketlar uchun, maxsus ajratilgan paketning Type of sevice (ToS) yoki Differentiated Services Code Point (DSCP) blokiga o'rnatiladi. Bu yo'l bilan asosan tarmoqni yuklanishiga sabab bo'luvchi va kanallarning o'tkazish polosasining ko'p qismini egallayotgan P2P (peer- to-peer), fayl almashuv protokollari asosidagi trafiklarni chegaralash orqali boshqa HTTP, SMTP kabi so'rovlarga imtiyoz berish mumkin. Tarmoqda paketning yo'qolishiga sezgir trafiklar mavjud, masalan FTP, SMTP. Hamda paketning kechikishiga sezgir bo'lgan trafiklar, VoIP, online video, kabilar. DPI tizimlari ularning bu kabi xususiyatlarini e'tiborga olib, kerakli xizmat ko'rsatadi.

DPI mahsuloti dastur ko'rinishida yoki alohida qurilma (texnologiya) ko'rinishida bo'lishi mumkin. Ikkisi ham o'ziga xos avfzallik va kamchiliklarga ega. DPI qurilmasi katta tezlikni va moslashuvchanlikni ta'minlaydi lekin narxi juda ham baland. Asosan undan Data center va ulkan korparativ tarmoqlar foydalanadi. Dasturga asoslangan DPI mahsuloti iqtisodiy jixatdan samarador, ammo ular markaziy protsessor resurslarining ko'p qismini iste'mol qiladi. Asosan bu turdagi DPI mahsulotidan past va o'rta tezlikli ma'lumotlar oqimiga ega, uncha katta bo'lmagan tarmoqlar foydalanadi. DPI texnologiyasi operator tarmog'i chegarasiga o'rnatiladi. Operator tarmog'idan chiqayotgan va kirayotgan barcha turdagi trafiklar DPI texnologiyasi orqali o'tadi. DPI texnologiyasini bunday joylashtirish tarmoq operatoriga ma'lumotlar oqimini monitoring qilish va boshqarish imkoniyatini beradi. Tarmoq trafigini samarali boshqarish orqali internet servis provayderlari tarmoq resurslaridan foydalanishni optimallashtira oladi. Bu yo'l bilan esa kapital, hamda ekspluatatsiya xarajatlarini qisqartiradi.

ILOVALARNI DASTURLASH INTERFEYSI (APPLICATION PROGRAMMING INTERFACE-API) DAN FOYDALANISH

O.N. Djuraev (TATU, katta o'qituvchi)

Dasturlash bilan shug'ullanganda avvaldan yaratilgan klasslar borligini tekshirib ko'rish lozim.

Misol uchun, foydalanuvchi tomonidan ma'lumot kiritish murakkab vazifa hisoblanadi. Ushbu murakkab vazifani *Scanner* klassi amalga oshiradi.

Matematik hisoblashlar ham ba'zi vaqtlar murakkab vazifa hisoblanadi. *Math*klassi matematik hisoblashlarni amalga oshiradi.

Avvaldan yaratilgan klasslar Ilovalarni Dasturlash Interfeysi *Application Programming Interface* (API) kutubxonasida saqlanadi.

API kutubxonasidan foydalanishdan avval klassni dasturga *import* qilish lozim. Misol uchun *Scanner* klassidan foydalanish uchun dastur boshiga quyidagi qatorni qo'shish kerak:

import java.util.Scanner;

Bu yerda *java.util* paket, *Scanner* esa klass hisoblanadi.Paket (package) klasslar guruhidir.

java.util paketi bir qancha klasslarni o'z ichiga oladi. Bizning misolda *Scanner* klassidan foydalanilgan.

Ba'zi klasslar muhim hisoblanganligi sababli Java kompilyator avtomatik ravishda siz uchun import qiladi. *java.lang* paketidagi klasslar avtomatik ravishda import qilinadi.

Math klassi avtomatik import qilinadigan klasslardan biri, shuning uchun *Math* klassini import qilish zarur emas.

Java kompilyatori avtomatik ravishda dasturning boshiga quyidagini joylashtiradi:

import java.lang.;*

API klasslardan foydalanayotganda ichini bilish zarur emas, faqatgina klassning interfeysidan qanday qilib foydalanish kerakligini bilish yetarli.

Klassning interfeysi deganda metodlardan qanday qilib foydalanish tushuniladi. Misol uchun *Scanner* klassining *next, nextLine, nextInt, nextDouble* va hokazo.

Metoddan foydalanish, qanday turdagi argumentlarni kiritish va qanday turdagi qiymatni qaytarishini bilish talab etiladi.

Misol ushun *Scanner* klassining *nextInt* metodi sarlavhasi quyidagicha bo'ladi:

public int nextInt();

nextInt metodini chaqirishga misol: *int days = stdIn.nextInt();*

Math klassi metodlarining ba'zi API sarlavhalari:

- *public static int abs(int num);*num ning absolyut qiymatini qaytaradi
- *public static double abs(double num);*num ning absolyut qiymatini qaytaradi
- *public static int max(int x, int y);*x va y ning kattasini qaytaradi
- *public static double max(double x, double y);* x va y ning kattasini qaytaradi
- *public static int min(int x, int y);* x va y ning kichigini qaytaradi
- *public static double min(double x, double y);* x va y ning kichigini qaytaradi
- *public static double pow(double num, double power);* Num ni power darajasini qaytaradi
- *public static double random();* 0.0 va 1.0 oralig'idagi ixtiyoriy sonni qaytaradi
- *public static long round(double num);* num ga yaqin butun sonni qaytaradi
- *public static double sqrt(double num);* num ning kvadrat ildizini qaytaradi
- *public static double ceil (double y);* y ni katta butun songa qarab yaxlitlaydi
- *public static double floor(double y);* y ni kichik butun songa qarab yaxlitlaydi
- *public static double exp(double d);* e ning d darajasini qaytaradi
- *public static double log(double d);* d ning natural algoritmini qaytaradi
- *public static doublesin(double x);* x ning sinusini qaytaradi
- *public static double cos(double x);* x ning cosinusini qaytaradi
- *public static double tan (doublex);* x ning tangensini qaytaradi
- *public static double asin(double x);* x ning arksinusini qaytaradi
- *public static double acos(double x);* x ning arkkosinusini qaytaradi
- *public static double atan(double x);* x ning arktangesini qaytaradi.

Math klassining barcha metodlarining chap qismida *static* modifikatori turibdi. *Math* klassining barcha metodlari statik (klass metodlari) hisoblanadi. Bu shuni anglatadiki klass nomi bilan ishlatiladi. Misol uchun:

int position1 = 15, position2 = 18;

int distanceApart = Math.abs(position1 - position2);

Math klassida *PI* konstantasi ham mavjud.*PI* matematikada π kabi yoziladi.Qiymati *double* turiga mansub: *3.14159265358979323846.PI* ga yangi qiymat o'zlashtirmoqchi bo'lsangiz xatolik ro'y beradi.*PI* ga ham murojaat etish uchun *Math* klassi nomidan so'ng *nuqta* qo'yib foydalanamiz *Math.PI.*

String klassi doimiy, shuning uchun bir marta yaratilgan *String* ob'yektini o'zgartirib bo'lmaydi. Ko'p o'zgartirishlar kiritish lozim bo'lsa *StringBuffer*yoki *StringBuilder*klasslaridan foydalangan ma'qul.

StringBuffer klassi metodlari:

- *public append(String s);*Qiymatning oxiriga qator qo'shadi. Argument sifatida boolean, char, int, long, Strings, va h.k. bo'lishi mumkin

- *public reverse();*Qiymatni teskarisiga aylantiradi

- *public delete(int start, int end);*start indexdan boshlab end indexgacha qatorlarni o'chiradi

- *public insert(int i, String s);*i indexdan boshlab s qatorini qo'shadi

- *replace(int start, int end, String str);*start indexidan boshlab end-1 indexigacha bo'lgan qatorni str bilan almashtiradi.

NETWORK TRAFFICS CONTROL AND CLASSIFICATION BY USING OPENFLOW

K.Sh. Khosilov (PhD, TUIT)
A.T. Shokirov (TUIT, master)

To turn the concept of SDN into practical implementation, two requirements must be met. First, there must be a common logical architecture in all switches, routers, and other network devices to be managed by an SDN controller. This logical architecture may be implemented in different ways on different vendor equipment and in different types of network devices, so long as the SDN controller sees a uniform logical switch function. Second, a standard, secure protocol is needed between the SDN controller and the network device.

Both of these requirements are addressed by *OpenFlow,* which is both a protocol between SDN controllers and network devices, as well as a specification of the logical structure of the network switch functions.

OpenFlow is defined in the *OpenFlow Switch Specification,* published by the *Open Networking Foundation* (ONF). ONF is a consortium of software providers, content delivery networks, and networking equipment vendors whose purpose is to promote software-defined networking.

Thus, OpenFlow can be used with network traffic involving a variety of protocols and network services. Note that at the MAC/link layer, only Ethernet is supported. Thus, OpenFlow as currently defined cannot control Layer 2 traffic over wireless networks.

We can now offer a more precise definition of the term *flow*. From the point of view of an individual switch, a flow is a sequence of packets that matches a specific entry in a flow table. The definition is packet-oriented, in the sense that it is a function of the values of header fields of the packets that constitute the flow, and not a function of the path they follow through the network. A combination of flow entries on multiple switches defines a flow that is bound to a specific path.

The *instructions component* of a table entry consists of a set of instructions that are executed if the packet matches the entry. Before describing the types of instructions, we need to define the terms "Action" and "Action Set." Actions describe packet forwarding, packet modification, and group table processing operations. The OpenFlow specification includes the following actions:

1. *Output:* Forward packet to specified port.
2. *Set-Queue:* Sets the queue ID for a packet. When the packet is forwarded to a port using the output action, the queue id determines which queue attached to this port is used for scheduling and forwarding the packet. Forwarding behavior is dictated by the configuration of the queue and is used to provide basic QoS support.
3. *Group:* Process packet through specified group.
4. *Push-Tag/Pop-Tag:* Push or pop a tag field for a VLAN or MPLS packet.
5. *Set-Field:* The various Set-Field actions are identified by their field type; they modify the values of respective header fields in the packet.

6. *Change-TTL:* The various Change-TTL actions modify the values of the IPv4 Time To Live (TTL), IPv6 Hop Limit, or MPLS TTL in the packet.

An *Action Set* is a list of actions associated with a packet that are accumulated while the packet is processed by each table and executed when the packet exits the processing pipeline. Instructions are of four types:

1. *Direct packet through pipeline:* The Goto-Table instruction directs the packet to a table farther along in the pipeline. The Meter instruction directs the packet to a specified meter.
2. *Perform action on packet:* Actions may be performed on the packet when it is matched to a table entry.
3. *Update action set:* Merge specified actions into the current action set for this packet on this flow, or clear all the actions in the action set.
4. *Update metadata:* A metadata value can be associated with a packet. It is used to carry information from one table to the next.

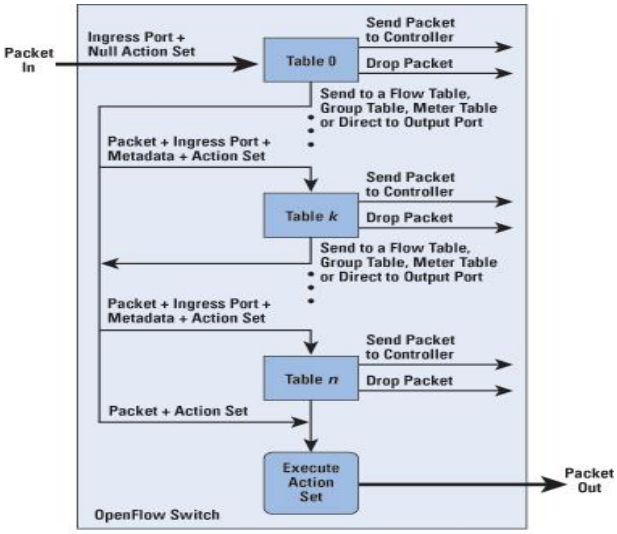


Figure 1. Packet Flow Through OpenFlow-Compliant Switch

When a packet is presented to a table for matching, the input consists of the packet, the identity of the ingress port, the associated metadata value, and the associated action set. For Table 0, the metadata value is blank and the action set is null. Processing proceeds as follows:

Find the highest-priority matching flow entry. If there is no match on any entry and there is no table-miss entry, then the packet is dropped. If there is a match only on a table-miss entry, then that entry specifies one of three actions:

a. Send packet to controller. This action will enable the controller to define a new flow for this and similar packets, or decide to drop the packet.
b. Direct packet to another flow table farther down the pipeline.
c. Drop the packet.

If there is a match on one or more entries other than the table-miss entry, then the match is defined to be with the highest-priority matching entry. The following actions may then be performed:

a. Update any counters associated with this entry.
b. Execute any instructions associated with this entry. These instructions may include updating the action set, updating the metadata value, and performing actions.
c. The packet is then forwarded to a flow table further down the pipeline, to the group table, or to the meter table, or it could be directed to an output port.

Message	Description
Controller-to-Switch	
Features	Request the capabilities of a switch. Switch responds with a features reply that specifies its capabilities.
Configuration	Set and query configuration parameters. Switch responds with parameter settings.
Modify-State	Add, delete, and modify flow/group entries and set switch port properties.
Read-State	Collect information from switch, such as current configuration, statistics, and capabilities.
Packet-out	Direct packet to a specified port on the switch.
Barrier	Barrier request/reply messages are used by the controller to ensure message dependencies have been met or to receive notifications for completed operations.
Role-Request	Set or query role of the OpenFlow channel. Useful when switch connects to multiple controllers.
Asynchronous-Configuration	Set filter on asynchronous messages or query that filter. Useful when switch connects to multiple controllers.
Asynchronous	
Packet-in	Transfer packet to controller.
Flow-Removed	Inform the controller about the removal of a flow entry from a flow table.
Port-Status	Inform the controller of a change on a port.
Error	Notify controller of error or problem condition.
Symmetric	
Hello	Exchanged between the switch and

Figure 2: OpenFlow Messages

The OpenFlow protocol describes message exchanges that take place between an OpenFlow controller and an OpenFlow switch. Typically, the protocol is implemented on top of SSL or Transport Layer Security (TLS), providing a secure OpenFlow channel.

The OpenFlow protocol enables the controller to perform add, update, and delete actions to the flow entries in the flow tables. It supports three types of messages, as shown in Figure 2.

The OpenFlow protocol enables the controller to manage the logical structure of a switch, without regard to the details of how the switch implements the OpenFlow logical architecture

DEEP PACKET INSPECTION AND ITS BENEFITS

A. A. Makhamadjonov (master of TUIT)

A number of researchers have examined DPI technology. For example, stated that DPI devices can operate on layers two through seven of the Open Systems Interconnect (OSI) model. Deep packet inspection is packet filtering that inspects the data payload of an IP packet.

DPI devices take deep looks into the data of each packet and either allows or denies passage according to some set of predetermined rules. As networks incorporate increasingly sophisticated services into their infrastructure, DPI uses application-specific data found in packet payloads to make routing decisions, to block or rate-limit unwanted traffic, to perform intrusion detection, and to provide quality of service. The DPI inspection engine parses each packet and compares the contents against its rule set. This rule set is comprised of known electronic signatures of content which allow identification of the packet's data. In the past, network packets were classified by their headers, but DPI now allows them to be classified by the actual content of their payloads.

To perform this functionality, DPI devices rely on a database of application signatures that are crosschecked against to determine the nature of the packet traversing the network. The DPI device groups the packets by protocol and security levels then processes the packets by "performing application level checks as well as stateful inspection". DPI devices look for any anomalies in the packets based on their know application signatures. If any packet is deemed out of the ordinary, it is not allowed to pass. An example would be the order in which commands are given for a certain protocol. An application will always order commands in the same sequence, where as a human attempting to hack into a system might issue the commands in some random order. By inspecting the packet for its application signature, then comparing that signature

against known parameters, DPI devices can thwart attacks that would have gotten past traditional packet inspection principles.Normally, DPI is used to monitor and shape IP traffic. ISPs can use DPI to monitor the type of traffic on their networks and give priority to the protocols they deem more important.This type of traffic shaping can slow down less important protocols, while not entirely cutting of access to the particular service.

Deep packet inspection does come with a heavy cost on the processing and bandwidth sides of the equation. To perform such a thorough look at each individual packet traversing a network, while keeping the throughput speed at normal levels, is quite a challenge. Becchi (2007) and Kumar (2006) showed that advanced algorithms are needed to enhance DPI's ability to meet the challenge. They argued the processing bottleneck is a result of the speed in which comparisons between known electronic signatures and quickly moving data occurs. As the data is moving at ever increasing speeds, it is necessary for the processing to increase at the same rate as the bandwidth. Not until recently have DPI device vendors been able to come close to real time DPI for mass market consumption. Even then, the financial costs can be prohibitive. Anderson (2007) noted that "...top-of-the-line products can set you back several hundred thousand dollars, but some of them can inspect and shape every single packet—in real time— for nearly a million simultaneous connections while handling 10-gigabit Ethernet speeds and above." The processing power needed to make DPI successful at real time speeds has been the major roadblock to widespread adaptation of the technology. Along with throughput concerns comes the fact that DPI devices depend upon software to match, categorize, interpret and finally decide which packets are allowed to pass. As with any software, there are bound to be some cases of vulnerability. According to Porter (2005), Remote Procedure Call (RPC) attacks, stack overflow attacks, buffer overflow attacks, VoIP command processing vulnerabilities and H.225 messages over TCP are all cases of known DPI vulnerabilities. Even though DPI provides a robust manner in which to monitor network communications, it is an evolving technology.

Deep packet inspection can provide many benefits for corporate and ISP environments. The addition of a DPI to a network monitoring portfolio can help to bolster the services and security provided by their respective networks. Increased service levels can be attained by utilizing content-based traffic management while increased understanding and control of their networks will help to cut operating and capital expenditures. Application aware switches can provide increased load balancing, authentication and monitoring capabilities. In addition to increased service levels and more control, DPI can help ISPs secure their networks by implementing network intrusion detection systems based on electronic signatures of well known threats.

Previous network monitoring devices only gave the network administrators an overview of bandwidth, services and the destination of network traffic. By adding DPI functionality, network monitoring takes a step up to the next level. Companies will be able to stop many network attacks in their tracks. Combining existing intrusion prevention technology with the additional filtering of DPI devices will allow for networks to identify and prevent many attacks that currently are able to bypass today's prevention measures. ISPs will be able to shape their bandwidth to better serve their customers most critical needs. DPI will allow them to throttle services at peak usage times to better accommodate the needs of their customers. While a DPI device is in use, ISPs and corporations will gain a deeper understanding of what their networks are actually being used for. This greater level of knowledge will allow them to focus on specific areas of need and not waste time or expense on areas that are performing up to par. As a result of a more controlled network, companies can focus on additional services and offerings that will help to generate additional opportunities for revenue generation. Hill (2006) wrote that "Once ISPs have networks under better control, it is time to look into how to extract additional revenue streams, and DPI can be leveraged to create additional tiers of service."

DEEP PACKET INSPECTION TECHNOLOGIES

J.SH. Makhsudov (PhD, TUIT)
Sh.E. Narzullayev (TUIT, 1-course master)

The explosion of the commercial use of the Internet has created specific business and technology demands for products that could allow organizations to explore the opportunities that arose without compromising their security. Thousands of internal networks, with a high level of trust for their owners, have been connected to a public and loosely controlled network; this has opened those organizations to a series of new security problems.

One of the first concerns was the need of having a security mechanism that could allow basic definitions in terms of access control. The development of a network security policy to determine what resources could be accessed by which users, including the operations that could be performed, was always recommended as a good first step. Once the organization had this basic definition of the permissions that should be enforced at the connecting point with this new external world, it was ready to implement technologies for achieving this goal.

This vast use of HTTP and the other protocols that have been mentioned have forced most network and security administrators to create specific rules in their firewalls for allowing these types of communication in an almost unrestricted way. Several software developers of applications such as instant messaging or Internet telephony have adapted them for using these open communication channels, in an attempt to avoid organization enforced restrictions and controls. Some have even adapted their code to search and use any open port in the firewall, through approaches that remember port scanners, tools historically used for network and host security evaluation and invasion, although the reason for doing that can go beyond network security issues.

The network access control needs to become more granular, going beyond the basic functions provided by most technologies. The point is not blocking or not unblocking the HTTP port, but guaranteeing that this open port is being used only for specific types of authorized HTTP traffic. This includes protection against things like:

- Unauthorized download of mobile code, like ActiveX controls and Java applets
- Application-level attacks against Web sites
- Malware propagation through authorized protocols
- Use of authorized open ports by unauthorized applications
- Specific behaviors that could characterize an attack.

Different technologies have been used in these tasks, with limited success. Intrusion detection systems (IDS) were one of them. Although the main purpose of these technologies was to work as an auditing tool, several vendors have promised effective protection through firewall integration or active responses, such as connection resets. However, a Gartner report, published in 2003, pointed out several fundamental issues with the use of those systems, urging customers to replace them by new emerging technologies capable of not only detecting attacks, but blocking them in real time. Basically, the key arguments were:

- IDS cannot block attacks effectively, only detect them.
- Their detection capabilities were also limited, with a high number of false positives and negatives.
- The management burden is huge, theoretically demanding 24-hour monitoring of their functioning.
- They were not able to analyze traffic at transmission rates greater than 600 Mbps.

Although the report had some flaws, including technical errors like the speed limit, a huge and passionate debate was initiated. Security managers and professionals that have invested their budgets in IDS tried to justify their decisions. Vendors went even further, attempting to disqualify Gartner's arguments. But, curiously, most vendors at that time were already offering in their product ranges new options known as intrusion prevention systems (IPSs). These are

probably the most stable and mature technology capable of doing some of the actions demanded by the research report, which indicates that even they were aware of some of their product's limitations. Additionally, the report has also mentioned another recent Gartner research document that focused on a technology called deep packet inspection (DPI), that was new and then still loosely defined.

Deep packet inspection (DPI) is normally referred to as a technology that allows packet-inspecting devices, such as firewalls and IPS, to deeply analyze packet contents, including information from all seven layers of the OSI model. This analysis is also broader than common technologies because it combines techniques such as protocol anomaly detection and signature scanning, traditionally available in IDS and anti-virus solutions.It is right to affirm that DPI is a technology produced by the convergence of traditional approaches used in network security, but performed by different devices. The improvement of hardware platforms and the development of specific hardware devices for network security tasks have allowed functions that used to be carried out by separate components to be carried out by just one. However, it is not possible to argue that this convergence is complete. Vendors are still maturing their technologies and there is a huge space for improvement.Due to this convergence, it is important to understand which technologies have preceded DPI and what their drawbacks are because they have driven the demand for new technologies by not fulfilling all current network security needs.

One of the first technologies used for performing network security were packet-filtering firewalls. Those systems were implemented, basically, by using access control lists (ACL) embedded in routers. Access control was one of the primary concerns of the early age of commercial use of the Internet in the 1990s. Because routers are the connection point between internal and external networks, their use as access control devices were very natural and appropriate.

Simple packet filters analyze each of the packets passing through a firewall, matching a small part of their contents against previously defined groups of access control rules. In general, we can say that basic limitations were:

- Because they analyze individual packets, they could not identify security violations that can only be visualized by screening more of the traffic flow;
- Very little information from the packets was analyzed, avoiding the identification of several problems that could only be seen in the application layer.
- The rules were static, creating many security problems for screening protocols that negotiate part of the communication options, like ports and connections, on the fly (the FTP service is a classic example).
- In general, router ACLs, implemented through command-line parameters, are harder to manage than rules created in easy-to-use graphical user interfaces.

Due to those deficiencies, an alternative, known as application-layer firewalls or proxies, was developed. Designed with the purpose of solving the security limitations of the packet-filtering technology, proxies have adopted a very effective approach in terms of security, but are radical from the networking point of view.However, from a security perspective, pattern-matching approaches are even more ineffective in IDS than in anti-virus software. Most anti-virus software can block viruses in real-time once they are found, while most IDS can only generate an alert. They can also send a command to the firewall, asking for blocking of the source of a just-identified attack. However, this approach has at least two serious problems:

- Some attacks, including several denial-of-service techniques, can be performed using very few packets, disrupting their targets before the firewall responsible for blocking them receives any notification.
- IDSs are famous for their false positives. In case of a false alarm, the firewall can block legitimate traffic, compromising the availability of the services and creating huge administrative problems.

DPI technologies are based on a number of old approaches that used to be implemented by different devices. Hardware and software advances have allowed the convergence of those

approaches into single-box architectures that increases the security provided by them and makes their administration easier.However, single-box architectures lack defense in-depth, a key network security concept that has been used for years, which could lead to unnecessary exposure. Additionally, they create single points of failure that can compromise network availability. Nevertheless, both can be solved using technology largely available from most vendors and correct security design principles, implementing network perimeters according to specific security needs of each network. The popularization of the use of protocols with native encryption reduces the effectiveness of such solutions, but do not make then dispensable. Integrated approaches, using intrusion prevention controls, that normally include DPI, both at host and network levels, will probably be the best approach in the medium and long terms.

BASIC STRUCTURE OF ARTIFICIAL NEURAL NETWORKS

J.SH. Makhsudov (PhD, TUIT)
Sh.E. Narzullayev (master of TUIT)

Neural networks or connectionist systems are a computational approach used in computer science and other research disciplines, which is based on a large collection of neural units (artificial neurons), loosely mimicking the way a biological brain solves problems with large clusters of biological neurons connected by axons. Each neural unit is connected with many others, and links can be enforcing or inhibitory in their effect on the activation state of connected neural units. Each individual neural unit may have a summation function which combines the values of all its inputs together. There may be a threshold function or limiting function on each connection and on the unit itself, such that the signal must surpass the limit before propagating to other neurons. These systems are self-learning and trained, rather than explicitly programmed, and excel in areas where the solution or feature detection is difficult to express in a traditional computer program.

An Artificial Neural network (ANN) is a collection of neurons in a particular arrangement or configuration. It is a parallel processor that can compute or estimate any function. Basically in an ANN, knowledge is stored in memory as experience and is available for use at a future time. The weights associated with the output of each individual neuron represent the memory which stores the knowledge. These weights are also called inter-neuron connection strengths. Each neuron can function locally by itself, but when many neurons act together they can participate in approximating some function. The knowledge that is being stored will also be referred to as “numeric data”, which is transferred between neurons through weights.

ANNs learn through training. There are various training algorithms for different types of ANN, based on the specific application. Based on the training, the weights associated with each neuron adjust themselves. By training, it is meant that a set of inputs is presented repeatedly to the ANN and the weights adjusted so that the weights reach an optimum value, where optimum means that weights either tend to minimize or maximize. An ANN is trained repeatedly and at one point it reaches a stage where it has ‘learned’ a particular desired function. With proper training it can generalize, so that even new data, which was not part of the training data, will yield the desired output.

When writing an ANN, this is mimicked by using a ”perceptron” as the basic unit instead of the neuron . The perceptron can take several weighted inputs and summarize them, and if the combined input exceeds a threshold it will activate and send an output. Which output it sends is determined by the activation function and is often chosen to be between 0 and 1 or −1 and 1. Since the derivative of the activation function is often used in the training of the network, it is convenient if the derivative can be expressed in terms of the original function value, as few additional computations are needed to calculate the derivative in this case.

One problem with the ANN approach is over-fitting of the data, which happens when the classifier becomes to good at recognizing the training examples, at the expense of not being able

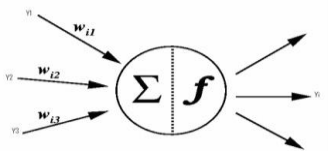
to recognize a general input. This can be avoided by cross-validation, where the network is trained on one set of data, and then evaluated on a separate one. When the error starts rising in the validation set, the network might be over-fitted. If previous networks are saved, the network can then be rolled back to the one which gave the smallest error.

The fundamental processing element of a neural network is a neuron. This building block of human awareness encompasses a few general capabilities. Basically, a biological neuron receives inputs from other sources, combines them in some way, performs a generally nonlinear operation on the result, and then outputs the final result.

Within humans there are many variations on this basic type of neuron, further complicating man's attempts at electrically replicating the process of thinking. Yet, all natural neurons have the same four basic components. These components are known by their biological names - dendrites, soma, axon, and synapses. Dendrites are hair-like extensions of the soma which act like input channels. These input channels receive their input through the synapses of other neurons. The soma then processes these incoming signals over time. The soma then turns that processed value into an output which is sent out to other neurons through the axon and the synapses.

Recent experimental data has provided further evidence that biological neurons are structurally more complex than the simplistic explanation above. They are significantly more complex than the existing artificial neurons that are built into today's artificial neural networks. As biology provides a better understanding of neurons, and as technology advances, network designers can continue to improve their systems by building upon man's understanding of the biological brain. But currently, the goal of artificial neural networks is not the grandiose recreation of the brain. On the contrary, neural network researchers are seeking an understanding of nature's capabilities for which people can engineer solutions to problems that have not been solved by traditional computing.

Neurons are basic building blocks of a neural network. They are processing elements that accept signal inputs, process them using a function and then form an output signal. They are also called basic nodes or units that accept inputs from an external source. Each input to a neuron has



a weight or gain associated with it. In Figure-1, the neuron output Y_i is a function of the weighted input that can be expressed by, $f\left(\sum_{j=1}^{3} W_{ij} * Y_j\right)$

W_{ij} are weights associated with the i W_{ij} th neuron where i=1, 2….n; j=1, 2, 3; n is

the number of neurons. The Y_j are the inputs to the neuron. Y_i is the output of the ith neuron. Figure-1 shows a simple neuron.

Figure-1. Simple neuron

A function is applied to the dot product of the weight vectors and input vectors. The dot product $W_{ij} * Y_j$ (for j = 1,2…n) is the net input to the ith neuron. Also the output of the neuron could be an input to some other neuron through another set of weights.

These networks need to be capable of an infinite number of responses. Applications of this type include the "intelligence" behind robotic movements. This "intelligence" processes inputs and then creates outputs which actually cause some device to move. That movement can span an infinite number of very precise motions. These networks do indeed want to smooth their inputs which, due to limitations of sensors, comes in non-continuous bursts, say thirty times a second. To do that, they might accept these inputs, sum that data, and then produce an output by, for example, applying a hyperbolic tangent as a transfer function. In this manner, output values from the network are continuous and satisfy more real world interfaces. The greatest advantage of ANNs is their ability to be used as an arbitrary function approximation mechanism that learns

from observed data. However, using them is not so straightforward, and a relatively good understanding of the underlying theory is essential.

- Choice of model: This will depend on the data representation and the application. Overly complex models tend to lead to challenges in learning.
- Learning algorithm: There are numerous trade-offs between learning algorithms. Almost any algorithm will work well with the correct hyperparameters for training on a particular fixed data set. However, selecting and tuning an algorithm for training on unseen data require a significant amount of experimentation.
- Robustness: If the model, cost function and learning algorithm are selected appropriately, the resulting ANN can be extremely robust.

With the correct implementation, ANNs can be used naturally in online learning and large data set applications. Their simple implementation and the existence of mostly local dependencies exhibited in the structure allows for fast, parallel implementations in hardware.

THE POLITICAL POTENTIALS OF DPI

M.B. Mirzaeva (PhD, TUIT)

States have been monitoring and analyzing citizens' telecommunications since the telegraph, to the point of retaining encrypted text and banning certain modes of communications for fear that they would undermine state surveillance. DPI lets network operators monitor communications remotely and in real time for content of interest. Given its capacity to monitor the content of communications, DPI can be helpful in supporting 'lawful access' legislation and limiting the transmission of content the state has outlawed.

Lawful access legislation enhances policing and intelligence powers. There are typically three types of access powers associated with such legislation: search and seizure provisions, interception of private communications powers, and production of subscriber data. Deep packet inspection equipment is most useful in intercepting communications, and can be thought analogously as installing wiretap capabilities into digital networks. By installing DPI routers at key points in ISPs' networks, it is theoretically possible to remotely monitor communications of those suspected of engaging in illegal acts by making copies of all data traffic or specifically targeting one type of traffic (e.g. VoIP, web browsing, or peer-to-peer) and not logging or monitoring traffic that falls outside of the specified rule set. It is important to recognize that, while using DPI might be seen as the logical technology to facilitate state-based surveillance, this mode of monitoring differs from traditional wiretapping capabilities because of the breadth of communications that occur online. Whereas a traditional wiretap would capture voice communications, DPI-facilitated surveillance can capture and perform front-line analysis on any type of digital transaction, be it a voice communication, text-based chat, web browsing session, or any other kind of non-encrypted transmission. As such, DPI-based 'wiretapping' arguably stretches what it meant by wiretapping to a considerable degree, and it may not constitute 'maintenance' of state surveillance powers but an expansion of these powers.

As private copyright holders may be motivated to monitor for infringing files coursing across digital networks for civil reasons, the government may be concerned with monitoring and preventing content transmission it has deemed illegal. Using techniques similar to those exercised to monitor for copyright infringement, but with policies designed to take action on data traffic rather than just watching the wire for it, government could try to blacklist files known to contain child pornography, viruses, malware, disapproved encryption protocols, confidential or secret government documents, and so forth. Blocking or monitoring content could take the form of a government requiring certain routing equipment be installed in network providers' infrastructure or demanding that those same providers install and operate the equipment on the government's behalf. Moreover, such analysis and identification requires massively monitoring communications streams. Such actions do not focus on specific individuals, as with a wiretap.

The political capacity to monitor, mine, and censor for certain data traffic will almost certainly depend on framing. Governments have historically used the language of safety, security, and order to justify blocking communications content. This language of "securitization," a process whereby issues, problems, and phenomena are defined in "security" terms and associated with a "protectionist reflex" can be used to legitimize extraordinary means to solve a perceived problem. While state agents could be responsible for ensuring that content is appropriately mediated, it is possible that the same end – blocking content – could be achieved by a shift towards intermediary liability.

Under such a liability approach "the intermediaries, or companies transmitting or hosting user's communications or other content, are held liable for their user's and customers behavior."

Companies' awareness of their technical capabilities, combined with their (perceived) protection from individual complaints about violations of freedoms of speech and association, can make them the ideal party to which to outsource Internet censorship. Of course, a widespread shift to this liability structure – where ISPs are held accountable for what their subscribers transmit and receive – would constitute a significant transition away from common carrier protections.

Such protections, in theory, immunize ISPs from legal liabilities for what their subscribers transmit so long as the ISPs themselves are not aware of what their networks are carrying. A shift towards ISP liability, however, would effectively mandate awareness of what traffic is being carried. Such a shift might serve to largely formalize already existing practices: today social networking companies, ISPs, journalism sites, and other interactive content communities often censor or block the sharing and posting of content deemed offensive or problematic by the organization in question. Scaling the magnitude of what is blocked or reported to authorities and formalizing the existence of such policies may constitute a quantitative shift but not necessarily a qualitative one in terms of the kinds of actions undertaken.

When simultaneously considering the technical, economic, and political potentialities of deep packet inspection technologies it's helpful to keep in mind that the potential uses of the technology may not necessarily be practically instantiated in real world networking situations. Further, some of the "pure" technical capabilities are infused with the values of control and awareness of the network, and those advocating that the technology be used to meet technical, economic, or political goals may differentially express such values. It is only as I move into the case studies, however, that I will ascertain both the specific drivers and configurations of technologies as well as whether the potentialities of the technology can be, or are being, practically instantiated in the real world.

DPI TIZIMINING TEXNIK TASHKIL ETILISHI

E.B. Normurodov (TATU, 1-bosqich magistranti)

Foydalanuvchilarning ma'lumot uzatish tarmoqlariga qo'yadigan talablari yildan yilga oshib bormoqda. Natijada, Internet provayderlari tashqi kanallar sonini ko'paytirish, yangi qurilmalarni qo'llash orqali tarmoq samaradorligini tushirmaslikka harakat qiladi, katta miqdordagi onlayn videoservislar, P2P tarmoqlaridan ommaviy foydalanish natijasida yangi qurilmalarning resurslaridan nooqilona foydalanishi yuz bermoqda. Bu holat esa operator tomonidan ilovalar trafigini boshqarish zaruratini keltirib chiqaradi. Bugungi kunda trafikni boshqarishning asosan quyidagi usullaridan foydalaniladi:

- ✓ MAC-adreslar yoki VLAN asosida;
- ✓ Uzatuvchi va qabul qiluvchilarning IP adreslari asosida;
- ✓ TCP va UDP portlari raqamlari orqali;
- ✓ Proksi-serverlarda domen nomlarini cheklash asosida.

Bu usullar OSI modelining faqatgina transport sathigacha ishlashga mo'ljallangan tarmoqlararo ekranda amalga oshirilishi mumkin. DPI texnologiyasini tadbiq qilish internet va

boshqa ma'lumot uzatish tarmoqlarida turli saytlarga ulanishni cheklash, tarmoqqa ruxsatsiz kirishni cheklash, tarmoqni virusli dasturlar va keraksiz axborotlardan tozalash, tarmoqlardagi turli noqonuniy reklamalarni kesib tashlash, xavfsizlikka tahdid soluvchi turli axborot paketlarini tutib qolish, bir so'z bilan aytganda provayder o'z tarmog'ini to'liq nazorot ostiga olish imkonini beradi. DPI tizimlari traffik klassifikatsiyasini to'g'ri va aniq amalga oshirishi uchun turli internet dasturlarini aks ettiruvchi katta hajmdagi signaturalar bazasi bilan ta'minlanishi lozim. DPI tizimiga qo'yiladigan muhim talablardan yana biri, u paketni ma'lumot uzatish kanali tezligida tekshirishi kerak. Bu esa tarmoqda bo'lishi mumkin bo'lgan yo'qotishlarni va yuklamalarni oldini oladi. DPI (Deep Packet Inspection) tizimi paketlarni OSI modelining 2-sathidan 7-sathigacha nazorat qilish imkoniyatiga ega.

DPI tizimi imkoniyatlari quyidagilardan iborat:

- ✓ turli ko'rinishdagi statistik ma'lumotlarni yig'ish;
- ✓ turli mezonlar asosida trafikni filtrlash (bunda odatiy "IP-adres+port"ga domen nomlari va protokollari ham qo'shiladi, masalan P2P yoki Skype trafiklarini aniqlash imkoniyati mavjud);
- ✓ foydalanuvchilarga turli darajada xizmat ko'rsatish;
- ✓ hujumlardan himoya qilish. Code Red, NIMDA , SQL Slammer, DoS, DDoS kabi tarmoq hujumlaridan himoyalash.

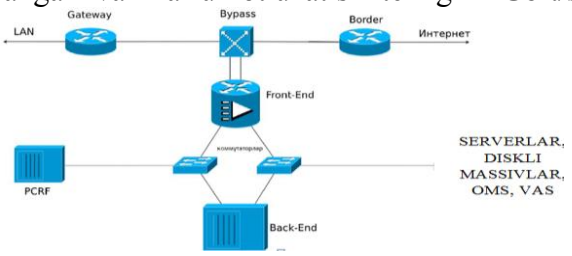
DPI tizimi aloqa operator tarmog'ining chegarasiga qo'yiladi. DPI texnik vositalari quyidagi komponentlardan tashkil topgan:

- ✓ Bypass;
- ✓ Front-End qurilmasi;
- ✓ Back-End qurilmasi;
- ✓ PCRF-serveri (Policy and Charging Rules Function);
- ✓ komponentlar orasida aloqani ta'minlaydigan kommutatorlar;
- ✓ serverlar (qo'shimcha);
- ✓ disk massivlari (qo'shimcha);
- ✓ VAS qurilmasi (Value Added Services – spam va viruslar tekshiruvi) (qo'shimcha). Umumiy sxemasi 1-rasmdagi ko'rinishga ega.

Birinchi bo'lib tarmoqqa Bypass, keyin esa unga Front-End ulanadi. Bypass ikkita ishlash rejimiga ega:

1. Himoya. Trafik to'g'ri liniyaga o'tib ketadi va Front-End qurilmasiga uzatilmaydi.
2. Ishchi. Trafik Front-End qurilmasiga uzatiladi.

Front-End ishdan chiqqanda, uning portlariga ulangan kabel shikastlanganda, DPI texnik vositalari elektr ta'minotidan uzilib qolganda Bypass himoya rejimiga o'tadi. Bypass elektr yoki optik turda bo'lishi mumkin. Elektr Bypass relega asoslangan bo'lib, mis simlar ulashga mo'ljallangan va ma'lumot uzatish tezligi 1 Gbit/s gacha bo'ladi.



1-rasm. DPI tizimining tipik sxemasi

Optik Bypass bir necha afzalliklarga ega: ma'lumot uzatish tezligi 10 Gbit/s gacha, trafikni akslantirish imkoniyati yuzaga keladi (trafik to'g'ri kanal bo'yicha ketayotganda uning nusxasi Front-End ga uzatiladi, trafik bilan hech qanday amallarni bajarish imkoniyati mavjud bo'lmasada, statistika olib borish mumkin bo'ladi). Front-End qurilmasida paketlar OSI modelinig kanal sathidan amaliy sathigacha tahlil qilinadi. Operator tarmoq

samaradoligini oshirish maqsadida alohida turdagi trafikni cheklab qo'yishi mumkin. SHuningdek, tarmoqdagi turli hujumlardan himoyalanish ham Front-End qurilmasida bajariladi. Back-End qurilmasida barcha qoidalar majmuasi, yig'ilgan ma'lumotlar statistikasi, signaturalar, akslantirish va qayta yo'naltirish marshrutlari yig'iladi.

PCRF-serverining asosiy vazifasi foydalanuvchi-qoida raqami mosligini saqlash. Front-End qurilmasi PCRF-serveriga abonent identifikatorini uzatadi, PCRF-serveri javob tariqasida Front-End qurilmasiga qoida raqamini uzatadi, Front-End qurilmasi bu qoidaning tavsifi yuzasidan Back-End qurilmasiga so'rov yuboradi.

THE TECHNICAL POSSIBILITIES OF DPI

A.S. Umarov (assistant, TUIT)
A. A. Makhamadjonov (master of TUIT)

Network administrators are concerned with the functioning of the network itself: are security incidents logged and kept to a minimum? Do network policies simultaneously ensure the functioning of the network and meet users' expectations and needs? Are the network's nodes appropriately configured to address congestion? Deep packet inspection helps administrators improve network security, implement access requirements, guarantee quality of service, and tailor service for particular applications. Each of these functions is dynamic, insofar as the technology can utilize layered rule sets and is incorporated within a broader networking assemblage to dynamically react to changes in the network. As a result of DPI's penetration into packet transfers, combined with its potentialities, the technology can be helpful in daily and long-term network operations.

DPI was initially meant to offer network providers improved intrusion detection and prevention mechanisms that could recognize and respond to contemporary threats. To respond to emerging threats, DPI appliances are reconfigurable and can scale to monitor high volumes of traffic and to provide logging and anomaly detection. Logging establishes a pattern of known behavior and lets the system (and system administrator, if they examine the logs) examine traffic 'offline'. Offline analysis facilitates a granular analysis of the traffic because it needn't occur in real time, thus mitigating some of the technical challenges associated with in-depth analysis of data packets while maintaining high data-transit speeds. As a result of logging traffic, systems and administrators can 'learn' how to sub-classify network traffic within applications. To make analysis process a bit clearer, consider a process of logging unencrypted HTTP, or web browser, traffic.

It is also possible to use logging-based learning to develop expected use-patterns for individual users and applications and to send notifications to administrators if deviations from the norms are detected. Such deviations may indicate that a known client's credentials are being used by a third-party to access the network, based on suspicious or deviant data transmissions and receptions, or that an application has been infected with malware. Because DPI systems afford high levels of control, if a particular detection signature is too 'chatty' – if a signature is being identified regularly but is uninteresting to the network administrator – the DPI system can be set to either ignore or more carefully monitor the signature in question. A more careful monitoring schema might narrow down the parameters of the inspection, such as shifting from monitoring for all encrypted communications across a corporation to monitoring for encrypted communication in specific business units that are not expected to engage in secure communications. Alternatively, the system might be set to avoid establishing a 'normal' activity pattern for authenticated 'guest' accounts because the logged in user(s) regularly changes, though the equipment could still watch for anomalous application behavior.

More generally, as a component of an integrated security processes, DPI can examine inbound and outbound data traffic and flag packets that warrant a more sustained analysis of their contents. This flagging might happen when the device cannot positively identify the

application responsible for the packet or when the device is configured to forward some packets to a proxy server prior to delivery. At the intermediary between the DPI appliance and destination, an algorithmic analysis may be performed. Such an analysis might examine whether an email attachment contains material that cannot enter or exit the network or might generate an alert requiring a human to evaluate the information, such as when abnormal packets are being received or transmitted, or to vet the appropriateness of email attachments. When directing data traffic beyond the network that the DPI is integrated into, the DPI device might add a prefix to a packet's header to indicate the quality of service it should receive, whether the packet is the bottom of a 'stack' or series of related packets, or the device might impose a time-to-live value that overwrites the value set by the client sending the packet. Stacks of tags might nest a series of attributes, such as Quality of Service or where the packet should be forwarded, and may be coded so that egress or ingress networks can act on the attributes. Such prefixes can also be used in establishing virtual private networks when partnered with perimeter edge routers that can maintain their own routing tables. Perimeter routers will identify what other routers traffic can be forwarded to, and they separate traffic so that users cannot see data outside of their network. Using this approach, encryption is not required because traffic cannot deviate from pre-programmed traffic routes.

Existing policy management tools and servers will often guide the technical management of data traffic. Policy control is "a broad concept" that "is usually based on the use of an automated rules engine to apply simple logical rules which, when concatenated, can enable relatively complex policies to be triggered in response to information received from networks." Network managers can examine which account is authenticated to a particular data stream, call the rules dictating how that user can transmit and receive data, and then examine the entire packet stream and mediate data flows as dictated by the policy governing the user. This management capability may mean that an ISP's entry-level client is prevented from transmitting any packets that are unrelated to HTTP (web-based) or SMTP (email-based) traffic, whereas premium users have all of their data traffic prioritized over that of other users of the network. Policy controls permit a vast range of rules, which may prioritize or deprioritize specific kinds of traffic either in perpetuity, at certain points in the day, or for certain users. Policy controls can block some content if the user's account does not permit its reception or transmission, or they can modify some data traffic in real time. Modifications might include changing HTTP traffic so users see a banner that notes that they are nearing or exceeding the volume of data they are provided within a billing cycle or warning them that they might be infected with a virus, worm, or other piece of malware in their web browser. The policies, and their associated servers, work hand-in-hand with DPI devices, often guiding how the devices themselves take action on packets traversing the network.

Deep packet inspection equipment can be used to mitigate the inconveniences associated with router congestion. By identifying and prioritizing packets in real time, DPI appliances can ensure that time-sensitive packets, such as those associated with voice over Internet protocol (e.g. Skype) communications, are moved up in the 'queue' of packets and those that are less sensitive, such as email, are dropped to be resent. Alternately, if the network operator has identified particular applications or application types that significantly contribute to router congestion, particular rules can be established to limit the amount of the router's bandwidth they can consume. Thus, 20% of a router's aggregate bandwidth might be allocated to the 'problem' application or application-type, and the remaining 80% of aggregate bandwidth might be available to all other data traffic. The administrator could forgo assigning bandwidth to any particular application and instead limit the amount of bandwidth that it could consume. Such limitations would restrict the associated application's potential data rates and, as a result, lessen 'problematic' applications' contributions to router congestion. These techniques have raised concerns: there is a fear that analyzing packets using DPI to assign packet priority levels may actually worsen congestion by ultimately requiring higher levels of packet retransmission than would occur without DPI-enhanced analysis and that such analysis may not identify the real

cause of congestion, the expansion of router buffers to hold more and more packets for transmission instead of dropping them more rapidly. Such concerns have not prevented network administrators from installing DPI equipment in their networks or from monitoring and acting on data packets.

The network operator has made some kind of decision about the appropriateness of the applications that end-users are employing: either some applications are more important than others or are identified as problematic and thus have special rules crafted to mediate their ability to generate congestion. Using DPI, a network operator can also shift focus from the application to the user. In this situation, an administrator might establish conditions concerning how clients can utilize available bandwidth. As an example, when a client has used its maximum allotted bandwidth for a 15-minute interval, it might have *all* of its traffic deprioritized or delayed for a period of time following the interval. This action has the effect of prioritizing 'bursty' traffic, that which transmits data in short intervals rather than over a long period of time. Accessing webpages generates bursty traffic, whereas long file transfers using either peer-to-peer applications or a file transfer client are non-bursty types of traffic. This user-centric approach can be seen as 'application agnostic', insofar as it does not target specific applications, though the rule set will disproportionately affect some applications, such as peer-to-peer and FTP clients, over others, such as web browsing.

THE ECONOMIC POTENTIALS OF DPI

A.S. Umarov (assistant of TUIT)
KH.N. Teshaboev (master of TUIT)

The ability to examine and act upon data packets in real time affords new revenue opportunities for ISPs and third parties alike, as well as offering ways to curtail threats to revenue maximization. Specifically, Internet service providers may be motivated to offer differentiated service plans that compete based on what applications customers can use to connect to the web, the priority that applications' packets are given at routers, or the speed at which users can access websites. ISPs may also prioritize their own 'value added' services, such as voice over Internet protocol, email, or home security systems, over services offered by their competitors. Parties other than network owners may also be interested in DPI: copyright holders may try to limit the sharing of files that infringe on copyrights, and advertisers may monitor and mine data traffic to identify consumer habits and subsequently modify packets to serve targeted ads.

ISPs have offered differentiated service plans since dial-up modem pools were used to connect to the Internet. Today, broadband connections mean that ISPs compete based on the rate that data is exchanged between the client's location and the Internet, the volume of data they are permitted to transfer each month, value-added services such as email accounts, and cost of service delivery. DPI lets ISPs further distinguish their offerings by selectively letting applications connect to the Internet; a web browser and email client connection might be included in a 'basic' Internet package, whereas video game applications or streaming music applications might be included in a 'premium' package. The fungibility of DPI and deep integration with policy control servers afford advantages over prior networking technologies, such as MPI, insofar as the same device is better able to mediate multiple different data forms and formats. Further, whereas some data types, such as web traffic, or data sources, such as a national online newspaper, might not be counted towards a monthly data quota, other data types and sources could. Alternatively, an ISP could limit or prevent access to the Internet unless customers pay for each connected device; DPI can be used to examine data traffic and ascertain whether 'registered' or 'unregistered' devices are attempting to access the Internet and, in the case of unregistered devices, limit their access until a fee is paid. Figure four gives a theoretical example of what these kinds of pricing formats might look like.

This limitation by device is part of an 'app-model' for the Internet, where connectivity is bundled with a particular application, such as an online movie watching application, or a particular device, such as a PC or tablet computer. In an app-based model, users may never see how much bandwidth volume or capacity they are afforded and instead enjoy only selective access to the Internet based on the services paid for on a monthly basis. This approach to Internet pricing might be combined with, or supplemented by, a prioritization of an ISP's own services to the detriment of competitors. The ISP's voice over Internet protocol client, or a client belonging to a company that had paid an ISP, might be 'free' with the basic package whereas competitors' VoIP traffic is given a lower priority. This approach could buttress an ISP's complementary products or enhance revenue when competitors pressure those complementary product lines. DPI could be used to identify favored applications and give them preferential treatment by guaranteeing higher levels of priority, making larger volumes of bandwidth available to them, or by not counting the data they generate against users' monthly volume limits. An ISP's exclusion of competing services or rent seeking may be logical from the stance of economics. More specifically, "[a]s long as the exclusion of rivals from its Internet-service customers translates into more sales of its complementary product, and the additional profits are larger than the costs of exclusion, exclusion will be a profitable strategy." Given the relative prevalence of viruses, malware, and spyware the exclusion of competing applications may be couched simultaneously in the languages of service and security, which mask the core economic drivers behind the facade of technical improvements to the network.

DPI also provides copyright holders with a tool to (try to) limit or monitor the traffic of infringing computer files and data streams that course across the Internet. To date, most analyses of infringing data traffic rely on questionable statistics or shoddy methodologies. In the case of the former, the United States' Government Accountability Office (GAO) has publicly rebuffed the monetary losses that American corporations claim to experience from infringement. The GAO notes that for widely cited statistics no studies exist that support estimated losses, and that efforts to evaluate actual losses suffer from methodological limitations. The introduction of detailed packet analysis equipment begins to resolve some of the methodological problems associated with quantifying infringing data traffic; by monitoring packets and cross-referencing them against their point of origin – are they from 'legitimate' digital retailers – and their contents – do the files contain copyrighted material – it is theoretically possible to develop an index of how much unencrypted data traffic is potentially infringing. If the copyright monitoring system isn't intended to prevent the movement of data, but merely log it, a DPI system could be established to do a quick analysis of packets to identify their likely contents. Where it identifies the packets as potentially holding infringing content, they could be passed to their destination, while copies are made and stored in a short-term offline storage system. Once in that system, a computer program could develop a hash value for the files and compare it against a known list of copyrighted files. Where the file was protected under copyright and the source of the transmission was an illegitimate online content provider, the storage system could call on the subscriber database, correlate the subscriber's personal information with the inappropriate exchange of infringing material, and notify an ISP administrator or member of council, copyright holders, authorities, or some other designated party.

One problem with using a hash-based analytic system is that minor changes in the file can result in different values being generated. These values would not align with the database of known hashes, and thus the DPI or offline analysis system would not identify the files as potentially infringing.

ASPECTS OF CELLULAR NETWORKS

E.M. Zarmasov (TUIT, assistant)

In 1921, Detroit police used a one-way dispatch communication in the range of 2 MHz to transmit information from a central transmitter to a receiver mounted on cars - it was the

beginning of the era of mobile communication . Since then much has changed, the mobile communication system has evolved in a very short time. Considering the evolution of mobile communication systems , we arrive at the concept of "generations". As we know, today there are four generations of mobile communication systems , and another is under construction .

The first generation : 1G

The story begins with the appearance in 1980 of several innovative network technologies : AMPS in the US and a combination of TACS and NMT in Europe. Although several generations of mobile services existed before , the three AMPS, TACS and NMT is considered the first generation (1G), because these technologies have enabled mobile phones to become a mass product . System of the first generation were analog , implemented on a sufficiently reliable networks, but with limited ability to offer services to subscribers .

The second generation : 2G

In the early 90s , a rise of the first digital cellular networks which have several advantages over analog systems. Enhanced sound quality , great security, increased productivity - are the main advantages . The most common standard of this generation is the GSM (Global System for Mobile Communications) . Since he mended the possibility of sending short text messages (SMS), as well as allowing you to transfer data faster - up to 14.4 kbit / s.

Increased demand for wireless Internet access has led to further development of the 2G. So a system called 2.5 G. An example of technology 2.5 G is GPRS (General Packet Radio Services) - a standardized packet data technology that allows you to use the mobile communication terminal to access the Internet with data transfer rates up to 100 kbit / s. However, over time, a set of services may offer 2G standards proved inadequate , leading to the appearance of third generation (3G).

The third generation : 3G

Since , in 2000, the International Telecommunication Union (ITU) has made a new standard - IMT- 2000 - approving the specification “real” 3G. It was the epoch of the wireless network. In 3G wireless network system is used , which gives so perfect sound as if it's a real conversation . Data is transmitted using packet switching . An example of a 3G system is a Universal Mobile Telecommunications System (UMTS). This standard allows you to provide subscribers with data rates up to 2 Mbit / s. Technology HSPA (3.5G), which is considered as an intermediary between the networks of the third and fourth generation , gives the rate is already up to 14 Mbit / s. Thus, network users can get a wide range of multimedia services (high-definition video , games , downloading large files) . However, even such a data transfer rate will meet the needs of the user network only up to certain limits . In this regard, began development of a standard fourth generation , which will remove the upper limit for a long time .

The fourth generation: 4G

Just as with the standard 3G, ITU took over 4G, tying him to the specification, known as IMT-Advanced. The document calls for the incoming data rate of 1 Gbit/s for stationary terminals and 100 Mbit/s for mobile. This 500 and 250 times faster than IMT-2000. This is a really great rate, which may overtake ordinary DSL-modem or direct connection to broadband. Wireless technologies play a key role in ensuring broadband access in rural areas. It is more cost-effective - to build one station 4G, which will provide a link to a distance of tens of kilometers, covering farmland than a blanket of fiber optic lines.

The fifth generation: 5G

Are currently under research and development towards the development and networking of the fifth generation . By the fifth generation networks claimed following requirements (compared with LTE): - Growth 10-100 data rate per subscriber ; - Growth of 1,000 times the average traffic consumed by the subscriber per month; -Ability To serve more (100 times) of the number of devices connected to the network ; - Lower total cost of network operation of the fifth generation .

Development of 5G networks engaged in several countries around the world. In 2015,

developers must be submitted holistic concept of standard 5G. The challenge now - to determine , on the basis of what technology will unfold new network. Optimization and standardization of equipment , as well as the first pilot launch is scheduled for 2015-2018 years , and in 2018-2020 is expected deployment of the first non- 5G networks for field testing . The commercial launch of the fifth-generation networks is not expected until 2020 .

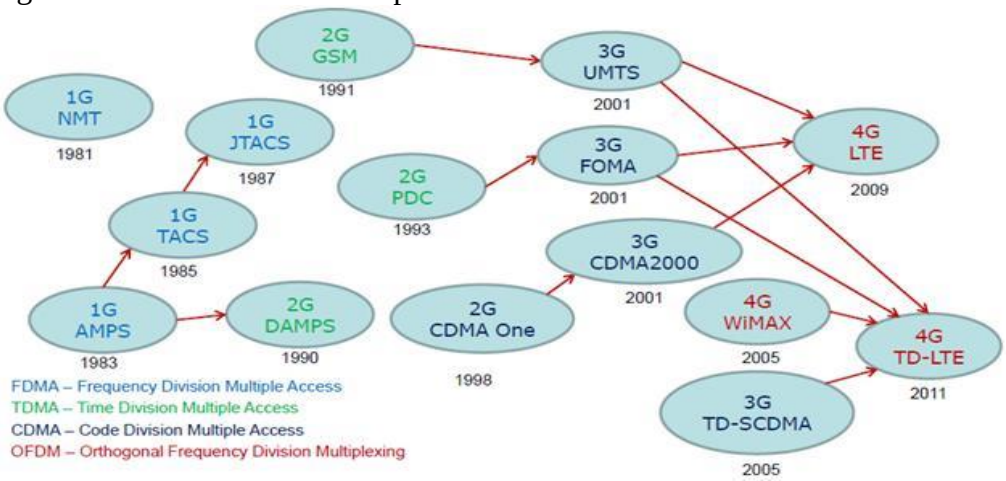


Fig-1. The evolution of mobile communication standards

Summarizing, we can say that reviewed the main direction of the evolution of network technologies in accordance with the network model proposed by the International Telecommunication Union. Identify the key factors that determine the evolution of the access network - the use of different physical environments and the need for the deployment of broadband access.

ЎРНАТИЛГАН ТИЗИМЛАРНИ VMLAB МУҲИТИДА ЛОЙИҲАЛАШ

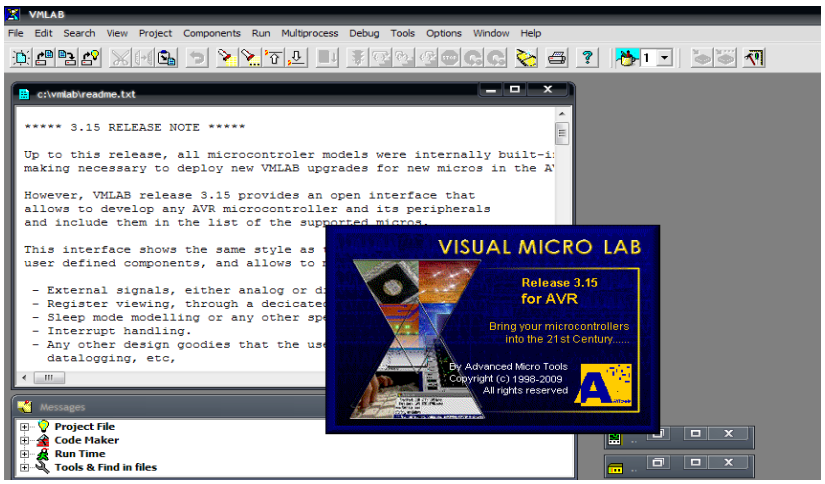
Х.Ю. Абасханова. (ТАТУ, катта ўқитувчи)

Мураккаб ўрнатилган тизимлар ривожланиши компьютерларнинг иши улкан элемент базаси асосида бажрилишидан бошланган,чунки уларнинг иш сифати талабга жавоб бермас эди. Компьютер тармоқларининг ривожланиши тақсимланган ахборот бошқарув тизимларинини ривожланишига сабаб бўлди.Интеграл микросхемаларининг ривожланиши бошқарув объктларининг МП ларини иш жараёнини ўзгаришига сабаб бўлди.

VMLAB - AVR микроконтроллерлари асосида рақамли қурилмаларни бошқариш дастурий пакетидир. Унинг таркибига ташқи қурилмалар билан уланиши мумкин бўлган виртуал қурилмалар киргани учун виртуал эмулятор деб хам айтилади. VMLAB жуда осон ассемблер ва СИ компиляторлари билан боғлана олади:

- Кучли кўп ойнали матн редактори;
- Символик дастурловчи;
- аралаш режимдаги аналог-рақамли моделлаштириш;
- кодни сифатли назорати.

VMLAB ўз навбатида иш жараёнида микроконтроллерлар асосида бошқариладиган қурилмаларни аппарат воситалари ва дастурий воситалари модели иш жараёнини яққол нмоён этади.



Расм 1. VMLAB мухити умумий кўриниши.

Эмулятор ўз навбатида светодиодлар, осциллограф, дастур ёрдамида температурани ўзгартириши, кристалл частотаси ва параллель равишда келтирилган қурилмаларда белгиланган параметрлар ишлаш жараёнини кузатиш мумкин.

e-ТОМ ПРИНЦИПИ ВА УНИНГ ТЕЛЕКОММУНИКИЯ ТАРМОҚЛАРИ ВА ХИЗМАТЛАРИНИ БОШҚАРИШДА ҚЎЛЛАНИЛИШИ

М.Н. Абдалимов (ТАТУ, ассистент)

Телекоммуникация олами фундаментал ўзгаришни бошдан кечирмоқда. Бундай ҳолат янгилик эмас. Кўплаб ривожланган мамлакатларда иқтисодий ва ҳуқуқий янгиланишга ўтиш телекоммуникация бозорини юритади, телекоммуникация инфрастуктурасини сезилмас ўсиши ва амалий бошқрилмаслиги олиб келди. Бу ўсиш ўз ичига ҳам сифатли ва миқдорий ташкил этувчиларни ўз ичига олади: юқори темпларда телекоммуникация ресурслари миқдорини ошиши ва шу билан биргаликда кўплаб янги телекоммуникация технологияларини ривожланиши.

Содир бўлган ўзгаришлар билан биргаликда “телекоммуникация” сўзини моҳияти ҳам ўзгарди. Ҳозирги кунда “ахборот технологиялари” ўсиб бораётган ўринни эгалламоқда. Ахборот технологиялари – маълумотларни сақлаш, қайта ишлаш ва жамият ҳаётида мультимедиа ахборотлприни алмашувини таъминловчи, анъанавий телекоммуникация тизим остига кирувчи технологик занжир узунлигини ташкил этувчиларидан бири ҳисобланади. Телекоммуникация ва компютер қурилмалари бугунги кунда анча мақтовли юқори даражада автоматлаштирилган тушунча. Масалан замонавий SDH мультиплексор алоқа қурилмаси ҳсобланиб, айрим интелектуал воситалар ахборотни қайта ишлайди ва белгиланган телекоммуникация масалаларини ечишда компютерлар каби мослашади. Ўзгарувчан автоматлаштирилган жараёнлар ва телекоммуникация қурилмаларини интелктуализацияси, административ бошқарув усулларини кескин ўзгариши телекоммуникация провайдерларини яшовчанлигини назорат қила олмаслигига олиб келди. Энг аввало бу “Миллий телекоммуникация назорати” ва халқаро телекоммуникация доирасида стандартлаштириш органларига таъсир кўрсатади.

Телекоммуникация бозорида ҳуқуқий масалалрини ташкиллаштиришда стандартизация усуллари ва телекоммуникация ресурсларини бошқариш тизими муамоларига дуч келамиз.

Телекоммуникацияни бошқариш доирасида стандартизация муаммолари билан бешга яқин халқаро ташкилотлар шуғулланади. Булардан ITU, ETSI ва ANSI ларни алоҳида такидлаб ўтиш жоиз. Расмий ташкилотлардан ташқаи, яна альтернатив хужатлар

ишлаб чиқарувчи ва мувофиқлаштирувчи, регламенлаштирш принциплари ва телекоммуникация хизматлари ва тармоқлари бошқариш тизимини қуриш технологияларни ишлаб чиқувчи кўплаб саноат консоцирумлар ва нотижорий бирлашмалар мавжуд. Альтернатив струтуралар TMForum (TeleManagement Forum) қаратилган. TMN кейиги ривожланиш ғояси TMForum (TMF) қаратилган. Янги индустрал TMF стандартлари бизнес жараёнларни амалга оширишга йўналтирилган.

TeleManagement Forum ёки TMF – бу глобал бошқарилмайдиган ва нотижорат ташкилот, у тармоқ ресурсларни эксплуатацияси ва телекоммуникация хизматларини бошқариш самараси ва сифатини ошириш мақсадида амалий ечимлар қабул қилиш ва стратегик бошқарув ташкил этиш маслаларини ечади.

TMF фаоллииги қуйидаги ишланма ва изланишлар доирасида тақсимланади:

- Бизнес жараёнларни моделлаштириш ва автоматлаштириш;
- Келгуси авлод тармоқ технологияларини бошқариш;
- Қурилмалар тизимини амалий реализацияси ва интеграцияси;
- Хизматларни бошқариш;
- Электрон коммерцияни бошқариш;
- Хизматлардан фойдаланувчилар билан ҳамкорликни регламентлаштириш.

Шуни айтиб ўтиш керакки, TMF телекоммуникация бошқаруви билан тўрта асосий сабабга кўра альтернатив ташкиллаштириш билан шуғулланади.:

- TMF нотижорат ташкилот ҳисобланиб, ихтиёрий ташкилот унинг аъзоси бўла олади;
- TMF хужатларини ишлаб чиқишда аъзоларнинг барчалари қатнашиши шарт эмас;
- TMF барча хужатлар телекоммуникация провайдерларининг бевосита амалий заруратидан келиб чиққан ҳолда ишлаб чиққади ва тасдиқлайди;
- TMF рационал тарзда ўз фаолиятида бошқа ташкилотлар ишлаб чиққан хужжатлар ва технологиялардан фойдаланади.

TM Forum аъзолари сервис провайдерлар, тармоқ операторлари, дастурий ва қурилма таъминотчилари ҳисобланади. Бундай истемолчилар ва хизмат кўрсатувчиларни ўзаро ҳамкорлик туфайли TM Forum натижалари юқори кўрсаткичларга эришмоқда. TM Forum фаолияти янги авлод ТДТ(System of Support Operation, OSS) ва дастурий таъминот (Software, SW), янги авлод OSS (New Generetion System of Support Operation, NGOSS) тизимларин қамраб оляпти.

Кўп поғонали абстракт бошқаришда қўллаш мумкин. Масалан тармоқ элементларини бошқариш, тармоқни бошқариш хизсатларни бошқариш. Хизматларни бошқариш поғонасини ажратиш клиентларни маълум бир хизматга ёки хизматлар гуруҳига уланишида индивидуал қараш имконини беради.

Бу модел умумий ёндошувини TMN да регламантлашдан асосий фарқи қуидагича:

- TOM-модель функция ёки функция тўпламини декларацияламасдан провайдердаги содир бўлаётган воқеаларни ўзаро муносабатини аниқлаб, бошқарувни ҳар бир поғонада жараён деб қабул қилиб жараёнларга ёндашувни намойиш этади;
- TOM дан фойдаланиш ёндашувини ишлаб чиқишда TMN дан фарқи “юқоридан қуйига”, яъни аввал технология ва тармоқ элементлари поғонасида бошқарув функцияси, сўнг тармоқ поғонасида ва ҳаказо регламентлаштирилади;
- TOM-моделда телекоммуникация провайдери ишини замонавий спецификацияси ҳар бир поғонада абонент билан боғлиқ поғона ишлаб чиқилган;
- TOM-модель TMN дан фарқли равишда тушунарли, оддий ва детализацияси катталиги билан фарқ қилади.

TOM-модель бирор технология ва хизматлар ўз ичига олувчи ташкилотга боғлиқ эмас. Шунингдек удан нафақат ҳозирги, балки кейинги ҳолатлар учун ҳам фойдаланиш мумкин.

TOM бизнес-жараённи қўллай олувчи бизнес-жараён тузилмаси жойини ва ўхшаш жиҳатларни аниқлайди. Хар бир провайдер хизматларни TOM модел аниқлаган жараён

тузилмасини тахлил қилади ва натижалар ички жараёнларни бизнес қоидалар ва сиёсати асосида шакиллантиради.

ТОМ моделни асосий вазифаси телекоммуникация доирасида тақдим этилаётган хизматларни автоматлаштириш ва шафоф интеграцияни ҳосил қилиш учун умумий тузилмани ишлаб чиқишдан иборат. У провайдерлар томонидан ички хизматлар мақсадларда ва ташқи ҳамкорликлар учун фойдаланиш мумкин. У хизмат кўрсатувчилар томониданишлаб чиқилган маҳсулотларни мувофиқлаштириш учун фойдаланилади.

Барча жараёнларни автоматаштириш ва реинжинеринг қилиш тизимли ёндашув томнидан тўғри бўлар, лекин провайдер ва операторлар доимо дастурий маҳсулотларни сотиб олишга тайёр эмас. Шунинг учун ТОМ-модели доирасида барча жараёнларни автоматлаштириш бир хил аҳамятга эга эмас. Албатта айрим поғоналарда автоматлаштириш зарур, лекин айрим жараён қисимлари бозордаги рақобабардошликка салбий таъсир этади. Шунинг учун автоматлаштириш қуидаги соҳалардан келиб чиқади:

- асосий ахборот жараёнларни доимий такроланиши кузатилади;
- таъсирчанлик тезлигига юқори талаблар мавжудлиги;
- юқори сифат талаб қилинади (аниқ ва тўлиқ).

Натижада провайдерлар ТОМнинг асосий йўналишларидан фойдаланиб, хизматлар қуйидагиларни келтириб чиқармоқда:

- ички ва ташқи мунозараларни тартибга солиш;
- бизнес жараёнларини бошқаруви учун қайта муҳандислаш(реинжиниринг) ва ишлаб чиқиш;
- эҳтиёжлар идентификациялаш, талаблар ишлаб чиқиш;
- интерфейс ва ахборот моделларга талаблар ишлаб чиқиш;
- интерфесларни автоматлаштириш ҳақида ҳамкорлар билан шартномалар тузиш;
- ТОМ- модели структурасида хизмат кўрсатувчиларни ўринини аниқлаш.

IPV4 ПРОТОКОЛИДАН IPV6 ПРОТОКОЛИГА ЎТИШ ТЕХНОЛОГИЯЛАР ТАҲЛИЛИ

А.И.Абдуллаев(ТАТУ, ассистент)

IPv4 – бу IP протоколнинг (Internet Protocol) тўртинчи версияси бўлиб, ҳозирги кунда Интернет тармоғининг асосий ва катта кисми бўлибҳизмат қилади. IPv4 протоколи компьютер тармоқларининг пакетлар алмашиш принципи асосида фаолиятини амалга ошириш қоидаларини ўрнатади. Бу протокол паст даражада бўлиб тармоқтугунлари ичида IP - манзиллари асосида алоқа ўрнатишга жавоб беради.

Ipv6 I.E.T.F ташкилоти томонидан ишлаб чиқарилишига интернетдаги ягона манзиллар заҳирасининг барчаси сарфланаётганлигига сабаб бўлган.

Дастлаб интернет тармоғи кичик миқдордаги тадқиқот тармоқлари алоқаси учун мўлжалланган эди. Шунинг учун ҳозирги вақтда Ipv4 –манзиллаш тизимининг манзиллар майдонида 4 млрд.га яқин ноёб манзиллар қўлланилиши мумкин. Янги тизимдаги ноёб манзиллар сони 10^{18} га етади.

IPv4 ишлаб чиқиш вақтида (яъни IP нинг жорий версияси) 32 разрядли IP-манзиллар интернет ривожи учун тамоман етарлидек тасурот колдиради. Бироқ Интернет усишининг жадаллашган темпи шуни курсатадики, 32-разрядли адресация купгина муаммоларни юзага келтиради. Бу муаммоларниенгиб ўтиш учун IPнинг кейинги авлодлари — IP 6 версияси (IPv6), ёки IP Next Generation спецификацияси ишлаб чикиш бошланди.

Қатъий шаклга келтиришдан олдин IPv6 бир катор алтернативаларда тахлили килинди. Энг машхур альтернатив ечимлар бўлиб TUBA (TCP and UDP with Bigger Addresses), CATNIP (Common Architecture for the Internet) ва SIPP (Simple Internet Protocol Plus) лар хисобланган. Учала лойихадан хам хеч бири янги версия олдига қўйилган

талабларга жавоб бера олмади лекин улар келишувлар излашда ва асосий спецификациясига ўзгартиришлар киритиш учун асос бўлиб хизмат қилади. Шундай қилиб 1992 йилдан бошлаб IPv6 (RFC-2460) протокол ишлаб чиқишга киришилди. Уша вақтда манзил оралигидаги муаммони хал этиш учун ишлаб чикилган эди. Манзил оралигини IPv6 да тарқатиш (Internet Assigned Numbers Authority – интернетдаги стандарт ракамлар комиссияси (RFC-1881) хал этилди ва бу регионал вакилларга эга бўлиб улар ўз сохаларида IP манзиллар бериш билан шуғулланадилар.

Куйида протоколнинг асосий ўзига хосликларининг қисқача рўйхати келтирилган.

- 32 разрядли манзиллар ўрнига 128-разрядли тармоқ манзиллари.
- Янги параметрларни ўз ичига олган ва имкониятлар кулами кенгайтирилган IP сарлавхаларинг самарали структураси.
- Ихтиёрий майдонга эга бўлган ихтиёрий сарлавхалар ни кушиш имконияти
- MAC манзиллари асосида IPv6 манзилларини автоматик тайинлаш.
- Аутентификация ва шифрлаш воситалари, IPv6 протоколлар куйидаги кулайликларга эга.
- IPv4 устига IPv6, IPv6нинг асосий сарлавхасини кайта ишлаш;
- IPv6 га IPv4 туннеллаштириш, алоқа узелининг харакатчанлиги;
- IPsec нинг ҳақиқийлигини текшириш, IPv6 устига UDP ва TCP узел ва маршрутизаторнинг фаолияти ;
- ICMPv6 протоколи, автоматик ва созланган туннеллар.

IPv6 протоколининг IPv4 протоколидан асосий фарки адресация вақтида купрок бит ишлатишида. IPv4 протоколи 32–битли тушунчадан фойдаланади. IPv4 манзил коида бўйича унламчи шаклда 4 та ракамнинг кетма кетлигида ифода этилган. IPv6 протоколида коидага биноан 16тали шакл такдим этилади ва 128 битни эгаллайди.

Хозирги пайтга келиб IPv4 весия адреслари камайиб бормоқда. Охирги блоклар расмий равишда сотиб юборилган, кенгроқ полосали адреслар эгаларида оз бўлсада захира мавжуд. Маълумки, келажакда IPv6 тизимига ўтиш лойихалаштирилмоқда. Кўпгина ташкилотлар бундай ўтишни бошлаб юборишган хам.

Ўтиш вариантлари:

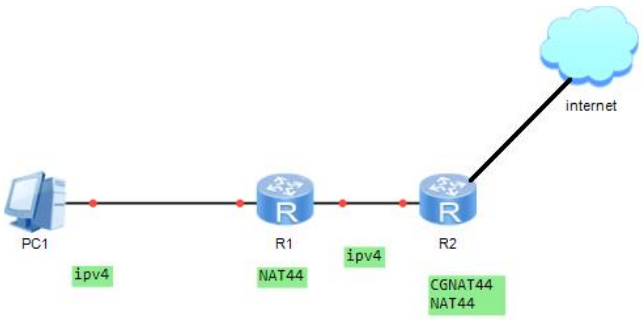
1. Параллел равишда тармоқларда хам IPv4 хам IPv6 ни қўллаш. Бунинг учун тармоқнинг барча қурилмаларида dual stack қуллаб қувватланилиши, хамда секин-аста IPv4 дан воз кечиб, Ipv6 формат адресларини тарқатиш керак. Кўпгинаохирги қурилмалар IPv6-технологиясини қуллаб қувватлайди, шунинг учун мижозларни қўшиш муаммо бўлмайди.
2. Тармоқ ядросини IPv4 технологиясида қолдириб, кириш имкон поғонасини IPv6 технологиясига ўтқазиш. Ундан кейин асосий элементларини IPv6 технологиясига ўтқазилади.
3. Аввал кириш имкон поғонасини IPv4 технологиясига қолдириб, сўнг тармоқ ядросини IPv6 технологиясида ўтқазиш. IPv4.

Бу муаммоларни хал этиш учун IPv4 ёки IPv6 қурилмалар орқали қурилган туннелдан трафик юбориш, хамда тармоқ манзилларини икки хил версияга ўгириш усули асосида қатор технологиялар яратилди. Улар қуйидагилар:

- Double NAT, NAT-PT, NAT 64, DS-Lite, DS-Lite A+P, IPV6 Rapid Deployment, 6PE/6VPE

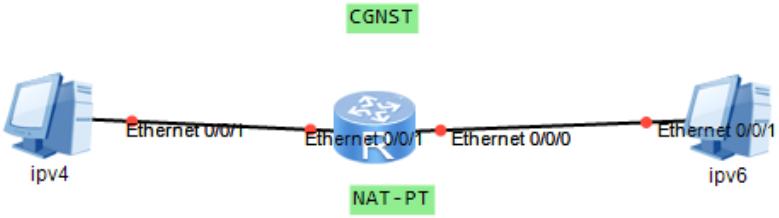
Double NAT (2-расм) технологияси IPv4 манзиллар маконини тугатилишини “кечиктириш” имконини беради. Мазмуни трансляция қилиш технологиясининг икки марта қўлланилиши.

Биринчи марта фойдаланувчининг хусусий манзилини бошқа хусусий манзилга трансляция қилинади. Ундан сўнг иккинчи марта Интернет манзилига трансляция қилинади. Бу усул IPv4 адрес диапазонини камайишини кечиктиради, лекин IPv6 адресларига ўтқизмайди.



Расм 2. Double NAT технологик ечими

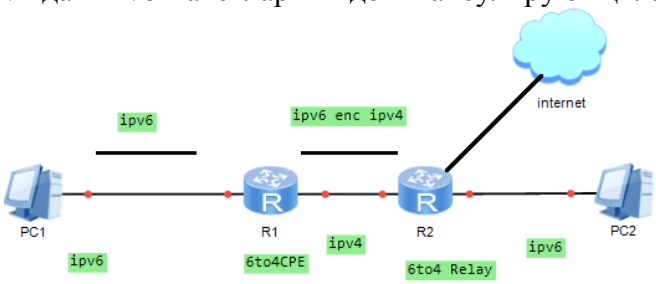
NAT 64 (3-расм) технологияси, Double NAT технлогияси каби функцияни бажариб, асосий фарқи DNS 64 функцияси борлигина талаб чилади. Хамда IPv4 технологиясидаги NAT-PT ни ўрнини босади.



Расм 3. NAT 64 технологияси

6to4 технологиясида (4-расм) IPv4 да IPv6 ўтишнинг энг енгил усули бўлиб, хизматлар провайдери томонидан хеч қандай ўзгартириш киритиши хожати йўқ.

Ягона шарти, IPv4 манзиллари хусусий булиши керак. Ушбу технологиядан фойдаланиш учун 6to4 relay деб номланувчи қурилмадан фойдаланилади. Бу қурилмалар мижозларнинг IPv4 дан IPv6-пакетларини деинкапсулируют қилади.



Расм4. 6to4 технологияси

ТЕХНОЛОГИЯ ИЗМЕРЕНИЯ КАЧЕСТВА ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ

У.М. Абдуллаев (ассистент, ТУИТ)

Оптические линии связи находят все более широкое применение - от магистральных линий и корпоративных систем передачи данных до локальных компьютерных сетей. Преимущество волоконных оптических линий неоспоримо: реализуемые в оптических каналах скорости передачи информации пока недостижимы для медных кабелей. Что бы проверить их работу в качестве компонентов систем волоконно-оптической связи, существуют различные лабораторные методы для измерения оптических волокон.

Затухание – это потеря оптической мощности вследствие поглощения, рассеивания, изгиба и других видов потерь во время передачи светового сигнала через волокно. Ослабление – это функция длины волны λ света. Общее затухание между точками X и Y в волокне это:

• A(db)= 10 log10 (Px/Py)

Px – это мощность сигнала в точке X. Py – мощность сигнала в точке Y. Точка X должна быть ближе к оптическому источнику чем точка Y. Коэффициент затухания или скорость затухания α рассчитывается:

• α(dB/km) = A/L

L – расстояние между точками X и Y.

Метод сокращения часто используется для измерения полного затухания оптического волокна. Способ заключается в сравнении мощности сигнала, передаваемого через длинный участок волокна и мощности сигнала, передаваемого через максимально короткий участок. Способ требует, чтобы короткий участок волокна был приближенно равен 2 метра. Сначала выполняется измерение выходной мощности сигнала Py тестируемого волокна известной длины L. Затем, не меняя условий, следует измерить мощность сигнала Px короткого волокна. После следует подсчитать затухание волокна A и коэффициент затухания.

Различные условия ввода могут привести к разным результатам. Для многомодового волокна распределение мощности между модами волокна должно быть под контролем. Это достигается путем контроля размерами и направленностью угла светового пучка.

Отсечка длины волны одномодового волокна — это длина волны, выше которой волокно распространяется только в основной моде. Отсечка длины волны является функцией радиуса кривизны волокон. Измерение отсечки длины волны включает передаваемой мощности от тестового волокна с мощностью эталонного волокна в зависимости от длины волны.

Передаваемая мощность сигнала Ps(λ) записывается, пока сканирование длины волны с шагом 10нм или менее в течение ожидаемой отсечки длины волны. Состояния запуска и обнаружения не изменяются во время сканирования в диапазоне длин волн. Для измерения эталонной мощности состояния запуска и обнаружения не меняются, однако волокно сворачивается в кольцо радиусом 30мм или менее что бы подавить вторичные моды в сканируемой длине волны. Получаемая мощность Pr(λ) записывается, и затухание Ad на каждой длине волны подсчитывается:

1. Ps(λ) = 10-As(λ)/10, Pr(λ) = 10-Ar(λ)/10,
2. Ps(λ)/Pr(λ) = 10-(As(λ)-Ar(λ))/10 = 10Ad(λ)/10,
3. Ad(λ)(dB) = 10 log10 (Ps(λ)/Pr(λ)).

Самая большая длина волны, при которой Ad(λ)/km равна 0.1 dB и есть отсечка длины волны волокна.

Ширина полосы пропускания многомодового оптического волокна может быть измерена путем измерения функции H(f) мощности передачи к полосе частот. Сигналы различных частот (f) проходят через тестируемое волокно и мощность сигнала конкретной частоты на выходе измеряется. Эта оптическая выходная мощность обозначается как Pout(f). Тестируемое волокно затем, заменяется на волокно короткой длины такого же типа. Сигналы с той же частотой запускаются в редуцированном волокне, и на выходе так же замеряется мощность сигнала. Она обозначается как Pin(f).

Величина частотного отклика определяется:

• H(f) = 10 log10(Pout(f)/Pin(f)).

Или, если было произведено два эксперимента, то:

• H(f) = 10 log10(Pout(f)Pin(0)/Pin(f)Pout(0)).

Полоса пропускания определяется как частота, при которой величина частотного отклика снизилась до половины значения нулевой частоты и H(f)=-3. Эта частота называется -3 децибела (dB) оптической мощности частоты (f3dB) и обозначается как полоса пропускания. Пропускная способность обычно дается в единицах мегагерц-километры (МГц-км). Преобразование в единицу длины помогает в анализе и сравнении производительности оптического волокна.

Хроматическая дисперсия возникает из-за того, что показатель преломления является функцией длины волны и различных длин волн света, проходящих через волокно с разной скоростью. Хроматическую дисперсию многомодовых и одномодовых волокон получают путем измерения времени, необходимого импульсу света с различными длинами волн проходить через длинный отрезок волокна. Эти измерения проводятся с помощью источников, способных выпускать пучок света с волнами разной длины.

Для измерения геометрии волокна, входной конец волокна переполняют и моды фильтруют. Выходной конец записывается на видео камеру, после, изображение посылается в компьютер. Компьютер анализирует изображение для того, что бы определить края сердцевины и оболочки. Диаметр оболочки определяется как средний диаметр. Диаметр сердцевины так же определяется как средний. Диаметр эллипсоидной оболочки — это разница между наименьшим и наибольшим радиусом, поделенная на средний радиус оболочки. Эллипсоидная сердцевина рассчитывается так же. Эллипсоидная сердцевина измеряется только на мультимодовых волокнах. Ошибка концентричности сердцевины и оболочки для многомодовых волокон представляет собой расстояние между центрами сердцевины и оболочки поделенное на диаметр ядра. Для одномодовых волокон определяется как расстояние между центрами сердцевины и оболочки.

Диаметр сердцевины определяется путем измерения распределения мощности в ближней зоне, близкой к концу волокна, когда расстояние между концом волокна и детектором находится в диапазоне микрометров. Диаметр ядра определяется как диаметр, при котором интенсивность 2.5% от максимальной интенсивности.

Числовая апертура (NA) является мерой способности оптического волокна для захвата света. Она определяется путем измерения распределения мощности в дальней зоне недалеко от конца волокна. Излучаемая модность на единицу площади записывается как функция угла θ некоторого расстояния от конца волокна. Расстояние между концом волокна и детектором в дальней зоне несколько сантиметров для многомодовых волокон и несколько миллиметров для одномодовых. Числовая апертура волокна определяется как 5 процентов или 0.05 уровень интенсивности. Этот уровень интенсивности 0.05 пересекает на сканируемых углах θA и θB. Числовая апертура волокна:

$A = \sin((\theta A - \theta B)/2)$

Диаметр поля моды (MFD) одномодового волокна связан с размером пятна основной моды. Это пятно имеет радиус поля моды r0. Диаметр поля моды равен 2r0. Одномодовые волокна с большим MFD более чувствительны к изгибу волокна. Волокна с маленьким MFD показывают более высокие потери связи при соединениях. MFD одномодового волокна может быть измерен путем измерения распределения мощности дальнего поля, используя набор апертур различного размера.

Потери состоят из потерь соединения связи и дополнительных потерь в волокне. В мультимодовом волокне, оптические соединители могут увеличить затухание в волокне после соединителя, нарушая распределение мощности моды. Отражения происходят в волоконно-оптических соединениях. Коэффициент отражения R это доля интенсивности падающего света, отраженного обратно в исходное волокно в точке соединения. Коэффициент отражения определяется с помощью оптического источника, подключенного одним входом к 2x2 оптического сплиттера. Свет продет через соединитель и вернется обратно в другой порт источника, подключенного так же к сплиттеру.

Проверка качества связи необходима для построения высокопроизводительной оптической волоконной сети. Изза поврежденных линий могут остаться без связи большие сегменты сети, поэтому, необходимо в краткие сроки локализовать проблему. В данной статье раскрываются все основные методы проверки характеристик волоконных линий. Так же они помогут понять, соответствует ли заявленные производителем качественные характеристики оптического волокна.

СЕТЕВЫЕ ПРОТОКОЛЫ PPPoE И IPoE

У.М. Абдуллаев (ассистент, ТУИТ)

Протокол PPPoE (расшифровывается PointtopointprotocoloverEthernet) требуется для системы авторизации пользователя. Данный протокол требует подтверждения его логина и пароля, чтобы установить доступ к Интернету. Особеннность этого способа - это встроенная процедура подлинности, позволяет правильно отслеживать время доставки и оплаты сетевых услуг. Когда заключается договор, заводится счет для подключения абонента и заносится в базы данных, абоненту присваивается логин и пароль.

Point to point protocol over Ethernet – это сетевой протокол канального уровня передачи кадров PPP поверх Ethernet. В основном используется XDSL услуги. Присутствуют дополнительные возможности (аутентификация, сжатие данных, шифрование).

В PPPoE используется туннелирование, которые позволяет настроить ikb инкапсулировать IP или другие протоколы, настроенные на PPP, через соединения Ethernet.

Это позволяет использовать PPP, как ориентированное программное обеспечение для настройки соединения,которое использует не последовательный канал, а пакеты ориентированные на сеть (например, Ethernet), чтобы сделать обычное подключение с логином и паролем.

PPPoE разработан UUNET, Redback Networks и RouterWare . Протокол описан в документе RFC 2516.

Обратите внимание, что некоторые из поставщиков оборудования, таких как: Cisco и Juniper используют термин PPPoEoE (PPPoE over Ethernet),который работает непосредственно с помощью Ethernet или другой сети IEEE 802.3 , а также PPPoE , в настоящее время отрабатывается в соответствующем Ethernet (Ethernet bridgedover) ATM для того, чтобы отличить его от PPPoEoA (PPPoE over ATM), который работает на ATMвиртуальный канале по спецификации RFC 2684 и SNAP и инкапсулирует PPPoE. Следует понимать, что точка- Point Protocol поверх ATM (PPPoA) , использует SNAP , в отличие от PPPoEoA.

PPPoE осуществляет свою работу следующим образом. Ethernet – среда, это несколько подключенных сетевых карт, каждой выдан свой MAC-адресов. Заголовки Ethernet - кадров содержат тип кадра, адрес получателя кадра, адрес кадра отправителя. Одну из карт слушает PPPoE-сервер. Клиент посылает широковещательный Ethernet - кадр, на который должен ответить PPPoE-сервер (отправитель кадров - ваш MAC - адреса отправителя и получателя кадра - FF:FF:FF:FF:FF: FF и тип кадра - PPPoE ActiveDiscoveryInitiation) . PPPoE сервер посылает ответ клиенту (отправителя кадра - ваш MAC - адреса отправителя и получателя кадра - MAC-адрес клиента и тип кадра - PPPoE ActiveDiscoveryOffer). Если в сети находится несколько серверов PPPoE, все они отправляют ответ. Клиент посылает запрос на соединение с наиболее соответствующему серверу. Сервер отправляет подтверждение с уникальным идентификатором сессии, все последующие кадры в сессии будут иметь этот идентификатор.Между сервером и клиентом создается виртуальный канал, который идентифицируется идентификатором сеанса и MAC- адрес сервера и MAC- адрес клиента. Затем устанавливается канал связи PPP, а IP- трафик упаковывается в пакеты PPP.

По сравнению с VPN соединением, PPPoE не нуждается в расходах на шлифование. Главное преимущество для Интернет-провайдеров, в том, что они могут сделать ограниченное количество IP-адресов. И эти IP-адреса назначаются пользователям, которые находятся в сети. Загрузка канала очень мала, если сравнивать его с другими системами авторизации i пользователя. И еще один плюс многоплатформенность.

Протокол работает только с Ethernet, а это недопустимо при использовании транзитных IP маршрутизаторов. PPPoE в основном используется в небольших отдельных сетях,так как поиск сервера очень длителен, и широковещательные пакеты могут задерживаться в маршрутизаторе.

Максимальный размер Ethernet-пакета составляет 1500 байт и максимальный размер пакета при отправке через PPPoE является 1492 байт (заголовок PPPoE - 6 байт, PPP Protocol ID - 2 байта). Если маршрутизатор использует Path MTU Discovery, который запрещает фрагментация пакетов устанавливается автоматически в зависимости от ICMP. Исходя из этого, между хостом может быть проблема с обменом данных, а на определенном этапе ICMP -пакеты могут быть отклонены.

IP over Ethernet подключение Ethernet к коммутатору провайдера. MAC - адрес устройства вводятся в базы данных DHCP-сервера, и как только вы включите DHCP-сервер сетевого провайдера дает либо белый или серый IP - адрес, операторского маршрутизатора (шлюза) и серверы имен адрес провайдера (DNS). Используя эти данные можно сразу, без установления промежуточных, выходить в Интернет. Этот тип соединения является наиболее предпочтительным. Большинство домашних маршрутизаторов, даже фирмы или D-Link TP-Link может работать в таких условиях. При прочих равных условиях, всегда выбирают этот тип соединения. Чипсеты Маршрутизаторы «Ralink» обеспечивают для таких соединений, максимально возможной скоростью, что значительно превосходит конкурентов с помощью аппаратной обработкой пакетов (блок PPE). Даже если частота процессора ниже, чем у конкурирующих в несколько сотен мегагерц. Например маршрутизатор «Zyxel Keenetic Giga », имея процессор с тактовой частотой 384 МГц в большинстве сетевых операций, работает быстрее, чем маршрутизатор Asus RT- N16U , процессор с тактовой частотой 480 или даже 533 МГц. В роутерах этому типу подключения могут соответствовать термины static (настройки IP, Gateway и DNS вводятся вручную) или dynamic (настройки берутся с DHCP-сервера).

IPoE в корне отличается от PPPoE. В общем, эта технология официально не существует,так как в RFC нет никаких стандартов , которые описывают его. Термин был изобретен, вероятно, в странах СНГ и является абстрактным. Термин означает следующее: IP поверх Ethernet. Пользователь получает статический или динамический IP- адрес - белый или серый IP- адрес с NAT. Контроль доступа в этом случае можно сделать с помощью IP - MAC привязки на коммутаторе или BRAS доступа или VLAN на абонента - так называемый VLAN - Client.

Нет привязки к логину, паролю и MAC - адреус.Некоторым абонентам из-за привязки к MAC-адресам очень неудобно пользоваться интернетом PPPoE,а доступ IPoE это ликвидируеат. Когда компьютер подключается к Интернету создается временное привязка, когда компьютер выключен она удаляется в течение нескольких минут. То есть, вы вполне можете отсоединить кабель от компьютера и нескольких минут, чтобы подключить его к любому другому ноутбуку и Интернет будет работать на этом ноутбуке. Купил новый компьютер - не нужно звонить в службу технической поддержки и отвечать на кучу вопросов к вам - вы просто включите кабель и будете использовать Интернет на компьютере, к которому требуется подключить кабель. Ограничений на количество таких переключений нет, единственный недостаток возможность работать только на одном устройстве. Но эта проблема решена. Так что если у вас есть компьютер и ноутбук, маршрутизатор необходим. Кроме того, необходимо учитывать интервал между сессиями 4,5 минут. Потому что система должна определить, что предыдущий компьютер отключен и подключен кабель к новому устройству.

Отличие IPoE от PPPoE:

1) Вам не нужно настраивать или перенастраивать соединение при переустановке операционной системы или установке маршрутизатора. Обычно от производителя

оборудования, программное обеспечение идёт с автоопределением настроек сети, и всё будет работать сразу же, вы просто должны подключить провода.

2) ниже нагрузки на центральный процессор. Доступ PPPoE занимает часть ресурсов процессора на обработку PPP. На компьютерах не особенно заметно, но недорогие маршрутизаторы, в которых процессор часто очень низкой производительности. Это позволяет увеличить пропускную способность маршрутизатора.

3) Вам не нужно учитывать dual-access. Раньше для работы локалки использовалось автополучение адреса и для доступа к Интернету отдельное соединение.Различные маршрутизаторы и различные операционные системы относятся к этому по-разному, некоторые из них не в состоянии работать так . Доступ IPoE устраняет отдельный подключение к Интернету. Данное решение позволяет разрешить общий доступ к интернет средствами windows без каких-либо дополнительных настроек, просто поставив галочку в настройках соответствующей сетевой карты.

4) Настроить Интернет очень легко, или вообще не нуждается в настройке.

5) Наименьшее количество проблем при устранении неполадок

6) Возможность подключения любого устройства. (Игровые консоли, медиаплееры, телевизоры и т.д.)

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ПРОЕКТИРОВАНИЯ СЕТЕЙ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ .

Р.П. Абдурахманов (доцент, ТУИТ)

В последние годы в Республике Узбекистан приоритетной задачей является создание и развитие национальной инфокоммуникационной инфраструктуры на основе новых сетевых технологий, включая технологии NGN. Это обусловлено тем, что инфокоммуникации, проникая во все инфраструктурные и базисные компоненты общества, становятся одним из мощных инструментов управления страной и катализатором её экономического роста. На сегодняшний день в Узбекистане для обеспечения стабильного развития телекоммуникационной отрасли принята антикризисная программа мер, в которой предусмотрены: широкое внедрение современных гибких технологий, развитие инфраструктуры сетей телекоммуникаций, оказание самых современных услуг телекоммуникаций путем внедрения передовых технологий, перехода на международные стандарты качества. Наряду с этим, интенсивное развитие национальной инфокоммуникационной инфраструктуры, базирующейся на сетях NGN, обусловливает появление ряда научных проблем, в том числе проблем, касающихся проектирования сетей NGN, которые являются одними из наиболее сложных.

Проектирование сети, является одним из этапов построения сети NGN, и на сегодняшний день является наиболее востребованной задачей. На текущий момент не выработан обобщенный метод исследования, обеспечивающий анализ эффективности функционирования NGN сетей. Многие крупные операторы, эксплуатирующие сети связи, стараются собственными силами проводить анализ и проектировать сети. При этом им необходимо разрабатывать свои или брать на вооружение новейшие методы проектирования NGN, в основном из зарубежных источников, или довериться опыту поставщиков оборудования, не имея возможности перепроверить полученный результат.

Методы расчета сетей связи следующего поколения являются основополагающими в процессе проектирования, так как полученные результаты являются опорными данными для дальнейшего построения сети. Однако, на сегодняшний день не существует одной общей и универсальной методики построения сетей связи следующего поколения. Выработка таких методик осуществляется путём глубокого анализа опыта в данной области и путём проведения полноценных научно-исследовательских работ. Таким образом, проектирование сетей следующего поколения, относящихся к сложным

системам, обуславливает необходимость проведения исследований для научно-обоснованного решения возникающих проблем. В целом, опираясь на исследования в рамках данной работы, проектирование NGN можно определить состоящим из двух стадий:

Первая стадия определяет системное проектирование, в ходе которого осуществляются научные исследования задач анализа и синтеза для уточнения архитектурных, функциональных и экономических аспектов построения сети. На этой стадии формируется проблема, определяются цели и задачи, описываются воздействующие на сеть внешние и внутренние факторы, выбираются характеристики, показатели и критерии оценки эффективности сети. Цели и задачи определяются потребностями пользователей, тенденциями развития современных технологий, технико-экономическими соображениями. Рассматриваются варианты построения сети, которые анализируются по выбранному критерию эффективности, исследование проводится на математических моделях, позволяющих выразить зависимость показателей эффективности от параметров внутренней и внешней среды, архитектуры технических средств, протоколов взаимодействия. Таким образом, на стадии системного проектирования решаются задачи формального анализа NGN, формируется концепция построения сети, выбираются математические методы оценки эффективности различных вариантов построения сети, формируется совокупность требований к основным характеристикам, определяется перечень задач анализа и синтеза, т.е. на базе системного подхода вырабатываются методики и общая методология проектирования NGN.

Вторая стадия исследований включает вопросы технического проектирования, связанные с разработкой функциональных и технических элементов, компонентов, систем и сети, с получением технических решений по основным характеристикам и параметрамNGN; здесь осуществляется выбор моделей трафика, моделей информационных каналов и систем, моделей транспортнойсоставляющий сети и сети абонентского доступа; решаются задачи анализа (оценка производительности систем, своевременности доставки информации, эффективность протоколов и т.д.) и синтеза.

Анализ работ, посвященных вопросам проектирования сетей следующего поколения, позволил сформулировать ряд эадач которые требуют детального исследования и разработку моделей, отражающих принципы построения и организации связи в сетях следующего поколения. Результаты исследования природы процессов, наблюдаемых в этих сетях, показали, что данное направление исследований на сегодняшний день требует создания адекватных аналитических и имитационных моделей, позволяющих комплексно оценивать и анализировать различные параметры и характеристики, учитывая сложную структуру трафика в таких сетях и иерархические многоуровневые связи в архитектуре. Факторы совершенствования телекоммуникационных технологий требуют адекватного развития теоретических основ проектирования сетей связи, которое должно осуществляться на основе систематизации уже известных подходов, а также разработке новых методов анализа и синтеза рассматриваемых сетей. Процесс проектирования и разрабатываемая методология должна будет учитывать факторы, связанные с обоснованием характеристик применяемого телекоммуникационного оборудования, анализа и формирования структуры сети, расчета и оптимизации пропускной способности систем передачи и коммутации сети при обеспечении требуемых показателей качества обслуживания (QoS). Для этого необходимо проведение дополнительных исследований вопросов обеспечения и поддержания QoS в сети следующего поколения с использованием и разработкой соответствующих моделей оценки показателей качества для различного типа трафика в сети.

Также следует отметить , что разработанные и используемые модели исследования процессов в современных сетях, не учитывают реальные характеристики потоков информации. Использование теории самоподобных процессов позволяет разрешить эту проблему и создать математические модели, учитывающие характерные особенности

мультисервисных сетей. Результаты анализа работ, посвященных моделированию компонентов сети следующего поколения показали, что анализ характеристик процессов функционирования сети как большой системы должен проводиться с применением системного подхода и предпосылок разработки ее комплексной модели. Выявлено , что для формализованного описания сетей ключевыми считаются идентификация класса процессов, протекающих в сети, и выбор рационального математического аппарата для их описания, а также проблемы определения уровней рассмотрения свойств системы, проблемы учета мультисервисности и гетерогенности современных сетей и способов формализованного отображения свойств иерархичности как самой сети, так и предоставляемых ею услуг. Кроме того, при формировании общей модели необходимо решить проблему взаимной увязки свойств отдельных подсистем, а также проблему сохранения свойств сети при переходе от одного уровня моделирования к другому. Анализ работ , также позволяет говорить о наличие трудноформализуемых факторов и ограничений, приближенность некоторых исходных данных и многокритериальный характер общей задачи проектирования сети следующего поколения, невозможности постановки и решения в рамках одной математической задачи всего комплекса проблем проектирования сети, что приводит в свою очередь к необходимости использования процедуры, основанной на декомпозиции, которая возможна как на структурном уровне, так и на уровне решения отдельных задач проектирования, и позволяет перейти от задачи большой размерности к последовательности задач меньшей размерности. Существующие и используемые в настоящее время подходы и методы проектирования сетей связи не учитывают в полной мере современные тенденции при разработке проектов мультисервисных сетей и сетей следующего поколения, в связи с чем метод многокритериального проектирования мультисервисных сетей связи представляется наиболее приемлемым при проектировании сетей следующего поколения , обеспечивая анализ эффективности их функционирования, а также синтез по критериям технико-эксплуатационных затрат, качества обслуживания, устойчивости функционирования сетей следующего поколения. При этом, проектируемая сеть может быть описана векторами ее системных и сетевых характеристик по соответствующим этапам развития сети с учетом того, что общим принципом функционирования систем NGN является их многопараметричность, присущая любым подсистемам сетей следующего поколения.

Процесс проектирования сети следующего поколения, являясь итерационным, предполагает возможные варианты проектируемой системы, с анализом характеристик, выбором наиболее подходящих вариантов, их оптимизацией, уточнением и детализацией (в том числе, определение ее пользовательских характеристик); на этапе оптимизации сети могут изменяться параметры системы, учет и проведение экспериментов для которых в реальном масштабе времени для огромного количества всевозможных сочетаний этих параметров практически невозможен. В связи с этим, при проектировании сетей следующего поколения, во многих случаях предпочтительным оказывается использование математического моделирования как совокупности соотношений, определяющих процесс изменения состояния сети в зависимости от ее параметров, входных сигналов, начальных условий и времени. При этом имитационные модели, как особый класс математических моделей являются современными инструментальными программными средствами проектирования сетей и позволяют ускорить процесс проектирования, а также сэкономить средства, которые впоследствии могут быть использованы на улучшение характеристик работы сети, ее модернизацию или же внедрение дополнительных сервисов, предоставляемых сетью. Сложной и одновременно трудоемкой задачей в процессе проектирования является определение исходных данных, которые характеризуют топологические, компонентные и нагрузочные сведения (о передающей сети, производительности составляющих ее маршрутизаторов, каналов связи, нагрузке сети, потоках трафика и т.п.), что непосредственно связано с задачей управления ресурсами сети: необходимостью улучшения качества обслуживания передаваемого трафика, т.е. к

снижению задержек, уменьшению потерь и увеличение интенсивности потоков трафика, а также максимально возможной загрузкой всех ресурсов сети для повышения объемов передаваемого трафика. Решение этой задачи основано на использовании математических моделей инжиниринга трафика для поддержки сквозного качества обслуживания, что позволяет определить необходимые параметры для проектирования для дальнейшего уточнения критериев технико-эксплуатационных затрат и качества обслуживания. Сложный многоэтапный процесс формирования взаимоувязанных технических решений при проектировании NGN целесообразно определять на основе разработанной за период исследования целостной методики проектирования, направленной на создание сети, способной обеспечить предоставление мультисервисных услуг в необходимом количестве и с требуемым качеством пользователям и учитывающей специальные требования к сети.

АНАЛИЗ ФАКТОРОВ ВЛИЯЮЩИЕ НА МЕТОДОЛОГИЮ ПРОЕКТИРОВАНИЯ СЕТЕЙ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Р.П.Абдурахманов (доцент, ТУИТ)

Создание информационного или электронного общества во всем мире способствует повышению эффективности внутреннего управления и функционирования государства, делает прозрачной и информационно открытой деятельность правительства, экономит средства при переходе к онлайновым тендерам на востребованные товары и услуги, приводит к ускорению позитивных социально-экономических процессов в обществе. Формирование глобальной информационной инфраструктуры, определяющей необходимость перехода к информационному обществу и получившие развитие в этих условиях инфокоммуникационные сети, подразумевают возрастание роли информационно-коммуникационной инфраструктуры в системе общественного производства. При этом интеграция средств связи и вычислительной техники, стирание границ между локальными и глобальными сетями, конвергенция сетей, предназначенных для передачи разных видов информации привели к разработке и внедрению сетей следующего поколения NGN (Next Generation Network, Сеть следующего поколения). Являясь удобным средством коммуникаций, предоставляемых пользователям посредством информационно-коммуникационных технологий, эти сети обоснованно подходят для развития инфокоммуникационной инфраструктуры в целом.

Постоянная конкуренция среди поставщиков оборудования и технологические достижения привели к снижению стоимости оборудования, и, как следствие, ускорению процесса построения сетей связи следующего поколения. Необходимо отметить, что существуют различные способы построения и перехода к NGN, которые предполагают создание сетей с радикальным изменением ее структуры или с изменением структуры по заранее выбранному плану. Однако опыт практической реализации NGN решений показывает, что способы их построения должны быть тщательно проработаны и связаны с состоянием существующих сетей связи. Применяемые технические решения должны обеспечить эффективность функционирования как отдельных подсистем, так и всей сети. В большей степени, это связано с тем, что в отличие от традиционных, в сетях NGN нет монолитных сетевых узлов, в которых сконцентрированы все функции: сети NGN имеют компонентное построение с использованием различных функциональных модулей или блоков. Однако, на сегодняшний день не существует одной общей и универсальной методики построения сетей связи следующего поколения. Выработка таких методик осуществляется путём глубокого анализа опыта в данной области и путём проведения полноценных научно-исследовательских работ. На фоне появления и совершенствования технологий для сетей связи и быстрых темпов развития и внедрения телекоммуникационного оборудования, выработка таких методик становится очень

трудной задачей. Исходя из этого, вопросы разработки методологии проектирования сетей следующего поколения обосновывают актуальность и своевременность усилий в этой области научных исследований.

Как известно, методология проектирования традиционных сетей заключалась в расчете отдельных вторичных сетей (телефонных, передачи данных и т.д.) и их суперпозиции для расчета первичной сети. При этом, для каждой из традиционных сетей за долгие годы исследований были определены свои показатели нагрузки, характера трафика, качества обслуживания и т.д., созданы свои математические модели, методы проектирования и расчета. Кроме того, большинство результатов теории телетрафика и её приложений были ориентированы преимущественно на задачи проектирования телефонных сетей; перенесение результатов статистических исследований, проведенных применительно к традиционным сетям на проектирование сетей следующего поколения становится практически невозможным и по ряду причин, может привести к серьезным ошибкам. Одной из причин является то, что прежде всего, изменился сам трафик, создаваемый пользователями, который является мультимедийным, определяемый внедрением новых услуг: мультимедийний трафик, создаваемый при представлении различных услуг в сетях следующего поколения сильно различается по своему составу, предъявляемым к нему требованиям и объему необходимых сетевых ресурсов. Исследования показывают, что в построенных сетях следующего поколения на базе коммутации пакетов трафик обладает так называемым свойством самоподобия, т.е. выглядит качественно одинаково при почти любых масштабах временной оси, имеет память (последействие), а также характеризуется пачечностью.

Реализация возможностей сети следующего поколения, в основном, обеспечивается важным свойством сетей NGN, а именно, разделением функции транспорта и сервиса]. В этом отношении функциональность этих двух принципиальных составляющих архитектуры NGN основана на независимом, отделенном друг от друга построении, при котором услуги (сервисы) предоставляются и развиваются (разрабатываются) с учетом горизонтального уровневого разделения (в отличие от вертикально разделенных сетей для каждого сервиса, как это было в традиционных сетях связи). При построении архитектуры NGN на основе такой мульти- или многослойной структуры, могут возникать разногласия по поводу взаимодействия отдельных функциональных блоков, приводящие к снижению эффективности, в случаях, если элементы или блоки находятся на различных уровнях/слоях и функционируют независимо друг от друга. В NGN, предусматривающей огромный набор услуг, предоставляемых пользователям, каждый пользователь должен будет обладать персонифицированным номером/именем независимо от используемых технологий доступа в любом удобном для него месте и в любое время; он должен иметь возможность соединиться с определенным номером/именем или оконечным оборудованием, либо приложением (в том числе для управления информацией), пользоваться мультимедийными приложениями в реальном времени с соблюдением гарантированного качества обслуживания «из конца в конец». В этих условиях особое внимание следует уделить рациональности использования сетевых ресурсов, конвергенции сетей связи, повышению качества и уменьшению стоимости предоставляемых пользователям услуг, а это невозможно без первоначального грамотного проектирования сети.

Исследование архитектурных и функциональных особенностей организации сетей следующего поколения, а также существующих методов и подходов к проектированию позволило определить факторы, которые целесообразно учитывать регулирующим органам в области связи и информатизации, а также лицам, участвующим в указанной деятельности, в том числе операторам, при проектировании, создании сети следующего поколения, а также на различных этапах ее реализации, в качестве приведенных ниже рекомендаций:

Во-первых, на текущий момент не существует обобщённого метода исследования, обеспечивающего анализ эффективности функционирования сетей связи следующего поколения, а также синтез по различным критериям (затраты, качество обслуживания, устойчивость и т.п.), при этом непрерывное совершенствование сетевых технологий, этапность жизненного цикла телекоммуникационных сетей и многообразие вариантов построения их структур, необходимость согласования противоречивых интересов пользователей, операторов связи и поставщиков услуг порождает широкий спектр задач, которые необходимо решать при проектировании (расчёте основных параметров) сетей связи следующего поколения и её компонентов, в связи с чем целесообразны:

-разработка отраслевой нормативной базы;

-разработка концепции построения NGN;

-проведение выбора и обоснование способов производства и предоставления услуг, сформированных путём объединения информационных ресурсов сети или нескольких сетей, входящих в состав NGN;

-учитывая исследованные принципы построения и реализации NGN, соответствующие методы и модели, а также наличие и использование стандартизированных аппаратных и программных средств, многообразие оборудования основного, специального и вспомогательного назначения.

Во-вторых, сети следующего поколения должны образовать единое телекоммуникационное пространство, для чего необходимы системные решения по присоединению, взаимодействию, порядку обмена трафика между различными сетями, при этом проектирование мультисервисных сетей, как составной задачи проектирования NGN должно основываться на максимально эффективном использовании ресурсов уже построенной цифровой инфраструктуры и обеспечивать экономическую эффективность за счет широкого использования услуг, предоставляемых региональными мультисервисными сетями. Учитывая, что различные производители сетевого оборудования применяют различные идеологии построения сетей, задача создания сетей следующего поколения должна сводиться к поэтапному объединению традиционных сетей связи на основе универсальной управляемой распределенной транспортной платформы, позволяющей осуществлять транспортировку разнотипных потоков данных.

В третьих, сети следующего поколения в перспективе должны образовать единое инфокоммуникационное пространство, в связи с чем технологическая и функциональная архитектуры инфокоммуникационной сети, которые полностью определяются потребностями пользователей в передаче и обработке различных видов информации с заданными параметрами качества услуг, должны создаваться на основе системного подхода, с учетом интеграции всех видов услуг в рамках единой сети. Выбор протокола обмена сообщениями на транспортной сети обоснованно основывается на протоколе MPLS, который позволяет объединить различные протоколы и повысить пропускную способность NGN.

В четвертых, определение требований к качеству обслуживания является неотъемлемой частью при оценке характеристик пропускной способности и объема телекоммуникационного ресурса для различных компонентов (уровней) сети следующего поколения. Наряду с этим, планирование оценки стоимости (приведенных затрат) общего сетевого решения первоначально включает в себя расчет пропускной способности сети и при проектировании должны быть учтены отдельные модули расчета пропускной способности сети, основанные на использовании моделей и методов теории телетрафика. Для их применения необходимо оценить виды, объемы и профили реального (прогнозируемого) трафика, задать показатели качества обслуживания, на основе которых определяется необходимый объем оборудования по уровням и направлениям связи, с учетом выбранной структуры сети следующего поколения. При этом, при проектировании NGN целесообразно использовать предложенную методологию, основанную на

комплексном использовании аналитических и имитационных моделей и методов проектирования.

В пятых, современный этап развития отрасли связи, информатизации и телекоммуникационных технологий сопровождается реализацией новых технологических решений, в связи с чем для поэтапной модернизации существующей сети необходим системный проект, обеспечивающий высокую конкурентоспособность оператора телекоммуникационной сети, который должен учитывать эффективное применение комплекса технических средств на основе новых технологических достижений и технических требований широкополосной сети (в том числе требования пользователей к показателям качества обслуживания, поддержание функций мобильного терминала, приложений и функциональных возможностей услуг Triple Play, поддержку сетью доступа любых сетевых технологий, различные среды передачи, интерфейсы и протоколы связи, а также функции агрегации и управления трафиком на стыке сетей доступа и транспорта).

CLOUD COMPUTING: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ, ТЕМПЫ РАЗВИТИЯ НА МИРОВОМ УРОВНЕ И В УЗБЕКИСТАНЕ

Б.З.Абдухалилов (ТУИТ ассистент)

Все меняется, мир не стоит на месте, и большинство пользователей Сети также меняют своё отношение к мировой паутине. Причиной тому - «облако», которое задаёт «моду» на пользование Интернета, и хранение файлов в Сети.

Принцип «облака» существует уже достаточно долгое время, так или иначе воплощая себя в деловом мире. В большинстве случаев этот термин означает сеть компьютеров, обеспечивающих работу определённой системы, предоставляющая потребителю услуги в виде пользования программным обеспечением или хранения данных. Данный принцип основан на теории «облачных вычислений».

Облачные вычисления – это модель предоставления удобного сетевого доступа в режиме «по требованию» к коллективно используемому набору настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ данных, приложений и/или сервисов), которые пользователь может оперативно задействовать под свои задачи и высвобождать при сведении к минимуму числа взаимодействий с поставщиком услуги или собственных управленческих усилий. Облачные технологии позволяют обеспечивать, и немалую степень гибкости в работе. В зависимости от ваших нужд, вы можете поднять или опустить ту планку используемых облаком ресурсов, за которой потребуется включение в работу дополнительного оборудования.

На сегодняшний день существует три основные модели обслуживания облачных вычислений:

1. *Платформа как услуга* (PaaS, Platform as a Service). Потребителю предоставляются средства для развертывания на облачной инфраструктуре создаваемых потребителем или приобретаемых приложений, разрабатываемых с использованием поддерживаемых провайдером инструментов и языков программирования. Она чаще используется разработчиками программного обеспечения. Обладает такими чертами как высокая надежность и безопасность.

2. *Программное обеспечение как услуга* (SaaS, Software as a Servise) – это такая модель продажи и использования программного обеспечения, согласно которой поставщик сам создает веб-приложение и управляет им, а заказчики получают доступ к программному обеспечению через сеть интернет.

3. *Инфраструктура как услуга* (IaaS, InfrastructureasaService). используется в основном крупными предприятиями. Клиенту предоставляется достаточно разнообразная

компьютерная инфраструктура: серверы, сетевое оборудование, системы хранения баз данных и программное обеспечение для управления этими ресурсами.

На сегодняшний день мировыми лидерами в области предоставления облачных услуг, считаются такие гиганты сферы информационно-коммуникационных технологий, как Google (GoogleDrive), Яндекс (Яндекс диск), Microsoft (OneDrive), Apple (iCloud) и DropboxInc. (Dropbox).

Также и у нас в республике уделяется особое внимание развитию облачного хостинга, примером можно привести нашумевший проект UZDisk. UZDisk – это наш собственный аналог Dropbox. UZDisk является облачным сервисом хранения файлов, и расположен в зоне TAS-IX. Не мало важным фактором является , что трафик для данного сервиса абсолютно бесплатен.

Также существует ряд фирм, которые на протяжении определенного периода оказывают данный вид услуг; в их числе "AtiveCloud" ТМ предоставляющая услуги VDS хостинга, VPS хостинга, виртуального хостинга и облачного хостинга, а также ООО "SHARKTELECOM" предоставляющая услуги VDS хостинга, VPS хостинга, виртуального хостинга, облачного хостинга и услугу collocation хостинг.

Рыночная доля облачных сервисов и платформ постоянно растет благодаря ряду преимуществ для обычных пользователей и организаций, среди которых в первую очередь можно отметить: при обработке данных система выбирает наиболее оптимальный из всех имеющихся ресурсов; скорость поиска и обработки данных высока, так как все соединено единой платформой; количество процессоров, объем оперативной памяти и дискового пространства в облачных системах теоретически ничем не ограничен; пользователям не нужно самостоятельно устанавливать и настраивать ПО, т.к. для доступа к облачным сервисам достаточно обычного web-браузера; организации получают сокращение затрат на техническую поддержку и обновление развернутых систем, а также высокую скорость внедрения, обусловленную отсутствием временных затрат на развертывание системы; отсутствует необходимость обучения – большинство пользователей уже умеют пользоваться web-браузерами и интернет-сервисами как классом услуг; обычно облачные системы обслуживаются высококвалифицированными профессионалами, что дает более высокий уровень качества обслуживания ПО.

А главное, благодаря тому, что все данные находятся в руках провайдера, нельзя исключать того, что недобросовестные компании могут воспользоваться этим.

Из выше сказанного можно придти к выводу, что рассмотрение вычислительных систем на примере технологии "cloudcomputing " будет иметь важное значение в развитии научно-технической деятельности и облачной конвергенции. Все это говорит нам о том, что сейчас данное направление является одним из самых актуальных, а значит, темпы развития облачных технологий будут только нарастать.

УПРАВЛЕНИЕ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ: АНАЛИЗ ИСПОЛЬЗУЮЩИХСЯ КОНЦЕПЦИЙ НА ПРАКТИКЕ

Б. З. Абдухалилов (ТУИТ ассистент)

В связи с появлением новых услуг в телекоммуникационной отрасли, внедряются новые технологии и элементы в телекоммуникационную сеть. В результате чего увеличивается количество элементов в сети. Соответственно приходится контролировать все эти услуги и элементы. Если не централизовать этот контроль неизбежно возникнут проблемы с координацией работы различных сервисов, дополнительные расходы на поддержку и администрирование. Кроме того, может ухудшаться QoS качество предоставляемых услуг в результате развитии аварийных ситуаций, и снижение производительности возникнут потеря информации. Для решения этой проблемы разработаны такие системы и концепции как OSS/BSS, TMN, eTOM, NGOSS. Эти

системы предназначены для комплексного управления телекоммуникационными ресурсами предприятия.

OSS/BSS (*Operation Support System/Business Support System)* — система поддержки операций/система поддержки бизнеса. Системы предназначены для комплексного управления телекоммуникационными ресурсами предприятия и OSS/BSS-решения комплексно автоматизируют операционную деятельность телекоммуникационных компаний в рамках бизнес-процессов, услуг и функций управления.

OSS относится к программному обеспечению, которое взаимодействует с телекоммуникационной средой. Это сети электросвязи, коммутационные оборудования, АТС, аппаратные комплексы обеспечения связи и предназначенные для поддержки эксплуатации телекоммуникационных систем предприятия связи. В основные функциональные возможности OSS входят такие проблемы как учёт и планирование телекоммуникационных ресурсов (номерные ёмкости, трафик), управление предоставлением услуг, управление показателями и уровнем качества услуг. А также к функциональным задачам OSS относятся контролирование мошенничества на уровне телекоммуникационных данных, прогнозирование и обеспечение спроса на услуги.

BSS включается прикладное программное обеспечение поддержки деловых процессов предприятия электросвязи, прежде всего — так или иначе замкнутое на взаимодействие с абонентами— биллинг, CRM (управление информацией об абонентах, поддержка взаимодействия с ними, продажи, маркетинговый анализ). ERP - системы, применяемые на предприятиях электросвязи для обеспечения процессов финансового менеджмента, бухгалтерского учёта, управления персоналом, проектами и основными фондами также относят к подкатегории BSS.

Сегодня ведущей организацией в области стандартизации построения OSS систем называют TMForum с концепцией NGOSS. Однако, стандарты и любые другие разработки в этой области – являются лишь решением задачи поставленной термином OSS.

Международная некоммерческая организация TM Forum, которая занимается вопросами развития и оптимизации бизнеса операторов связи, а также стандартизацией управления сетями связи и построения OSS / BSS систем нового поколения разработала концепцию NGOSS для решения существующих актуальных проблем.

NGOSS (NextGenerationOperationsSystemsandSoftware) – новое поколение эксплуатационных систем и программного обеспечения. Концепция NGOSS - это комплексная, целостная модель формализации, разработки, внедрения и развития систем OSS/BSS операторов связи в виде согласованных и общепринятых на уровне телекоммуникационной отрасли пакетов стандартизованных спецификаций и рекомендаций, и базируется на четырех взаимосвязанных между собой частей, которые охватывают все важнейшие сферы деятельности оператора связи:

1. Enhanced Telecom OperationsMap (eTOM) – Структура бизнес процессов Оператора связи.
2. TelecomApplicationMap (TAM) – Инфраструктура прикладных задач (приложений) оператора связи.
3. SharedInformation/DataModel (SID) – Информационная модель данных корпоративного уровня.
4. TechnologyNeutralArchitecture (TNA) – Принципы интеграции систем на базе технологически нейтральной архитектуры.

eTOM (EnhancedTelecomOperationsMap) - расширенная модель операций для телекоммуникаций. Модель бизнес-процессов eTOM помогает Операторам связи, разработчикам OSS, системным интеграторам и производителям сетевого оборудования говорить на одном языке и мыслить процессы единообразно. eTOM – это один из инструментов концепции NGOSS, который позволяет упростить формализацию, анализ и реструктуризацию процессов эксплуатации Оператора связи. Данная модель представляет

собой язык описания эксплуатационной деятельности, который выражен в виде законченного иерархического списка бизнес-процессов.

Модель eTOM представляет собой набор формализованных бизнес-процессов с зафиксированными названиями и смыслом. При описании специфичной деятельности Оператора связи по концепции NGOSS нужно использовать стандартные бизнес-процессы eTOM, выстраивая из них цепочки. Множество процессов, сформированное таким образом, представляет собой стандартное описание деятельности Оператора.

TMN (Telecommunications Management Network) – сетьуправлениятелекоммуникациями. TMN - это по сути дела международный стандарт определяющий технологию построения систем управления телекоммуникационными сетями и определяющий все аспекты их функционирования. Логическая многоуровневая модель TMN. Эта модель определяет взгляд на распределение функций управления TMN с точки зрения конечных потребителей, а если говорить точнее - с точки зрения операторов и провайдеров телекоммуникаций. Суть ее заключается в том, чтобы определить приоритеты построения системы управления согласно факторам административной и экономической целесообразности.

Рисунок 1. Общая структура TMN

Уровень управления сетевыми элементами - система управления этого уровня позволяет управлять каждым сетевым элементом в отдельности, без интегрированного вида всей сети.

Уровень управления сетью. Данный уровень должен предоставлять услуги интегрированного мониторинга и управления сетью в целом, безотносительно к технологиям, используемым на сети и количеству сетевых элементов.

Уровень управления услугами абстрагирован от большинства технических задач управления сетями телекоммуникаций. Задачами данного уровня является отслеживание качества предоставляемых услуг, ведение биллинга, прием заявок от потребителей на предоставление услуг и ведение реестра услуг и потребителей.

Уровень управления бизнесом - реализация управления на этом уровне предполагает управление всем предприятием оператора (провайдера) в целом.

Следует отметить эффективность подхода к построению логической многоуровневой иерархии. Каждый последующий уровень базируется на функциональности и информации предыдущего уровня, отбирая нужные сервисы предыдущего уровня и отбрасывая лишние.

Подводя итоги, можно определить что если нынешнее время телекоммуникацию рассматривать как науку или как бизнес, будет очевидно что есть потребность организовать управления от всех видов услуг до маркетинга. Проведения научных исследований в направлении “Управление телекоммуникационными сетями” даст большие успехи в развитии науки. И соответсвенно это дает возможности выбора оптимальных вариантов управления бизнеса и услуг в сфере телекоммуникации.

МОДЕЛИРОВАНИЕ СЕНСОРНЫХ СЕТЕЙ В ТЕХНОЛОГИИ INTERNETOFTHINGS

Абдухалилов С.Ғ.(ТУИТ, магистрант)

Развитие технологии InternetofThings - IoT («Интернет вещей) предполагает использование встраиваемых сетевых устройств, так называемых умных объектов, в окружающие нас вещи. Можно привести много примеров подобных устройств: мобильные телефоны, персональные устройства здравоохранения, устройства домашней и промышленной автоматизации, системы учета и мониторинга окружающей среды и т. п.

В основе технологии IoT лежит принцип построения беспроводных сенсорных сетей на базе современных маломощных ZigBee модулей. Точное количество узлов сети то есть размер сети, реализованной на принципах технологии InternetofThings на сегодняшний день трудно оценить, так как рост данных сетей не зависит от количества пользователей в них. Предполагается, что эта составляющая скоро превысит остальную часть сети Интернет по размеру и будет продолжать расти быстрыми темпами. Долгосрочный потенциальный размер IoT сейчас оценивается триллионами устройств. Сказанное убедительно доказывает важность исследования вопросов моделирования сенсорных сетей на базе маломощных ZigBee модулей с целью оптимизации процесса проектирования и построения сетей IoT.

Среди средств имитационного моделирования отдельных событий и состояний беспроводных сенсорных сетей на базе стандарта IEEE 802.15.4-2006 наибольшее распространение получили следующие среды. NS-2 - объектно-ориентированная среда имитационного моделирования дискретных событий и состояний с открытым исходным кодом. OPNETModeler - мощная среда имитационного моделирования дискретных событий и состояний. OMNET++ - среда имитационного моделирования дискретных событий и состояний с открытым исходным кодом, основанная на компонентах ZigBee. Основная область применения - моделирование сетей передачи данных, ИТ систем и бизнес процессов.

Был проведен сравнительный анализ различных симуляторов. Проведенный анализ показал, что в условиях некоммерческого использование средства моделирования использование программного комплекса OPNETModeler представляется проблематичным из-за его дороговизны. NetworkSimulatorNS-2 также не подходит из-за несоответствия спецификации модулей ZigBee, на которых базируются структуры, реализованные по технологии InternetofThings. Таким образом, из проанализированных симуляторов для моделирования ZigBee-сетей на сегодня программный комплекс OMNET++ являются наилучшим вариантом.

Результаты сравнительного анализа симуляторов приведены в таблице. Наличие каждого параметра в характеристике симулятора помечается символом «+», отсутствие - символом «-».

Параметры	S-2	OPNET	OMNET++
Расчет потребляемой узлами энергии	-	+	+
Определение энергии в текущем канале	-	+	+
Открытый код	-	-	+
Мобильность узлов	-	-	+
Соответствие спецификации ZigBee	-	-	+
Наличие протоколов маршрутизации	-	+	+

В подтверждение выводов авторами была построена событийно- имитационная модель для типовой беспроводной сенсорной сети. На ее основе сымитирована работа и определено максимальное время работы сети. Основной акцент сделан на вопросы

потребления энергии каждым устройством беспроводной сенсорной сети. Была смоделирована сеть с топологией звезда состоящая из 20 станций и использующих стандарт 802.15.4 для беспроводной связи. В приведенном примере максимальное время работы сети без подзарядки (смены) автономных источников питания составило 130 часов непрерывной работы при минимальном потреблении энергии узлами сети. Также были проведены расчеты эффективной скорости передачи данных, энергопотребления и времени работы при заявленной и рассчитанной скорости.

В каждой беспроводной сенсорной сети может быть только одно устройство-координатор. Основная задача координатора заключается в установке параметров и создании сети, выборе основного радиочастотного канала, в задании уникального сетевого идентификатора. Важным при моделировании БСС является соответствие используемой модели реальным сетям. В наибольшей мере это относится к модели канала связи. Для разрешения этого вопроса требуется реализовать проверку результатов моделирования сети относительно результатов работы реальной беспроводной сенсорной сети. Проведенные исследования показали эффективность использования моделирующей среды OMNET++, позволяющей определить основные параметры и структуру сенсорной сети на этапе ее проектирования. Данное программное обеспечение позволяет адекватно смоделировать проектируемую сеть и определить ее основные параметры и характеристики.

Таким образом можно сделать вывод, моделирование сенсорных сетей в технологии InternetofThings на сегодняшний день рационально проводить с помощью симулятора OMNET++, который показывает наилучшие характеристики, в частности для небольших сетей, построенных на ZigBee-модулях.

РАЗРАБОТКА СИСТЕМЫ НЕЧЕТКОГО ВЫВОДА В ИНТЕРАКТИВНОМ РЕЖИМЕ В СРЕДЕ MATLAB

С.Ғ.Абдухалилов (ТУИТ, магистрант)

В последнее время применение нечетких множеств для синтеза управления сложными системами является одним из наиболее перспективных направлений прикладных исследований в области информационных технологий. Применение нечеткой логики оказывается особенно полезным, когда в описании технических систем присутствует неопределенность, которая затрудняет или даже исключает применение точных количественных методов и подходов. В области информационных технологий применение нечеткой логики позволяет получать более адекватные результаты по сравнению с результатами, которые основываются на использовании традиционных аналитических моделей и алгоритмов управления. Диапазон применения нечетких методов с каждым годом расширяется, охватывая такие области, как проектирование промышленных роботов и бытовых электроприборов, управление доменными печами и движением поездов метро, автоматическое распознавание речи и изображений.Целью данной работы является рассмотрение примера разработки системы нечеткого вывода в интерактивном режиме в среде Matlab.Для реализации процесса нечеткого моделирования в среде Matlab предназначен специальный пакет расширения FuzzyLogicToolbox. В рамках этого пакета, пользователь может выполнять необходимые действия по разработке и использованию нечетких моделей в одном из следующих режимов:в интерактивном режиме с помощью графических средств редактирования и визуализации всех компонентов систем нечёткого вывода. Для разработки и дальнейшего применения систем нечеткого вывода в интерактивном режиме используем следующие графические средства, из состава пакета FuzzyLogicToolbox:

- Редактор систем нечеткого вывода FIS (FISEditor);
- Редактор функций принадлежности системы нечеткого вывода;

- Редактор правил системы нечеткого вывода (RuleEditor);
- Программа просмотра правил системы нечеткого вывода.

В качестве примера разработки системы нечеткога вывода в интерактивном режиме с помощью графических средств пакета FuzzyLogic Toolbox рассмотрим следующую нечеткую модель. Задача состоит в том, чтобы разработать некоторую экспертную систему, которая была бы реализована в виде системы нечеткого вывода и позволяла бы определять величину уязвимости данных угрозам на основе примерных оценок в области защиты информации.

В качестве входных параметров системы нечеткого вывода используем две нечеткие лингвистические переменные: "качество облуживания" (оборудования) и "качество используемой защиты", а в качестве выходных параметров - нечеткую лингвистическую переменную "уровень угрозы". В качестве терм множества первой лингвистической переменной "качество обслуживания" рассматриваем множество T1={"плохое", "хорошее", "отличное"}, а в качестве терм множества второй лингвистической переменной "качествозащиты" будем использовать множество T2= {"хорошая", "плохая"}. В качестве терм множества выходной лингвистической переменной "уровень угрозы" будем использовать множество T3= {"малый", "средний", "высокий"}. Каждый из термов первой и второй входной переменной будем оценивать по 10-балльной порядковой шкале, при которой цифре 0 соответствует наихудшая оценка, а цифре 10 - наилучшая оценка. Что касается термов выходной переменной, то предположим, что малая угроза составляет около 5%, средняя - около 25%, а высокая - около 45% потерь информации. С учетом уточнений, рассмотренная информация о величине угрозы может быть представлена в форме 3-х правил нечетких продукций следующего вида:

Правило 1: ЕСЛИ "качество обслуживания отличное" ИЛИ "защита высокая" ТО "угроза малая";

Правило 2: ЕСЛИ "качество обслуживания хорошее", ТО "угроза средняя";

Правило 3: ЕСЛИ "качество обслуживания плохое" ИЛИ "защита слабая" ТО "угроза высокая". Процесс разработки системы нечеткого вывода в интерактивном режиме состоит из следующей последовательности действий:

- Вызов редактора системы нечеткого вывода FIS (команда: fuzzy).
- Добавление в разрабатываемую систему FIS еще одной входной переменной;
- Замена имен входных и выходных переменных, предложенных системой Matlab по умолчанию;
- Изменение имени системы нечеткого вывода, предложенное по умолчанию;
- Определение термов и их функций принадлежности для входных и выходных переменных нашей системы нечеткого вывода. Для этого используем редактор функций принадлежности, в котором делаем со-ответствующие задания диапазонов входных переменных, названий термов, тип функций принадлежности;
- Задаем правила нечеткого вывода для разрабатываемой экспертной системы (используя конструктор базы правил);
- После задания правил нечеткого вывода оказывается возможным получить результат нечеткого вывода (значение выходной переменной) для конкретных значений входных переменных (программа просмотра правил);

Наиболее эффективным интерактивный режим оказывается для сложных нечетких моделей с большим числом переменных и правил нечеткого вывода. В этом случае задание переменных и функций принадлежности их термов в графическом режиме, а также визуальное представление правил позволяют существенно уменьшить трудозатраты на разработку нечеткой модели, снизить количество возможных ошибок и сократить общее время нечеткого моделирования.

ЭФФЕКТИВНЫЕ СЕТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ: ПРИМЕНЕНИЕ И РАЗЛИЧИЕ

Б.У.Акмурадов (ТУИТ, ассистент)

Сетевая операционная система необходима для управления потоками сообщении между рабочими станциями и серверами. Она может позволить любой рабочей станции работать с разделяемым сетевым диском или принтером, которые физически не подключены к этой станции.

В некоторых компьютерных сетях есть выделенный автономный компьютер который выполняет функции только файлового сервера. Такие системы называются локальные вычислительные сети (ЛВС) с файловым сервером. В других, малых ЛВС, рабочая станция может одновременно выполнять и функции файлового сервера. Это одно ранговые ЛВС.

Компоненты сетевой операционной системы на каждой рабочей станции и файловом сервере взаимодействуют друг с другом посредством языка, называемым протоколом. Одним из общих протоколов является протокол фирмы IBM NetBIOS (Network Basic Input Output System -Сетевая операционная система ввода-вывода). Другим распространенным протоколом является IPX (Internet-work Packet Exchange - Межсетевой обмен пакетами) фирмы Novell.

Novell производила как аппаратные средства, так и программные, однако в последнее время фирма Novell сконцентрировала усилия на программных средствах ЛВС.

ОС NetWare способна поддерживать рабочие станции, управляемые DOS, DOS и Windows, OS/2, UNIX, Windows NT, Mac System 7 и другими ОС.

ЛВС NetWare может работать с большим количеством различных типов сетевых адаптеров, чем любая другая операционная система. Для достижения поставленных целей вы можете выбрать аппаратные средства от множества разных поставщиков. С NetWare можно использовать ARCnet, EtherNet, Token Ring или практически любой другой тип сетевого адаптера.

NetWare допускает использование более, чем 200 типов сетевых адаптеров, более чем 100 типов дисковых подсистем для хранения данных, устройств дублирования данных и файловых серверов.

Фирма Novell имеет контракты о поддержке ОС NetWare с наиболее крупными и мощными из независимых организаций, таких как Bell Atlantic, DEC, Hewlett-Packard, Intel, Prime, Unisys и Xerox.

Файловый сервер в NetWare является обычным ПК, сетевая ОС которого осуществляет управление работой ЛВС. Функции управления включают координацию рабочих станций и регулирование процесса разделения файлов и принтера в ЛВС. Сетевые файлы всех рабочих станций хранятся на жестком диске файлового сервера, а не на дисках рабочих станций.

Имеется три версии ОС NetWare. Версия 2.2 может работать на компьютере 80286 (или более поздних моделях), используемом в качестве файлового сервера. При покупке ОС необходимо приобретать лицензию на число пользователей (5, 10, 50, 100). Версии ОС NetWare 3.12 и более новая 4.0 ориентированы на 32 разрядные шинные архитектуры и процессоры 80386, 80486 или Pentium. Есть также варианты сетевой ОС NetWare, предназначенные для работы под управлением многозадачных, многопользовательских операционных систем OS/2 и UNIX. Версию 3.12 ОС NetWare можно приобрести для 20, 100 или 250 пользователей, а версия 4.0 имеет возможность поддержки до 1000 пользователей.

Все версии ОС хорошо совместимы между собой, поэтому в одной и той же компьютерной сети можно иметь файловые серверы с разными версиями ОС NetWare.

В NetWare различают три типа накопителей: локальные накопители, сетевые накопители и поисковые накопители. Локальные накопители физически подключены к рабочим станциям. Сетевые накопители - это накопители на жестких дисках файлового сервера. Аналогично тому, как в DOS, применяется средство PATH для задания списка накопителей и директорий, в которых по умолчанию разыскиваются прикладные программы, в ОС NetWare используется понятие поискового накопителя.

ОС NetWare позволяет манипулировать файлами и директориями различными способами. Можно копировать, уничтожать, переименовывать, записывать, распечатывать и разделять файлы в ЛВС. Есть также определённая система прав доступа к файлам и директориям.

Как файлы так и директории на сервере в ЛВС под управлением ОС NetWare имеют атрибуты. Эти атрибуты могут отменять права, предоставленные пользователям в ЛВС.

Есть некоторые отличия сервера ЛВС NetWare от обычного ПК. Для накопителя на жестком диске этого компьютера применена структура форматирования совершенно отличная от той, которая применяется в DOS. Невозможно получить доступ к жесткому диску такого сервера, если вы загрузили DOS с дискеты. Но для пользователя ЛВС который работает под управлением DOS и получил доступ к серверу со своего терминала ,жесткий диск сервера представляется просто как дополнительный к уже существующим.

Формат записи данных на жестком диске, который применен в ОС NetWare, включает большее количество информации о файлах и директориях, чем это было возможно в DOS. Файлы в ОС NetWare наряду с атрибутами “только для чтения”, “скрытый” и “архивный” могут дополнительно иметь атрибут “неразделяемый” и “разделяемый” (он указывает на возможность разделения файла в ЛВС многими пользователями одновременно). Кроме этого, ОС NetWare добавляет к информации о файле следующие элементы: исходную дату создания, имя создателя файла, дату последнего доступа к файлу, дату последней модификации файла, дату и время последней архивации файла.

Система защиты данных в ЛВС NetWare включает в себя следующие меры:

- защита от несанкционированного присоединения к ЛВС путем присвоения имен и паролей пользователям, а также ограничениями на доступ к ЛВС пользователей с определенными именами в определенное время дня.
- система доверяемых прав (trustee rights), позволяющая контролировать, к каким файлам и директориям может имеет доступ пользователь, а также какие операции он может производить с ними.
- система атрибутов для директорий или файлов, которые определяют возможность копирования, просмотра, записи и разделения их в ЛВС.

Отказоустойчивость является на сегодняшний день одной из наиболее важных характеристик, и разработчики NetWare уделили должное внимание этому вопросу. В версиях 2.2, 3.12 и 4.0 ОС NetWare применена технология SFT *(*System Fault Tolerant-Система защиты при отказах оборудования). Система защиты при отказах оборудования означает бесперебойную работу файлового сервера при различного рода отказах аппаратных средств. Во всех версиях NetWare имеются средства минимизации потерь данных в случае физических повреждений поверхности накопителей. Система SFT пошла дальше в этом отношении предложив методы зеркального отображения дисков и дублирования дисков

В системе NetWare имеется возможность контроля сигналов источника бесперебойного питания UPS. При обнаружении перебоя с подачей электроэнергии ОС уведомляет пользователей об этом и сообщает им каким промежутком времени они располагают для завершения своей работы. По истечении этого промежутка времени ОС автоматически закроет все файлы в системе и выключит себя.

Рассматриваемые сетевые операционные системы LAN Manager и LAN Server дают возможность контролировать доступ к клавиатуре и экрану файлового сервера. В специальном невыделенном режиме работы файловый сервер позволяет пользователям просматривать и управлять очередями печати, но не разрешает изменять псевдонимы зарегистрированных пользователей или другие административные данные. Для доступа к экранам с административными данными пользователь должен задать специальный пароль. NetWare допускает использование более, чем 200 типов сетевых адаптеров, более чем 100 типов дисковых подсистем для хранения данных, устройств дублирования данных и файловых серверов.

Главным требованием, предъявляемым к операционной системе, является выполнение основных функций эффективного управления ресурсами и обеспечение удобного интерфейса для пользователя и прикладных программ. Современная ОС, как правило, должна поддерживать мультипрограммную обработку, виртуальную память, свопинг, многооконный графический интерфейс пользователя, а также выполнять многие другие необходимые функции и услуги.

SMART GRID В ПЕРЕДАЮЩИХ СИСТЕМАХ

Н.Ю. Амурова (старший преподаватель ТУИТ)

В наступившие цифровые времена стали конкурентными две логичные концепции: строительство своей системы связи и взаимодействие с операторами связи. Но жизнь – это, как правило, компромисс, и что-то должно быть в наличии у самих энергетиков, а что-то нужно заказывать у профессиональных операторов.

Объекты энергетики, будучи протяжёнными и высотными, позволяли совместно решать многие вопросы связистов и энергетиков, например, прокладывая в грозотросах ЛЭП волоконно-оптические линии (ВОЛС) или используя высотные сооружения энергетики для радиосвязи разного рода. На этом этапе уже понадобились технологии и методы геоинформационных систем (ГИС), в том числе для точного расчёта оптики в условиях провисания провода или расчётов зон радиовидимости. Однако, при всей плодотворности взаимоотношений двух отраслей на начальном цифровом периоде, они были объективно не слишком плотными. Одной из причин был тот факт, что связь ушла от аналога (кто-то помнит декадно-шаговые телефонные станции?) к тотальной цифре, а энергетика только сегодня начала переход от аналоговых к цифровым подстанциям. При этом надо понимать, что это в основном касается режимов управления передачей или распределением электроэнергии. Но постепенно и энергетика стала цифровой, появились компьютеры, программы, сенсоры и т.п. И это новое качество назвали Smart Grid, т.е. “умная (интеллектуальная) электрическая сеть”.

Фундаментальный фактор, способствующий Smart Grid – широкая доступность безопасной телекоммуникационной платформы. Технологические решения и активы, находящиеся у операторов мобильной связи, могут стать такой платформой для Smart Utilities, в том числе благодаря своему покрытию, безопасности, опыту в обслуживании миллионов распределённых объектов и абонентов, объемов передаваемых данных, а также финансовой силе и стабильности мобильной “экосистемы”.

Энергопередающие сетевые предприятия нуждаются в таких телекоммуникациях, которые охватывали бы всю территорию их деятельности, что позволило бы им предложить своим клиентам новые продукты и услуги, связанные с доставкой электроэнергии и других коммунальных удобств. Это требует всеобъемлющего покрытия двухсторонней системой связи. Операторы мобильной связи располагают широкополосными беспроводными сетями, покрывающими населенные районы, и могут быстро запустить надежные и безопасные коммуникационные системы типа “машина-

машина” (M2M) с гарантированным уровнем мощности/пропускной способности и управляемым качеством сервисов (например, VPN / VPLS; QoS / CoS и т.д.).

Система на основе Smart Grid будет поддерживаться множеством сложных и гетерогенных телекоммуникационных сетей. Энергетический сектор нуждается в практическом опыте построения и управления масштабными телекоммуникационными сетями партнёров. А индустрия мобильной связи имеет наибольший опыт в развертывании сетей и создании экономически эффективной и надежной телекоммуникационной инфраструктуры.

Сильные стороны отрасли мобильной связи в области технологии и финансовой эффективности должны быть сосредоточены на направлениях усовершенствования измерений, автоматизации распределения, автоматизации подстанций, распределённой генерации, реагирования на изменения потребления, хранения запасенной энергии и интеграции с инфраструктурой для электромобилей, а также на дополнительных услугах. Каждое из этих направлений предполагает создание современных сервисов и обладает значительным потенциалом для извлечения прибыли для сервис-провайдеров, даже помимо предоставления каналов связи.

Мобильные операторы могут также стать энергетическими реселлерами, работающими напрямую с частными и бизнес-потребителями. Возможность для потребителей осуществлять мониторинг, управлять и контролировать свое энергопотребление и эмиссию CO2 со своего мобильного телефона практически из любой точки в режиме реального времени, скорее всего, будет хорошо воспринята как потребителями, так и регулирующими органами. Более того, совместный брендинг мобильных и энергокомпаний может помочь повысить осведомленность потребителей и будет способствовать более быстрому принятию потребителями новых интеллектуальных услуг в области энергоснабжения. Создание и внедрение технологий Smart Grid и Smart Utility предоставляют перспективную глобальную возможность для операторов сетей связи сервис-провайдеров, производителей оборудования, разработчиков системного и прикладного программного обеспечения, системных интеграторов и хостеров. Осознание объемом этих возможностей зависит от тщательного изучения сектора инженерных коммуникаций и энергетики, а также от технических, коммерческих и законодательных требований к Smart Grid и Smart Utility. Более того, поставщики продуктов и сервисов для сектора инженерных коммуникаций должны в ближайшее время предпринять ряд эффективных инициатив, чтобы гарантировать эффективное позиционирование предлагаемых решений.

Инфраструктура передачи служит для транспортировки электроэнергии от точек генерации к передающим подстанциям, снижающим напряжение, и затем к распределительным подстанциям, которые снова снижают напряжение, чтобы электричество могло использоваться промышленностью, бизнесом и жителями. Затем питающие провода получают электроэнергию от этих подстанций и доставляют её до конечных потребителей. Развитие сетей передачи в большинстве стран мира прошло путь от систем с отдельными «изолированными» электростанциями, через изолированные локальные системы к региональным и, наконец, к большим комплексным межрегиональным энергосистемам, которые существуют сегодня. Накопление и управление сведениями о состоянии энергетических сетей и их модель (CIM), как правило, реализуются с участием инструментария ГИС.

Поскольку электроэнергия не может эффективно накапливаться и сохраняться в значительных объёмах, подача в каждый момент должна быть сбалансирована с потреблением. Балансировка подачи и потребления в больших (высоковольтных) системах относится к зоне ответственности системных операторов. На некоторых рынках, например в США, системный оператор может являться собственником передающих активов, или же системный оператор может быть независим от владельца передающих сетей, при этом он носит название Независимого системного оператора (НСО).

Системные операторы взаимодействуют с операторами генерирующих активов для балансировки сети. Они добиваются этого за счет анализа потребления, анализа перетока мощности и прогнозирования, что определяет спрос, действующего напряжения в электросети, в то время как оптимальный поток мощности определяет оптимальную диспетчеризацию ресурсов для обеспечения надежного соответствия нагрузке.

Коммуникации играют ключевую роль в эффективности оптовых энергосистем и Smart Grid в передающих системах. Мониторинг и прогнозирование потребления, балансировка нагрузки и поставок – все это требует надежных, высокоскоростных коммуникаций между участниками оптового рынка электроэнергии. Регулирование спроса становится возможным благодаря распределенным, высокоскоростным коммуникациям с устройствами контроля нагрузки. Кроме того, мониторинг состояния и параметров передающих активов, таких как частота, температура, напряжение и сила тока, фазовый угол позволяет владельцам и операторам передающих компаний управлять надежностью и производительностью передающей системы.

Инфраструктура мобильных операторов – цифровые станции, кабели, в т.ч. ВОЛС, активное и пассивное оборудование, вышки сотовой связи – также часто хранится в ГИС, как пространственная инфраструктура и модель.

Делая вывод нужно сказать, что автоматизированные устройства управления коммутацией и напряжением являются неотъемлемым элементом безопасности и надежности энергосети. Автоматизация передающих подстанций – это ключевая функция, возможность которой обеспечивает коммуникационная инфраструктура энергосети. Надежные, высокоскоростные двусторонние коммуникации сегодня стали незаменимыми для обеспечения более сложного мониторинга, контроля и управления энергопередающей сетью.

ОБЪЕКТЫ И СИСТЕМЫ ЭНЕРГЕТИЧЕСКИХ СЕТЕВЫХ КОМПАНИЙ

Н.Ю. Амурова (старший преподаватель ТУИТ)

Телекоммуникации, информационные технологии, цифровые медиа – сфера, которая во всем мире подвержена непрерывным, стремительным, кардинальным изменениям. Отрасль коммуникаций и новых технологий, проникая во все сферы повседневной деятельности человека, является одной из самых значимых по степени влияния на нашу частную и рабочую жизнь, социальную сферу, экономику, имидж и статус страны в мировом сообществе. При информатизации общества основное внимание уделяется комплексу мер, направленных на обеспечение полного использования достоверного, исчерпывающего и своевременного знания во всех видах человеческой деятельности.

Сетевые энергетические компании эксплуатируют и поддерживают развитую сеть распределительных объектов: воздушные и кабельные линии электропередачи, подстанции, трансформаторы, выключатели, конденсаторы и пр.

Важнейшей задачей в этой связи является мониторинг в режиме реального времени состояния и параметров распределительной сети и обнаружение сбоев. Но способность компаний осуществлять его может существенно различаться, поскольку коммуникационные системы распределительных подстанций пока еще не достаточно распространены.

Сетевые энергетические компании работают в соответствии с обязательством обеспечивать бесперебойную поставку электроэнергии, и их решения направлены на соблюдение этого обязательства.

Цена на электроэнергию, конечно, также имеет значительный вес в процессе принятия решений. Smart Grid поможет сделать деятельность таких компаний более эффективной за счет возможности осуществлять надежные коммуникации, их

инспектирование и обслуживание в зависимости от текущих условий, что помогает повысить надежность и снизить издержки. Такой мониторинг и обслуживание могут выполняться удаленно: управление активами M2M («Machine-2-Machine»), например, уже предлагается многими поставщиками мобильных услуг.

Автоматизация фидеров – важная функция в эксплуатации и управлении распределительными системами. С ее помощью можно измерять и более точно контролировать напряжение, доходящее до потребителя, а также управлять переключателями между фидерами для локализации неисправности и минимизация времени отключения, то есть для общего повышения надежности.

Распределительные системы подают энергию на территорию потребителя. В настоящее время потребление отслеживается с помощью механических счетчиков, но сейчас они эволюционируют в сторону автоматического считывания показаний через расширенную инфраструктуру измерений (AMI). И это также ключевая возможность для обслуживания клиентов, предоставляемая Smart Grid.

AMI дает возможность взаимодействовать с потребителем и понимать их поведение. Благодаря частой загрузке данных, AMI может дать сетевой энергетической компании огромный массив информации для анализа потребительского поведения.

Эффективно управляя этой информацией, компания может внедрить прямой контроль нагрузки, программы Demand Response и удаленное подключение/отключение, надежный мониторинг частной генерации (например, солнечных батарей на крыше).

Ни одна из этих возможностей не может быть реализована без коммуникационной системы, которая позволяет энергокомпании быть в надежном «контакте» с эксплуатационными показателями на всей своей территории обслуживания. А пространственный анализ ситуации помогут обеспечить ГИС.

Традиционные системы оперативной связи исторически сфокусированы на четырех областях, критичных для отрасли поставок электроэнергии.

Во-первых, это связь системы диспетчерского контроля и сбора данных (SCADA), используемой для мониторинга параметров производительности и надежности электрораспределительной сети, таких как напряжение, мощность, качество электроэнергии и вольт-амперно реактивная мощность (VAR), а также для уведомления о нештатных или неожиданных событиях, таких как перегрузки или неисправность автоматического выключателя, и может осуществлять контроль деятельности на подстанциях и на фидерах.

Во-вторых, это полевая связь – системы наземной мобильной радиосвязи (LMR).

Далее, это транзитная связь – средства для поддержки нужд связи с высокой пропускной способностью, включая радиорелейные каналы и оптоволоконные линии.

Наконец, это телемеханическая релейная защита или защита магистральных систем электропередачи высокого и сверхвысокого напряжения – выполняется специализированными системами высокочастотной связи по ЛЭП или выделенными каналами связи (медными или оптоволоконными) между реле телемеханической защиты.

Новое поле деятельности и требования поддержки энергетического бизнеса, реализуемые в т.ч. поставщиками коммунальных услуг для обеспечения современных сервисов и возможностей, включают желание или необходимость:

- интеграции возобновляемых/цикличных источников энергии (солнечной, ветровой и др.) в существующую систему, которая разработана для управляемого крупномасштабного генерирования и одностороннего потока энергии;
- усиления КПД при распределении электричества; повышения качества и улучшения стабильности и доступности сети передачи/распределения электроэнергии;
- повышения гибкости системы с возможностью восстановления в случае стихийного бедствия, физической или кибернетической атаки;

• повышения эффективности работы, в том числе путем автоматизации и сокращения численности персонала, необходимого для эксплуатации и техобслуживания системы передачи/распределения;

• снижения затрат, связанных с фиксацией показаний счетчиков, для согласования тарификации потребителей в зависимости от времени суток и/или пиковой нагрузки с фактическими затратами сетевых энергетических предприятий, контроль нагрузки на стороне потребления и/или стимуляция потребителей использовать электроэнергию в часы с низкой нагрузкой;

• постепенного прекращения использования устаревшего оборудования связи с высокой стоимостью обслуживания. Оборудование поставщиков и операторов связи эволюционирует к коммутируемым сетям передачи данных и новым интеллектуальным оконечным устройствам (IED), которые заменяют старые RTU. Подобные устройства включают в себя связь IP/Ethernet.

Большое внимание в рамках Smart Grid уделяется вопросам коммуникационной и информационной безопасности и защиты от кибератак (“кибербезопасность”). К энергетическим сетевым предприятиям в США предъявляются жесткие требования Североамериканской корпорации надёжности электроэнергетики (NERC) для защиты объектов жизнеобеспечения (CIP). CIP определяет методологию, которая выявляет критические ресурсы инфраструктуры и связанные кибернетические ресурсы с "квалифицированной подключаемостью”.

Подобные требования к защите критических ресурсов выполняются также в Европе и в других регионах. Принимая во внимание, что большинство CIP фокусируются на средствах и системах “массовой поставки электроэнергии”, системы DA и AMI восприимчивы к требованиям NERC CIP.

Например, системы, которые могут контролировать и, соответственно, поддерживать 300 MW требования или больше, таких как спуфинг команд разъединения интеллектуальных счетчиков AMI к 300K потребителей или более, приняты большинством сетевых энергетических предприятий для соответствия требованиям киберзащиты NERC CIP.

Подводя итог вышесказанному видно, что эти стремления выдвигают расширенные или совершенно новые требования к связи со счетчиками потребителей вплоть до счетчиков в домашней локальной сети, а также к расширенной автоматизации распределения (DA), обеспечивающей дополнительные точки контроля и мониторинга вдоль линий передачи и подстанций. Они обеспечивают расширение покрытия и ёмкости, повышение доступности и безопасности, контроль устаревания, снижение стоимости.

ЗАМОНАВИЙ ЎРНАТИЛГАН ТИЗИМЛАРИНИНГ АППАРАТ ВА ДАСТУРИЙ ТАЪМИНОТИ

Ф.И. Ахунов (ТАТУ, доцент)

Ҳисоблаш техникасининг мураккаблиги ошиши билан лойиҳалаш жараёнларини тизимлаш ва тузилишини аниқлаш ҳаракатлари талаб қилина бошланди. Лойиҳанинг миқёси ошганда хатолар сони кўпайиши мураккаблик танглиги бўлиб кўрсатилади. Мураккаб дастурларни тузишда алгоритм блок-схемаси катта лойиҳаларда керакли самарадорлик бераолмай қолди. Дастурий тизимларни структуравий ва хатти-ҳаракатли ташкил этувчилари кўринишида баён этиш таклифлари пайдо бўлди. Тизимни лойиҳалашга умумий муносабат билан бирлашган лойиҳалаштириш технологиялари вужудга келди.

Бу лойиҳалаштириш технологиялари структуравий деб номланди. Дастурий таъминот миқёсида бу лойиҳалашга ёндашув дастурларни бажариладиган иш тартиби ва маълумотлар структурасига бўлинди. Бу ерда архитектуравий лойиҳалаш қўшилди.

Архитектуравий лойиҳалашга ўтишда биринчи қадам бўлиб дастурларни оддий матн кўринишида инсоний сўзлаш таклифлари бўлди. Кейинчалик бу тасвирлашлар структуравий инглиз (рус ва х.к.) ёки имзосиз(нутқий) номини олди. Дастурий таъминотни имзосиз тасвирлашни камчилиги бундай усул билан тасдиқланишларни тўғрилигини математик исботи мумкин эмаслигидир.

Дастурий таъминотни архитектурасини тасвирлашда бир неча усуллари ёрдамида амалга оширилади. Асосан дастурий таъминотни тасвирлашда хатти-ҳаракатли «маълумотлар», «жараён», «бошқаришни узатиш», «маълумотларни сақлайдиган жой» (DFD, CFD, SADT) схемалари қўлланилган. Маълумотлар базасини тасвилаш учун бир бирига боғлиқ бўлганлик асосидаги структуравий баён қилиш ўйлаб топилди. Эрта яратилган лойиҳалаш усуллари вақт омилларини ҳисобга олмаганлар. Дастурий таъминотни масъул қисмлари учун туб автоматлар кўринишидаги тасвирлаш қўлланила бошланди.

Структуравий ёндашув аппарат таъминотини лойиҳалашни ечишда қўлланилар эди. Аппарат тизими структуравий, функционал, электр принципиал схемалар ва вақт диаграммалар тўплами билан тасвирланган.Одатда аппарат таъминоти дастурий таъминотдан алоҳида ишлаб чиқилган.

Ўрнатилган тизимларни киритиш-чиқаришини ўрнатилган реал вақтли операцион тизимни (РВОТ - RTOS) архитектураси мисолида кўриб чиқамиз.

Киритиш-чиқариш қурилмалари процессор билан қандай уланиши ва дастурий таъминот улар билан боғланишини тушуниш учун замонавий ўрнатилган қурилмаларда ўхшаш киритиш-чиқаришини архитектурасини кўриб чиқиш лозим.

Маълумотларни хотирага ва киритиш-чиқариш қурилмаларга процессорлар шина орқали узатишлари керак. Шина адресли ахборотга маълумотлар миқдори ва шина ҳолати ва у бажарадиган амал (ўқиш ёки ёзиш) ҳақидаги маълумот узатишга мўлжалланган.

Замонавий ҳисоблаш тизимлари мураккаб бўлиб ҳақиқатда турли турдаги шиналар иерархиясига эга. Ҳар бир шина турли нарх ва ўтказиш полосасини ўз ичига олади. Одатда, кенг ўтказиш полосаси қимматроқ бўлади ва айрим шиналар мерос қурилмаларни қўллашга керак бўладилар.

Ҳотира ва киритиш-чиқариш қурилмалари процессор микросхемаси ва дастурий таъминот билан бир-бирига таъсир қилишини тушуниш учун бу маълумотлар компьютер шиналари орқали узатиш асосларини тушуниш керак.

РВОТнинг хусусият ва имконларини тушуниш учун ўрнатилган тизимларда қўлланиладиган коммерцияли РВОТ архитектураси ва хусусиятлари текширилади. Кенг қўлланиладиган операцион тизимлар (масалан, стол устидаги шахсий компьютерлар) реал вақтдаги жавоб реакциясини таъминлаб бера олмайди , аппарат ёрдамини ва замонавий ўрнатилган қурилмаларга кўра катта энергия таъминотини талаб қилади.

Ўрнатилган қурилмалар кўпчилигида қўлланиладиган коммерцияли РВОТда Windows Embedded CE энг оммабоп бўлади. Windows CE операцион тизимини шаклини ўзгартирилмаган версияси эмас, бу бутунлай янги ОТ ва ҳотира ҳажми ва процессор қуввати камроқ бўлганларга мўлжалланган.

Реал вақдаги CE таъсирланиш вақти тезроқ, ядро катталиги умумий стол устидаги ОТ дан кичикроқ.

CE C/C++ и C# кросс-компиляторлари, йиғиш тизими, ва стол устидаги ШКда бажариладиган созлаш асбобларнинг катта тўпламига эга. Бу асбоблар ОТда ва иловаларда тузувчилар томонидан қўлланилади ва уларда браузер, Word Pad, хабарлар алмашиш хизмати , медиа-плеер ва бир неча ўйинлар киритилган. ОТ ни янги ядросини генерациялашда Visual Studio да бажариладиган Platform Builder деб номланадиган GUI асосидаги махсус асбоб қўлланилади. X86, ARM, SHx, и MIPSларни ўз ичига олган бир неча оммавий ўрнатилган процессорларнинг оиласи киритилади. CE архитектураси Kernel и User имтиёзли режимлар атрофида яратилган. ОТ да базавий хизматларни кўрсатадиган фундаментал тизимли қисмлари имтиёзли Kernel режимида бажарилади,

қўлланиладиган процесслар ва dill кутубхоналари имтиёзсиз User режимида бажарилади. Имтиёзли компонентлар ядрони, қурилмалар ва файл тизимини бошқарувчисини, ва GWESни ўз ичига олади.

Ядрони имтиёзли режимида бажариладиган компонентлар, ядрони узилишларини истеъмол қилишини ва маълумотларни маршрутлашни ташкил этмайдилар. Ядро режими компонентлари орасидаги чақириқлар ядро таъсирисиз амалга оширилади. APIни кўпчилик чақириқлари турли хил тизимли серверлар (filesys, device, kernel, ва х.к.) бир чақириқни тамом қилиш учун ёрдамини талаб қиладилар . Бу тизимли серверлар CE6.0 ядросига фойдаланувчи режимини алоҳида процессорларидан силжитилади. Бу ўзгариш тизимли API кўп чақириқларини унумдорлигига жавобгар бўлади.

ЎРНАТИЛГАНТИЗИМЛАРДА ЭНЕРГИЯИСТЕМОЛ ҚИЛИШНИ КАМАЙТИРИШДА МИКРОКОНТРОЛЛЕРЛАРНИ ҚЎЛЛАШ АФЗАЛЛИКЛАРИ

Ф.И.Ахунов (ТАТУ, доцент)
М.Б.Мирзаева (ТАТУ, ассистент)

Ўрнатилган тизимларни лойихалаш жараёнида микроконтроллерларни энергия истемол қилишни камайтириш мухим масала бўлиб қолади. Энергия истемол қилишни камайтириш автоном электр энергия манбаларидан (батареялар, аккумуляторлар) ишлайдиган контроллерларни ишлаш вақтини кўпайтиради ва ёпиқ худудда (борт электроникаси) пассив совутиладиган (совутиш вентиляторларсиз) тизимларни ишлашида харорат режимини яхшилайди, энергия манбаи схемасини соддалаштиради.

Энергия истемол қилишни камайтириш бўйича қўйилган масалалар айрим ёки биргаликда қўллаш мумкин бўлган бир неча усуллари мавжуд: - платадаги ташқи қурилмаларни энергия таъминотини ўчириш;

- микроконтроллерни такт частотасини камайтириш;
- «уйқу» режими;
- айни пайтда қўлланмайдиган микроконтроллер блокларини ўчириш;
- киритиш-чиқариш портларини минимал энергия истемол қилишга ўтқазиш.

Хар бир холатда ишлатиладиган қурилма схемасини, микроконт-роллерлар ва электрон компонентларни етқазиб берувчи фирмаларни фойдаланувчи учун қўлланма ва қўшимча фикрларни (applicationnotes) мукаммал ўрганиш керак. Керакли натижага эришиш учун платани энергия истемол қилишни мультиметр ёрдамида доимо ўлчаш ва езиб бориш керак.

Бутун схемани энергия таъминотини ўчириш учун микроконтроллер билан ишловчи бир қатор ташқи микросхемаларни манбааларини схемотехник ўчириш имконини таъминлаш керак. Бу схемаларни энергия билан таъминлашни микроконтроллер чиқишлари орқали бажариш мумкин.

Процессорни такт частотасини камайтириш энергия истемол қилишни кенг тарқалган ва содда усули бўлиб қолади . Микроконтроллер турига кўра энергия истемол қилишни камайтириш бирдан ўн баробаргача етиши мумкин. Энергия истемол қилишни камайиши микроконтроллердаги транзисторли каскадларни ўчириш ва ёқишлари сони камайиши билан амалга ошади. Айрим схемаларни энергия истемол қилиши частотага кўпроқ боғлиқ айримларида эса камроқ. Шунинг учун энергия истемол қилиш частотага боғлиқлиги микроконтроллер турига, унга уланган блоклар сонига, киритиш-чиқариш портлар созланишига ва ташқи нагрузкага боғлиқ.

«Уйқу» режими энергия истемол қилишни камайтириш усулларидан энг кучлиги. Микроконтроллер турига кўра энергия истемол қилишда жуда катта ютуққа эришиш мумкин. Бу режимда микроконтроллерни тактлаш ва дастурни бажариш тўхтатилади, энергия истемол қилиш минимал бўлиб қолади.

Режимдан чиқиш қуйидаги холатларда мумкин:

- манбаани ўчириш ва қайта ёқишда ;
- RESET сигнали бўйича, шу билан бирга қўриқчи (wtachdog) таймер сигнали билан;
- тадқиқ этилган узилиш пайдо бўлганида.

Микроконтроллер турига кўра «уйқу» режими такт генератори , регистрлар, хотира ва периферия қурилмалари холатларига таъсир усуллари бўйича фарқланиши мумкин.Хозирги вақтда турли «уйқу» режимларини белгилашда инглиз тилидаги sleep, standbay, stop, wait ва х.к. терминлари қўлланилади.

Одатда ўрнатилган тизимларни «уйқу» режимида ишлаши қуйидагича:

- ташқи ходисалар бўлмаганда тизим уйқу холатида бўлади,
- энерго истемол минимал холатда;
- айрим ходиса пайдо бўлганда микроконтроллер ўйғонади ва керакли амал-ларни бажариб яна «уйқу» холатига қайтади.

«Уйқу» холатини қўллашда даврий ва даврий бўлмаган ишлаш режимлари бўлиши мумкин. Даврий режимда микроконтроллер таймер узиши бўйича уйқудан бирхил вақт оралиғида чиқади. Даврий эмас режимда уйқудан чиқиш ташқи сигнал келишда амалга ошади. Баланд тезкорлигда ечиладиган масала тезроқ бажарилади ва микроконтроллер олдинроқ уйқуга киради ва электр энергияни харажатини камайишига олиб келади.

Микроконтроллер ёқиш ва ўчириш мумкин бўлган кўплаб блоклардан иборат (UART, CAN, I2C контроллерлар, РАЎ, АРЎ, таймерлар ва х.к.). Қўлланилмайдиган блоклар ўчирилса энергия қўлланилиш камаяди.

Киритиш-чиқариш портларини конфигурациялашдан энергия истемолидан ташқари схемаларни ишчанлиги боғлиқ. RESET сигналидан сўнг киритиш-чиқариш портларини конфигурациялари бошланғич холатга ўтади.

Оддий режим ва «уйқу»ни бир режимларида ишлатиладиган қувватни тахминий қийматлари 2-жадвал

Микроконтроллер	**Оддий режим**	**«Уйқу» режими**
Atmelmega	128 33 мВт	75 мкВт
MicrochipPIC	20 мВт (20 МГц)	10 мкВт
TIMSP 430	3 мВт	15 мкВт
STMicroelectronicsARM	74,0 мВт	1.0 мВт
Motorola 68HC705	150 мВт (48 МГц)	33 мкВт

Микроконтроллернирақамликиришларидаминималистемолэтишкиришдагикучлани шнолгаёкиманбаакучланишигаяқинбўлгандаэришилади. Айрим холларда кириш портларни энергия истемолини камайтириш учун аналог режимига ўтказиш афзал.

НЕКОТОРЫЕ АСПЕКТЫ ЭКОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ

Е.А.Борисова (ТУИТ, старший преподаватель)

Разнообразие аспектов экологических проблем, значительные масштабы их решения, которые обусловлены экономическими причинами и отраслевыми особенностями, требуют научного подхода, ориентированного на улучшение экологического состояния окружающей среды в условиях ограниченности ресурсов.

Реализация требований к развитию современных экономических систем предполагает эффективное управление любой экономической системой, которое связано с необходимостью оценки и поддержания механизмов ее безопасности. Учитывая это обеспечение устойчивого развития промышленных предприятий предполагает поддержание их эколого-экономической безопасности, характеризуемой способностью системы предприятия сохранять свои внутренние связи и характеристики функционирования долгое временя под влиянием различных факторов.

Эколого-экономическая безопасность это сложная социально-экономическая категория, которая обеспечивает соблюдение интересов общества и государства, от

различных форм воздействий и негативных процессов, которые создают угрозу здоровью населения и функционированию экологических систем и выживанию человечества.

Для обеспечения эколого-экономической безопасности нужно выявлять и учитывать масштабы негативного воздействия производства, а также оценка экономического ущерба от загрязнения природной среды, что реализуется с помощью математического моделирования, позволяющего в условиях вероятностной природы разнородных величин прогнозировать результаты.

С учетом этого разработка теоретических подходов к эффективному обеспечению эколого-экономической безопасности и развития отраслевой экономики на основе моделирования последствий возникающих опасностей очень актуально.

Эколого-экономическая безопасность определяет устойчивость функционирования предприятий. Все это требует эффективного управления рисками, как экономическими, так и экологическими. В отдельных случаях экологические последствия техногенных катастроф являются главным фактором ущерба окружающей среде.

Моделирование эколого-экономической безопасности, учитывающей воздействия внешних и внутренних факторов на процесс ее обеспечения, а также разработка механизмов причинно-следственного взаимодействия элементов системы эколого-экономической безопасности промышленного предприятия являются злободневными научными задачами.

Разработка методики обеспечения эколого-экономической безопасности на предприятии на основе решения средствами нечеткой логики в динамических условиях изменчивости внешней среды это первоочередная задача современности.

Для сохранения и экономического роста необходимо в системе экономической статистики сформировать новое пространство, способное отразить в себе как экономическое развитие, так и развитие окружающей среды.

Эколого-математическая модель (ЭБ)может быть представлена в виде схемы модели объекта и в виде функциональной временной зависимости состояния объекта:

$$O(t) = f(X, A, G, Y, O, I),$$

где G- вектор факторов состояния объекта (A) на входе, состояния управления (X), выходных факторов (G, Y) и факторов внешней среды (Q).

При этом все факторы рассматриваются как векторные временные величины. При моделировании данного объекта могут быть применены различного вида модели и процессы для исследования тех или иных его элементов с определенной целью.

Особенностью экологии являются сложности проведения проверки математических моделей, так как главным в ней являются сложно воспроизводимые процессы. Поэтому основным направлением в моделировании экспериментов экологических процессов является информационное моделирование, создание теоретически схожих имитационных моделей, построенных на аппарате математической логики.

Разработка нечетких моделей эколого-экономической безопасности промышленных предприятий позволяет получить численную оценку складывающейся эколого-экономической ситуации.

Также целесообразно использовать инструменты имитационного моделирования и аппарат нечетких множеств, например, в системе компьютерного моделирования MatLab, что позволяет разработать семейство нечетко-множественных моделей эколого-экономической безопасности для оценки, анализа и визуализации эколого-экономических показателей предприятий промышленной сферы.

Принципы моделирования экологических систем должны учитывать, что эколого-математические модели — это комбинированные модели математического характера, логических построений, схем, единая система матриц, которые имеют экологический и экономический смысл.

Подводя итог вышесказанному можно сказать, что моделирование с использованием математического аппарата является главным инструментом эколого-

экономического анализа; это направленное использование математических методов и моделей, соответствующих технических средств для их реализации, методологический подход, взгляд на экологические и эколого-экономические процессы, их внутреннее содержание, свойства, динамика в математическом моделировании эксперимента. Использование эколого-математических методов и моделей позволяет получить новые качественные выводы об экономических процессах и явлениях в их тесной взаимосвязи с экономической обстановкой.

МОДЕЛИРОВАНИЕ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В ЭКОЛОГИИ

Е.А.Борисова (ТУИТ, старший преподаватель)

Для прикладных исследований четкие модели не всегда могут быть получены или являются слишком громоздкими. Информации о таких них часто доступна лишь в виде экспертных данных. Эта информация может быть нечеткой и недостаточно полно определенной, чтобы быть представленной строгими математическими зависимостями. При этом информация о системе может быть разнородной, а оценка значений параметров - проводиться с использованием различных масштабов и шкал. Очень часто описание процессов функционирования этих систем доступно в виде нечетких правил или различного типа отношений. Неопределенность знаний о системе связана с неопределенностью или нечеткостью выделения и описания границы системы, ее состояний, и внешних входных и выходных воздействий.

Кроме того, обработка нечеткой информации, при не точных и корректно заданных параметрах и входных данных требует адекватных нечетких подходов.

Нечеткая логика является эффективным подходом к решению проблемы оценки уровня эколого-экономической безопасности.

Многие индикаторы эколого-экономической безопасности являются недоступными для точного измерения, включают компонент, невозможный оценить в количественном выражении. В терминах теории нечетких множеств этот компонент описывается как переменная лингвистического характера с множеством значений, а связь количественного значения индикатора с его качественным лингвистическим описанием задается так называемыми функциями m-принадлежности фактора нечеткому множеству.

Решение поставленной проблемы требует нечеткой характеристики набора переменных, которые участвующих в построении системы принятия решений. С использованием системы Matlab можно применять основные средства графического интерфейса пользователя, обеспечивающие доступ к инструментам нечеткой логики: редакторы системы нечеткого вывода, функции принадлежности, правил вывода, а также средства просмотра правил и поверхности вывода. Однако надо учитывать, что правила нечетких множеств и функции принадлежности должны покрывать всю предметную область, на которой они определены, при этом осуществление перехода от одной функции к другой, сохраняя соответствующие принадлежности, не должно содержать разрывов, поскольку не должна содержать разрывов и поверхность вывода.

В качестве инструментального средства, реализующего рассмотренный подход, можно использовать пакет прикладных программ FuzzyLogicToolbox среды компьютерной математики MatLab, позволяющий создавать системы нечеткого логического вывода и нечеткой классификации с возможностью их интегрирования в программу Simulink. Базовым понятием FuzzyLogicToolbox является FIS-структура, которая содержит данные для функционального отображения «входы-выходы». Структура получаемой системы нечеткого логического вывода представлена на рис.1

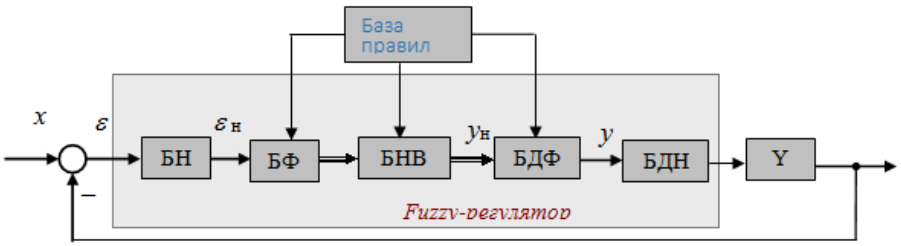


Рис. 1. Алгоритм системы нечеткого логического вывода.

На рис. 1 использованы следующие обозначения:

X - входной четкий вектор;

БН - блок нормирования. Здесь поступающий четкий сигнал вектора е умножается на масштабный коэффициент ke.н.< 1, преобразуется к интервалу, ограниченному [-1,+1];

БФ - блок фаззификации формирует значение функции принадлежности, соответствующее нормированному значению ен;

БНВ - блок нечёткого вывода, в котором на основе нечеткой информации о векторе е делается вывод о соответствующем нечётком множестве значений у, здесь реализуется инференц-процедура, в процессе которой агрегируются выводы отдельных правил. Результатом агрегирования являются «усеченные» нечёткие множества;

БДФ, БДН - блоки дефаззификации и денормирования выполняют обратные процедуры: по нескольким «усеченным» функциям принадлежности вычисляется четкое значение нормированного значнияун и соответствующее ему ненормированное значение у = ун / ку..н. (ку..н< 1);

Y - выходной четкий вектор управляемых параметров экологической безопасности.

Исходными данными для оценки, анализа и визуализации эколого-экономических показателей исследуемого объекта нужно использовать годовые объёмы размещаемых отходов производства и потребления.

В соответствии с вышеизложенным необходима разработка комплекса нечетких моделей в системе MatLabFuzzyLogicToolbox, которая позволяет получить интегральную оценку состояния экологической безопасности промышленного предприятия.

Таким образом, можно обеспечить требуемый уровень эколого-экономической безопасности на уровне промышленных предприятий. Моделирование систем обеспечения эколого-экономической безопасности позволяет получить сравнительные характеристики этих величин при малозатратных регулирующих мерах на основе оценки трансграничного загрязнения окружающей среды с помощью интеллектуальных компьютерных систем.

ИСПОЛЬЗОВАНИЕ ШИМ В AVR МИКРОКОНТРОЛЛЕРАХ

Э.М.Зармасов (ТУИТ ассистент)
М.Н.Абдалимов (ТУИТ ассистент)

ШИМ (PWM) - широтно-импульсная модуляция. Не нужно пугаться данного термина. Это всего навсего способ регулирования напряжения. Допустим подсветка монитора горит слишком ярко, вы меняете яркость. А что же происходит в этот момент на самом деле?

Представим себе, что подсветка монитора это несколько светодиодов. Питается все это дело от постоянного напряжения. Но вот нам понадобилось уменьшить яркость монитора. Логично ответить, что это можно сделать переменным резистором. На маленьких токах - возможно. Но на больших, резистор будет сильно греться. Сильно возрастут габариты, потери, энергопотребление.

Поэтому люди придумали схему на транзисторах, которая делает из постоянного напряжения пульсирующее. Оказывается, пульсирующее напряжение, в зависимости от заполнения периода будет эквивалентно постоянному напряжению. Т.е. если в течение периода напряжение 50% времени было включено, 50% выключено, то эквивалент постоянного напряжения будет равен 50% от номинального.

В цифрах это просто - было 5В постоянного напряжения прогнали через ШИМ - получили 2,5В. Если заполнение импульса равно 75%, то эквивалентное постоянное напряжение будет 3,75В. Думаю идея понятна.

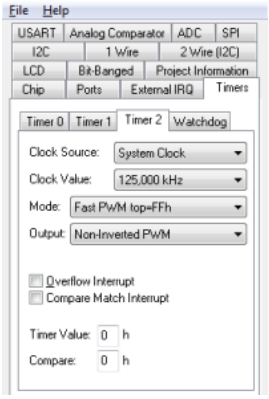
Теперь приступим к практической реализации. Будем при помощи микроконтроллера изменять заполнение от 0 до 100%, потом от 100% до нуля. Конечный результат должен выглядеть так:

Чтобы было более наглядно, подключим светодиод. В результате у нас будет плавно включаться и отключаться светодиод.

Запускаем наш любимый CodeVision. Создаем проект при помощи мастера. В разделе таймеров (Timers), выбираем Timer 2 и выставляем настройки как на рисунке.

Если попробовать сгенерировать проект, то прога может ругнуться. Соглашаемся, ведь у нас нога 3 порта В должна быть настроена как выход.

Уделим внимание строке OCR2=0x00; Эта переменная как раз и отвечает за величину заполнения импульса. Изменяется данная величина от 0 до 255(0xFF), т.е. 255 соответствует 100% -му заполнению (постоянный ток). Следовательно, если нужно 30% заполнение (255/100)*30=77. Далее 77 переводим в шестнадцатеричную систему OCR2=0x4D;



TCCR2=0x6C; Изменяя данную величину мы можем регулировать частоту ШИМ. Величина частоты работы ШИМ кратна частоте, на которой работает микроконтроллер. В проекте использована частота микроконтроллера 8 МГц, частоту ШИМ использовали 125кГц, следовательно делитель равен 8/125=640x6C в двоичной системе счисления 1101100, открываем даташит на Atmega8 и видим описание регистра TCCR2, так вот 1101100 последние цифры 100 и отвечают за выбор частоты работы ШИМ.

ХАРАКТЕРИСТИКА И МЕХАНИЗМЫ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ МУЛЬТИВЕЩАНИЯ В СЕТЯХ LTE

Х.Б.Мирзоқулов (Самаркандский филиал ТУИТ, ассистент)
Ж.Х.Нурмуродов (ТУИТ, магистрант)

В сетях сотовой подвижной связи третьего и четвертого поколений UMTS и LTE увеличение спроса на высокоскоростные услуги, такие как мобильное вещательное телевидение, видеоконференции, привело к необходимости решения задачи эффективного использования ограниченного объема частотно временных ресурсов сети. Подход к решению этой задачи был найден в проводных сетях, в которых при предоставлении аналогичных услуг применяется многоадресный режим передачи информации, или

мультивещание. В беспроводных сотовых сетях для этой цели разработана отдельная подсистема MBMS (Multimedia Broadcast Multicast Service), реализующая передачу данных в режимах мультивещания и широковещания. Особенности беспроводной среды, в том числе, мобильность абонентов между сотами, приводят к необходимости постоянного мониторинга наличия пользователей, подключенных к той или иной услуге мультивещания. За подобный мониторинг в рамках нескольких сот отвечает отдельный функциональный элемент архитектуры MBMS — контроллер, — отслеживающий через небольшие по продолжительности такты времени (20 мс) наличие хотя бы одного пользователя, подключенного к каждой из поддерживаемых услуг мультивещания. Контроллер устроен таким образом, что за один такт времени получает информацию не об одной услуге, например, одном телевизионном канале, а сразу о нескольких услугах, т.е. обрабатывает информацию "группами". Именно этот принцип и позволил авторам статьи описать процесс предоставления услуг мультивещания, а если говорить точнее, соответствующий процесс мониторинга, в виде системы с групповым обслуживанием заявок. Проведен анализ ключевой характеристики системы — средней задержки реагирования контроллера на изменение состояния услуги мультивещания — "включена" / "выключена", — что сказывается, в первую очередь, на задержке подключения пользователей к услугам.

К подсистеме MBMS выдвигается ряд требований, одним из которых является процесс постоянного мониторинга наличия пользователей, подключенных к той или иной услуге мультивещания. Выполнение этого требования необходимо для того, чтобы избежать занятия частотновременных ресурсов соты, в которой нет ни одного пользователя, заинтересованного в получении данной услуги мультивещания. Первоначально это требование предполагалось выполнять путем подсчета пользователей, заинтересованных в ее получении. Однако данная процедура требует большого количества ресурсов для передачи сигнальной информации между пользователями и сетевым контроллером (в качестве которого выступает, например, базовая станция). Очевидным решением, снижающим нагрузку на сеть радиодоступа, является:

1) переход от подсчета точного количества пользователей к определению наличия в соте хотя бы одного пользователя, аинтересованного в получении услуги мультивещаиия;

2) перемещение сигнального трафика с верхних уровней стека протоколов на нижние, в том числе первый физический уровень (L1).

Рассмотрим архитектуру подсистемы MBMS, которая является дополнительным компонентом, встроенным в базовую архитектуру сети LTE. На рис. 1 ключевые элементы базовой архитектуры отмечены белым цветом, а элементы подсистемы MBMS- серым цветом. Компоненты подсистемы MBMS входят как в сеть радиодоступа (EvolvedUniversalTerrestrialRadioAccessNetwork, E-UTRAN), так и в базовую сеть (EvolvedPacketCore, EPC). На рисунке также отмечены интерфейсы между элементами архитектуры — как для передачи медиа-трафика (сплошные линии), так и для сигнального трафика (пунктирные линии).

Главным элементом в архитектуре сети сотовой связи для оказания услуги MBMS является центр вещательных услуг BM-SC (BroadcastMulticastServiceCenter). Центр BM-SC осуществляет функции обработки запросов пользователей, инициации, управления и прекращения соединения, тарификации, а также может выступать в роли входной точки для третьей стороны (контент-провайдера), желаю щей предоставлять свои услуги через подсистему MBMS вещания оператора.

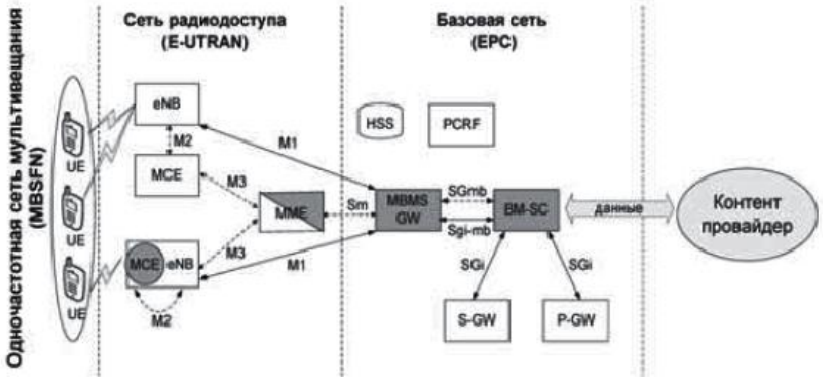


Рис. 1. Архитектура сети LTE с подсистемой MBMS

Шлюз мультимедийного вещания MBMSGW (MBMSGateway) контролирует входящий широковещательный/многоадресный трафик. Его роль заключается в трансляции пакетов на все базовые станции в пределах зоны обслуживания, а также в управлении MBMS сессиями (например, начало сессии и окончание сессии).

Интерфейс между пользователем и сетевым контроллером к настоящему времени не до конца стандартизован, именно поэтому существует множество решений по организации их взаимодействия. Одним из решений является процесс мониторинга сетевым контроллером наличия пользователей, подключенных к той или иной услуге мультивещания.

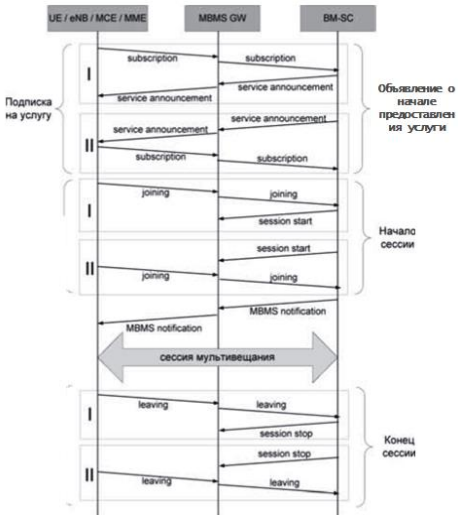


Рис. 2. Диаграмма установления и завершения сессии мультивещания

В сетях LTEвыделение частотно-временных ресурсов для услуги мультивещания происходит после того, как пользователь подписывается на эту услугу, при этом он может не сразу ее подключить. Таких пользователей будем называть заинтересованными. Освобождение частотно-временных ресурсов происходит тогда, когда в соте нет ни одного заинтересованного пользователя. Поэтому необходимо отслеживать, существует ли в соте хотя бы один пользователь, заинтересованный в получении услуги мультивещания.

ТАРМОҚ ФАОЛИЯТИНИ МОНИТОРИНГ ҚИЛИШ ТИЗИМЛАРИ

У. Назаров (ТАТУ, магистрант)

Тармоқ қурилмалари актив ва пассив қисмларга бўлинади. Биз биринчи навбатда актив қурилмаларни кузатиб туришимиз керак бўлади. Буларга хаб, свитч, маршрутизатор кабилар киради. Албатта пассив қисмсиз бунга эришиб бўлмайди.Тармоқ қурилмаларини доимий кузатиб туриш орқали биз тармоқнинг тури қандай бўлишидан қатьий назар уни

узлуксиз ишлашини таъминлаймиз. Тармоқда содир бўладиган хар қандай ўзгариш унинг ишлашига таъсир кўрсатади. Айниқса актив қурилмларнинг ичида содир бўладиган кичик бир хато бутун бошли тизимни ишдан чиқишига олиб келиши мумкин. Хар бир қурилма ўзининг холати хақидаги хабарни ўзида ёки бўлмаса ташқи қурилмаларда сақлай олади. Уларни биз логлар деб атаймиз.Логларни кўриш, қайта ишлаш ва ўқиш учун бир қанча дастурлардан фойдаланиш мумкин. Буларга Zabbix, Cacti, Syslog, Kiwi Syslog кабиларни мисол қилиб келтириш мумкин. Сиз ахамиятсиз қолдирган ихтиёрий бир хабарда мухим маълумот бўлиши мумкин. Шунинг учун, ўзини хурмат қиладиган хар бир тармоқ администраторига маслахат: қурилмаларни доимий кузатиб боринг.Тармок курулмаларини ишлашини куриб турмокчи булсангиз IP адресига ping бериб куринг. Агар ping утмаса tracert билан кайси IP адресга бориб колишини куриш мумкин. Дастурга келадиган булсак Fpinger хам тармок мониторинг дастури.

«Мониторинг» АТ да ишлаётган компютерларга ахборот хавфсизлигини таъминлашга қўйиладиган талаблар:

1. Компютерларгарухсатсиз кириш имконияти бўлмайдиган хоналарда жойлашиши ва уларга ваколатсиз шахсларнинг кириши тақиқланган ҳолда эксплуатация режими таъминланган бўлиши керак.
2. Компютерларни ёқиқ бўлган ва дастурий таъминот ишлаб турган пайтда назоратсиз қолдириш таъқиқланади. Қисқа муддатли танаффус пайтида экранни ўчириш тавсия этилади, экранни активлаштириш паролни қўллаш билан бўлиши лозим.
3. Компютерларда фақатгина битта операцион тизим ва «Мониторинг» АТ ишлашида керакли бўладиган дастурлар ўрнатилган бўлиши керак.
4. Компютерлар махсус дастурлар ёки антивирус ҳимоя аппарат воситалари (тармоқли ёки шахсий) ва тармоқ ҳимояси (шахсий firewall) ёрдамида ҳимояланган бўлиши керак.
5. Мунтазам равишда антивирус базаларини ва компютерда ўрнатилган операцион тизим, дастурий таъминотнинг хавфсизлигини янгилаб туриш керак (шу жумладан,антивирус тизимлари, фаервол, офис дастур иловалари ва б.).

Хулоса қилб айтганда тармоқ фаолиятини назорАт қилиш тармоқда ишлаш сифатини оширишга хизмат қилади.

ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ С ПРИОРИТЕТНЫМ ОБСЛУЖИВАНИЕМ

С.С. Парсиев (ТАТУ, доцент)

Анализ моделей с приоритетным обслуживанием относится к задачам, которые можно считать одним из самых сложных в теории телетрафика. В работе приводится математические модели приоритетного обслуживания разнородных потоков информации связанных с изучением системы массового обслуживания (СМО), в которых применяются дисциплины приоритетного обслуживания потоков информации и будут приведены основные результаты исследования однолинейных СМО с относительными приоритетами.

Для СМО данного вида вводятся два допущения, во – первых, что потоки заявок любого приоритета можно считать пуассоновскими. Во-вторых, количество мест для ожидания не ограничено.

При приоритетном обслуживании каждому поступающему сообщению (пакету) ставится в соответствии некоторое число – его приоритет, определяющий очередность выбора пакетов на обслуживание, так что пакеты с одинаковым приоритетом обслуживаются в порядке поступления, а пакеты с более высоким приоритетом – раньше, чем пакеты с более низким. Указанные типы систем массового обслуживания (СМО) именуются соответственно как системы с абсолютными и относительными приоритетами.

Основным методом расчета качественных характеристик телекоммуникационной сети, в нашем случае является, модель СМО $\vec{M}_k \frac{\vec{G}_k}{\vec{1}} /_{\infty}$ с относительным приоритетами на случай **P** приоритетов с ненадежным обслуживающим прибором.

Пусть пакеты с **P** приоритетами поступают в однолинейную СМО и образуют пуассоновские потоки с интенсивностью λ_k, $k = \overline{1,P}$.

Суммарный поток является пуассоновским с интенсивностью $\sigma = \sum_{k=1}^{p} \lambda_k$.

В такой СМО протекает два основных независимых процесса:

- процесс ожидания, характеризуемый случайным временем t_{wk} с функцией распределения (ФР) $W_k(t)$;

- процесс обслуживания, характеризуемый случайным временем t_{hk} с ФР $H_k(t)$.

Учитывая вышеприведенных случайное время доставки пакета с к –м приоритетом представляется ФР времени пребывания пакета в системе

$$V_k(t) = W_k(t) * H_k(t) \quad , \qquad (2)$$

где * - стилтьевсовская свертка.Из выражения (2) получается среднее время пребывания пакета к-го приоритета в звене передачи данных

$$T_k = \int_0^{\infty} t \cdot dV_k(t) \qquad (3)$$

Для нахождения времени обслуживания t_{hk} пакетов к-го приоритета в звене передачи воспользуемся преобразованием Лапласа- Стильтьеса (ПЛС) с ФР $H_k(t)$ времени обслуживания пакетов к –го приоритета в момент времени t .

Согласно (2)

$$Q_k(\nu) = \int_0^{\infty} e^{-\nu t}\, dV_k(t) = \omega_k(\nu) \cdot h_k(\nu) \qquad (4)$$

где ν – интенсивность старения информации $\nu = \frac{1}{T_z}$, где $\mathbf{T_z}$ – среднее время старения;

$\omega_k(\nu)$ – ПЛС от ФР $W_k(t)$ времени ожидания начала обслуживания пакетов к-го приоритета в момент времени t;

$h_k(\nu)$ – ПЛС от ФР $\mathbf{H_k(t)}$ времени обслуживания пакетов к-го приоритета в момент времени t.

Формализуя процесс передачи в звене сети NGNc помощью СМО типа с относительным приоритетам получим выражение ПЛС от ФР времени ожидания начала обслуживания к-го приоритета:

$$/\ \nu - \lambda_{\downarrow} k\ B_{\downarrow} k\ (\nu + \sigma_{\downarrow}(k-1)\ (1 - h_{\downarrow}(k-1)\ (\nu)\ ) \ , \qquad (5)$$

где :

$$h_0(\nu) = \sigma_0 = 0; \sigma = \sum_{i=1}^{p} \lambda_i; \sigma_{k-1} = \sum_{i=1}^{k-1} \lambda_i;$$

В частности, если время исправной работы и время восстановления являются экспоненциально распределенным случайными величинами с параметрами **c** и **d,** то

$$e(\sigma) = \int_0^{\infty} e^{-\sigma t}\, dE(t) = \int_0^{\infty} e^{-\sigma t}\, d(1 - e^{-ct}) = \frac{c}{\sigma + c};$$

$$\varphi(\nu) = \int_0^{\infty} e^{-\nu t}\, dD(t) = \int_0^{\infty} e^{-\nu t}\, d(1 - e^{-dt}) = \frac{d}{\nu + d};$$

$$\varphi_1 = \int_0^\infty t\, dD(t) = d\int_0^\infty t\, e^{-dt} dt = \frac{1}{d};$$

где: $\nu -$ интенсивность старения пакета;

$\mathbf{d} -$ интенсивность восстановления канала;

$\mathbf{c} -$ среднее время исправной работы обслуживающего прибора;

$$\mathbf{h_{k-1}(\nu) = \frac{1}{\sigma_{k-1} + c}\left\{\sum_{i=1}^{k-1} \lambda_i B_i\left(\nu + (\sigma_{k-1} + c)\cdot(1 - h_{k-1}(\nu))\right) + c\varphi(\nu)\right\}}, \quad (6)$$

$B_i(\nu)$ – ПЛС ФР времени обслуживания для i - го приоритета

$$B_i(\nu) = \int_0^\infty e^{-\nu t}\, dB_i(t) \quad (7)$$

$$B_i(t) = \begin{cases} 0, & t < t_i \\ I, & t < t_i \end{cases} \quad (8)$$

Где $L_i, H_i -$ объем информационной и служебной части пакетов i - го приоритета соответственно; $C_M -$ скорость модуляции в цифровом канале связи.

Полученные модели позволяют учитывать широкий набор факторов:

- многомерный входящий поток пакетов;
- комбинированную приоритетную процедуру обслуживания пакетов речевой информации, данных и других потоков информации;
- надежностные характеристики сети;
- времени ожидания начала обслуживания в очереди, с учетом отказов звена передачи данных;
- времени обслуживания пакета;

Таким образом, на базе известных ФР времени передачи и ожидания с помощью ПЛС получены математические модели с относительным приоритетным обслуживанием разнородного трафика в звене передачи телекоммуникационной сети, учитывающие специфику передаваемых потоков информации.

АНАЛИЗ ПАРАМЕТРОВ СТРУКТУРЫ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

С.С. Парсиев (ТАТУ, доцент)

Структура телекоммуникационных сетей определяет значительную часть важнейших характеристик инфокоммуникационной системы. По этой причине задачи анализа и оптимизации структуры телекоммуникационной сети образуют самостоятельное направление среди прикладных исследований, проводимых в интересах всех участников инфокоммуникационного рынка. Безусловно, анализ и оптимизация структуры сети нельзя полностью отделить от других процессов создания и развития инфокоммуникационной системы. Тем не менее, для изучения сложного объекта или процесса необходимо выделить в нем ряд самостоятельных задач.

Задачи анализа и оптимизации структуры сети объединяются общностью конечных целей, методологическим подходом и математическим аппаратом. Конечная цель этих задач – построение оптимальнойинфокоммуникационной системы, которая обеспечивает выполнение установленных функций и способна развиваться. Методологический подход к анализу и оптимизации структуры сети можно считать общим в силу универсальности и неразрывности возникающих задач.

Задачи анализа структуры, как правило, решаются для эксплуатируемой сети. Цель анализа обычно состоит в выявлении "узких мест", свойственных сети, в разработке предложений, направленных на ее развитие (качественное и количественное), в оценке стоимости сети. В каждом из этих трех случаев используется разный подход. Тем не менее, математический аппарат анализа структуры сети остается неизменным.

При анализе структуры сети обычно решаются две задачи.

Первая задача состоит в том, чтобы определить соответствие структуры сети требованиям, поставленным перед инфокоммуникационной системой в целом.

Вторая задача связана с возможностью адаптации структуры сети к новым требованиям. Телекоммуникационная сеть связи общего пользования всегда имеет иерархическую структуру. Выбор уровней иерархии обычно осуществлялся с учетом административного деления страны.

Для оптимизации структуры телекоммуникационных сетей, эксплуатируемых в настоящее время, были разработаны соответствующие математические методы. Они базировались на классических методах теории графов, оптимизации, управления запасами, принятия решений. Большинство принятых ранее решений нельзя изменить. Поэтому представляется целесообразным рассматривать задачи оптимизации перспективных телекоммуникационных сетей как возможность минимизировать имеющиеся недостатки. Сложившееся положение в значительной мере обусловлено объективными причинами.

В проблеме создания и развития телекоммуникационных сетей важное место занимают вопросы оптимизации технико-экономических показателей. Правильное решение этих вопросов позволяет проектировать и развивать телекоммуникационные сети, достигать минимальных сетевых затрат и заданного технического эффекта. К настоящему времени задачи структурной оптимизации телекоммуникационных систем рассматривались только в узком направлении, применительно к какой-либо структуре телекоммуникационной системы, например, только к беспроводным телекоммуникационным системам или системам на основе пассивных оптических технологий.

Практика проектирования и планирования телекоммуникационных сетей остро нуждается в эффективных методах оптимизации структуры сети, не ограниченных ее масштабами, легко адаптируемых для различных проектных и управленческих ситуаций, учитывающих устойчивую тенденцию развития сетей связи на интеграцию. В современных условиях возникает необходимость в разработке единого комплекса методов организации телекоммуникационных систем, ориентированного на сокращение расходов и повышение качества работы сервисов. Для сокращения расходов необходимо решать задачу структурной оптимизации на этапе проектирования, относящуюся к классу задач дискретной оптимизации и, как следствие, имеющую комбинаторный характер.

Важнейшей частью задачи оптимизации структуры сетей связи является задание целевой функции и выбор критериев.Целевая функция должна существенно зависеть от внешних параметров или части этих параметров; в противном случае оптимизация по данной целевой функции не имеет смысла. Для целей оптимизации сложных систем наиболее часто используется целевая функция, рассматриваемая как сумма параметров одной размерности или сумма монотонно возрастающих функций этих параметров.

Решение задачи оптимизации структуры, использующей в качестве целевой-функции технико-экономической критерии и, в частности, приведенные затраты, позволяет выбрать для реализации сетей вариант ее структуры, имеющий наилучшие технико-экономические характеристики при сохранении эксплуатационных характеристик на уровне заданных требований.

Развитие телекоммуникационных сетей связи говорит о том, что в качестве критериев целесообразно выбрать экономические критерии. При этом можно рассматривать в качестве критериев капитальные затраты, приведенные затраты и срок окупаемости. В качестве критерия предлагается выбрать минимизацию целевой функции, равной сумме капитальных затрат и произведения эксплуатационных расходов на нормативный срок окупаемости, т.е. общесетевые приведенные затраты на создание и эксплуатацию сетей.

Решение задачи оптимизации структуры телекоммуникационных сетей ищется в классе иерархических, однородных по уровням структур, для которых: межуровневые подсети имеют радиальную структуру; подключение оконечных пунктов (ОП) и концентраторов (КЦ) производится также по радиальному принципу; внутри уровневые подсети однотипны как по структуре, так и по техническому оснащению и описываются одной из базовых топологий.

Таким образом, задача оптимизации структуры телекоммуникационных сетей сводится к поиску компонентов вектора X, доставляющего минимум функции общесетевых приведенных затрат и включающего в свой состав:

$$X = [R, W_r, W_{r-1,r}, n_{ir}, m_{jr}, m_{jr-1,r}], \qquad (1)$$

где R – число ступеней иерархии, топологию W_r , $r = \overline{1,R}$, подсетей r-ой ступени иерархии, топологию W_{r-1}, $r = \overline{2,R}$, межуровневых подсетей n_{ir}- число узлов коммутации (концентратов и центров КП и КК) i-го типа по r-ой ступени иерархии, m_{jr}- число каналов связи (КС) j-го типа по r-ной ступени иерархии, $m_{jr-1,r}$- число каналов связи (КС) j-го типа в межуровевой подсети с индексом (r-1,r).

Задача оптимизации структуры телекоммуникационных сетей имеет следующий вид: минимизировать общесетевые приведенные затраты

При выполнении норм по качеству обслуживания пользователей сети, т.е. нормы на среднее время T_k доставки пакета данных к-го приоритета и вероятность P_k **{T≤ t }** доставки пакета речи за случайное время **T,** не должна превышать заданного **t.**

Для иерархической телекоммуникационных сетей общесетевые приведенные затраты П(X) имеет вид:

где: R-число ступеней иерархии;

-нормативный коэффициент экономической эффективности капитальных затрат.

I - число типов концентратов () и центров коммутации пакетов (каналов), различающихся функцией стоимости

где , - производительности центров КП и КК соответственно коэффициентом готовности (), интенсивностью восстановления (d_i^Y) $i = \overline{1,I}$;

J-число типов каналов связи (КС) различающихся функцией стоимости $C_j^K\{V_j, L_j\}$,(где V_j - скорость в КС, L_j - длина КС);

N_{ir} - число узлов коммутации I-го типа на r-ной ступени иерархии;

M_{jr} - число КСj –го типа между (r-1)–й и r– й ступенью иерархии;

Применение вышеприведенной модели позволяет определить топологию телекоммуникационной сети, осуществить распределение потоков, выбрать пропускную способность КС и производительности узлов коммутации, рассчитать общесетевые приведенные затраты и определить оптимальную структуру сети.

ПРИМЕНЕНИЯ ПЛОСКОЙ ИЗМЕРИТЕЛЬНОЙ ОБМОТКИ ЭЛЕКТРОМАГНИТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ ТОКА

И.Х. Сиддиков (Профессор, д.т.н., ТУИТ)
С.М. Абдуллаева (Старший преподаватель, ТУИТ)

Классические однофазные трансформаторы тока имеют сложную преобразовательную часть, большие весогабаритные показатели, трудоемки при проектировании и эксплуатации в системах управления, не обеспечивают унифицированность выходной величины при совместной работе с современной техникой

обработки информации. Они не учитывают взаимовлияния магнитных потоков и полей, созданных токами трехфазной электрической сети энергосистем.

Востребованность исследований обоснована тем, что классические однофазные первичные измерительные преобразователи тока и напряжения не позволяют обеспечения устройств контроля и управления достоверной и одновременной информацией о величинах и параметрах электрической энергии трехфазной электрической сети. Указанные обстоятельства обусловливают необходимость разработки и внедрения надежных, унифицированных, точных электромагнитных преобразователей тока в напряжение, учитывающих несимметрию токов трехфазной электрической сети, отличающихся друг от друга и по величине, и по фазе, чем объясняется востребованнность данного исследования.

Исследуемые электромагнитные преобразователи тока в напряжение с плоскими измерительными обмотками (ЭМПТН с ПИО) в общем случае представляет собой электромагнитное устройство, предназначенное для преобразования тока электрической сети ЭС в переменное выходное напряжение той же частоты. Принцип действия таких устройств основан на преобразование входного тока через магнитную систему в выходное напряжение на ПИО.

Очевидно, что значение и направление магнитной индукции $\vec{B}$ движущегося заряда будет зависеть от величины самого заряда, его скорости и удаленности до точки измерения индукции. Если вместо заряда взять элементарный проводник – элемент тока – $Id\vec{l}$, можно рассчитать для него вектор магнитной индукции для любой точки пространства, в котором находится ПИО.

ЗаконБио-Савара-Лапласа позволяет определить вектор индукции магнитного поля, созданного элементом тока:

$$d\vec{B} = \frac{\mu\mu_0}{4\pi}\frac{\left[d\vec{l}\,\vec{r}\right]I}{r^3}, \qquad (1)$$

Где $Id\vec{l}$ – элемент тока; I – сила тока в проводнике; $d\vec{l}$ – вектор, равный по модулю длине dl проводника и совпадающий по направлению с направлением тока; μ – магнитная проницаемость среды); $\mu_0 = 4\pi \cdot 10^{-7}$ Гн/м – магнитная постоянная воздуха; $\vec{r}$ – радиус-вектор, проведенный от середины элемента проводника к точке, в которой определяется магнитная индукция.

Направления вектора $d\vec{B}$ – силовые линии магнитного поля – определяются правилом векторного произведения и представляют собой концентрические окружности, центр которых лежит на прямой, проходящей через элемент $d\vec{l}$. Векторы $d\vec{l}$, $\vec{r}$, $d\vec{B}$ образуют правовинтовую систему (рис.1). Величина вектора магнитной индукции $d\vec{B}$ в магнитной системе выражается следующим образом:

$$\left|d\vec{B}\right| = \frac{\mu\mu_0}{4\pi}\cdot\frac{I\sin\alpha}{r^2}dl, \qquad (2)$$

где: α – угол между векторами $d\vec{l}$ и $\vec{r}$.

Для более подробного понимания процесса преобразования рассмотрим круговой проводник – первичную обмотку с током.

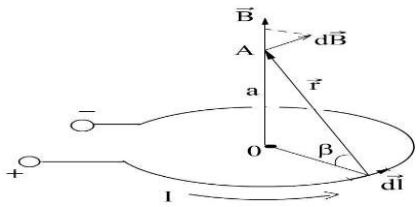


Рис. 1. Векторы $d\vec{l}$, $\vec{r}$, $d\vec{B}$ магнитного поля

Определим величину и направление вектора магнитной индукции $\vec{B}$ в какой-либо точке, лежащей на перпендикуляре, проведенном через центр этого витка (рис. 2).

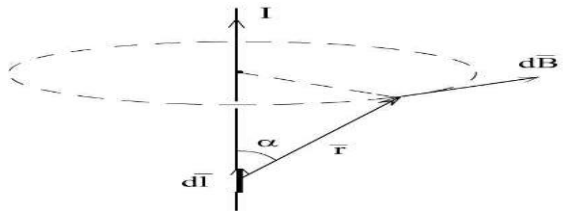


Рис. 2. Направление в магнитной системе вектора магнитной индукции $\vec{B}$

Выделим на проводнике с током радиуса R элемент $d\vec{l}$. От этого элемента проведем радиус - вектор $\vec{r}$, лежащую на оси симметрии. Направление вектора $d\vec{B}$ определяется векторным произведением (3).

Результирующее поле будет направлено вдоль оси симметрии, а его величину вычислим интегрированием

$$B = \int_L dB\cos\beta = \frac{\mu\mu_0}{4\pi} I\cos\beta \frac{\sin\alpha}{r^2} \int_0^{2\pi R} dl \quad , \qquad (3)$$

где: α – угол между вектором $\vec{r}$ и вектором $d\vec{l}$ (α= 90^0);β – угол между вектором $\vec{r}$ и радиусом проводника R, проведенном к элементу $d\vec{l}$; $2\pi R$ – длина проводника.

Проведя интегрирование, получим

$$B\mu = \frac{\mu\mu_0}{4\pi} I\cos\beta \frac{2\pi R}{r^2} = \frac{\mu\mu_0}{2} \frac{IR^2}{\left(a^2+R^2\right)^{3/2}} \quad , \qquad (4)$$

где: а – расстояние от центра кольца до точки А, I – сила тока в ПИО.

ПИО находится в воздухе, поэтому магнитную проницаемость среды μ_0 , входящую в формулу (4), можно приближенно считать равной 1.

Для ПИО, имеющей n близко расположенных витков, величина магнитной индукции на оси кругового проводника

$$B_0 = nB_\mu . \qquad (5)$$

Выходное напряжение $U_{\text{эвых}}$, пропорциональное к э.д.с. $E_э$, соответствующее индукционному току, определяется законом Фарадея:

$$U_{\text{эвых}} = -\frac{d\Phi}{dt} = -\frac{d}{dt}\left(\vec{B}S\right) = -\frac{dB}{dt} S\cos\varphi \quad , \qquad (6)$$

где S – площадь витка ПИО;φ – угол между положительной нормалью к ПИО и вектором магнитной индукции.

Исследованием установлено, что значение и направление магнитной индукции $\vec{B}$ движущегося заряда будет зависеть от величины самого заряда, его скорости и удаленности до точки измерения индукции. Если вместо заряда взять элементарный проводник – элемент тока – $Id\vec{l}$, можно рассчитать для него вектор магнитной индукции для любой точки пространства, в котором находится ПИО.

Исследованием установлено, что наиболее эффективное для применения в электромагнитных преобразователях тока в напряжение являются плоские измерительные обмотки в виде треугольной, петлевой, круглой и их дифференциальные

выполнения и расположенные в регулируемом воздушном зазоре магнитопровода, что обеспечивает получение унифицированного выходного сигнала при параметрах: напряжение - 20 В, ток 100 мА для совместной работы с микропроцессорной системой управления.

ПРЕОБРАЗОВАНИЕ СИГНАЛА О НЕСИММЕТРИИ ТОКОВ НА ОСНОВЕ ЭЛЕКТРОМАГНИТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ

И.Х.Сиддиков (Профессор, д.т.н., ТУИТ)
С.М.Абдуллаева (Старший преподаватель, ТУИТ)

Электрическая энергия характеризуется тремя основными показателями: напряжением, частотой и формой кривой электрического тока. Напряжениев энергосистеме (ЭС) является показателем баланса реактивной мощности. Если в ЭС существует нехватка реактивной мощности, то напряжение у потребителей становится ниже номинального. При избытке реактивной мощности напряжение у электроприемников превышает номинальное значение.

Напряжения, выделяемые ЭМПТН сигнала о несимметрии трехфазного тока, используются для выполнения необходимых операции: приведение в действие электроавтоматики управления и контроля величнами и параметрами ЭС. ЭМПТН сигнала о первичных токов во вторичное напряжение выполняется с тремя или четырьмя входными первичными обмотками – токопроводами в зависимости от того, имеет ли трехфазная электрическая сеть, к которой приключается нулевой провод, а также в зависисмости от конструктивных особенностей и типа самого ЭМПТН. Число выходных узлов ЭМПТН сигнала о токов может быть равно двум в случае контроля однофазной электрической нагрузки, трем – в случае трехфазной нагрузки, трем и четырем – в случае двух однофазных электрических нагрузок электрической сети ЭС и т.д.. Суть преобразования сигнала о несимметрии трехфазного тока электрической сети ЭС заключается в том, что к входным узлам ЭМПТН, включенного в четырехпроводную или трехпроводную электрическую цепь подходят фазные токи $I_{эвхA}$, $I_{эвхB}$, $I_{эвхC}$ или разность фазных токов $I_{эвх\ AB}$, $I_{эвхBC}$, $I_{эвхCA}$, а трехфазная электрическая сеть ЭС, являющая первичной обмоткой ЭМПТН т.е. токи $I_{эвхA}$, $I_{эвхB}$, $I_{эвхC}$ или разностью фазных токов $I_{эвх\ AB}$, $I_{эвхBC}$, $I_{эвхCA}$ (табл.1), и являются источниками магнитных потоков $Ф_1$, $Ф_2$ и $Ф_3$.

Разработанная авторами данной работы ЭМПТН сигнала о симметрии токов трехфазной сети ЭС (табл.1.) работает следующим образом.

При протекании токов $I_{эвхA}$, $I_{эвхB}$, $I_{эвхC}$ в фазах трехфазной электрической сети ЭС, в магнитопроводе с общим основанием появляются магнитные потоки $Ф_1$, $Ф_2$ и $Ф_3$, которые в зазоре между торцом четырех стержней и дополнительным сердечником пересекают витки – плоской измерительной обмотки (ПИО), при этом:

$$Ф_1 = (I_{эвхA}W_{п1}) / R_{м1\Sigma} , \quad (1)$$

$$Ф_2 = (I_{эвхB}\, W_{п2}) / R_{м2\Sigma} ; \quad (2)$$

$$Ф_3 = (I_{эвзC}W_{п3}) / R_{м3\Sigma}, \quad (3)$$

где: $I_{эвхA}$, $I_{эвхB}$, $I_{эвхC}$ - первичные фазные токи, протекающие по токопроводам трехфазной электрической сети ЭС,

$W_{п1}$, $W_{п2}$, $W_{п3}$ – числа витков первичной обмотки возбуждения (в данной конструкции $W_{п1} = W_{п2} = W_{п3} = 1$ -каждая первичная обмотка в виде одного витка токопровода, одна первичная обмотка располагается в выемке между стержнями магнитопровода),

$R_{м1\Sigma} = R_{м2\Sigma} = R_{м3\Sigma}$ – соответственно суммарные магнитные сопротивления стержней магнитопровода с стрежнями трехлучевой звездообразной формы, воздушного зазора и дополнительного сердечника на пути магнитных потоков $Ф_1$, $Ф_2$ и $Ф_3$, причем: $R_{м1\Sigma} = R_{м\,м} + R_{м\,серд} + R_{м\,возд}$, $R_{м\,м} = l_{м\,м} / (м\,F)$, $R_{м\,серд} = l_{м\,серд} / (м\,F)$, $R_{м\,возд} = (2\,\delta)/(м_0\,F)$,

где: $R_{м\ м}$ - магнитное сопротивление одного стержня магнитопровода;$R_{м\ серд}$ - магнитное сопротивления участков дополнительного сердечника;$l_{м\ \ м}$ – активная длина стержней магнитопровода и по которой протекает магнитный поток Ф;$R_{м\ серд}$ = $l_{м\ серд}$ / (м F) - магнитное сопротивление участков дополнительного сердечника;$l_{м\ серд}$ – активная длина участков дополнительного сердечника, по которой протекает магнитный поток Ф;F = Д $l_{м\ м}$ Д $l_{м\ серд}$ – сечение общего основания и параллельных стержней магнитопровода и участков дополнительного сердечника;$R_{м\ возд}$ - магнитное сопротивление воздушных зазоров между стрежнями магнитопровода, участков дополнительного сердечника и воздушного зазора между торцами участков дополнительного сердечника, причем: $R_{м\ возд}$>>$R_м$ и и $R_{м\ возд}$>>$R_{м\ серд}$;δ - длина воздушного зазора между торцами параллельных стержней магнитопровода с общим основанием и участков дополнительного сердечника.

Напряжение на выходе каждой из ПИО $U_{эвых1}$, $U_{эвых2}$, $U_{эвых3}$ и $U_{эвых4}$, определяются в зависимости от величины магнитного потока в стержнях магнитопровода с общим основанием, в воздушных зазорах, дополнительных сердечниках, числом витков плоских измерительных обмоток и частотой питающей электрической сети (рис.1):

$U_{эвых1}$ = 4.44 $fW_{ПИО1}$ $Ф_1$, (4)

$U_{эвых2}$ = 4.44 $fW_{ПИО2}$ ($Ф_1$ - $Ф_2$), (5)

$U_{эвых3}$ = 4.44 $fW_{ПИО3}$ ($Ф_2$ - $Ф_3$), (6)

$U_{эвых4}$ = 4.44 $fW_{ПИО4}$ $Ф_3$, (7)

При симметричном трехфазном токе электрической сети выходные напряжения ПИО $U_{эвых2}$ и $U_{эвых3}$ равны нулю и следовательно выходные напряжения $U_{эвыхв}$ и $U_{эвыхс}$, пропорциональные разности потоков ($Ф_1$ - $Ф_2$) и ($Ф_2$ - $Ф_3$) также равна нулю:

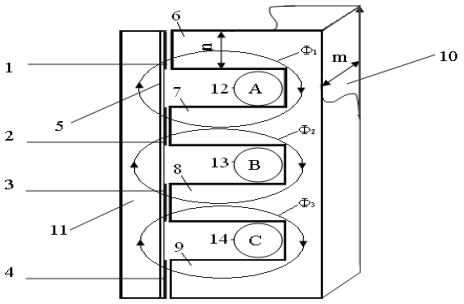
$U_{эвыхв}$ = 0; (8)

$U_{эвыхс}$ = 0. (9)

Выходное напряжение $U_{эвыха}$ определяется на основе встречного соединения ПИО 1 и 4:

$U_{эвыха}$ = $U_{эвых1}$ – $U_{эвых4}$ = 4.44 $fW_{ПИО1}$ $Ф_1$ – 4.44 $fW_{ПИО4}$ $Ф_3$ = 4.44 fWпио ($Ф_1$ – $Ф_1$), (10)

и при симметрии фазных токов $I_{эвхА}$ = $I_{эвхВ}$ = $I_{эвхС}$: напряжение $U_{эвыха}$ = 0.



1, 2, 3 и 4 – ПИО; 5 - изоляционная пластинка; 6, 7, 8 и 9 - четыре стержня; 10- общее основание; 11- сердечник; 12 (фаза А), 13 (фаза В) и 14 (фаза С) обмотки.

Рис.1. Электромагнитный преобразователь тока в напряжение с плоскими измерительными обмотками с четырехстержневым магнитопроводом

Как видно из формулы (9), напряжение $U_{эвыха}$ определяется как разность напряжения первой и четвертой ПИО, путем их встречного соединения. Такое соединение ПИО обуславливается необходимостью определения и обеспечения зависимости выходного напряжения $U_{эвых\ а}$ от магнитных потоков $Ф_1$ и $Ф_3$ крайних стержней магнитопровода.

Магнитные потоки $Ф_1$, $Ф_2$ и $Ф_3$, созданные токами фаз $I_{эвхА}$, $I_{эвхВ}$, $I_{эвхС}$ трехфазной электрической сети, в четырех торцах стержней магнитопровода с общим

основанием и дополнительным сердечником позволяют получить информацию – сигнала о несимметрии трехфазных токов электрической сети в виде выходных напряжении $U_{эвыха}$, $U_{эвыхв}$, $U_{эвыхс}$, которые появляются при неравенстве магнитных потоков $\Phi_1 \neq \Phi_2 \neq \Phi_3$ и следовательно первичных токов $I_{эвхА}$, $I_{эвхВ}$, $I_{эвхС}$ трехфазной электрической сети ЭС.

Выводы по работе:

1. Подтверждено, что трехфазная электрическая сеть ЭС является сбалансированной или симметричной, когда напряжения и токи каждой из фаз имеют одинаковую амплитуду, а сдвиг амплитуды по фазе равен 120^0. Если не выполняется хотя бы одно из этих условий и этот фактор должень быть учтен при управлении источниками электроэнергии.

2. Установлено, что значение частоты при преобразовании несиметрии трехфазного тока ЭС должно определяться требованиями к коэффициенту мощности в режиме передачи энергии по электрическим сетям ЭС.

3. Разработана конструкция электромагнитного преобразователя тока в напряжение, в которой при преобразовании несимметрии трехфазных первичных токов во вторичное напряжение магнитная система выполняется в виде параллельных стержней.

ИДЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ СЕТЕВЫМ ТРАФИКОМ С ПОМОЩЬЮ СТАТИСТИЧЕСКИХ МЕТОДОВ КЛАССИФИКАЦИИ

Х.Н. Тешабоев (ТУИТ,магистрант)
А.Т. Шокиров (ТУИТ, магистрант)

Использование в современных телекоммуникационных сетях (ТС) большего количества сетевых сервисов и приложений, аппаратного и программного обеспечения приводит к появлению в сети большого разнообразия трафиков. При этом для проведения эффективного мониторинга и управления ТС решение задачи точной идентификации и классификации трафиков относительно сетевых сервисов, приложений и протоколов является очень важной. Потому, что сетевой трафик является одним из важнейших фактических показателей работы ТС. Сетевой трафик является носителем информации о поведении пользователей и функционировании ТС. На основе статистического анализа сетевого трафика можно косвенно определить статистические характеристики поведения КС. Идентификация и классификация сетевого трафика особенно важна для решения таких задач, как определение приоритетов при формировании полосы пропускания для отдельных трафиков, установление правил по управлению сети, обеспечение безопасности сети, диагностический мониторинг ТС.

Прежде чем классифицировать сетевой трафик, очень важно определить их классификационные характеристики. Эти характеристики могут быть определены в результате анализа свойств, описывающих сетевой трафик, к которым могут относиться различные особенности общего сетевого трафика ТС. Классификацию сетевого трафика можно определить как анализ трафиков, созданных различными сетевыми приложениями. Для классификации сетевого трафика обычно применялись простые методы, основанные на анализе информации, характеризующей пакеты (номера портов, IP адреса отправителей и получателей, типы приложений и протоколов и т.д.). Наиболее часто применяемые виды классификации трафика на основе известного номера порта и исследовании полезной нагрузки сетевых пакетов имеют ряд ограничений. Для их преодоления используются статистические методы распознавания шаблонов сетевого трафика. В связи с актуальностью на сегодняшний день проблемы распознавания трафика возникла задача исследования статистических методов классификации. Классификация IP-трафика основывается на исследовании TCP и UDP номеров портов пакетов (классификация, основанная на портах), реконструкции сигнатуры протокола из его полезной нагрузки (классификация, основанная на полезной нагрузке), статистических методов анализа

характеристик обмена пакетами между хостами и статистических свойств сетевого трафика. Каждый из подходов обладает своими достоинствами и недостатками.

В некоторых случаях шифрование IP уровня может запутать TCP и UDP заголовки, что делает невозможным определение фактического номера порта. Чтобы избежать полной зависимости от номеров портов и собрать сведения об используемом протоколе, многие современные промышленные продукты используют восстановление состояния сеанса и прикладную информацию из содержимого каждого пакета.

Рассмотрим проблемы классификации трафика с точки зрения возможных методов проверки, а также перечень методов обработки, которые могут быть использованы в рамках классификации на основе полезной нагрузки.Можно выделить четыре различных степени проверки:

-Первая степень проверки основана на сигнатуре, ее цель состоит в поиске некоторых сигнатур в рамках полезной нагрузки прикладного уровня. Так, например, HTTP-пакет начинается с команды, следующей за URL и версией протокола, в то время как большинство Edonkey пакетов имеет поля, содержащие размер полезной нагрузки. Метод на основе сигнатур строится на соответствии полезной нагрузки (или ее части) с сигнатурой, определенной для данного протокола. Сигнатуры, как правило, являются регулярными выражениями;

-Второй уровень проверки – синтаксический. Он может рассматриваться как более точная версия сигнатурной проверки, поскольку направлен на проверку правильности переданных данных с синтаксической точки зрения (к примеру, предполагается, что полезная нагрузка HTTP должна содержать HTTP заголовки). В этом случае необходимо декодировать все поля, содержащиеся в сообщении, и гарантировать, что сообщение является хорошо сформированным;

-Третья степень контроля связана с протоколом соответствия. Например, она контролирует, что на HTTP GET запрос от клиента следует действительно ответ от сервера. Такая форма контроля является более точной, поскольку она может проверять в соответствии со спецификацией реальное поведение протокола;

-Четвертая степень контроля относится к семантике данных. К примеру, она способна проверить, является ли объект, передаваемый по протоколу HTTP, изображением или какой-либо другой формой содержания. Такой контроль очень полезен для обнаружения "туннелей", в которых приложение использует другой протокол для транспортировки данных. На данный момент это наиболее неформализованный метод.

Рассмотрим различные методы обработки, которые могут быть использованы в рамках классификации на основе полезной нагрузки.

Простейшим методом является PBNS, который работает, проверяя значения некоторых полей (например, TCP/UDP порты), присутствующих в каждом пакете. Этот метод очень прост с точки зрения вычислений (должны быть обработаны только заголовки пакета до L4), для него не требуется хранить состояния.

Второй метод – PBFS требует реализации таблицы сеансов, в которой каждая запись включает идентификатор сеанса (пять кортежей IP источник/назначения, транспортный протокол, порт источника/назначения), и соответствующий протокол прикладного уровня (ID протокола). Каждая таблица занимает по нескольку десятков байт.

Работа третьего метода MBFS основана на сообщениях. Для этого метода требуется модуль нормализации3 TCP/IP пакетов. Технологии на основе MBFS могут выполнить те же самые проверки, что и PBFS, но работают на сообщениях, следовательно, их средства управления могут быть расширены на все сообщение целиком взамен первого сегмента данных. В таком случае, требуемые объемы памяти увеличиваются из-за дополнительной информации о состояниях, которая должна быть сохранена для каждого сеанса (например, порядковый номер TCP) и из-за буферов, требуемых TCP/IP нормализатором. Все эти параметры сильно зависят от природы

трафика, то есть от количества фрагментированных пакетов и “ненормальных” (с пропущенными сегментами и т.д.) TCP сеансов. В зависимости от реализации, некоторые продукты могут выполнить синтаксическую проверку для всех сообщениях.

Четвертая категория MBPS точно интерпретирует, что передает и получает каждое приложение. Обработчик MBPS понимает не только семантическую часть сообщения, но и различные этапы обмена сообщениями (например, HTTP GET, должен сопровождаться соответствующим кодом ответа от веб-сервера), так как этот метод полностью понимает конечный автомат протокола. Требуемые объемы памяти становятся еще большими, потому что надо учитывать не только состояние транспортного сеанса, но также и состояние каждого сеанса прикладного уровня. Производительность является самой высокой среди всех методов – все данные прикладного уровня должны быть обработаны, чтобы проверить соответствие протокола. Реализации, основанные на технологии PBFS, обычно с каждым сеансом связывают некоторое дополнительное состояние, чтобы выполнить более точную классификацию. Например, некоторые приложения (Skype, VoIP), могут быть обнаружены, проверяя шаблон из нескольких последовательных пакетов.

Однако использование в модели классификации сетевого трафика метода обучения без учителя может создать определенные преимущества. Основным преимуществом является то, что модель позволит идентифицировать новые приложения и группировать их в новый кластер, тогда как модели, использующие методы обучения с учителем, могут идентифицировать трафики, для которых созданы обучающие примеры, и не могут обнаружить новых приложений.

При классификации сетевого трафика методы без учителя не нуждаются в начальной ручной разметке входных данных, они только основываются на подобии между классифицируемыми объектами и в качестве входных данных используются статистические характеристики потока сетевых данных. Для создания модели классификации сетевого трафика в качестве метода обучения без учителя в работах предложено использовать кластеризацию.

ПРИМЕНЕНИЕ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ В ОБРАБОТКЕ РЕЧЕВЫХ СИГНАЛОВ

У.Р. Хамдамов (доцент, ТУИТ)

Вейвлет – математическая функция, позволяющая анализировать различные частотные компоненты данных. График функции выглядит как волнообразные колебания с амплитудой, уменьшающейся до нуля вдали от начала координат. Однако это частное определение - в общем случае анализ сигналов производится в плоскости вейвлет-коэффициентов. Вейвлет-коэффициенты определяются интегральным преобразованием сигнала.

В начале развития области употреблялся термин «волночка». Английское слово «wavelet» означает в переводе «маленькая волна», или «волны, идущие друг за другом». Вейвлеты - это семейство функций, которые локальны во времени и по частоте, и в которых все функции получаются из одной посредством её сдвигов и растяжений по оси времени.

Разработка вейвлетов и идеи использования теории вейвлетов в задачах обработки сигналов были связаны с несколькими отдельными нитями рассуждений, начавшимися с работ Хаара в начале XX века. Например, Хаар опубликовал в 1910 году полную ортонормальную систему базисных функций с локальной областью определения. Эти функции называются теперь вейвлетами Хаара.

В конце XX века появился инструментальные средства по вейвлетам в системах компьютерной математики Mathcad, MATLAB и Mathematica. В настоящее время

вейвлеты широко применяются в технике обработки сигналов и изображений, в частности, для их компрессии и очистки от шума. В настоящее время исследования в области вейвлетов ведутся по многим направлениям. В частности, разработана лифтинговая схема выполнения вейвлет-преобразований, имеющая ряд преимуществ по сравнению с традиционной. Активно исследуется целочисленное вейвлет-преобразование.

Цель настоящей статьи - изложить основы теории вейвлет-преобразований и дать обзор основных способов применения вейвлет-преобразований к задаче кодирования речевых сигналов.

Вейвлеты могут быть ортогональными, полуортогональными, биортогональными. Эти функции могут быть симметричными, асимметричными и несимметричными. Некоторые функции имеют аналитическое выражение, другие - быстрый алгоритм вычисления связанного с ними вейвлет-преобразования. Вейвлеты различаются также степенью гладкости. Для практики желательно было бы иметь ортогональные симметричные или асимметричные вейвлеты. Исходя из, сферы применения существует различные виды вейвлет функций: вейвлет Хаара, вейвлеты Добеши, вейвлеты Гаусса, вейвлет Мейера, вейвлеты Морле, вейвлет Пауля, вейвлеты Койфмана, вейвлет Шеннона и сплайн-вейвлеты.

Может показаться, что вейвлеты не являются чем-то фундаментально новым. В самом деле, сходные идеи появлялись на протяжении последних десятилетий: субполосное кодирование, успешно применяемое при кодировании речи, пирамидальные схемы кодирования изображений, преобразование и функции Габора. С развитием теории вейвлетов произошло как бы объединение и взаимообогащение этих идей, что привело к качественно новому результату. Одним из основных средств обработки сигналов является линейное преобразование. Традиционно, кодеры, основанные на линейном преобразовании, делят на кодеры с преобразованием и субполосные.

Вейвлет-преобразование - интегральное преобразование, которое представляет собой свертку вейвлет-функции с сигналом. Вейвлет-преобразование переводит сигнал из временного представления в частотно-временное. Способ преобразования сигнала в форму, которая или делает некоторые величины исходного сигнала более поддающимися изучению, или позволяет сжать исходный набор данных. Вейвлетное преобразование сигналов является обобщением спектрального анализа. Вейвлет-преобразования обычно делятся на дискретное вейвлет-преобразование (ДВП) и непрерывное вейвлет-преобразование (НВП).

В численном и функциональном анализе дискретные вейвлет-преобразования относятся к вейвлет-преобразованиям, в которых вейвлеты представлены дискретными сигналами. Наиболее широко ДВП используется в кодировании сигналов, где свойства преобразования используются для уменьшения избыточности в представлении дискретных сигналов, часто - как первый этап в компрессии данных.

Непрерывное вейвлет-преобразование - это преобразование, отображающее данную вещественнозначную функцию $\mathbf{x(t)}$, определенную на временной оси переменной , в функцию двух переменных τ и s.

$$\gamma(\tau, s) = \int_{-\infty}^{+\infty} \frac{x(t)1}{\sqrt{s}} \varphi^{*}\left(\frac{t-\tau}{s}\right) dt$$

здесь τ представляет параллельный перенос, s представляет масштаб и $\varphi(t)$ - материнский вейвлет.

Для осуществления вейвлет-преобразования вейвлет-функции должны удовлетворять следующим критериям:

1. Вейвлет должен обладать конечной энергией:

$$E = \int_{-\infty}^{\infty} |\psi(t)|^2 dt < \infty$$

2. Если $\hat{\psi}(\square)$ фурье-преобразование для $\psi(\mathbf{f})$, то есть

$$\widehat{\psi}(f) = \int_{-\infty}^{\infty} \psi(t) e^{-i(2\pi f)t}\, dt$$

тогда должно выполняться следующее условие:

$$C_{\psi} = \int_{0}^{\infty} \frac{\left|\widehat{\psi}(f)\right|^2}{f} df < \infty$$

Это условие называется условием допустимости, и из него следует что вейвлет при нулевой частотной компоненте должен удовлетворять условию $\widehat{\psi}(0) = 0$ или, в другом случае, вейвлет $\psi(t)$ должен иметь среднее равное нулю.

3. Дополнительный критерий предъявляется для комплексных вейвлетов, а именно, что для них Фурье-преобразование должно быть одновременно вещественным и должно убывать для отрицательных частот.

4. Локализация: вейвлет должен быть непрерывным, интегрируемым, иметь компактный носитель и быть локализованным как во времени, так и по частоте. Если вейвлет в пространстве сужается, то его средняя частота повышается, спектр вейвлета перемещается в область более высоких частот и расширяется. Этот процесс должен быть линейным - сужение вейвлета вдвое должно повышать его среднюю частоту и ширину спектра также вдвое.

Вейвлет-преобразование широко используется для анализа сигналов. Помимо этого, оно находит большое применение в области сжатия данных. В дискретном вейвлет-преобразовании наиболее значимая информация в сигнале содержится при высоких амплитудах, а менее полезная - при низких. Сжатие данных может быть получено за счет отбрасывания низких амплитуд. Вейвлет-преобразование позволяет получить высокое соотношение сжатия в сочетании с хорошим качеством восстановленного сигнала. Вейвлет-преобразование было выбрано для стандартов сжатия изображений JPEG2000 и ICER. Однако, при малых сжатиях вейвлет-преобразование уступает по качеству в сравнении с оконным Фурье-преобразованием, которое лежит в основе стандарта JPEG.Выбор конкретного вида и типа вейвлетов во многом зависит от анализируемых сигналов и задач анализа. Для получения оптимальных алгоритмов преобразования разработаны определенные критерии, но их еще нельзя считать окончательными, так как они являются внутренними по отношению к самим алгоритмам преобразования и, как правило, не учитывают внешних критериев, связанных с сигналами и целями их преобразований. Отсюда следует, что при практическом использовании вейвлетов необходимо уделять достаточное внимание проверке их работоспособности и эффективности для поставленных целей по сравнению с известными методами обработки и анализа.Таким образом, вейвлетные базисы могут быть хорошо локализованными как по частоте, так и по времени, базисные вейвлеты могут реализоваться функциями различной гладкости и вейвлетные преобразования обладают всеми достоинствами преобразований Фурье.

РУКОВОДСТВО ПО НАСТРОЙКЕ ДИНАМИЧЕСКОГО DNS (DDNS)

У.Р. Хамдамов (ТУИТ, доцент)
С.Ш. Пулатов(ТУИТ, магистрант)

Динамический DNS это технология, позволяющая информации на DNS-сервере обновляться в реальном времени и (по желанию) в автоматическом режиме. Она применяется для назначения постоянного доменного имени компьютеру с изменяемым IP-адресом. Это может быть IP-адрес, полученный по DHCP или по IPCP в соединениях PPP, PPPoE и им подобных (например, при удалённом доступе через модем). Другие машины в Интернете могут устанавливать соединение с этой машиной по доменному имени и даже не знать, что IP-адрес изменился.

Время устаревания адреса (TTL) для динамической записи делается очень маленьким (не более двух-трёх минут), иначе другие DNS-серверы поместят её в свой кэш, а когда она изменится, их клиенты долго будут получать устаревшую информацию.

Таким образом, схематично, процесс выглядит так:

- Регистрируемся у провайдера динамического DNS, выбираем имя для своей системы и записываем его в форму на сайте.
- Конфигурируем свой компьютер так, чтобы он обновлял данные на сервере провайдера динамического DNS.
- Теперь извне к нашей машине можно обращаться по заданному доменному имени, причем неважно, какой реальный IP-адрес используется сейчас.

Для начала надо определиться, как мы будем информировать сервер об изменении IP. Если у Вас ADSL, и вы не поскупились купить модем, способный работать в качестве роутера, то почти наверняка он сам умеет обновлять соответствующие данные без всякого вмешательства со стороны компьютера.

Если же Вы подключены к Сети иным способом, придется установить на своем компьютере программу-клиент для обновления данных и настроить ее. Программы такие можно скачать с сайтов соответствующих провайдеров динамического DNS, там обычно бывают версии для разных ОС, так что задействовать такую схему под Linux или FreeBSD обычно труда не составляет.

Провайдеры динамического DNS

Таких провайдеров существует немало. Наиболее известны из них:

- no-ip
- TZO
- DynDNS
- DynDNS.DK
- FreeDNS
- ChangeIP

Каждый провайдер предоставляет свои услуги платно. Но часть услуг бесплатна. Это обычно очень маленькая часть, возможности динамического DNS много шире, но нам ее хватит. Советую внимательно ознакомиться с соответствующими сайтами, набор бесплатных услуг у всех свой, возможно, Вас заинтересуют какие-то дополнительные возможности.

Пример регистрации.

Итак, рассмотрим регистрацию доменного имени (для примера, на сервисе DynDNS).

Шаг 1. Создание аккаунта.

Сначала идем на DynDNS.com и регистрируемся (Create Account). В регистрации указываем пользовательские данные (любые, никто их все равно не проверяет) и реальный адрес e-mail (это важно! На него придет подтверждение регистрации, без этого ничего не будет работать!). По прибытии на почту письма с подтверждением, активируем учетную запись, перейдя по ссылке в письме.

Шаг 2. Создание доменного имени.

Итак, мы зарегистрировались. Теперь надо выбрать себе подходящее имя и связать его со своим аккаунтом. Бесплатно таких имен можно занять до 5 штук, этого вполне достаточно для наших задач. Кстати, никто не запрещает создать любое количество аккаунтов с разных e-mail... Авторизуемся на сайте и начинаем создавать аккаунт:

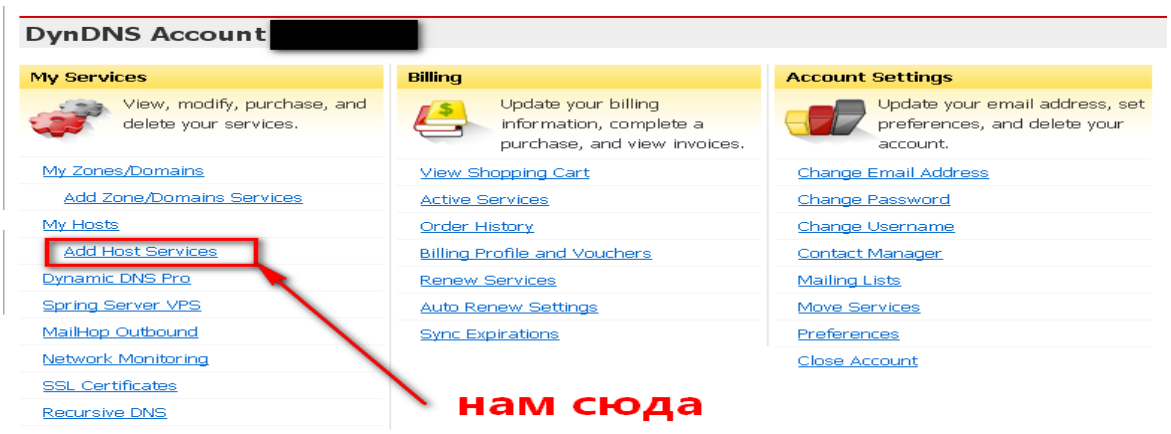


Рисунок-1. Окно DynDNSAccount

Теперь привяжем текущий адрес к имени. Ссылка "Edit TTL" позволяет определить частоту обновления записи:

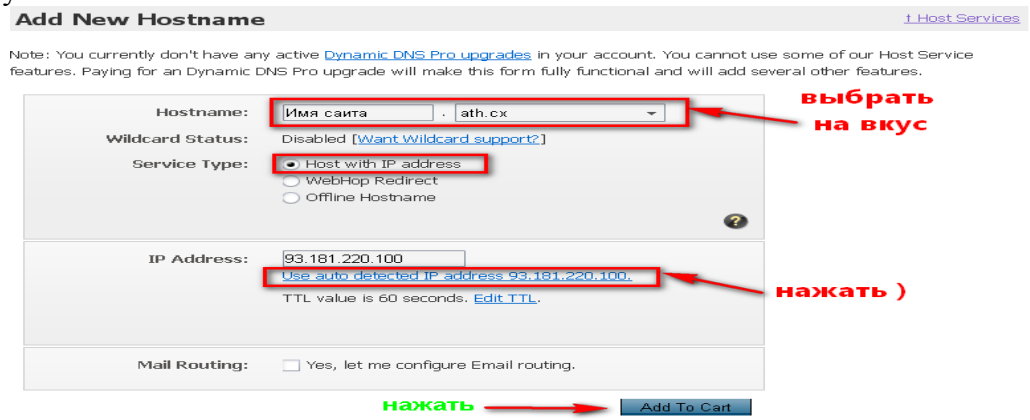


Рисунок-2. Окно AddNewHostname

Теперь необходимо подтвердить условия использования сервиса. В нашем случае бесплатные услуги:

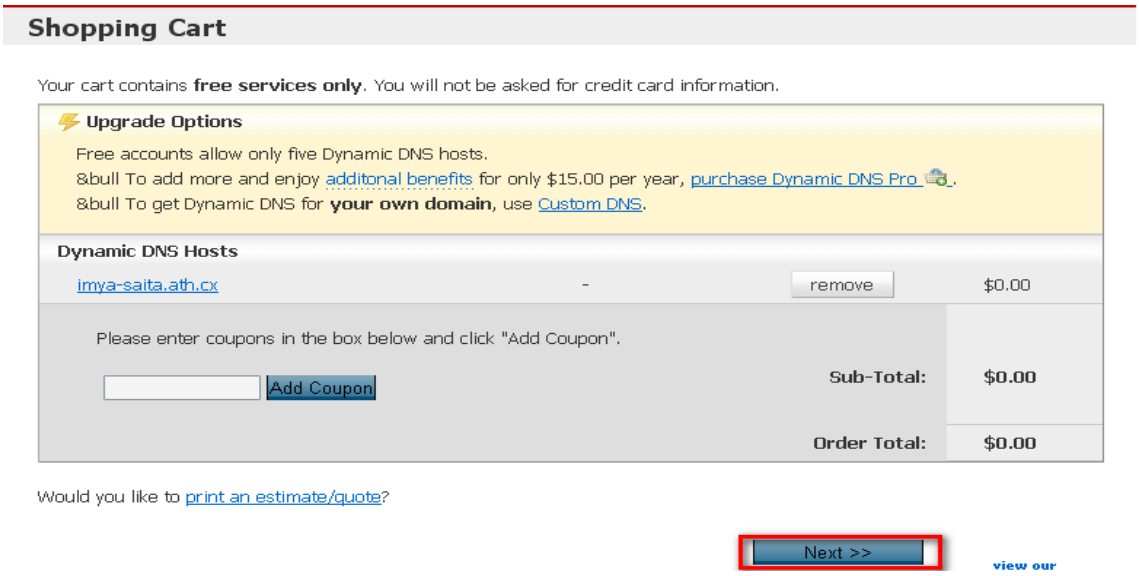


Рисунок-3. Окно ShoppingCart.

Теперь надлежит подтвердить активацию доменного имени:

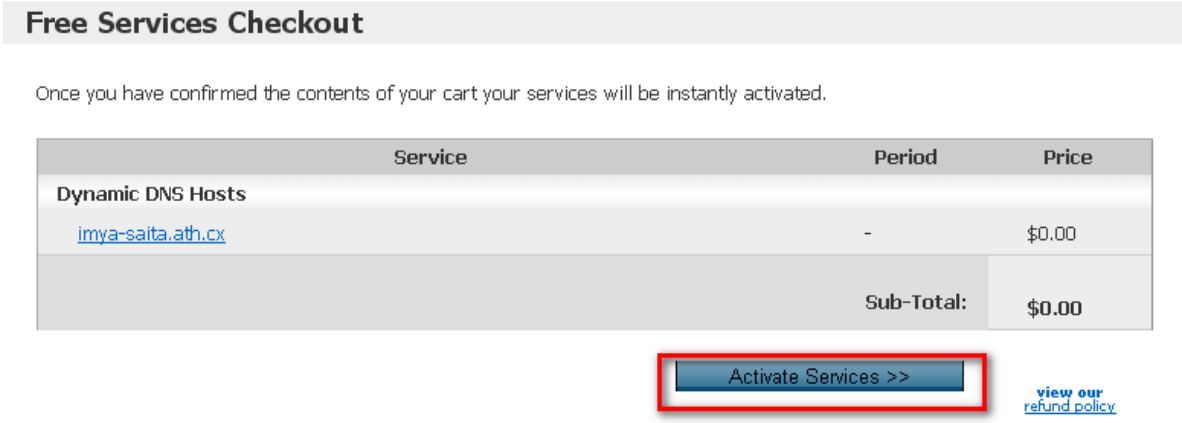


Рисунок-4. Окно Free Services Checkout.

Адрес создан, Вам показан список созданных адресов.

Шаг 3. Обновление сопоставления Domain-IP.

Обновление ip для сервисов динамического DNS происходит либо аппаратно (если Ваш модем это умеет), либо программно.

Если же Вы работаете не через DSL-модем, либо Ваш модем не поддерживает такую функцию, ничего не поделаешь, придется обходиться программным информатором.

Готово, теперь выбранное Вами доменное имя будет всегда однозначно вести на Ваш IP-адрес, безотносительно того, какой это адрес! А если проще, то Ваше имя теперь заменяет Ваш IP.

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ ПРОТОКОЛОВ УРОВНЯ ДОСТУПА К СРЕДЕ В БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЯХ

К.Ш.Хосилов (ассистент, ТУИТ)

В последнее время исследователями прилагаются значительные усилия по увеличению производительности беспроводных локальных сетей. Большинство исследований сосредотачивалось на уменьшении задержек при передаче кадров, избегании потерь пакетов, коллизий, и увеличении общей производительности сети. Одним из вариантов организации доступа к среде передачи данных является функция распределенной координации (Distributed Coordination Function, DCF), основанная на методе коллективного доступа с обнаружением несущей и механизмом избежания коллизий (CarrierSenseMultipleAccess/CollisionAvoidance, CSMA/CA).

Алгоритм DCF описан стандартом IEEE 802.11 и является важным предметом исследований. Для беспроводных локальных сетей были представлены новые решения по организации равноправного доступа к среде.

Одним из решений по увеличению производительности стал алгоритм Double Increment Double Decrement (DIDD), вносящий ряд изменений в работу алгоритма DCF. Основные изменения коснулись окна конкурентного доступа (Contention Window, CW). Стандарт IEEE 802.11e описывает новый алгоритм Enhanceddistributedchannelaccess (EDCA), определяющий серию улучшений в качестве обслуживания (Quality of Service, QoS) и повышающий общую производительность беспроводной локальной сети. Целью наших исследований являлось рассмотрение способа моделирования беспроводных вычислительных и телекоммуникационных систем с динамической топологией сети.

Задачами, результаты решения которых описаны в статье, являлись: рассмотрение особенностей функционирования протоколов DCF, DIDD и EDCA уровня доступа к среде в беспроводных локальных сетях, рассмотрение программного комплекса Network Simulator 2 как средства моделирования вычислительных и телекоммуникационных сетей

с динамической топологией сети, получение характеристик производительности протоколов уровня доступа к сети посредством модельных экспериментов (сценариев) и сравнительная оценка эффективности их работы. Network Simulator 2 (NS-2) является объектно-ориентированным программным обеспечением, ядро которого реализовано на языке C++. Язык скриптов (сценариев) OTcl (Object oriented Tool Command Language) используется в качестве интерпретатора. NS-2 полностью поддерживает иерархию классов C++ (называемую в терминах NS-2 компилируемой иерархией) и подобную иерархию классов интерпретатора OTcl (называемую интерпретируемой иерархией). Обе иерархии обладают идентичной структурой (рис. 1), т.е. существует однозначное соответствие между классом одной иерархии и таким же классом другой.

Использование двух языков программирования в NS-2 объясняется следующими причинами. С одной стороны, для детального моделирования протоколов необходимо использовать системный язык программирования, обеспечивающий высокую скорость выполнения и способный манипулировать достаточно большими объемами данных.

По результатам исследования можно сделать следующие выводы:

1. Алгоритм DIDD незначительно увеличивает производительность беспроводной сети в сравнении с традиционным DCF. Основным его преимуществом является простота, т. к. он использует элементарные параметры. К недостаткам можно отнести бульшие задержки при передаче пакетов в сетях с большим количеством узлов.

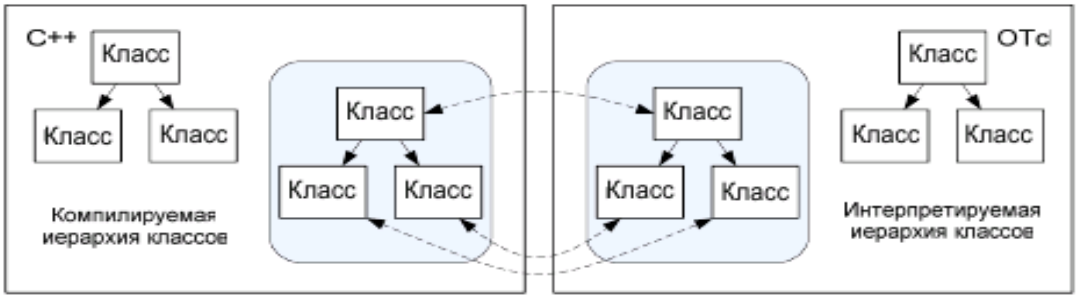


Рис. 1. Отличие алгоритма DIDD от BEB.

2. Алгоритм EDCA стандарта IEEE 802.11e в целом увеличивает производительность беспроводных локальных сетей и вносит ряд улучшений по передаче трафика с высоким приоритетом. Алгоритм EDCA, так же как и DCF, использует технологию случайного доступа к среде, а потому не является идеальным, т. к. не может гарантировать определенный уровень качества для трафика с высоким приоритетом.

3. Полученные результаты средних задержек, средней пропускной способности и коэффициентов доставки протоколов DCF, DIDD и EDCA показывают лучшую работу протокола EDCA. В целях улучшения эффективности работы QoS протокол EDCA требует дальнейших исследований.

ТАРМОҚДА СИГНАЛЛАРНИ ҚАЙТА ИШЛАШДА ХААР ВЕЙВЛЕТЛАРИ АСОСИДА АЛГОРИТМЛАШ

Ж.Б. Элов (ТАТУ, катта ўқитувчи)

Ахборот коммуникация технологияларининг хозирги замон тараққиётида рақамли сигналлардан кенг фойдаланиш соҳа жабҳаларида сифатли натижаларга эришиш учун асосий восита бўлиб хизмат қилмоқда. Шундай экан рақамли сигналларни қабул қилиш ва қайта ишлаш замон талаби ҳисобланади. Рақамли сигналларни қайта ишлаш бир қанча алгоритмлар ва функциялар асосида амалга оширилади. Вейвлет – бу умумлашган вақтинча фойдаланиладиган математик функция ҳисобланади. Математика сохасида вейвлет терминини пайдо бўлиши сигналлар билан ишлаш жараёнини самарали тарзда

яхшилади. Вейвлет сўзи инглизча Wavelet сўзидан оланган бўлиб “Кичик тўлқин” деган маънони билдиради.

Хаара вейвлети бир ўлчовли ва кўп ўлчовли сигналларни қайта ишлашда кенг қўлланилади. Сигналларни қайта ишлашда Хаар вейвлети қўйидаги кўринишда ҳисобланади.

Бу ерда

S_{2i} ва S_{2i+1} - сигнал қийматлари ҳисобланади

ва b_i лар берилган сигнал қийматларини қайта ишлаш ёрдамида ҳосил бўган натижа

Олинган сигнал қийматлари юқорида кўрсатилган формула ёрдамида бир неча марта такрорланиб ишлатилади. Сигналларни сиқиш бизга жуда хам қулайликларни яратиб беради ҳамда ҳисоблаш ишларида аниқ натижалар олишга, шу натижалар асосида эса сигнал графикларини тасвирлашда юқори имкониятларни тақдим этади. Кўп ўлчовли дискрет сигналлар қиймати матрица кўринишида ифодаланади. Кўп ўлчовли сигналларни қайта ишлаш юқори аниқликда натижалар олишга имконият яратади. Кўп ўлчовли сигналларни Хаар вейвлети ёрдамида қайта ишлаганимизда куйидаги алгоритмдан фойдаланамиз: Бир ўлчовли дискрет сигналларни қайта ишлаш алгоритми такрорланади. Яъни матрица қийматлари қаторлар бўйича хаара вейвлети ёрдамида ҳисоблаймиз. Натижада янги икки матрица ҳосил бўлади. Иккинчи қадамда матрица қийматларини устунлар бўйича ҳисоблаймиз ва яна иккита матрицага эга бўламиз. Бу алгоритмни яна бир марта такрорлаймиз ва нол кийматга яқин қийматларни ҳисобга олмаймиз, натижада матрица кўринишда берилган қиймат хаар вейвлети ёрдамида жуда ҳам содда кўринишга келади. Бу усул орқали тасвирларни сиқишда жуда ҳам самарали натижа олиш мумкин.

ТАРМОҚНИ ДАСТУРЛАШДА JAVA ДАСТУРЛАШ ТИЛИ ВА УНИНГ ИМКОНИЯТЛАРИ

Ж.Б. Элов (ТАТУ, катта ўқитувчи)

Java дастурлаш тили тақсимланган илованинг барча компонентлари ўртасида динамик маълумот алмашишни ташкил қилиш учун барча воситаларга эга. Шунинг учун Java масофадан мониторинг, диагностика қилиш ва бошқариш учун ДТ ишлаб чиқишда қулай хисобланади.

Java технологияси ўта содда, хавфсизликни юқори даражада таъминлаб бера оладиган, кучли, тўла обектга йўналтирилган дастурлаш тили бўлиб, муҳит (платформа)га боғлиқ бўлмаган ҳолда ишлайди. Java технологияси тўлалигича Java Virtual Machine (JVM) га асосланган. JVM нинг вазифаси таржимонлик яъни, дастлаб биз ёзган *.java файлни сомпилятор ёрдамида байт кодга ўгирилади ва JVM ёрдамида эса машина тилига ўгирилади. Жава технологиялари:

– Java SE – Java SE ёки Java Standart Edition, серверда, шахсий компютерда ишловчи дастурлар яратиш учун ишлатилади. Бу технология ёрдамида яратилган дастурлар деярли барча Операцион тизимларда ишлай олади. Шу билан бирга JavaSE бошқа Java турларининг асоси ҳисобланади.

– JavaEE – JavaEnterpriseEditionJava технологиялари орасида энг кенг тарқалган тури ҳисобланиб унда асосан серверда ишловчи дастурлар яратилади. Масалан, кўп фойдаланувчиларга мўлжалланган web-сайтлар яратишда кенг қўлланилади.

– JavaME – JavaME ёки JavaMicroEdition JavaSE нинг баъзи қисмларини ўз ичига олади. JavaME ёрдамида кичик қурилмалар учун даструлар ёзиш мумкин. Масалан, мобил телефон учун ўйинлар, дастурлар яратиш мумкин.

Java дастурлаш тилига асосланган ечимлар қуйидаги афзалликларга эга:

– Java нисбатан оддийроқ дастурлаш тили бўлиб ҳисобланади. Ишончли дастурий кодни тезда яратишга хотиранинг автоматик бошқарилиши, кўп каррали ворислик ва кўрсаткичларнинг бўлмаслиги ёрдам беради;

– Java нинг байтли коди кўп ҳолларда операцион тизим ёки процессордан мустақил бўлади. Шу сабабли Жава тилидаги иловалар бошқа платформаларга осонлик билан ўтказилади;

– JNIvaCORBA технологиялари ёрдамида бошқа дастурлаш тилларида яратилган обектлар билан алоқани ташкил қилиш мумкин.

Java дастурлаш тилининг энг асосий камчилиги жуда катта аппарат ресурсларидан фойдаланиши ҳисобланади. Бир хил вазифа С, С++ дастурлаш тилига қараганда Java тилида 1,5-2 баравар секинроқ амалга ошади. Бунда оператив хотирага жуда катта юкланиш берилади. Windows операцион тизимида Java тилида ишлаб чиқилган дастурни ўрнатиш учун Javavirtualmachine компонентини ўрнатиш лозим.

ОТКРЫТОЕ ШИФРОВАНИЕ НА ОСНОВЕ ПИФАГОРОВЫХ ТРОЙКИ ЧИСЕЛ

Д.Ю. Юнусов (ТПКИТ, доцент)

Информационные и телекоммуникационные технологии в последней половине прошедшего века существенно повлиляли на ускорение темпов развития мирового сообщество, создание базы для перевода многих национальных экономик на инновационный путь развития на основе производства и использования знаний, проникли практически во сферы жизни и деятельности людей. Несомненно, их динамичное развитие и применение станет одним из наиболее важных факторов, определяющих развитие человеества в двадцать первом веке.

В связи с этим значительно возрастает актуальность проблем, связанных с обеспеченинм безопасности личности, общества и государства при использовании современных информационных и телекоммуникационных технологий, с созданием благоприятных условий для гармонизации интересов различных государств в информационной сфере.При этом эффективность использовании методов и средств защиты информации, информационных технологийи систем зависит не только от степени изученности защищаемых объектов и анализа реальных условий, в которых они функционируют, но во многом определяется и моделированием возможных способов защиты и правильным выбором той или иной модели для решения практических вопросов создания системы защиты [1] .

В теории криптогарфии применяются различные методы защиты информации. Каждый алгоритм друг от друга отличаются по различным способам применение математиеского аппарата, каждый из которых имеют свои преимушество и недостатки.

В данной работе разрабатывается алгоритмы защиты информаци на основе анализа симметричных булевых функциях (СБФ) при исследование проблемы Ферми, почему уравнение имеет решения в натуральных числах и возможно ли этих чисел применить для криптографических анализов[3,4]. Рассмотрение начнём с определения:

Определение 1. [2]. Булева функция называется симметричной, если она не изменяется при любом переименовании переменных этой функции.

Известно, что уравнение (1) при n=2

$$\mathbf{x^2 + y^2 = z^2 \quad (2)}$$

является пифагоровы тройки чисел x,y,z и имеет решения в натуральных числах, первым из которых является числа.

В работе показываются, что если эти числа теперь представить в двоичной системе счисления (Таб.1),

Таблица 1. Представление чисел

	q_4	q_3	q_2	q_1	q_0
	2^4	2	2	2	2
	16	8	4	2	1
$X = 3$	0	0	0	1	1
$Y = 4$	0	0	1	0	0
$Z = 5$	0	0	1	0	1

то значение X ва Y будет определять логическую функцию трех переменных и имеет вид [3]

$$f(x,y) = S^3_{0,3}\,(q_2, q_{\bar{1}}, \overline{q_0}). \qquad (3)$$

Если значение арифметически умножить на ΔV (когда она равен кратному $2^к$,где к=0,1,…,n),то двоичные значение X,Y и Z на к-разрядов в лево увеличивая их значение. Для значение отличное от $2^к$ (когда ΔV равное 3,5,6,7,9,…) производится арифметическое сложение(например $\Delta V =$ 5 =1+4)$\Delta V =$ 1 и $\Delta V = 4$, т.е. для X =15 двоичное 1-1-1-1 получено от

0-1-1
+
<u>1-1-0-0</u>
= 1-1-1-1

Анализируя подобным образом установлено, что между значениями Y'' и Z существует линейная зависимость

где ΔV - является коэффициентом умножением для новых значений .

Если теперь значение уравнение (4) подставим в уравнение (2), тогда получим

Решая данное уравнение относительно то получаем

Анализируя (6) установлено, что между значениями пифагоровых троек X,Y и Z и ΔV существуют линейная зависимость, которых можно применить к решение задачи криптогарфического анализа . В работе предлагается алгоритмы шифрование и дешифрирование на основе пифагоровых троек X,Y и Z и ΔV .

М У Н Д А Р И Ж А

4-ШЎЪБА.
АХБОРОТ-КУТУБХОНА ВА АРХИВЛАР ЖАРАЁНЛАРИНИ БОШҚАРИШ

1.	***Ганиева Б. И.*** Ёшларда китобхонлик кўникмаларини шакллантиришда оиланинг тутган ўрни	4
2.	***Рахматуллаев М.А.*** Электронная библиотека по технической реабилитации	6
3.	***Хайруллаев Б.А., Рахматуллаев М.А.*** Создание индекса цитирования в Узбекистане: проблемы и перспективы	8
4.	***Махмудов М.Х.*** Ахборот-кутубхона, архив ва музей муассасаларида фойдаланувчиларга ахборот хизмати кўрсатишнинг умумий ва ўзига хос томонлар	10
5.	***Xundibayev A.M.*** Kutubxonalarda interaktiv xizmatlarni tashkil etish	11
6.	***Khasanova M.*** Basic concepts and analysis of the use of ICT in medical rehabilitation	12
7.	***Eshboyev E. A., Shodiyev F. Yu.*** Kutubxonada avtomatlashtirilgan ish o'rnini tashkil etishning vizual modeli	14
8.	***Ганиева Б.И.*** Талабаларда ахборот олиш маданиятини шакллантиришнинг муҳим йўналишлари	15
9.	***Ғуломова К.М.*** Ахборот-кутубхона соҳаси кадрларининг малакасини ошириш ва уларни қайта тайёрлаш истиқболлари	17
10.	***Зиёдуллаева Г.Э.*** Авторитет маълумотларга функционал талаблар	19
11.	***Каримов Ў. У.*** Корпоратив тармоқда очиқ ресурслар электрон кутубхонаси	21
12.	***Матқурбонова Н.Ш.*** Дунёнинг йирик кутубхоналари таҳлили	23
13.	***Раҳимова Ш.А.*** Жамиятда ахборот алмашинуви маданиятини оширишнинг социал жихатлари	24
14.	***Моллаходжаев У. Э.*** Рекламная деятельность информационно-библиотечных учреждений	26
15.	***Мухаммаджонов Ш.М.*** Архив ҳужжатлари йиғма электрон каталогини яратиш ва ҳужжат қидириш масалалари	28
16.	***Султанова З.Ш.*** Ахборот маданиятини шакллантириш масалалари	31
17.	***Ануфриева Ю.Г.*** Роль информационной культуры в формировании профессиональных навыков будущих специалистов	32
18.	***Норматов Ш.*** Электрон кутубхоналар хавфсизлигини таъминлашнинг долзарблиги	34
19.	***Holboyev I.A.*** RFID (Radio Frequency Identification) tehnologiyasini axborot-kutubxona tizimlarida joriy qilish	36
20.	***Норматов Ш.Б.*** Кутубхона ресурслари хавфсизлигини таъминлашнинг ҳуқуқий жиҳатлари	37
21.	***Юсупова К.Н.*** Ахборот маданиятини шакллантириш орқали ўқувчини китобхонга айлантирамиз	39
22.	***Jumanazarova R.*** Kutubxona foydalanuvchilari orasida noyob adabiyot manbalarini targ'ib qilish	40
23.	***Файзиев М.*** Ахборот кутубхона муассасаларида замонавий ахборот-кутубхона хизматлари	42
24.	***Моллаходжаев У.*** Особенности рекламы в деятельности информационно-библиотечных учреждений	44

5-ШЎЪБА.
АХБОРОТ ХАВФСИЗЛИГИНИНГ ЗАМОНАВИЙ МУАММОЛАРИ ВА РИВОЖЛАНИШ ИСТИҚБОЛЛАРИ

25.	***Ганиев С.К., Гуломов Ш.Р.*** К вопросу функционирования межсетевого экрана в специальной фильтрации трафика	48
26.	***Каримов М.М., Гуломов Ш.Р.*** Иерархия процессов измерения сетевого трафика	49
27.	***Ганиев А.А.*** Ахборот тизимлари аудитининг COBIT стандарти хусусида	52
28.	***Ганиев А.А.*** Ахборот тизимлари аудитини тартиблаш масаласи ҳақида	54
29.	***Юсупов С.Ю.*** Перспективы биометрической идентификации и аутентификации	55
30.	***Юсупов С.Ю., Мамажонов У.О.*** Тармоқда маълумотларни ҳимоялашда миллий тармоқлараро экран дастурини ишлаб чиқиш муаммолари	57
31.	***G'ulomov Sh.R., Yusupov B.K.*** Axborot xavfsizligi insidentlariga javob qaytarishni tashkil etish jarayoni	58
32.	***Юсупов Б.К.*** Зараркунанда дастурларни содда динамик таҳлили	60
33.	***Ганиев С.К., Худойқулов З.Т.*** Биометрик криптотизимларнинг хавфсизлиги таҳлили	62
34.	***Ғаниев С.К., Кучкаров Т.А.*** Ахборотни ҳимоялашда тизимли ёндашишдан фойдаланиш масаласига доир	65
35.	***Исломов Ш.З., Нурмухаммедов Н.К.*** Биометрик аутентификациялашдан фойдаланишдаги муаммолар ҳақида	66
36.	***Ҳамдамов Д.Б.*** Криптографик алгоритмларнинг математик асоси	68
37.	***Авлаев Д.А., Имамалиев А.Т.*** Киришни назоратлаш ва бошқариш тизими таркибидаги контроллерларнинг таҳлили	70
38.	***Ғуломов Ш.Р.*** Корхонада ахборот хавфсизлиги инцидентларини тергов қилиш усуллари ва баҳолаш	72
39.	***Бекмирзаев О.Н.*** Ахборот хавфсизлигида хавф-хатарларни аниқлашнинг умумий тавсифи	74
40.	***Корабаев Э.А.*** Интернетда ахборот алмашинувининг хавфсизлигини таъминлашда SSL протоколининг аҳамияти	77
41.	***Yusupov B.K., Salimov S.B.*** Zararkunanda dasturlarning kengaytirilgan dinamik tahlili va amalga oshirish usullari	79
42.	***Қахрамонов Э.Қ.*** Корхонада ахборот хавфсизлиги хавф-хатарларини таҳлил қилиш усуллари	81
43.	***Каримова Д.К., Кадиров М.М.*** Проблемы информационной безопасности компьютерных сетей и основные функции систем защиты информации	82
44.	***Irgasheva D.Y., Nabiyev I.M.*** Kompyuter tizimlarini himoyalashda ikki omilli autentifikatsiyalash usulining o'rni	85
45.	***G'aniyev S.K., Olimov I.S.*** Simmetrik kriptotizimlar uchun ishlab chiqilgan kalitlarni tasodifiylikka tekshiruvchi testlarning tahlili	87
46.	***Кадиров М.М., Кадиров М.М.*** Использование матрицы установления полномочий в разграничении доступа	89
47.	***Oripov P.Kh.*** Current intrusion detection and prevention methodologies	91
48.	***Rashidov M.A.*** Tarmoq tizimlari monitoringi va vositalarini tahlil etish	93
49.	***Gulyamova D.R., Hojiyev S.A.*** Web saytlarni xavfsizligini taminlashda hujum turlari va usullarini tahlili	94
50.	***Shodmonova X., Salimov S.*** Threats and protection ways of mobile networks	96
51.	***Tadjieva M., Nurmuxamedov N.*** Analyzing E-government protection threats	98
52.	***Юсупов Б.К., Юсупов З.К.*** Ахборот хавфсизлиги инцидентлари терговида гуруҳлар тузилмасини ташкил этиш ҳақида	100
53.	***G`aniyev S.K., Turdiboyev B.Y.*** An analysis of access control models	102

54.	***Temirova G.A.*** Kompyuter tarmoqlarida axborotdan ruxsatsiz foydalanish va chiqib ketishini cheklash usullari	104
55.	***Xamdamov D.B.*** Simmetrik kriptotizimlarning matematik nuqtai nazardan qiyosiy tahlili	106
56.	***Qodirov Z.Z., Hojiyev S.A.*** Web saytlarni turli hujumlardan himoyalash dasturiy vositasi	108
57.	***Қудратов А.Н., Абдураимов Д.Э.*** Ахборот тизимларида хавф эҳтимолини таҳлили	110
58.	***Имамалиев А.Т. Юсупов Б.К.*** Киришни назоратлаш ва бошқариш тизимлари архитектураларининг таҳлили	111
59.	***Имамалиев А.Т.***Қўриқланаётган объект хавфсизлигини таъминлаш муаммосига доир	113
60.	***Азизова З.*** Системы мониторинга как одно из средств обеспечения информационной безопасности	115
61.	***Алланов О.М.*** Тармоқ хавфсизлигини таъминлаш усули	116
62.	***Алланов О.М.*** Криптографик ХЭШ функцияларнинг ахборот хавфсизлигини таъминлашдаги ўрни	119
63.	***Шамшиева Б.М.*** Анализ способов обеспечения сетевой административной безопасности	121
64.	***Худойқулов З.Т., Имомалиев А.Т.*** Расм маълумотларда ахборотни стеганографик яширишнинг самарали усули	122
65.	***Халимтаева И.У.*** Хавфсиз SMS-хабар алмашиниш усулларининг тадқиқи	125
66.	***Ибрагимов Р.Р.*** Применение DPI как средства антивирусной защиты	127
67.	***Насруллаев Н.Б., Ганиев А.А., Ширинов Л.Т.*** Интернет тармоғида ахборот хавфсизлигини таъминлаш	128
68.	***Мирзаева М.Б.*** Корхоналарда ахборот хавфсизлиги хавф-хатарларини баҳолаш алгоритми	130
69.	***Лазарева М.В., Горовик А.А.*** Достоинства и недостатки политики безопасности в реляционных базах данных	132
70.	***Лазарева М.В.*** Кибертерроризм – новые угрозы XXI века	134
71.	***Сайфуллаева Н.А.*** Организация защиты мультисервисной сети с помощью межсетевых экранов	135
72.	***Сайфуллаева Н.А.*** Способы организации и механизмы защиты беспроводных сетей	137
73.	***Ганиев А.А., Ахмедова Н.Ф.*** Ахборот тизимлари самарадорлигини баҳолашнинг долзарблиги ва муаммолари	139
74.	***Бекмирзаев О.Н., Негматов Ж.А.*** Корхона ва ташкилотларда ахборот хавфсизлигини таъминлаш бўйича мажбуриятларни тақсимлаш	140
75.	***Кулдашов О.Х., Муминов К.З.*** Имитационная модель защиты информации в волоконно-оптической линии связи	142
76.	***Юсупов Б.К., Мамажонов У.О.*** Тармоқ хавфсизлигини таъминлашда тармоқлараро экран (Firewall) дастурларининг амалий ахамияти	143
77.	***Рахманов Қ.С., Махманов Б.Қ.*** Олий таълим муассасалари ахборот тизимларидан фойдаланишни бошқаришда ролли моделининг ўрни	145
78.	***Нематова С.А.*** Тақсимланган тизимларни мониторинглаш усуллари таҳлили	147
79.	***Иргашева Д.Я., Ҳамидов Ш.Ж.*** Тармоқ ҳужумларни аниқлаш усулларининг тадбиқи	150
80.	***Муминова С.Ш.*** “Электрон ҳукумат” тизимини самарали ташкил этишда ахборотни руҳсатсиз чиқиб кетишидан ҳимоялаш	152
81.	***Кучкаров Т.А., Рашидов М.И.*** Маршрутизация данных в беспроводных сетях смешанного типа	154

82.	***Халмуратов О.У., Хўжамов Д.Ж.*** Ахборот-коммуникация технологияларида ахборот хавфсизлигини баҳолашнинг замонавий усуллари	156
83.	***Tashev K.A., Bo'riyev Y A.*** Axborot xavfsizligi hodisasini ko'chirish qoidalari	158
84.	***Кудратов С.Г., Холбоев И.А.*** Возможности RFID технологии	159
85.	***Самаров Х.К.*** Об одном подходе написания безопасных веб-приложений	161
86.	***Юсупов С.Ю., Ганиев А.А.*** Ахборот хафсизлиги инцидентларига жавоб қайтариш процедурасининг ҳаёт даври	162
87.	***Mardiyev U.R.*** A biometric approach to linux login access control	164
88.	***Ибрагимов Р.Р.*** Применение wireshark для определения параметров сетевых атак	166
89.	***Порубай О.В.*** Безопасность персональной информации на компьютерах и ноутбуках	167
90.	***Порубай О.В.*** Распространение Ddos-атак посредством бот-сетей	170
91.	***Салимов М.*** Специальная фильтрация трафика с использованием платформы фильтрации Windows	171
92.	***Рахманова Г.С.*** Веб-иловалар заифликларини аниқлаш усулларининг таҳлили	173

7-ШЎЪБА.
ТЕЛЕКОММУНИКАЦИЯ ТАРМОҚЛАРИ ВА КОММУТАЦИЯ ТИЗИМЛАРИНИНГ РИВОЖЛАНИШ ТАМОЙИЛЛАРИ

93.	***Abdurakhmonova K.B.*** Optik tolali aloqa liniyalarining rivojlanish istiqbollari	176
94.	***Abdurakhmonova K.B.Eshmuradov A.M***. Atmosferali optik aloqa liniyasida ko‘p kanalli tizimni qo‘llash	177
95.	***Gulturaev N.X., Qadamov S.Q.*** Virtual xususiy tarmoqlar transportining asosiy texnologiyalari	178
96.	***Karimov Sh.Sh.,Sadchikova S.A.***Traffic offload:How it’s work on femtocell/lte network	180
97.	***Mirzayeva I.A.*** Optik abonent kirish tarmoqlarini kogerent va nokogerent ocdma asosida qurishni tahlil qilish	181
98.	***Muzafarov F.A.*** Performance analysis of a next generation converged network	183
99.	***Nasimov R.H.*** Requirements of quadruple play services	183
100.	***Son V.A., Sadchikova S.A.*** Network transparency methods in 4G	185
101.	***Xidirov A.M.,Vaydullayev I.*** FTTH texnologiyasini tashkil qilishning afzallik va kamchiliklari	186
102.	***Абдужаппарова М.Б.*** Расчёт пропускной способности сети доступа на основе первой формулы Эрланга	187
103.	***Абдужаппарова М.Б.*** Метод расчёта пропускной способности оптической сети доступа по второй формуле Эрланга	189
104.	***Алламуратова З.Ж., Кутлымуратов А., Абдуганиева О.И***. Геоинформационная база данных телекоммуникационной сети Кегейлийского района республики Каракалпакстан	191
105.	***Алламуратова З.Ж., Кутлымуратов А., Нартбаева М.*** К вопросу разработки системы поддержки принятия решений в области телекоммуникаций	193
106.	***Kuchkorov T.A., Allamuratova Z., Ajibayeva K.*** Spatial analysis characteristics of arcgis for environmental monitoring	194
107.	***Бабажанова Т.М.*** Анъанавий тармоқдан дастурий конфигурацияланадиган тармоқларга ўтиш сабаблари	195
108.	***Байжонова Л.Э.*** Алгоритм формирования транспортной сети	197
109.	***Байжонова Л.Э.*** Виртуал хусусий тармоқларни ташкил этиш муаммолари	197
110.	***Бекмуратов Ф.К., Хидиров А.М.*** IP-телефония для повышения экономической эффективности корпоративных организаций	198

111.	***Гультураев Н.Х.*** Модель формирования транспортной сети	200
112.	***Гультураев Н.Х.*** Повышение живучести транспортной сети связи	200
113.	***Давлетова Х.Р.*** Особенности взаимоотношений операторов связи для поддержки QoS	202
114.	***Давлетова Х.Р.*** Способ защиты информации при облачных вычислениях	203
115.	***Зуфарова Н. Н.*** Особенности применения оптических коммутаторов	204
116.	***Зуфарова Н. Н.*** Обзор особенностей оптических коммутаторов	205
117.	***Ибатова Д.Х.*** Янги технология асосида шаклланган оптик толалар	206
118.	***Исаев Р.И., Абдукадиров А.А.*** Информационная безопасность оптических систем связи	208
119.	***Исаев.Р.И.,Тлеумуратов Ж.Б.*** Анализ механизов обеспечения информационной безопасности семейства протоколов IPV6	209
120.	***Исманов Қ.А.***TCP ва UDP протоколларининг ўтказувчанлик қобилиятини баҳолаш	211
121.	***Исманов Қ.А.*** Янги авлодлар хизматлари сифати параметрларини тестлаш ва назорат қилиш усуллари	213
122.	***Каримова А.О., Сапарова Б.М.*** IP-тармоқ бўйича реал вақт овозли хабарларини узатиш сифатига таъсирларни камайтириш чоралари	214
123.	***Миразимова Г.Х.*** Тўлқин узунлиги бўйича зичлаштиришли тизимларда узатиладиган гуруҳли сигнал қувватини назорат қилиш	216
124.	***Миразимова Г.Х.*** Тўлқин узунлиги бўйича зичлаштиришли тизимларда узатиладиган гуруҳли сигнал қувватига қўйиладиган талаблар	218
125.	***Мирзаева И.А.*** Методы оценки надежности оптических сетей доступа	220
126.	***Музафаров Ф.А.*** Кейинги авлод конвергент тармоқларида маршрутлаш технологияларининг қиёсий таҳлили	223
127.	***Мурадова А.А.*** Обеспечение сервиса IP Quality Manager на уровне приложения инфокоммуникационной сети	223
128.	***Мурадова А.А.*** Обеспечение качества обслуживания оборудования сети доступа инфокоммуникационной сети	225
129.	***Мухитдинов Х.А., Абдуллаев А.А.*** Перспективы применения технологии IMS в современных телекоммуникационных сервисах	227
130.	***Набиев С.Б.*** Особенности технологии атмосферной оптической связи	229
131.	***Набиев С.Б.*** Практика применения технологии атмосферной оптической связи	230
132.	***Насимов Р.Ҳ.*** Интеллектуал уйлар учун аутентификацияга асосланган химоя алгоритмини яратиш	231
133.	***Норматова Д.Т.*** NGN тармоғида чақирувларга интеллектуал хизмат кўрсатиш марказини моделлаштириш масалалари	233
134.	***Нурмухамедов Т.Р.*** Информационные системы железнодорожного транспорта Узбекистана	234
135.	***Раджапова Р.Н.*** Пакетли коммутацияга асосланган корпоратив тармоқларда мультимедиали трафиклар ўтишини оптималлаштириш	235
136.	***Раджапова Р.Н.*** Телекоммуникация тармоқларида MPλS ни қўллаш	237
137.	***Сайдиакбаров С. М.*** NGN Тармоғида инфокоммуникация хизматларини тақдим этиш	238
138.	***Сапарова Б.М.*** Безопасность беспроводных WLAN	239
139.	***Тургунов Б.А.*** Локал тармоқларда замонавий, тезкор оптик технологиялар	241
140.	***Турсунбаев Ф.К.*** Принципы построения высокопроизводительного статическо-пространственного многозначного элемента информационно-вычислительной техники	242
141.	***Турумбетов Б.К.,Рейпназаров Е.Н.*** Юқори сифатли маълумотларни реал вақтда узатишда SCTP транспорт протоколини қўллаш	244

142.	***Фозилжонова Л.И.*** Атмосферная оптическая связь и её преимущества	245
143.	***Фозилжонова Л.И.*** WDM-PON технологияси асосида кенг полосали тармоқда инновацион ечимларининг таҳлили	246
144.	***Хайдаров И.С.*** Организация приоритетов по ценности информации в компьютерных сетях и системах с разнотипными каналами и изменяющийся структурой	246
145.	***Хайтбаев А.Ф.*** Виртуал шахсий тармоқ транспортини ташкил қилиш усуллари	249
146.	***Хайтбаев А.Ф.*** Кириш тармоғида мультисервис трафигини интервалли усулда таҳлил қилиш	250
147.	***Эшмурадов А.М.*** Вопросы применения АОЛС в телекоммуникации на участке «последней мили»	251
148.	***Эшмурадов А.М.*** Атмосферали оптик алоқа линиясининг самарадорлигини ошириш усули	251
149.	***Юнусов Н.Ю.*** Методы стабилизации мощности источника излучения передающего оптоэлектронного модуля ВОСС	252
150.	***Юнусов Н.Ю.*** ТОАТ ларда ёруғлик манбаи нурланиш интенсивлигини ТТЛ интеграл мантиқ элементи ёрдамида модуляциялаш усуллари	254
151.	***Абдуллаев Д.Б.*** Принципы нарушения доступности в сети передачи данных	256
152.	***Абдуллаев М.М., Атажанов З.Р.*** Дастурий конфигурацияланадиган тармоқ технологияси, унинг афзаллик ва камчиликлари	258
153.	***Абдуллаев М.М., Маликов Х.Х.*** Булутли ҳисоблаш технологиясида ахборот хавфсизлигига тахдидлар	260
154.	***Амирсаидов У.Б., Таджибаев А.З.*** Метод балансировки нагрузки в кластерных подсистемах IMS	261
155.	***Амирсаидов У.Б.*** Приоритетное обслуживание запросов на установления соединения в сети IMS	263
156.	***Атажанов З.Р.*** OpenFlow протоколи асосида ишлайдиган дастурий конфигурацияланадиган тармоқ	266
157.	***Балтаев.Ж.Б.*** Методы диагностики микропроцессорных устройств с использованием многоканального сигнатурного анализатора	268
158.	***Балтаев. Ж.Б., Тоштемиров Т.Қ.*** Анализ технологий коммутации для сетей следующего поколения	269
159.	***Бойманов Р.Ж.*** Анализ влияния показателей контролепригодности на надежностные характеристики сети ПД	271
160.	***Джаббаров Ш.Ю.*** АТМ технологияда IPSec ва SSL протоколларининг ишлатилиши	272
161.	***Джаббаров Ш.Ю., Халмурадов Т.Н.*** Основные проблемы, задачи и требования к защите информации в технологиях NGN	274
162.	***Джураев Р.Х***. Взаимосвязь характеристик качества услуг и информационной безопасности сетей передачи данных	276
163.	***Джураев Р.Х.*** Модель и методы оценки информационной безопасности сетей передачи данных	278
164.	***Ибраимова Р.М.*** Анализ среды облачных вычислений как объекта обеспечения качества обслуживания	281
165.	***Iskandarova S.N.*** Xemmingning neyron to’rlari asosida tasvirni tanish	282
166.	***Iskandarova S.N.*** XOPFILDNING neyron to’rlari asosida tasvirni tanish	284
167.	***Khamdamova Kh.A.*** GSM security overview	286
168.	***Кадыралиев И.А.*** Анализ модели трафика в сетях с коммутацией пакетов	288
169.	***Kilichov J.R., Maxammadiyev M.M.*** Mahaliy telefon tarmog’i uchun triple-play xizmatlarini taqdim etish	289

170.	***Qodirov A.A.*** Virtual tarmoqlarni dasturiy konfiguratsiyalangan tarmoqlar (DKT) asosida tashkil etish	291
171.	***Qodirov A.A.*** Telekommunikatsiya tarmog‘ida IP SLA monitoringini o‘tkazish orqali xizmat ko‘rsatish sifatini baholash	292
172.	***Қодирова Г.Ю.*** ДТS-3100 тизимнинг умумий тавсифи ва тизимни бошқариш	295
173.	***Қодирова Г.Ю.*** NGN тармоғига ўтишда телекоммуникация тармоғининг технологияси, топологияси ва хизматлари	297
174.	***Matkurbonov D. M., Rahmanov B.I.*** Algorithm for access network optimization	299
175.	***Матқурбонов Д.М.*** Абонент фойдалана оладиган тармоқларини оптималлаштириш масалалари	301
176.	***Махаммадиев М.М., Холматов Н.М.*** Беспроводные технологии для предоставления услуги IPTV	303
177.	***Махмудов С.О.*** Дастурий конфигурацияланадиган тармоқда тармоқ оқимини эксперт нейрон тармоғи асосида бошқариш	305
178.	***Махмудов С.О.***Тармоқни бошқариш масалаларида мавҳум тўплам ва мантиқни қўллашни аҳамияти	307
179.	***Нишонбоев Т.Н., Абдулхаев Н.М.*** Инфокоммуникация тармоғи ресурсларини сервисга йўналтирилган архитектура усули негизида тақдим этиш асослари	309
180.	***Нишонбоев Т.Н., Жумабаев А.А***. Фойдаланувчи сўровини ИКТ сатҳларида бажарилиш вақтининг йиғиндисини ҳисоблаш алгоритми	311
181.	***Нурматова С.Б.*** Роль цифровых процессоров в телекоммуникационных сетях	314
182.	***Нурматова С.Б.*** Телекоммуникация тармокларида ахборотни кодлаштиришнинг самарали усуллари	316
183.	***Садатдийнов К.Е.*** OpenFlow коммутатори ишлаш тамойили ва унинг тармоқдаги ўрни	318
184.	***Саитахмадов М. Б.*** Алгоритмы построения фрактальных объектов и вычисления показателя Херста	320
185.	***Сайдирасулов Н.С., Махаммадиев М.М.*** Программно конфигурируемые сети	322
186.	***Сулаймонов Ф.А.,Жумабаев А.А.*** Инфокоммуникация тармоғи кириш сатҳининг ишончлилик кўрсаткичларини аниқлаш алгоритми	324
187.	***Тангриберганов Ғ.А.*** Анализ компонентов сети и услуг IPTV	326
188.	***Тангриберганов Ғ.А.*** Качество восприятия в IPTV	328
189.	***Тоштемиров Т.Қ.*** Построение диагностической экспертной системы на основе теории нечетких множеств	329
190.	***Турдахматов А.А.*** Анализ методов маршрутизации в сетях передачи данных	331
191.	***Умирзаков Б.М.*** Тармоқ хавфсизлигини миқдорий баҳолаш	333
192.	***Умирзаков Б.М.***Тармоқ хавфсизлигини таъминлашда хизмат кўрсатиш сифати мониторинги	335
193.	***Usmanova N.B., Suyunov A.X.*** Challenging issues of fog computing in big data processing in tandem internet of things	337
194.	***Усманова Н.Б, Жамолова Г.М.*** Телекоммуникация тармоқларида QoS ни таъминлаш механизмларига оид	339
195.	***Халмурадов Т.Н.*** Характеристики информационной безопасности и особые требования к безопасности сетей NGN	341
196.	***Холиқов С.С., Назаров Б.Б.*** Организация WI-FI сети в подвижном составе	343
197.	***Xolliyev I.T.*** Cloud computing, consepts and milestones	344
198.	***Abdullayev S.A.*** Telekommunikatsiya tarmoq trafigini klassifikatsiyalash usullari	346
199.	***Abduraxmonov R.P., Abdullayev .S.A.*** Telekommunikatsiya tarmoq trafigini boshqarishda packetc dasturlash tili imkoniyatlari	348
200.	***Алламуратов Ш.З. Мамутова В.Н.*** Методы пакетной синхронизации средств электросвязи мультисервисных сетей	349

201.	***Axunov F.I., Normurodov E.B.*** IP tarmoq trafigini boshqarishda dpi texnologiyasining o'rni	351
202.	***Djuraev O.N.*** Ilovalarni dasturlash interfeysi (application programming interface-api) dan foydalanish	352
203.	***Khosilov K.SH., Shokirov. A.T.*** Network traffics control and classification by using openflow	354
204.	***Makhamadjonov A.*** Deep packet inspection and its benefits	356
205.	***Makhsudov J.SH., Narzullayev. Sh.E.*** Deep packet inspection technologies	358
206.	***Makhsudov J.SH. , Narzullayev .Sh.E.*** Basic structure of artificial neural networks	360
207.	***MirzayevaM.B.*** The political potentials of DPI	362
208.	***Normurodov E.B.*** DPI tizimining texnik tashkil etilishi	363
209.	***Umarov A.S., Makhamadjonov A.A.*** The technical possibilities of DPI	365
210.	***Umarov A.S., Teshaboev. KH.N.*** The economic potentials of DPI	367
211.	***Zarmasov E.M.*** Aspects of cellular networks	368
212.	***Абасханова Х.Ю.*** Ўрнатилган тизимларни Vmlab муҳитида лойиҳалаш	370
213.	***Абдалимов М.Н.*** е-ТОМ тамойили ва унинг телекоммуникация тармоқлари ва хизматларини бошқаришда қўлланилиши	371
214.	***Абдуллаев А.И.*** IPV4 протоколидан IPV6 протоколига ўтиш технологиялар таҳлили	373
215.	***Абдуллаев У.М.*** Технология измерения качества оптических линий связи	375
216.	***Абдуллаев У.М.*** Сетевые протоколы PPPoE и IPoE	378
217.	***Абдурахманов Р.П.*** Исследование особенностей проектирования сетей следующего поколения	380
218.	***Абдурахманов Р.П.*** Анализ факторов влияющих на методологию проектирования сетей следующего поколения	383
219.	***Абдухалилов Б.З.*** CLOUD COMPUTING: преимущества и недостатки, темпы развития на мировом уровне и в Узбекистане	386
220.	***Абдухалилов Б.З.*** Управление телекоммуникационными сетями: анализ использующихся концепций на практике	387
221.	***Абдухалилов С.Ғ***. Моделирование сенсорных сетей в технологии INTERNET OF THINGS	390
222.	***Абдухалилов С.Ғ.*** Разработка системы нечеткого вывода в интерактивном режиме в среде MATLAB	391
223.	***Акмурадов Б.У.*** Эффективные сетевые операционные системы: применение и различия	393
224.	***Амурова Н.Ю.*** SMART GRID в передающих системах	395
225.	***Амурова Н.Ю.*** Объекты и системы энергетических сетевых компаний	397
226.	***Ахунов Ф.И.*** Замонавий ўрнатилган тизимларининг аппарат ва дастурий таъминоти	399
227.	***Ахунов Ф.И Мирзаева. М.Б.*** Ўрнатилган тизимларда энергия истеъмол қилишни камайтиришда микроконтроллерларни қўллаш афзалликлари	401
228.	***Борисова Е.А***. Некоторые аспекты экологического моделирования	402
229.	***Борисова Е.А.*** Моделирование системы принятия решений в экологии	404
230.	***Зармасов Э.М., Абдалимов М.Н.*** Использование широтно-импульсная модуляция в AVR микроконтроллерах	405
231.	***Мирзоқулов Х.Б., Нурмуродов Ж.Х***. Характеристика и механизмы реализации технологии мультивещания в сетях LTE	406
232.	***НазаровУ.А.*** Тармоқ фаолиятини мониторинг қилиш тизимлари	408
233.	***Парсиев С.С.*** Телекоммуникационные сети с приоритетным обслуживанием	409
234.	***Парсиев С .С.*** Анализ параметров структуры телекоммуникационной сети	411

235.	***Сиддиков И.Х., Абдуллаева С.М***. Применения плоской измерительной обмотки электромагнитных преобразователей тока	413
236.	***Сиддиков И.Х., Абдуллаева С.М.*** Преобразование сигнала о несимметрии токов на основе электромагнитных преобразователей	416
237.	***Тешабаев Х.Н., Шокиров А.Т.*** Идентификация и управление сетевым трафиком с помощью статистических методов классификации	418
238.	***Хамдамов. У.Р.*** Применение вейвлет-преобразований в обработке речевых сигналов	420
239.	***Хамдамов. У.Р., Пулатов .С.Ш***. Руководство по настройке динамического DNS (DDNS)	422
240.	***Хосилов К.Ш.*** Анализ производительности протоколов уровня доступа к среде в беспроводных локальных сетях	425
241.	***Элов Ж.Б.***Тармоқда сигналларни қайта ишлашда Хаар вейвлетлари асосида алгоритмлаш	426
242.	***Элов Ж.Б.*** Тармоқни дастурлашда java дастурлаш тили ва унинг имкониятлари	427
243.	***Юнусов Д.Ю***. Открытое шифрование на основе пифагоровых тройек чисел	428