ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

ЎҚУВ–УСЛУБИЙ МАЖМУА

КОМПЬЮТЕР ТАРМОҚЛАРИ ХАВФСИЗЛИГИ

“Компьютер инжиниринги” йўналиши

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ОЛИЙ ТАЪЛИМ ТИЗИМИ ПЕДАГОГ ВА РАҲБАР КАДРЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШНИ ТАШКИЛ ЭТИШ БОШ ИЛМИЙ - МЕТОДИК МАРКАЗИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

“Компьютер инжиниринги ”
йўналиши

“КОМПЬЮТЕР ТАРМОҚЛАРИ ХАВФСИЗЛИГИ”

МОДУЛИ БЎЙИЧА

Ў Қ У В –У С Л У Б И Й М А Ж М У А

Тошкент - 2021

Модулнинг ўқув-услубий мажмуаси Олий ва ўрта махсус таълим вазирлигининг 2020 йил 7 декабрдаги 648-сонли буйруғи билан тасдиқланган ўқув дастури ва ўқув режасига мувофиқ ишлаб чиқилган.

Тузувчилар: Муҳаммад ал-Хоразмий номидаги ТАТУ, “Ахборот хавфсизлиги” кафедраси доценти, PhD Ш.Ғуломов.

Тақризчилар: Беларусь-Ўзбекистон кўшма тармоқлараро амалий техник квалификациялар институти, илмий ишлар ва инновациялар бўйича директор ўринбосари в.б., доц. Л.Набиулина,
Муҳаммад ал-Хоразмий номидаги ТАТУ, “Ахборот технологиялари” кафедраси мудири, проф. Х.Зайнидинов.

Ўқув-услубий мажмуа Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Кенгашининг 2020 йил 29 октябрдаги 3(705)-сонли қарори билан маъқулланган.

МУНДАРИЖА

I БЎЛИМ

ИШЧИ ДАСТУР

Кириш

Дастур Ўзбекистон Республикасининг 2020 йил 23 сентябрда тасдиқланган “Таълим тўғрисида”ги Қонуни, Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги “Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида”ги ПФ-4947-сон, 2019 йил 27 августдаги “Олий таълим муассасалари раҳбар ва педагог кадрларининг узлуксиз малакасини ошириш тизимини жорий этиш тўғрисида”ги ПФ-5789-сон, 2019 йил 8 октябрдаги “Ўзбекистон Республикаси олий таълим тизимини 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-5847-сон ва 2020 йил 29 октябрдаги “Илм-фанни 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-6097-сонли Фармонлари ҳамда Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2019 йил 23 сентябрдаги “Олий таълим муассасалари раҳбар ва педагог кадрларининг малакасини ошириш тизимини янада такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги 797-сонли Қарорида белгиланган устувор вазифалар мазмунидан келиб чиққан ҳолда тузилган бўлиб, у олий таълим муассасалари педагог кадрларининг касб маҳорати ҳамда инновацион компетентлигини ривожлантириш, соҳага оид илғор хорижий тажрибалар, янги билим ва малакаларни ўзлаштириш, шунингдек амалиётга жорий этиш кўникмаларини такомиллаштиришни мақсад қилади.

Қайта тайёрлаш ва малака ошириш йўналишининг ўзига хос хусусиятлари ҳамда долзарб масалаларидан келиб чиққан ҳолда дастурда тингловчиларнинг мутахассислик фанлар доирасидаги билим, кўникма, малака ҳамда компетенцияларига қўйиладиган талаблар такомиллаштирилиши мумкин.

Ушбу дастурда компьютер тармоқларининг турлари, компьютер тармоқлари протоколлари, мультимедиали тармоқ технологиялари, SMART – технологиялари, IoT - буюмлар интернети хусусиятлари, криптография усуллари, очиқ калитли шифрлаш, хеш функция, киберхавфсизик вазифалари, киберхавфсизлик сиёсати баён этилган.

Модулнинг мақсади ва вазифалари

“**Компьютер тармоқлари хавфсизлиги**” **модулининг мақсад ва вазифалари:**

– тингловчиларга компьютер тармоқларида хавфсизликни таъминлаш билан боғлиқ масалаларни ечишда ахборот-коммуникация тизимларида ахборотларни ҳимоялаш технологияларининг ўрни ва истиқболли йўналишлари профилига мос билим, кўникма ва малакани таълим стандартида талаб қилинган билимларни шакллантиришдир;

– компьютер тармоқларида хавфсизликтушунчаси, уни қўлланиш соҳаси ҳамда ахборот хавфсизлигини таъминлаш чора тадбирлари, усуллари ва воситаларини таҳлил қилиб улар асосида ахборотни ҳимоялаш қобилиятларини эгаллаш;

– компьютер тармоқлари ва тизимини самарали ҳимоялаш усул ва воситасини таҳлил қилишдан иборатдир.

Модул бўйича тингловчиларнинг билими, кўникмаси, малакаси ва компетенцияларига қўйиладиган талаблар

“**Компьютер тармоқлари хавфсизлиги**” курсини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида**:**

Тингловчи:

- компьютер тармоқларининг турлари, компьютер тармоқлари протоколлари, мультимедиали тармоқ технологиялари, SMART – технологиялари, IoT - буюмлар интернети хусусиятлари, криптография усуллари, очиқ калитли шифрлаш, хеш функция, киберхавфсизик вазифалари, киберхавфсизлик сиёсати ҳақида **билимларга** эга бўлиши лозим;
- компьютер тармоқларида ахборотни ҳимоя қилиш, тармоқда маълумотлар хавфсизлигининг ускунавий ва дастурий таъминотлари билан ишлаш, IoT - буюмлар интернети соҳасида хавфсизликни таъминлаш **кўникмаларини** эгаллаши лозим;
- компьютер тармоқларида ахборот хавфсизлигини ва киберхавфсизлик сиёсатини бошқариш **малакаларини** эгаллаши лозим;
- ҳимояланган компьютер тизимлари ва тармоқларини қуриш концепцияси асосида ахборот хавфсизлигини бошқариш **компетенцияларни** эгаллаши лозим.

Модулни ташкил этиш ва ўтказиш бўйича тавсиялар

“**Компьютер тармоқлари хавфсизлиги**” курси маъруза ва амалий машғулотлар шаклида олиб борилади.

Курсни ўқитиш жараёнида таълимнинг замонавий методлари, педагогик технологиялар ва ахборот-коммуникация технологиялари қўлланилиши назарда тутилган:

– маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион ва электрон-дидактик технологиялардан;

– ўтказиладиган амалий машғулотларда техник воситалардан, экспресс-сўровлар, тест сўровлари, ақлий ҳужум, гуруҳли фикрлаш, кичик гуруҳлар билан ишлаш, коллоквиум ўтказиш ва бошқа интерактив таълим усулларини қўллаш назарда тутилади.

Модулнинг ўқув режадаги бошқа модуллар билан боғлиқлиги ва узвийлиги

“**Компьютер тармоқлари хавфсизлиги**” модули мазмуни ўқув режадаги “Булутли ҳисоблаш технологиялари“ модули мазмуни ўқув режадаги “Компьютер инжиниринги”, “Катта маълумотларни қайта ишлаш усул ва воситалар”, ўқув модуллари билан узвий боғланган ҳолда педагогларнинг ахборот хавфсизлиги бўйича касбий педагогик тайёргарлик даражасини оширишга хизмат қилади.

Модулнинг олий таълимдаги ўрни

Модулни ўзлаштириш орқали тингловчилар ахборот хавфсизлигидаги таҳдид ва ҳужумларни таҳлил қилиш, ахборотни шифрлаш ва дешифрлашни ўрганиш, амалда қўллаш ва ахборотни ҳимояланганлигини баҳолашга доир касбий компетентликка эга бўладилар.

Модул бўйича соатлар тақсимоти

№	Модуль мавзулари	Аудитория уқув юкламаси			
		Жами	жумладан		
			Назарий	Амалий машғулот	Кўчма машғулоти
1.	Компьютер тармоқларининг турлари. Компьютер тармоқлари протоколлари. Мультимедиали тармоқ технологиялари.	2	2		
2.	SMART – технологиялар. IoT - буюмлар интернети. IoT - буюмлар интернети соҳасида хавфсизлик масалалари.	2	2		
3	Компьютер тармоқларида ахборотни ҳимоя қилиш усуллари. Криптография усуллари. Симметрик криптотизимлар. Очиқ калитли шифрлаш. Хеш функция.	2	2		
4	Тармоқда маълумотлар хавфсизлигининг ускунавий ва дастурий таъминоти.	2	2		
5	Киберхавфсизик вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш.	2	2		
6	Шифрлаш алгоритмлари.	4		4	
7	Тармоқлараро экран.	4		4	
8	Тармоқларда ахборот хавфсизлиги	4		4	
	Жами:	**22**	**10**	**12**	**0**

НАЗАРИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-маъруза. Компьютер тармоқларининг турлари. Компьютер тармоқлари протоколлари. Мультимедиали тармоқ технологиялари (2 соат).

Компьютер тизимлари ва тармоқлари ҳақида умумий тушунчалар. Компьютер тармоқларининг классификацияси (таснифланиши). OSI эталон модели. TCP/IP эталон модели. Мультимедиали тармоқ технологиялари.

2-маъруза. SMART – технологиялар. IoT - буюмлар интернети. IoT - буюмлар интернети соҳасида хавфсизлик масалалари. (2 соат).

SMART – технологиялар ва IoT (Internet of things) – буюмлар интернети замонавий тармоқ хизматлари сифатида. LPWAN технологияси. NB-IoT технологияси. IoT - буюмлар интернети соҳасида хавфсизлик масалалари

3-маъруза. Компьютер тармоқларида ахборотни ҳимоя қилиш усуллари. Криптография усуллари. Симметрик криптотизимлар. Очиқ калитли шифрлаш. Хеш функция. (2 соат).

Тармоқда ахборотни ҳимоя қилишнинг асосий воситалари. Криптография усуллари. Симметрик криптотизимлар. Очиқ калитли шифрлаш. Хеш функция.

4-маъруза. Тармоқда маълумотлар хавфсизлигининг ускунавий ва дастурий таъминоти. (2 соат).

Ipsec (Internet protocol security) хавфсизлик протоколи. VPN (Virtual Private Network) виртуал хусусий тармоқ. Ахборот тармоғи хавфсизлиги қурилмалар ва дастурий таъминоти. Тармоқлараро экраннинг пакетларни филтрлаш қоидалари.

5-маъруза. Киберхавфсизик вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш. (2 соат).

Киберхавфсизликнинг фундаментал тушунчалари. Киберхавфсизлик сиёсати ва уни бошқариш. Хавф-хатарларни бошқариш. Ҳужум инцидентлари ва уларга қарши реакция.

АМАЛИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-амалий машғулот. Шифрлаш алгоритмлари. (4 соат)

Содда симметрик шифрлаш усуллари. Цезар усули. Ўрин алмаштириш шифрлари. Ўрнига қўйиш шифрлари. Частотавий таҳлил усули. Замонавий шифрлаш алгоритмлари. DES шифрлаш стандарти. RSA очиқ калитли шифрлаш усули. Оқимли шифрлаш усуллари. A5/1 оқимли шифрлаш алгоритми.

2-амалий машғулот. Тармоқлараро экран (4 соат)

Тармоқлараро экран технологияси. Тармоқ ҳимоясида тармоқлараро экран воситаларидан фойдаланиш. Тармоқлараро экран турлари. Тармоқлараро экран воситаларини ўрнатиш ва созлаш. Янги қоидалар яратиш. Тизимни назоратлаш.

3-амалий машғулот. Тармоқларда ахборот хавфсизлиги (4 соат).

TCP/IP протоколида мавжуд заифликлар. SSL тармоқ протоколи ва унинг вазифаси. Ўртага турган одам ҳужуми. SSL протоколини созлаш. X.509 сертификати. Симсиз тармоқда мавжуд заифликлар. Симсиз тармоқда фойдаланилган хавфсизлик протоколлари. WEP протоколи. WPA ва WPA2 протоколлари. Симсиз тармоқлардан фойдаланишда бериладиган хавфсизлик тавсиялари.

ЎҚИТИШ ШАКЛЛАРИ

Мазкур модул бўйича қуйидаги ўқитиш шаклларидан фойдаланилади:

- маърузалар, амалий машғулотлар (маълумотлар ва технологияларни англаб олиш, ақлий қизиқишни ривожлантириш, назарий билимларни мустаҳкамлаш);
- давра суҳбатлари (кўрилаётган лойиҳа ечимлари бўйича таклиф бериш қобилиятини ошириш, эшитиш, идрок қилиш ва мантиқий хулосалар чиқариш);
- баҳс ва мунозаралар (лойиҳалар ечими бўйича далиллар ва асосли аргументларни тақдим қилиш, эшитиш ва муаммолар ечимини топиш қобилиятини ривожлантириш).

II БЎЛИМ

МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

II. МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

«Блум кубиги» методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билиимларни ўзлаштирилишини енгиллаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун “Очиқ” саволлар тузиш ва уларга жавоб топиш машқи вазифасини белгилайди.

Методни амалга ошириш тартиби:

1. Ушбу методни қўллаш учун, оддий куб керак бўлади. Кубнинг ҳар бир томонида қўйидаги сўзлар ёзилади:
   - **Санаб беринг, таъриф беринг (оддий савол)**
   - **Нима учун (сабаб-оқибатни аниқлаштировчи савол)**
   - **Тушинтириб беринг (муаммони ҳар томонлама қараш саволи)**
   - **Таклиф беринг (амалиёт билан боғлиқ савол)**
   - **Мисол келтиринг (ижодкорликни ривожлантировчи савол)**
   - **Фикр беринг (таҳлил килиш ва бахолаш саволи)**

2. Ўқитувчи мавзуни белгилаб беради.

3. Ўқитувчи кубикни столга ташайди. Қайси сўз чиқса, унга тегишли саволни беради.

“KWHL” методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билиимларни тизимлаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун мавзу бўйича қўйидаги жадвалда берилган саволларга жавоб топиш машқи вазифасини белгилайди.

Изоҳ. *KWHL:*
Know – нималарни биламан?
Want – нимани билишни хоҳлайман?
How - қандай билиб олсам бўлади?
Learn - нимани ўрганиб олдим?.

“KWHL” методи	
1. Нималарни биламан: -	***2. Нималарни билишни хоҳлайман, нималарни билишим керак:*** -
3. Қандай қилиб билиб ва топиб оламан: -	***4. Нималарни билиб олдим:*** -

“W1H” методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билиимларни тизимлаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун мавзу бўйича қўйидаги жадвалда берилган олтита саволларга жавоб топиш машқи вазифасини белгилайди.

What?	Нима? (таърифи, мазмуни, нима учун ишлатилади)	
Where?	Қаерда (жойлашган, қаердан олиш мукин)?	
What kind?	Қандай? (параметрлари, турлари мавжуд)	
When?	Қачон? (ишлатилади)	
Why?	Нима учун? (ишлатилади)	
How?	Қандай қилиб? (яратилади, сақланади, тўлдирилади, таҳрирлаш мумкин)	

“SWOT-таҳлил” методи.

Методнинг мақсади: мавжуд назарий билимлар ва амалий тажрибаларни таҳлил қилиш, таққослаш орқали муаммони ҳал этиш йўлларни топишга, билимларни мустаҳкамлаш, такрорлаш, баҳолашга, мустақил, танқидий фикрлашни, ностандарт тафаккурни шакллантиришга хизмат қилади.

S – (strength)	• кучли томонлари
W – (weakness)	• заиф, кучсиз томонлари
O – (opportunity)	• имкониятлари
T – (threat)	• хавфлар

“BEEP” методи

Методнинг мақсади: Бу метод мураккаб, кўптармоқли, мумкин қадар, муаммоли характеридаги мавзуларни ўрганишга қаратилган. Методнинг моҳияти шундан иборатки, бунда мавзунинг турли тармоқлари бўйича бир хил ахборот берилади ва айни пайтда, уларнинг ҳар бири алоҳида аспектларда муҳокама этилади. Масалан, муаммо ижобий ва салбий томонлари, афзаллик, фазилат ва камчиликлари, фойда ва зарарлари бўйича ўрганилади. Бу интерфаол метод танқидий, таҳлилий, аниқ мантиқий фикрлашни муваффақиятли ривожлантиришга ҳамда ўқувчиларнинг мустақил ғоялари, фикрларини ёзма ва оғзаки шаклда тизимли баён этиш, ҳимоя қилишга имконият яратади. “Beep” методидан маъруза машғулотларида индивидуал ва жуфтликлардаги иш шаклида, амалий ва семинар машғулотларида кичик гуруҳлардаги иш шаклида мавзу юзасидан билимларни мустаҳкамлаш, таҳлили қилиш ва таққослаш мақсадида фойдаланиш мумкин.

Методни амалга ошириш тартиби:

тренер-ўқитувчи иштирокчиларни 5-6 кишидан иборат кичик гуруҳларга ажратади;

тренинг мақсади, шартлари ва тартиби билан иштирокчиларни таништиргач, ҳар бир гуруҳга умумий муаммони таҳлил қилиниши зарур бўлган қисмлари туширилган тарқатма

ҳар бир гуруҳ ўзига берилган муаммони атрофлича таҳлил қилиб, ўз мулоҳазаларини тавсия этилаётган схема бўйича тарқатмага ёзма баён қилади;

навбатдаги босқичда барча гуруҳлар ўз тақдимотларини ўтказадилар. Шундан сўнг, тренер томонидан таҳлиллар умумлаштирилади, зарурий ахборотлр билан тўлдирилади ва мавзу якунланади.

Муаммоли савол					
1-усул		**2-усул**		**3-усул**	
афзаллиги	камчилиги	афзаллиги	камчилиги	афзаллиги	камчилиги
Хулоса:					

“Кейс-стади” методи

«Кейс-стади» - инглизча сўз бўлиб, («case» – аниқ вазият, ҳодиса, «stadi» – ўрганмоқ, таҳлил қилмоқ) аниқ вазиятларни ўрганиш, таҳлил қилиш асосида ўқитишни амалга оширишга қаратилган метод ҳисобланади. Мазкур метод дастлаб 1921 йил Гарвард университетида амалий вазиятлардан иқтисодий бошқарув фанларини ўрганишда фойдаланиш тартибида қўлланилган. Кейсда очиқ ахборотлардан ёки аниқ воқеа-ҳодисадан вазият сифатида таҳлил учун фойдаланиш мумкин.

“Кейс методи” ни амалга ошириш босқичлари

Иш босқичлари	Фаолият шакли ва мазмуни
1-босқич: Кейс ва унинг ахборот таъминоти билан таништириш	✓ якка тартибдаги аудио-визуал иш; ✓ кейс билан танишиш(матнли, аудио ёки медиа шаклда); ✓ ахборотни умумлаштириш; ✓ ахборот таҳлили; ✓ муаммоларни аниқлаш
2-босқич: Кейсни аниқлаштириш ва ўқув топшириғни белгилаш	✓ индивидуал ва гуруҳда ишлаш; ✓ муаммоларни долзарблик иерархиясини аниқлаш; ✓ асосий муаммоли вазиятни белгилаш
3-босқич: Кейсдаги асосий муаммони таҳлил этиш орқали ўқув топшириғининг ечимини излаш, ҳал этиш йўлларини ишлаб чиқиш	✓ индивидуал ва гуруҳда ишлаш; ✓ муқобил ечим йўлларини ишлаб чиқиш; ✓ ҳар бир ечимнинг имкониятлари ва тўсиқларни таҳлил қилиш; ✓ муқобил ечимларни танлаш
4-босқич: Кейс ечимини ечимини шакллантириш ва асослаш, тақдимот.	✓ якка ва гуруҳда ишлаш; ✓ муқобил вариантларни амалда қўллаш имкониятларини асослаш; ✓ ижодий-лойиҳа тақдимотини тайёрлаш; ✓ якуний хулоса ва вазият ечимининг амалий аспектларини ёритиш

“Ассесмент” методи

Методнинг мақсади: мазкур метод таълим олувчиларнинг билим даражасини баҳолаш, назорат қилиш, ўзлаштириш кўрсаткичи ва амалий кўникмаларини текширишга йўналтирилган. Мазкур техника орқали таълим олувчиларнинг билиш фаолияти турли йўналишлар (тест, амалий кўникмалар, муаммоли вазиятлар машқи, қиёсий таҳлил, симптомларни аниқлаш) бўйича ташҳис қилинади ва баҳоланади.

Методни амалга ошириш тартиби:

“Ассесмент”лардан маъруза машғулотларида талабаларнинг ёки қатнашчиларнинг мавжуд билим даражасини ўрганишда, янги маълумотларни баён қилишда, семинар, амалий машғулотларда эса мавзу ёки маълумотларни ўзлаштириш даражасини баҳолаш, шунингдек, ўз-ўзини баҳолаш мақсадида индивидуал шаклда фойдаланиш тавсия этилади. Шунингдек, ўқитувчининг ижодий ёндашуви ҳамда ўқув мақсадларидан келиб чиқиб, ассесментга қўшимча топшириқларни киритиш мумкин.

Ҳар бир катакдаги тўғри жавоб 5 балл ёки 1-5 балгача баҳоланиши мумкин.

Тест	**Муаммоли вазият**
Тушунча таҳлили (симптом)	**Амалий вазифа**

“Инсерт” методи

Методни амалга ошириш тартиби:

➢ ўқитувчи машғулотга қадар мавзунинг асосий тушунчалари мазмуни ёритилган матнни тарқатма ёки тақдимот кўринишида тайёрлайди;

➢ янги мавзу моҳиятини ёритувчи матн таълим олувчиларга тарқатилади ёки тақдимот кўринишида намойиш этилади;

➢ таълим олувчилар индивидуал тарзда матн билан танишиб чиқиб, ўз шахсий қарашларини махсус белгилар орқали ифодалайдилар. Матн билан ишлашда талабалар ёки қатнашчиларга қуйидаги махсус белгилардан фойдаланиш тавсия этилади:

Белгилар	Матн
“V” – таниш маълумот.	
“?” – мазкур маълумотни тушунмадим, изоҳ керак.	
“+” бу маълумот мен учун янгилик.	
“– ” бу фикр ёки мазкур маълумотга қаршиман?	

Белгиланган вақт якунлангач, таълим олувчилар учун нотаниш ва тушунарсиз бўлган маълумотлар ўқитувчи томонидан таҳлил қилиниб, изоҳланади, уларнинг моҳияти тўлиқ ёритилади. Саволларга жавоб берилади ва машғулот якунланади.

III БЎЛИМ

НАЗАРИЙ МАТЕРИАЛЛАР

III. НАЗАРИЙ МАТЕРИАЛЛАР

1-маъруза. Компьютер тармоқларининг турлари. Компьютер тармоқлари протоколлари. Мультимедиали тармоқ технологиялари. (2 соат)

Режа:

1.1. Компьютер тизимлари ва тармоқлари ҳақида умумий тушунчалар.
1.2. Компьютер тармоқларининг классификацияси (таснифланиши).
1.3. OSI эталон модели.
1.4. TCP/IP эталон модели.
1.5. Мультимедиали тармоқ технологиялари.

Таянч иборалар: *компьютер тизимлари, компьютер тармоқлари, OSI эталон модели, TCP/IP эталон модели, мультимедиали тармоқ технологиялари, RTVC сервиси, видеоконференция, H.32x стандарти, H.323 стандарти.*

1.1. Компьютер тизимлари ва тармоқлари ҳақида умумий тушунчалар.

Компьютер тизими (КТ) деганда – ахборотни ўлчаш, унинг шаклини ўзгартириш ва ишлаш учун мўлжалланган, функционал жиҳатидан бирлаштирилган ҳамда истъемолчига, яъни фойдаланувчига у талаб қиладиган кўринишда ахборотни (маълумотни) тақдим этадиган тизим тушунилади. Компьютер тизимлари – ўлчаш, ҳисоблаш ва бошқа ёрдамчи техник воситалар мажмуасидан иборат бўлади.

Компьютер тизимини қуришдан мақсад – бирор-бир жараённи мантиқий бошқариш вазифасини амалга ошириш, техник диагностика вазифалари, тасвирларни ишлаш ва кўпгина бошқа-бошқа вазифалардан бирини ёки бир нечтасини амалга ошириш ҳисобланади.

Компьютер тизимларининг бир-нечта белгиларига асосан қуйидагича умумлаштирилган классификациясини келтирамиз:

1. Қўлланиладиган соҳасига қараб – саноатда, тижоратда, молия ва маркетинг соҳаларидаги компьютер тизимлари.

2. Бошқариладиган объектнинг хилига қараб – корхонадаги технологик жараёнларни бошқариш учун мўлжалланган КТлари, лойиҳалашни автоматлаштириш учун мўлжалланган КТлари ва корхонани бошқариш учун мўлжалланган КТлари.

3. Натижавий ахборотни қандай қўлланилишига қараб:

- ахборот-қидирув тизимлари, улар ахборотни йиғиш, сақлаш ҳамда фойдаланувчининг сўровига қараб керакли маълумотларни топиб бериш вазифаларини бажаради;
- ахборот-маслаҳат берувчи тизимлар, улар фойдаланувчига қарорлар қабул қилиш учун тавсиялар бериш вазифасини бажаради;
- ахборот-бошқариш тизимлари, улар бошқариш учун керак бўладиган маълумотларни етказиб бериш вазифасини бажаради.

Компьютер тизимларини бошқариш – марказлаштирилган ва марказлаштирилмаган тарзда амалга оширилади. Компьютер тизимларининг

воситалари – бир жойга тўпланган ҳолда, ёйилган ҳолда, маълумотларни бир сатҳли ишлаш воситалари сифатида ва кўп сатҳли ишлаш воситалари сифатида қурилади.

Компьютер тармоғи (Computer NetWork, net – тармоқ ва work - иш) – бу Компьютерлар ўртасида ахборотлар алмашинуви тизимидир.

Компьютер тармоғи – бу иккита ёки ундан кўпроқ компьютерларнинг ва бошқа қурилмаларнинг бир бирига узатиш муҳити ёрдамида ўзаро боғланган тармоқдир.

Компьютер (ҳисоблаш) тармоғи – алоқа каналлари ёрдамида маълумотларни тармоқланган қайта ишлашнинг ягона тизимига уланган Компьютерлар ва терминаллар тўплами бўлиб, у кўп машинали бирлашманинг энг юқори шаклидир.

Компьютер тармоғи "тармоқ абоненти", "станция" ва "физик узатиш муҳити" каби таркибий қисмлардан ташкил топган бўлади.

1. Тармоқ абоненти тармоқда ахборотни юзага келтирувчи ёки уни истеъмол қилувчи об`ектдир.

2. Станция – ахборот узатиш ва қабул қилиш билан боғлиқ вазифаларни бажарувчи об`ектдир.

Алоҳида компьютерлар, компьютер мажмуалари, терминаллар, саноат роботлари, программавий бошқарувли дастгоҳлар ва шу кабилар тармоқ абонентлари бўлишлари мумкин ва хар бир абонент станцияга уланади.

Абонент ва станция биргаликда "абонент тизими“ деб аталади. Абонентларнинг ўзаро алоқасини ташкил этиш учун физик узатиш муҳити мавжуд бўлиши керак.

3. Физик узатиш муҳити – электр, радио ёки бошқа сигналлар ёрдамида амалга ошириладиган алоқа канали ва маълумотларни узатиш, қабул қилиш қурилмаларидир.

Физик узатиш муҳити негизида абонент тизимлари ўртасида ахборот узатишни таъминловчи коммуникасион тармоқ ташкил этилади. Бундай ёндашув ҳар қандай компьютер тармоғини абонент тизимлари ва коммуникасион тармоқ йиғиндиси сифатида кўриш имконини беради.

Компьютерларни бир-бири билан боғлашда икки хил усулдан фойдаланилади:

- кабел ёрдамида боғлаш. Бунда компьютерлар бир-бири билан коаксиал, жуфтли ўрамли ва шиша толали кабеллар орқали махсус тармоқ платаси ёрдамида боғланади.

- симсиз боғланиш. Бунда Компьютерлар бир-бири билан симсиз алоқа воситалар ёрдамида, яъни радио тўлқинлар, инфрақизил нурлар, WiFi ва Bluetooth технологиялари ёрдамида боғланади.

1.2. Компьютер тармоқларининг классификацияси (таснифланиши)

Компьютер тармоқлари қуйидаги белгилари бўйича таснифланади:

1. География (ҳудудий) жойлашуви бўйича;
2. Ишлаб чиқариш бўлимларининг миқёси бўйича;
3. Бошқариш усули бўйича;
4. Ахборотни узатиш тезлиги бўйича;
5. Алоқа (уланиш) топологияси тузулиши бўйича.

Компьютер тармоқлари географик (ҳудудий) жойлашуви бўйича

қуйидагиларга бўлинади:

PAN – (PERSONAL- AREA NETWORK) – шахсий тармоқ бўлиб, бу компьютер қурилмаларининг симсиз тармоғи.

LAN (LOCAL-AREA NETWORK) - Локал тармоқ чегараланган соҳадаги компьютерларни бирлаштириш имкониятини беради.

CAN (CAMPUS-AREA NETWORK) - Кампус тармоқ, ўзаро яқин биноларда жойлашган локал тармоқларни бирлаштириш учун мўлжалланган.

MAN (METROPOLITAN AREA NETWORK) – шаҳар каби катталикдаги географик минтақани қамраб олган алоқа тармоғи. MAN лардан фойдаланишдан мақсад узоқ масофалада телефон симларини тарқатишни олдини олишдан иборат. Уяли телефон тизимлари асосан МАНлардан иборат.

WAN (WIDE AREA NETWORK) – давлат каби йирик географик ҳудудни ўз ичига олади. Уларга Tymnet, TeleNet, UniNet, AccuNet ларни мисол келтириш мумкин. Интернет тармоғи минглаб WAN ларни бирлаштиради. Албатта, кўпгина телефон тизимлари ҳам WAN лардан иборат.

GAN (Global-Area Network) - барча давлатлар ва континентларни бирлаштирувчи ҳамда ер шарининг ихтиёрий нуқтасидаги ахборот ресурсларига мурожаат қилиш имкониятини берувчи умумпланетар тармоқ.

Ишлаб чиқариш, ташкилот миқёси бўйича тармоқлар қуйидача фарқланади:

Бўлимлар тамоғи;

Кампуслар тармоғи;

Ташкилот, компания тармоқлари.

Коорпоратив тармоқ асосан маълум корхонанинг ўзи ва унинг ходимларига хизмат кўрсатиб, ўз тармоғига эгалик қилади. Корпоратив тармоқ ҳар – хил ўлчовлик бўлиб катта корхона тармоғида ўз локал тармоғи ва глобал тармоқ билан уланган бўлиши мумкин.

Корпоратив тармоқ 3 турга бўлинади – бўлим тармоғи, бино ёки кампус тармоғи, корхона кенглигидаги тармоқ.

Бўлим тармоғи – бу тармоқ солиштирганда катта бўлмаган хизматчилар гуруҳи бўлиб, корхонанинг бир бўлимда ишловчи ва умумий вазифани (ҳисобхона, маркетинг) бажарувчилардир. Одатда хизматчилар сони 30 дан ошмаган бўлиб, бундай локал тармоқда умумий маълумотлардан фойдаланилади: маълумотлар, иловалар, модем ва лазерли принтерлардир.

Бино тармоғи – корхонанинг ҳар – хил бўлимларини бир корхона ва бинолар чегарасида умумлаштирувчи тармоқдир.

Кампус тармоғи – бир ҳудудда бир неча кв/км майдонни эгаллаб, тармоқ иреархия асосида ўзининг магистр каналларига эга бўлади.

Корхонанинг асосий вазифаси тармоқ кесимида информацион хизматларни кўрсатиш ҳисобланади. Алоқа оператор тармоғи информацион хизматларни кўрсатмаслиги мумкин, сабаби фойдаланувчиларнинг Компьютерлари операторнинг хизмат кўрсатиш зонасидан ташқарида бўлганлиги учун.

Корхонанинг тармоқ ўлчами инфокоммуникация мисолида бўлиб, у телекоммуникация муҳитида «оролча» локал тармоқ ҳисобланади. Фойдаланувчилар ва уларнинг Компьютерлари минглаб бўлиши, серверлар сони юзлаб бўлиши мумкин. Буларнинг ажралиб турадиган ҳусусиятлари:

Катта масофа – узоқда жойлашган LAN ва компьютерни улаш учун ҳар – хил

телекоммуникация воситалари қўлланилади – бирламчи тармоқ каналлари сони , радиоканаллар, сунъий йўлдош алоқаси.

Юқори даражадаги ҳар хиллиги (гетрогенност) – ҳар хил турдаги компьютерлар (Main Fraim to PC) ОС ларнинг ҳар хил иловалари.

Бошқариш усуллари бўйича тармоқлар қуйидагича бўлиши мумкин:

“Мижоз – сервер” тармоқлари;

– Мижоз – бу тармоққа сўровлар берувчи (Компьютер ёки дастур) объектдир. Ёки бошқача айтганда Мижоз - бу тармоқни абоненти бўлиб, фақат тармоқ ресурсларидан фойдаланади, я`ни тармоқ унга хизмат қилади.

– Сервер – бу тармоққа хизмат кўрсатувчи (Компьютер ёки дастур) об`ект. Ёки бошқача айтганда Сервер- бу тармоқни абоненти бўлиб, бошқа абонентларга ўзининг ресурсларини тақдим этади, ўзи эса бошқа абонентларни ресурсларидан фойдаланмайди, яъни фақат тармоқга хизмат қилади.

“Peer–to Peer” (тенг ҳуқуқли) тармоқлар бир рангли тармоқлар, яни тармоқдаги барча Компьютерлар бир хил кириш ва ресурслар ҳуқуқига эга.

Ахборотларни узатиш тезлиги бўйича (нисбий!):

Маълумотларни узатишнинг кичик тезлиги– бунда маълумотларни узатиш тезлиги 10 дан 100 гача килобит бўлади;

Маълумотларни узатишнинг ўртача тезлиги– бунда маълумотларни узатиш тезлиги, бирдан бир неча ўнлаб мегабит диапазонда бўлади;

Маълумотларни узатишнинг юқори тезлиги– бунда маълумотларни узатиш тезлиги 100 дан юқори мегабит ва гегабит диапазонда бўлади.

Территориал соҳаси асосида тармоқлар иерархияси:

1. Магистрал тармоқлар сатҳлари
2. Шаҳар маштабидаги тармоқлар сатҳлари
3. Локал тармоқлар сатҳлари

1.1-жадвал

Компьютер тармоқлари таснифи ва ҳусусиятлари

Масофа бўйича тартибланиши	Жойлашуви	Синф
1 м	Бир киши атрофидаги ҳудуд	(PAN) Шахсий тармоқ
10 м	Хона (синф)	(LAN) Локал тармоқ
100 м	Бино	(LAN) Локал тармоқ
1 км	Шаҳар тумани	(LAN) Локал тармоқ
10 км	Шаҳар	(MAN) Шаҳар миқёсидаги тармоқ
100 км	Континент	(WAN) кенг миқёсидаги тармоқ
10000 км ва ундан ортиқ	Планета	(GAN) Интернет

Бу тармоқ турлари турли компьютерлар, сақлаш ва коммуникация қурилмаларини ўз ичига олиши мумкин. Шахсий тармоқ (PAN) – бу Компьютер қурилмаларининг симсиз тармоқ Bluetooth технологияси ёрдамида ўзаро боғланиши тушунилади. PAN тармоғи қисқа масофада ахборот алмашинувчи яна бир технология RFID смарт-карт ёрдамида ҳам амалга оширилиши мумкин.

Тармоқ коммутация усули қуйидагича фарқланади:

пакетли коммутация тармоғи, бу иккига бўлинади: датаграмм тармоқ (Ethernet), мантиқий уланишга асосланган – IP тармоқ, транспорт поғонасида TCP протоколи қўлланилади;

виртуал каналга асосланган тармоқ (MPLS - тармоқ);

коммутация канал тармоғи – мисол учун, телефон тармоғи 64 к\бит сек.га асосланган.

1.3. OSI эталон модели.

OSI эталон модели стандартлаштириш бўйича халқаро ташкилотнинг (OSI - International Standards Organization) ривожланишига асосланади ва турли даражаларда ишлатиладиган протоколларни халқаро стандартлаштириш йўлидаги биринчи қадамдир (Дай ва Зиммерман, 1983). Кейин 1995 йилда қайта кўриб чиқилган (Дай, 1995). Ушбу структура очиқ ISO тизимларининг ўзаро таъсири учун мос ёзувлар модели деб номланади. ISO OSI (Open System Interconnection) алоқа модели, чунки у очиқ тизимларни, яъни бошқа тизимлар билан алоқа қилиш учун очиқ бўлган тизимларни бирлаштиради.

OSI модели етти қатламга эга. Бундай тузилманинг пайдо бўлиши қуйидаги мулоҳазалар билан боғлиқ:

Алоҳида мавҳумлик даражаси учун зарур бўлган даражани яратиш керак.

Ҳар бир даража қатъий белгиланган функцияни бажариши керак.

Ҳар бир даража учун функцияларни танлаш стандарт халқаро протоколларни яратишни ҳисобга олган ҳолда амалга оширилиши керак.

Сатҳлар орасидаги чегаралар интерфейслар орасидаги маълумот оқими минимал бўлиши учун танланиши керак.

Архитектура катта ҳажмга эга бўлмаслиги учун турли хил функциялар бир даражага кераксиз равишда бирлаштирилмаслиги учун даражалар сони етарлича катта бўлиши керак.

OSI модели билан танишиш тармоқда рўй бераётган жараённи яхши тушунишга ёрдам беради. Ҳамма тармоқдаги бажариладиган вазифалар (функциялар) моделда 7 та босқичга бўлинган (1.1-расм). Юқори ўриндаги бос қичлар анча мураккаб, глобал масалаларни бажарадилар. Бунинг учун пасдаги босқичларни ўз мақсадлари учун ишлатиб уларни бошқарадилар. Пастда жойлашган босқичларнинг мақсади – юқорида босқичга хизмат кўрсатиш, юқори жойлашган босқичлар учун кўрсатиладиган бу хизматнинг майда қисмларининг бажарилиш тартиби муҳим эмас.

7. Amaliy bosqich
6. Prezentatsiya bosqichi
5. Aloqa vaqtining bosqichi
4. Transpor bosqich
3. Tarmoqli bosqich
2. Kanalli bosqich
1. Jismoniy bosqich

1.1-расм. OSI моделининг етти босқичи.

Пастда жойлашган босқичлар анча содда, анча аниқ вазифаларни бажаради. Идеал ҳолда ҳар бир босқич ўзидан тепадаги ва пастдаги босқич билан мулоқот қилади. Юқори босқич айни вақтда иловага ишлаётган, амалий масалага тўғри келса, пастки босқич эса сигнални алоқа канали орқали узатишга тўғри келади. 1.2-расмда келтирилган босқичлар вазифаси тармоқ абонентларининг ҳар бири томонидан бажарилади.

Бир абонентдаги ҳар бир босқич шундай ишлайдики у бошқа абонентнинг худди шу босқичи билан тўғри алоқаси бордек, яъни тармоқ абонентларининг бир хил номли босқичлари ўртасида виртуал алоқа мавжуд. Бир тармоқ абонентлари ўртасидаги реал алоқа фақат энг паст биринчи босқичда мавжуд (жисмоний босқич). Ахборот узатаётган абонентда ахборот барча босқичлардан юқоридан бошлаб пастдаги босқичда тугайди. Қабул қилувчи абонентда эса қабул қилинган ахборот тескари йўналишда, пастки босқичдан бошлаб юқори босқичга ҳаракат қилади (1.2-расм).

Амалий босқич (Application, прикладной уровень) ёки иловалар босқичи, у қуйидаги хизматларни амалга оширади: фойдаланувчининг иловасини шахсан тасдиқлайди, масалан, файллар узатишнинг дастурий воситалари, ахборотлар базаси билан боғланиш, электрон почта воситалари, серверда қайд қилиш хизмати. Бу босқич қолган 6 та босқични бошқаради.

1.2-расм. Ахборотни абонентдан абонентга ўтиш йўли.

Тақдимот (Презентация) босқичи (Presentation, презентативный уровен) ёки ахборотни таништириш босқичи, бу босқичда ахборотни аниқланади ва ахборот форматини кўриниш синтаксисини тармоққа қулай равишда ўзгартиради, яъни таржимон вазифасини бажаради. Шу ерда ахборот шифрланади ва

дишифрацияланади, лозим бўлган тақдирда уларни зичлаштирилади.

Алоқа ўтказиш вақтини бошқариш босқичи (Session, сеансовый уровень) алоқа ўтказиш вақтини бошқаради (яъни алоқани ўрнатади, тасдиқлайди ва тамомлайди). Бу босқичда абонентларни мантиқий номларини таниш, уларга боғланиш ҳуқуқини назорат қилиш вазифалари ҳам бажарилади.

Транспорт босқичи (Transport) пакетни хатосиз ва йўқотмасдан, керакли кетма-кетликда етказиб беришни амалга оширади. Шу ерда яна узатилаётган ахборотларни пакетга жойлаш учун блокларга тақсимланади ва қабул қилинган ахборотни қайта тикланади.

Тармоқ босқичи (Network, сетевой уровень) бу босқич пакетларни манзиллаш, мантиқий номларни жисмоний тармоқ манзилига ўзгартириш, тескарига ҳам ва шунингдек, пакетни керакли абонентга жўнатиш йўналишини танлашга (агарда тармоқда бир неча йўналиш мавжуд бўлса) жавобгар.

Канал босқичи ёки узатиш йўлини бошқариш босқичи (дата линк), бу босқич стандарт кўринишдаги пакет тузишга бошлаш ҳамда тамом бўлишни бошқариш майдонини пакет таркибига жойлашишига жавобгардир. Шу ерда яна тармоқ боғланиш, узатишдаги хатоликларни аниқлаш ва яна қабул қилиш қурилмасига хато узатилган пакетларни қайтатдан узатишни бошқариш амалга оширилади.

Жисмоний босқич (Physical, физический уровень) – бу моделни энг қуйи босқичи бўлиб, узатилаётган ахборотни сигнал катталигига кодлаштиради, узатиш муҳитига қабул қилишни ва тескари кодлашни амалга оширишга жавоб беради. Шу ерда яна уланиш мосламаларига, разъемларга, электр бўйича мослаштириш ва ерга уланиш ҳамда тўсиқлардан ҳимоя қилиш ва ҳоказоларга талаблар аниқланади. Моделни қуйи икки босқичининг (1 ва 2) вазифасини одатда қурилмалар бажаради (2 босқич вазифасини бир қисмини тармоқ адаптерининг дастурий драйвери бажаради). Айнан шу босқичларда тармоқ топологияси, узатиш тезлиги, ахборот алма шишни бошқариш усули ва пакет формати (ўлчами) яъни тармоқ турига тўғри тааллуқли кўрсаткичлар аниқланади (Ethernet, Token-Ring, FDDI). Юқори босқичлар тўғридан-тўғри бирор аниқ қурилма билан ишламайди, ваҳолангки 3,4 ва 5 босқичлар қурилма хусусиятларини ҳисобга олишлари мумкин. 6 ва 7 босқичлар умуман қурилмаларга ҳеч қандай алоқаси йўқ. Тармоқ қурилмаларидан бирини бошқа бирорта қурилма билан ўзгартирилган тақдирда ҳам улар буни ҳеч вақт сезмайди. 2-босқичда (канал босқичи) иккита босқич ости ажратилади.

Юқори босқич ости (LLC-Logical Link Control, верхний подуровень) бу босқич ости мантиқий улашни амалга оширади, яъни виртуал алоқа каналини ўрнатади (унинг вазифасини бир қисмини тармоқ адаптерларининг драйвер дастури бажаради).

Қуйи босқич ости (MAC-Media Access Control, нижний подуровень) – бу босқич ости алоқа узатиш муҳити (алоқа канали) билан тўғридан-тўғри боғланишни амалга оширади. У тармоқ қурилмаси билан тўғри боғланган. OSI моделидан ташқари, 1980-йили феврал ойида қабул қилинган (802 сони - йил, ойдан келиб чиққан) IEEE Project 802 модели ҳам мавжуд. Бу моделни OSI моделини аниқлаштирилган ва ривожлантирилган модели деб қараш мумкин.

Бу модел аниқлаштирган стандартлар (802 – спесификасия) ўн иккита тоифага бўлиниб, уларнинг ҳар бирига номер берилган.

802–1 – тармоқларни бирлаштириш.

802–2 – мантиқий алоқани бошқариш.

802–3 – «Шина» топологияли CSMA/CD боғланиш усули маҳаллий ҳисоблаш ва тармоқ (Ethernet).

802–4 – «Шина» топологияли маҳаллий тармоқ, маркерли боғланиш.

802–5 – «Ҳалқа» топологияли маҳаллий тармоқ, маркерли боғланиш.

802–6 – шаҳар тармоғи (Metropolitan Area Network, MAN).

802–7 – кенг миқёсда алоқа олиб бориш технологияси.

802–8 – шиша толали технология.

802–9 – товушни ва ахборотларни узатиш имконияти бор интеграл тармоқ.

802–10 – тармоқ хавфсизлиги.

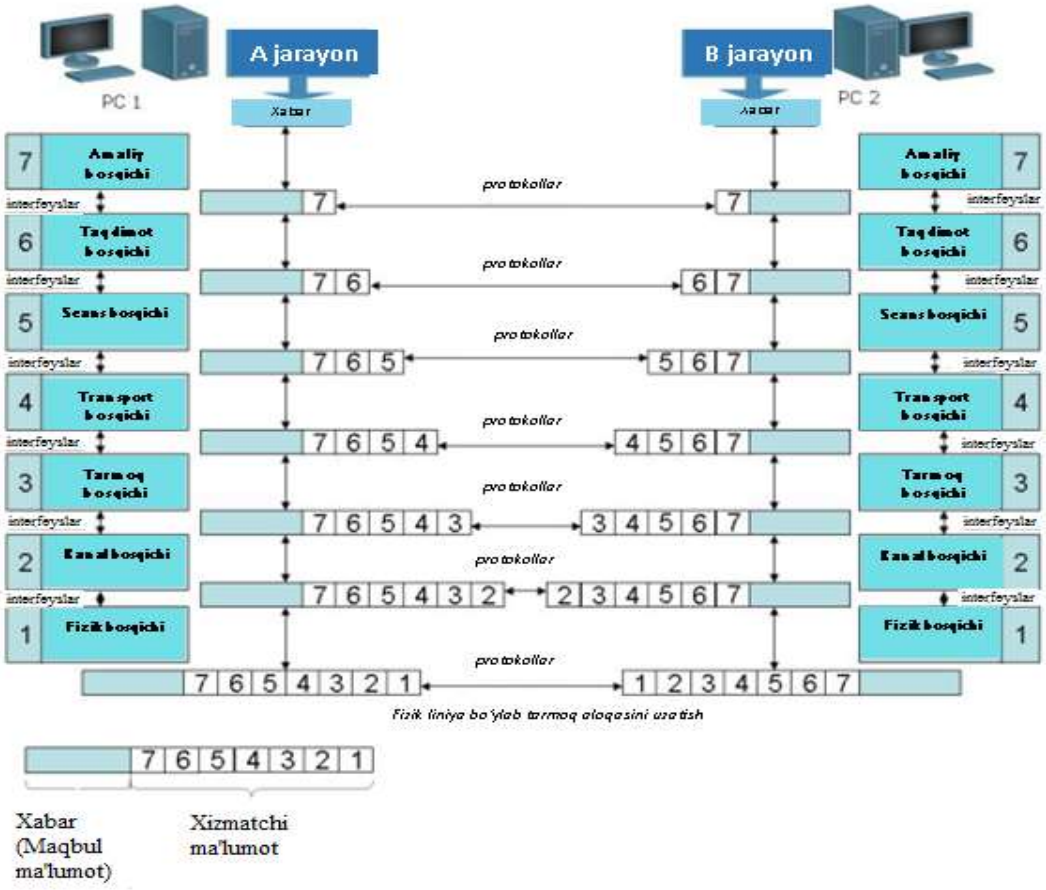
802–11 – симсиз тармоқ.

802–12 – «Юлдуз» топологияли марказни бошқаришга эга маҳаллий тармоқ (100 VG-Any LAN).

802.3, 802.4, 802.5, 802.12 стандартлар OSI модел эталонининг иккинчи (канал) босқичига қарашли MAC босқич ости таркибига тўғри келади. Қолган 802 – спесификациялар тармоқнинг умумий масалаларини ҳал қилади.

1.4. TCP/IP эталон модели

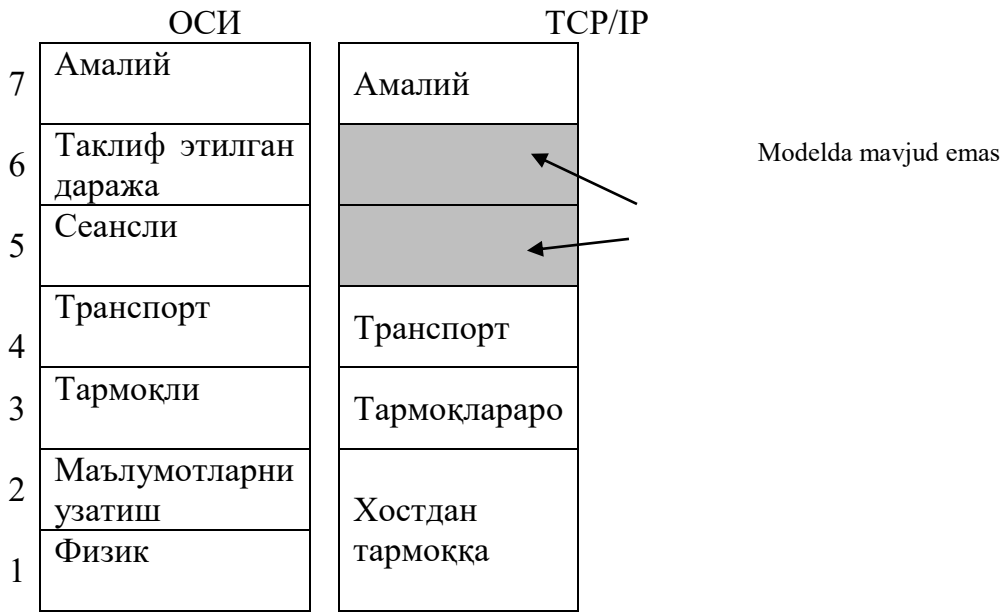
Йўлдош ва радио тармоқлари пайдо бўлганда, мавжуд протоколлар ёрдамида бошқа тармоқларни улар билан улашда катта муаммолар юзага келди. Ушбу архитектура кейинчалик иккита асосий протоколларига мувофиқ TCP/IP мос ёзувлар модели деб номланди. Унинг биринчи таърифи Керф ва Каннинг китобида учрайди (1974), кейинчалик у стандартга айланади (Браден, 1989). Моделнинг дизайн хусусиятлари 1988 йилда Кларкда муҳокама қилинган.



1.3-расм. Очиқ тизимларда эталон моделининг ўзаро таъсири

Каналли даража - ушбу талабларнинг барчаси турли хил тармоқларда ишлайдиган уланишсиз қават асосида пакетли уланадиган тармоқни танлашга олиб келди. Моделдаги энг паст даража- канал даражаси, уланиш ўрнатмасдан, ушбу тармоқ сатҳининг эҳтиёжларини қондириш учун қандай ва қайси каналлар, масалан, кетма-кет чизиқлар ва классик этҳернет. Бу аслида сўзнинг оддий маъносида умуман даража эмас, балки узатиш каналлари ва тугунлари ўртасидаги интерфейсдир. TCP/IP моделидаги дастлабки материаллар бу ҳақида жуда кам маълумот беради.

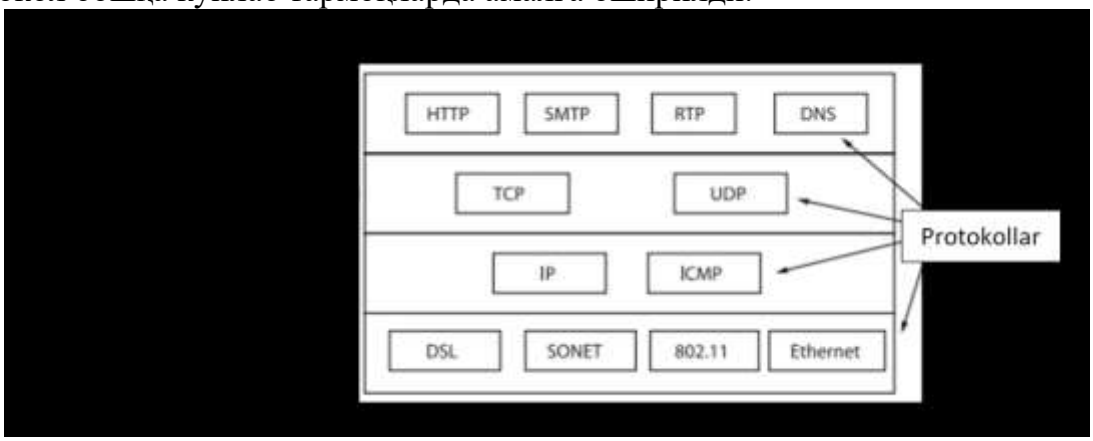
Тармоқлараро даража. Бу талабларнинг барчаси уланишсиз тармоқ сатҳига асосланган пакетли коммутация қилинган тармоқ моделини танлашга олиб келди. (1.4- расм). Интернет қатлами деб номланган ушбу қават бутун архитектуранинг асосидир. Унинг вазифаси ҳар бир хостнинг пакетларни исталган тармоққа юбориши ва ўз манзилига (масалан, бошқа тармоққа) мустақил равишда боришини таъминлашдир. Улар юборилганидан бутунлай бошқача тартибда келишлари мумкин. Агар жўнаш тартибига риоя қилиш талаб этилса, бу вазифани юқори даражалар бажаради. Эътибор беринг, "Интернет" сўзи асл маънода ишлатилади, гарчи бу даража Интернетда мавжуд бўлса. Шлюз қатлами ихтиёрий ICMP (Internet Control Messae Protocol) билан расмий пакет форматини ва IP протоколини белгилайди. Тармоқ протоколи мақсади IP-пакетларни манзилларга етказиб бериш. Бу ерда асосий жиҳатлар пакетли маршрутни танлаш ва транспорт артерияларини тўсқинлик қилишнинг олдини олишдир.



1.4- расм. TCP/IP эталон модели

Транспорт даражаси. TCP/IP моделининг шлюз қатламидан юқорида жойлашган қатлам одатда транспорт қатлами деб аталади. У қабул қилувчи ва узатувчи хостлардаги бир хил даражадаги объектлар OSI моделининг транспорт қатламига ўхшаш алоқа ўрнатиши учун яратилган. Ушбу даражада, иккита тугатиш протоколи тасвирланиши керак. Биринчиси, TCP (Transmission Control Protocol - Трансмиссияни бошқариш протоколи) - бу уланишни ўрнатиш билан ишончли

протокол бўлиб, байт оқимини битта машинадан бошқасига интеграцияланган тармоқдаги бошқа машиналарга этказиш имконини беради. Кириш байт оқимини алоҳида хабарларга ажратади ва уларни шлюзга ўтказади. Белгиланган жойда қабул қилинадиган TCP жараёни йиғилади, қабул қилинган хабарларнинг чиқиш оқими. Бундан ташқари, TCP тезкор юборувчи секин қабул қилувчини енгиб ўтмаслиги учун оқимни бошқаришни таъминлайди. Ушбу даражадаги иккинчи протокол, UDP (User Datagram Protocol) - бу кетма-кет TCP оқимини бошқариш воситасидан фойдаланмайдиган, лекин ўзига тегишли бўлган ишончсиз уланишсиз протокол. Бундан ташқари, у бир марталик мижоз-сервер сўровлари ва иловаларида кенг қўлланилади, бунда самарадорлик аниқликдан муҳимроқ бўлади, масалан овоз ва видеони узатишда. IP, TCP ва UDP протоколларининг ўзаро боғлиқлиги 1.5- расмда кўрсатилган. IP протоколи яратилгандан бери ушбу протокол бошқа кўплаб тармоқларда амалга оширилди.



1.5- расм. TCP/IP моделида протоколлар ва тармоқлар

Амалий даража. TCP/IP моделида сеанс ёки тақдимот даражаси мавжуд эмас. Ушбу даражалар шунчаки керак эмас эди, шунинг учун улар моделга киритилмади. Бунинг ўрнига, иловалар шунчаки сеанс ва тақдимот хусусиятларини ўз ичига олади. OSI моделидаги тажриба бу фикрни тўғри эканлигини исботлади: аксарият дастурларга ушбу даражаларнинг оз қисми керак. Транспорт қатламининг тепасида дастур қатлами жойлашган. Унда барча юқори даражадаги протоколлар мавжуд. Эски протоколлар орасида Virtual Terminal Protokoli (TELNET), Файл узатиш протоколи (FTP) ва электрон почта протоколи (SMTP) мавжуд. Йиллар давомида бошқа кўплаб протоколлар қўшилди. Биз кўриб чиқадиган баъзи энг муҳимлари 2.1.5-расмда. Бу DNS (Домен номи хизмати) бўлиб, ҳост номларини тармоққа, HTTP-га, бутун дунё бўйлаб веб-саҳифаларни яратишда ишлатиладиган протоколга, шунингдек, RTP - реал вақт режимида мультимедия, масалан товуш ёки филм каби тақдим этиш протоколи.

1.5. Мультимедиали тармоқ технологиялари.

Рақамли узатиш тизимларининг жадаллик билан ривожланиши, аналог узатиш тизимлари билан солиштирганда бир қанча афзалликлари билан фарқ қилади, масалан: шовқинга мувозанатлилигининг юқорилиги, алоқа линиясининг узунлигига узатиш сифатининг заиф боғланиши, алоқа каналларининг электрик параметрларини мўтадиллиги, дискрет хабарларни узатишда ўтказувчанлик қобилиятини қўллашнинг самарадорлиги ва бошқалар.

Телеграф алоқа ўрнига маълумотларни узатиш, электрон почта, факсимил алоқа каби хужжатли электр алоқа турлари кириб келди. Бир вақтнинг ўзида алоқа хизматларининг сони ошиши билан, оддий телефон хизматидан тортиб то интеграл рақамли алоқа тармоқларини таъминловчи мултимедиа хизматларигача уларнинг сифати ўзгаради. Кўпгина мутахассислар, телекоммуникация технологияларининг кейинги эволюцияси, ахборотларни узатиш тезлигини ошириш, тармоқни интелектуаллаштириш ва фойдаланувчиларнинг мобиллигини таъминлаш йўналиши бўйича кетади деб такидлашмоқда.

Тезликнинг юқорилиги. Тасвирларни узатиш, жумладан телевизион, мултимедиа иловаларида турли кўринишдаги ахборотлар интеграцияси, локал, шаҳар ва территориал тармоқлар учун зарур.

Интеллектуаллик. Тармоқнинг мослашувчанлигини ва ишончлилигини ошириш, глобал тармоқларни анча осон бошқариш имконини беради. Тармоқнинг интелектуаллиги туфайли хизматдан пассив фойдаланувчи актив мижозга айланади, яъни, мижоз зарур бўлган хизматга буюртма берган ҳолда ўзи тармоқни фаол бошқариши мумкин.

Мобиллик. Электрон қурилмаларни миниатюризатсиялаш соҳасидаги мувоффақиятлар, уларнинг нархини пасайиши, якунловчи мобил қурилмаларни глобал тарқалишига замин яратади. Бу, ҳар қандай жойда ва ҳар қандай вақтда ҳар бир талабгорга алоқа хизматини етказишни реал масаласи ҳисобланади.

Ҳозирги кунда дунёнинг ахборот телекоммуникация инфраструктураси орқали узатиладиган ахборот ҳажми ҳар 2-3 йилда икки мартага ошиб бормоқда.

Келажакдаги алоқа тармоқлари қуйидаги талабларга жавоб бериши лозим:

- мултисервислик - транспорт технологияларига хизматларни етказувчи технологияларнинг боғлиқ эмаслиги;
- кенг полосалилик - одатда фойдаланувчи талабларига боғлиқ ҳолда кенг диапазонда ахборотни узатиш тезлигини мос рейингга динамик ўзгариши имкони;
- мультимедиалик - тармоқни, реал вақтда ва мураккаб уланиш конфигуратсиясини қўллаган ҳолда, кўп компонентли ахборот (овоз, мазкур видео, аудио)ларни шу компонентлар учун зарур бўлган синхронизация билан узатиш қобилияти;
- интеллектуаллик - фойдаланувчи ёки хизматларни таъминловчи томондаги чақириқ ёки уланиш хизматларини бошқариш имкони;
- инвариантлик уланиш - қўлланилаётган технологияларга боғлиқ бўлмаган ҳолда хизматларга уланишни таъминлаш имкони тушунилади;
- кўп операторлик - хизматларни тақдим этишда ва уларнинг масъулиятини фаолият сохасига мос холда тақсимлашда бир нечта операторларнинг қатнашиши.

Шунингдек келажакдаги алоқа тармоқларига бўлган талабларни шакллантиришда хизматларни таъминловчининг фаолиятини хусусиятларини ҳисобга олиш лозим.

Хизматларни таъминловчига бўлган талабларга қуйидагилар киради:

- “мултиоператорлик” муҳитида қурилмаларнинг ишини таъминлаш имконияти яъни бир нечта алоқа оператори тармоғига (жумладан уланиш сатхига ҳам) уланиш учун интерфейслар сонини ошириш;
- биргаликда етказиш учун хизматларни таъминловчи узелларни биргаликда ишлашини таъминлаш;
- қурилмаларнинг дастлабки минимал нархини белгилашда

“масштабланувчан” техник ечимларни қўллаш имкони.

Ҳозирги вақтда каналларни ва пакетларни коммутатсиялашга эга бўлган мавжуд умумий фойдаланувчи алоқа тармоқлари юқорида айтиб ўтилган талабларга жавоб бермайди. Одатдаги тармоқларнинг имкониятларини чегараланганлиги янги инфокоммуникация хизматларини яратиш йўлида бардош бериш омили ҳисобланади. Бошқа томондан етказиладиган инфокоммуникация хизматларининг ҳажмини ошиши, мавжуд алоқа тармоқларининг базавий хизматларини, чақириқларга хизмат кўрсатиш сифат кўрсаткичларига салбий таъсир кўрсатиши мумкин. Буларнинг барчаси, пейинг авлоднинг алоқа тармоқларини яратиш йўналишида, одатдаги алоқа тармоқларини ривожлантириш усулларини режалаштиришда инфокоммуникация хизматлари мавжудлигини ҳисобга олиш лозимлигига мажбур қилади.

“Алоқа тармоғи” терминини икки нуқтаи назардан қараш мумкин.

Биринчидан, алоқа тармоғини, маълумотларни алмашиш учун техник воситалар мажмуасидан иборат бўлган мустақил объект каби қараш мумкин.

Иккинчидан, алоқа тармоғини, глобал ахборот инфраструктураси (ГАИ)ни муҳим компоненти деб қараш мумкин.

Видеоконференция – бу компьютерларнинг мультимедиа имкониятлардан фойдаланган ҳолда тармоқ бўйича иккита ва ундан ортиқ инсонларнинг мулоқоти ҳисобланади. Тамроққа уланган компьютер видеокамера, микрофон ва аудиоколонкалар билан таъминланган бўлиши керак. Видеоконференция тизимлари учун ишлатиладиган қурилмалар поғонага қараб персонал, гуруҳли ва студияли видеоконференцияларга бўлинади.

1990 йилида видеоконференция соҳасида биринчи ҳалқаро стандарти чиққан эди – ISDN бўйича видеоконференцияларни қувватлаш учун H.320 спесификацияси. Ундан кейин ITU видеоконференцияларга тегишли бўлган бир нечта серияли тавсифномаларни қабул қилди. Бу сериядаги тавсифномалари, H.32x билан номланиб, H.320 дан ташқари, хар хил тармоқлар учун керак бўлган H.321 – H.324 стандартларни ўз ичига олади.

90-йилларнинг иккинчи ярмида IP тармоқлар ва Интернет ривожланиши бошлаган. Улар маълумотлар узатиш иқтисодий муҳитга айландилар ва хамма жойда ишлатилиши бошлаган эди. Лекин ISDH га қараганда IP тармоқлар аудио ва видео оқимларни узатиш учун ёмон мосланган эди. IP тармоқларнинг бор структурани ишлатиш мақсадида 1996 йилда H.323 стандартини пайдо бўлишига олиб келинди (Visual Telephone Systemsand Terminal Equipment for Local Area Network swhich Providea Non-Guaranteed Quality of Service, кафолатланмаган хизмат кўрсатиш билан локал тармоқлар учун видеотелефонлар ва терминал қурилмалари). 1998 йилда H.323 v.2 (Packet-based multimedia communication systems, пакетлар коммутация билан тармоқлар учун мультимедиа алоқа тизимлари) стандартнинг икиинчи версияси чиқди, 1999 йилда тавсифномаларнинг учинчи версияси, 2001 йилда H.323 стандартнинг тўртинчи версияси қабул қилинди. Ҳозир H.323– бу сериянинг муҳим стандартларнинг бири ҳисобланади. H.323–бу кафолатли хизмат кўрсатишни таъминлаб бермайдиган (QoS) ҳисоблаш тармоқларда мултимедиа иловалар учун ITU-T тавсифномалари. Бундай тармоқлар Ethernet, Fast Ethernet ва Token Ring базасида IP ва IPX пакетли коммутатсия тармоқлар ўз ичига олади.

H.323 тавсифномалари таъминлаб беради:

Ўтказиш полосани бошқариш;
Тармоқлараро конференцияларни ташкил қилиш имконияти;
Платформали мустақиллиги;
Кўпнуқтали конференцияларни қувватлаш;
Кўпадресли узатишни қувватлаш;
Кодеклар учун стандартлари;
Мослашиш ва ихчамлиги.

Ўтказиш полосани бошқариш. Аудио ва видео ахборотларни узатиш алоқа каналларни кўп юклатади, агар юклама оширишини кузатмаса, мухим тармоқ сервисларнинг иши бузилиши мумкин. Шунинг учун H.323 тавсифномалари ўтказиш полосани бошқаришни таъминлаб беради. H.323 хамма иловалар учун бир вақтли уланиш сонларни ва умумий ўтказиш полосани чегаралаш мумкин. Бу чегаралар бошқа тармоқ иловалар иши учун керак бўлган ресурсларни сақлашни ёрдам беради. H.323 хар битта терминали конференциянинг аниқ сессияда ўзини ўтказиш полосани бошқариш мумкин.

Тармоқлараро конференцияларни ташкил қилиш имконияти. H.323 тавсифномалари хар хил турдаги тармоқларда (масалан, IP ва ISDN, IP ва PSTN) видеоконференция қатнашувчиларни улаш воситасини тақдим этади.

H.32x стандарт протоколларнинг асосий характеристикалари 1.2-жадвалида келтирилган.

1.2 жадвал.

H.32x стандарт протоколлари

Тавсифнома	H.320	H.321	H.322	H.323 B1/B2	H.324
Қабул қилиш йили	1990	1995	1995	1996/1998	1996
Тармоқ	Тор полосали ISDN	Кенг полосали ISDN, ATML AN	Пакетли коммутатсия тармоғи ва кафолатланган хизмат кўрсатиш сифати билан (isoEthernet)	Пакетли коммутатсия тармоғи ва кафолатланмаган хизмат кўрсатиш сифати билан (Ethernet)	Умумий фойдаланиш телефон тармоғи (PSTN ёки POTS)
Видео	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Аудио	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728 G.723 G.729	G.723
Мултиплексорлаш	H.221	H.221	H.221	H.225.0	H.223
Бошқариш	H.230 H.242	H.242	H.242 H.230	H.245	H.245
Кўпнуқтали конференциялар-ни қувватлаш	H.231 H.243	H.231 H.243	H.231 H.243	H.323	–
Маълумотларни алмашиш	T.120	T.120	T.120	T.120	T.120

Тармоқли интерфейс	I.400	AAL I.363 AJM	I.400 & TCP/IP	TCP/IP	V.34 Modem

Платформали мустақиллиги. H.323 қурилмалар ёки дастурий таъминоти билан боғлиқ хеч қандай технологик ечимларга уланмаган. Бир бири билан боғлиқ иловалар хар хил платформалар, хар хил операцион тизимлари билан яратилиши мумкин.

Кўпнуқтали конференцияларни қувватлаш. H.323 тавсифномалари учта ва ундан ошиқ қатнашувчилари билан конференцияни ташкил қилиш мумкин. Кўп нуқтали конференциялар марказий MSU (кўп нуқтали конференция қурилмаси) ишлатилиши ёки ишлатмаслиги билан ўтказилиши мумкин.

Кўп адресли узатишни қувватлаш. H.323 агар тармоқ гуруҳли адресация бошқариш протоколини қувватласа (масалан, IGMP) кўпнуқтали конференцияда кўпадресли узатишни қувватлайди. Кўпадресли узатиш пайтида ахборотнинг битта пакети ортиқча дубллаштиришмасдан керак бўлган манзилларга юборилади. Кўпадресли узатиш ўтказиш полосани эффектив ишлатади, чунки хамма қатнашувчи манзилларга битта оқим юборилади.

Кодеклар учун стандартлари. H.323 хар хил ишлаб чиқарувчилар қурилмаларни мослашишни таъминлаб бериш мақсадида аудио ва видеооқимларни кодлаш ва декодлаш учун стандартларни ўрнатади. Бу стандарт жуда ихчам ҳисобланади. Бажаришни талаб қиладиган талаблар мавжуд ва опциал имкониятлар хам бор. Бундан ташқари ишлаб чиқарувчи мультимедиа маҳсулотларга ва иловаларга қушимча имконятларни киритиш мумкин, агар улар стандарт талабларга мос бўлса.

Мослашиш. Конференция қатнашувчилари улар ўртасида мослашиш масаласи бўйича ўйламасдан бир-бири билан мулоқотда бўлади. H.323 тавсифномалари охирги фойдаланувчилар қурилмаларнинг умумий имкониятларни аниқлашни қувватлайди ва конференция қатнашувчилари учун энг яхши кодлаш, чақирув ва бошқариш протоколларни ўрнатади.

Ихчамлиги. H.323 конференцияси хар хил имкониятли охирги қурилмаларга эга бўлган қатнашувчиларни ўз ичига олиш мумкин. Масалан, қатнашувчиларнинг биттаси фақат аудио имкониятлари билан терминални ишлатиш мумкин, конференциянинг бошқа қатнашувчилари эса хам видео хам маълумотларни қабул қилиш /узатиш имкониятларга эга бўлиши мумкин.

Стандартда кўрсатилган H.323 «объектлари»га терминаллар, мултимедиа шлюзлари, кўп нуқтали конференцияларни бошқариш қурилмалари ва зона назоратчилари кирадилар.

Терминал (Terminal) – конференцияда қатнашиш учун мўлжалланган охирги мултимедиа қурилмаси (овоз, видео, маълумотлар).

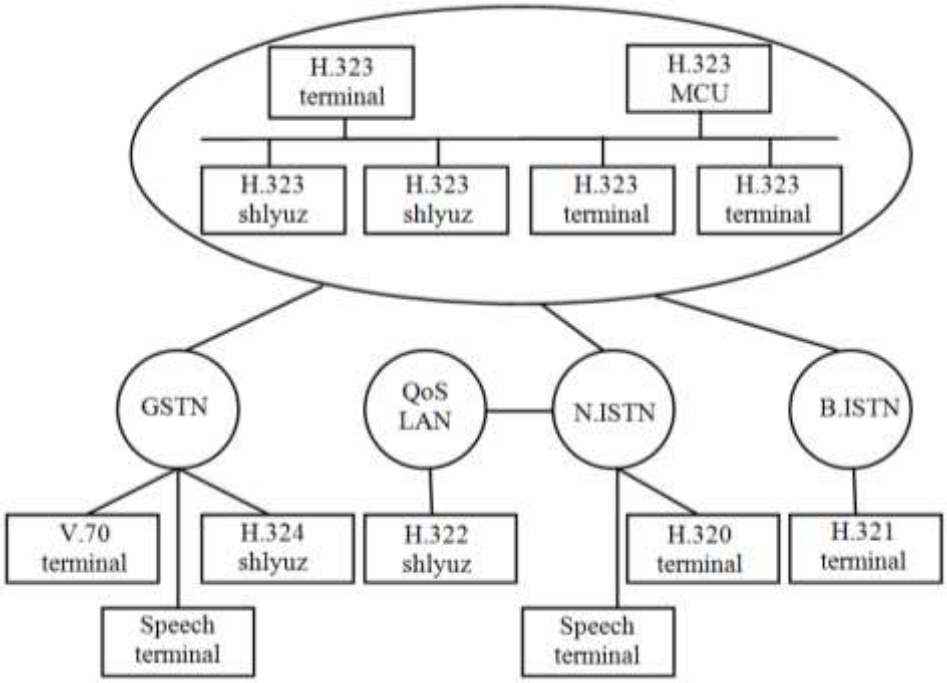
Мултимедиали шлюз (Gateway) – хар хил турдаги тармоқларни бирлашиш учун мултимедиа ва бошқариш ахборотларни ўзгартириш учун мўлжалланган қурилмаси.

Кўп нуқтали конференцияларни бошқариш (Multipoint Control Unit – MCU) – учта ва ундан ортиқ қатнашувчилар билан конференцияни ташкил қилиш учун мўлжалланган.

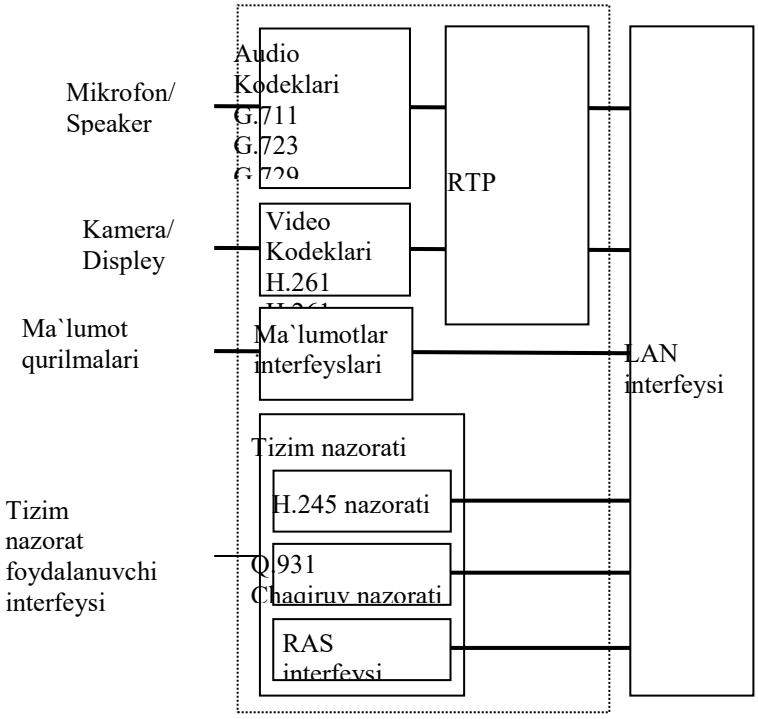
Зона назоратчиси (Gatekeeper, Privratnik, Konferens-menedjer) – тармоқни

бошқаришни таъминлаб берадиган ва виртуал телефон стансия вазифасини бажарадиган тавсия қиладиган, лекин мажбурий эмас, қурилмаси.

Терминал тушунчада (2.6- расм) стандарт реал вақтда бир бири билан мулоқотда бўлган фойдаланувчиларга рухсат берадиган тармоқнинг охирги нуқталар қурилмаси деб тушунади.



1.6 -расм. H.323 стандартнинг базали архитектураси.

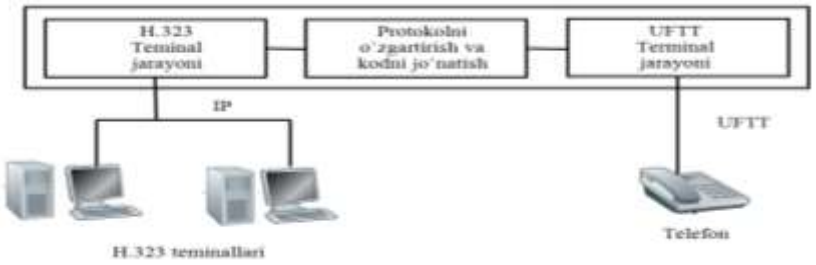


1.7-расм. H.323 терминалнинг структураси.

Терминаллар H.245 – уланиш параметрларни мослашиш, Q.931 – шу уланишни параметрларни мослашиш ва уланишни ўрнатиш протоколларни, RAS канали (Registration/Admission/ Status) зона назоратчи билан улаш (Gatekeeper), RTP/RTCP протоколи аудио ва видео пакетлари билан ишлаш учун, G.711 протоколи аудио оқимларни сиқиш учун. Тавсифномаларга қараб, H.323 терминали учун видеокодекларни, T.120 протоколни ва MCU имкониятларни қувватлаш яхши деб ҳисобланади. Стандартда видео функсиялари шарт эмас деб қарамасдан, хамма видеоимконятлари билан терминаллар H.261 кодекни қувватлаш керак, хамда H.261 кодекнинг ривожланиши деб ҳисобланган H.263ни қувватлаш деб яхши ҳисобланади.

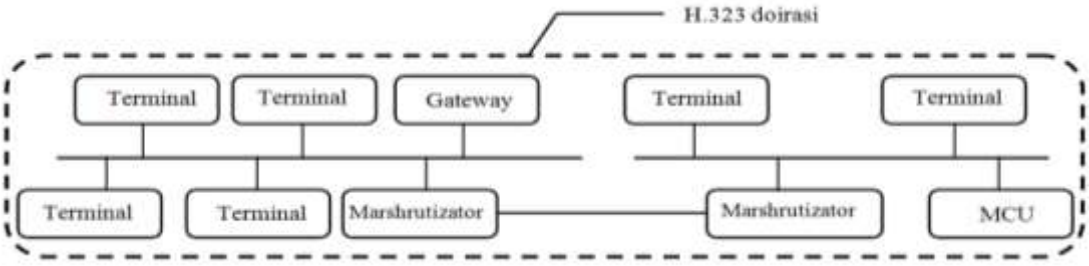
H.263 кодек ёрдами билан олинган видеорасм ёқори сифатга эга бўлади, чунки харакатни кўрсатиш учун ярим пиксел технологияси ишлатилади. Бундан ташқари, Хаффман бўйича ишлатилган кодлаштириш пастроқ узатиш тезликлари билан ишлаш учун оптималлаштирилган.

Мультимедиа шлюз – бу конференцияда опционал элементи ҳисобланади. У хар хил функцияларни бажариш мумкин. Унинг асосий функцияси узатиш протокол форматларни ўзгартириш масаласи ҳисобланади (масалан, H.225.0 ва H.221). Одатда мултимедиа шлюзлари хар хил турдаги тармоқлар ўртасида боғланишни қувватлаш учун ишлатилади. 1.8- расмда H.323/PSTN шлюзи кўрсатилган.



1.8- расм. H.323/PSTN мултимедиа шлюзи.

Зона назоратчиси (1.9-расм) – тармоқ бошқарувини таъминлаб берадиган ва виртуал телефон стансия вазифасини бажарадиган тавсия қиладиган, лекин мажбурий эмас, қурилмаси ҳисобланади.



1.9-расм. Зона назоратчиси (Gatekeeper)

Зона назоратчининг асосий функциялари:

– Чақирувларни бошқариш ва адресациялаш;

– UATS учун мўлжалланган телефон маълумотномаси ва хизматлар асосий хизмат турларини таъминлаб бериш (чақирувларни узатиш ва йўналтириш ва ҳ.к.);

– Хизмат кўрсатиш сифатини (QoS) таъминлаб бериш учун H.323 иловаларнинг ўтказиш полосани ишлатишни бошқариш;

– Тармоқ ресурсларни умумий фойдаланишни бошқариш;

– Тизимли администратсиялаш ва хавфсизлигини таъминлаш.

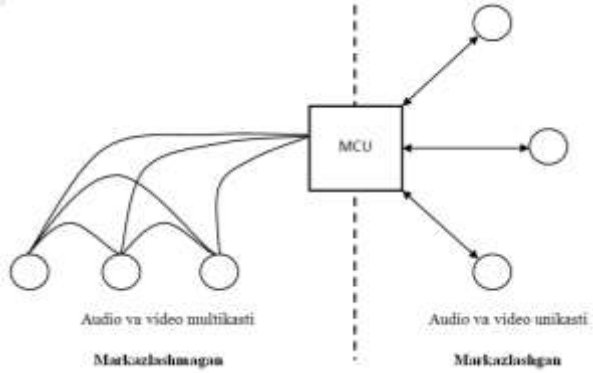
H.323 тавсифномаси зона назоратчини шарт эмас компонент деб аниқлайди, шунга қарамасдан бу қурилма бўлмаса IP-телефония ва мултимедияли телеконференция иловалари учун H.323 стандарт яратувчилари томонидан назарга олинган хар хил хизматлардан фойдаланиш имконият бўлмайди.

Кўпнуқтали конференцияни бошқариш қурилмаси (МСУ) – учта ва ундан ортиқ қатнашувчилари ўртасида конференцияни қувватлаш учун мўлжалланган. Бу қурилмада назоратчи Multipoint Controller (MC) бўлиши керак, ва процессорлар Multipoint Processors (MP) хам бўлиши мумкин. Назоратчи MCN.245 протоколини қувватлайди ва терминаллар ўртасида аудио ва видео оқимларни қайта ишлаш параметрларни мослаштириш учун мўлжалланган. Процессорлар шу оқимларни комматуциялаш, микширлаш ва қайта ишлаш билан шуғулланади.

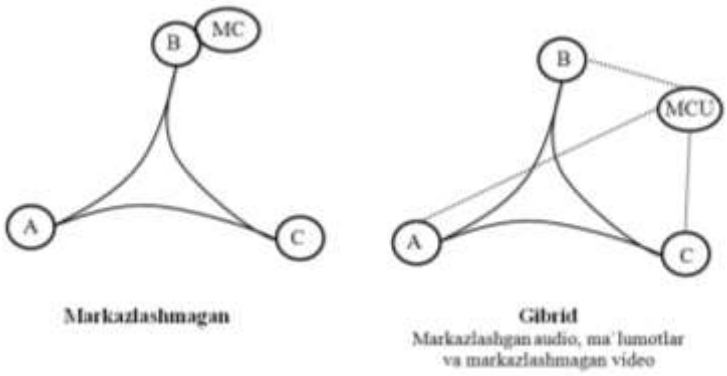
Кўпнуқтали конференциянинг конфигуратсияси марказлашган, марказлашмаган (2.10-расм), гибридли ва аралаш бўлиши мумкин (2.11-расм).

Марказлашган кўпнуқтали конференция MCU қурилмани борлигини талаб қилади. Хар битта терминал MCU билан аудио, видео, маълумотлар оқимлари ва “нуқта-нуқта” схема бўйича бошқариш командалари билан алмашади. Назоратчи MC H.245 протоколини фойдаланиб хар битта терминал имкониятларни аниқлайди. Процессор MP хар битта терминал учун керак бўлган мультимедияли оқимларни шакллантиради ва уларни юборади. Бундан ташқари, процессор ахборотларнинг хар хил тезлиги билан хар хил кодеклардан оқимларни ўзгартиришни таъминлаб бериш мумкин.

Видеоконференсалоқани ташкил қилишнинг гибридли схемаси иккита олдингиларнинг комбинацияси ҳисобланади. Конференцияда қатнашганлар H.323 терминаллари MCU га юбормасдан хамма қолган қатнашувчиларга фақат аудио ёки фақат видео оқимларни кўпадресли узатишни амалга оширади. Қолган оқимларни узатиши терминаллар ва MCU ўртасида “нуқта -нуқта” схема бўйича амалга оширади. Бу холатда хам назоратчи, хам MCU протсессори ишга тушади.



1.10- расм. H.323да конференцияларни марказлашган ва марказлашмаган ташкил қилишнинг схемалари.



1.11- расм. H.323да конференцияларни марказлашмаган ва аралаш ташкил қилиниш схемалари.

Видеоконференцияни ташкил қилишнинг аралаш схемада терминалларнинг битта гурухи марказлашган, бошқа гуруҳи эса марказлашмаган схема бўйича ишлаши мумкин. Марказлашмаган кўпнуқтали конференция гурухли адресатсия технологиясини ишлатади. Конференцияда қатнашадиганлар H.323 терминаллари MCUга юбормасдан қолган қатнашувчиларга мултимедиа оқимларни кўпадресли узатишни амалга оширади. Назорат ва бошқарув маълумотларни узатиши терминаллар ва MCU ўртасида “нуқта нуқта” схема бўйича амалга оширади. Шу холатда кўпнуқтали узатиш назорати MC назоратчи томонидан амалга оширилади.

Назорат саволлари:

1. Компьютер тармоқлари деганда нимани тушунасиз?
2. Компьютер тармоқларининг афзалликлари нималардан иборат?
3. Тармоқнинг қандай турлари мавжуд?
4. Компьютер тармоқлари қандай таснифланади?
5. Шахсий тармоқ (PAN) -нима?
6. OSI модели нечта қатламга эга?
7. TCP/IP эталон модели нима?
8. Амалий даражанинг TCP/IP эталон моделидаги ўрнини аниқланг?
9. Мультимедиали тармоқ технологиялари ҳақида маълумот беринг.
10. Замонавий алоқа тармоқлариган бўлган талаблар ҳақида маълумот беринг.
11. Замонавий алоқа хизматларининг хусусиятлари нимада?

Адабиётлар ва Интернет сайтлари:

1. Эшмурадов А.М., Абдужалилов Ж.А. “Интернет тармоқлари ва хизматлари” фанидан ўқув-услубий мажмуа. – Тошкент: ТАТУ. 2016.

2. Олифер Виктор, Наталия Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Сн-Петербург: Издательство ПИТЕР, 2016, 992 с.

3. Douglas E. Comer. Computer Networks and Internets (6th Edition). Pearson. USA, 2015. 672 p.

4. Компьютерные сети и технологии. http://www.xnets.ru/

5. http://www.network.xsp.ru/

2-маъруза. SMART – технологиялар ва IoT - буюмлар интернети. IoT - буюмлар интернети соҳасида хавфсизлик масалалари. (2 соат)

Режа:

2.1. SMART – технологиялар ва IoT (Internet of things) – буюмлар интернети замонавий тармоқ хизматлари сифатида
2.2. LPWAN технологияси
2.3. NB-IoT технологияси
2.4. IoT - буюмлар интернети соҳасида хавфсизлик масалалари

Таянч иборалар: *SMART, SMART – технологиялари, IoT (Internet of things), буюмлар интернети, LPWAN технологияси, NB-IoT технологияси.*

2.1. SMART – технологиялар ва IoT (Internet of things) – буюмлар интернети замонавий тармоқ хизматлари сифатида.

Ахборот – коммуникация технологиялари бугунги кунда жуда тез суръатлар билан ривожланмоқда. Интернет ва унинг хизматлари маълумотларни узатиш ҳамда қабул қилиш тармоғи сифатида инсонларнинг кундалик ҳаётининг турмуш тарзига айланмоқда. Шунингдек, ахборот – коммуникация технологиялари жамиятнинг ривожланиш тенденсиясига таъсир этувчи асосий омиллардан бири бўлиб, илм-фан, бизнес ва бошқа бир қатор соҳаларда улкан ютуқларга эришишга имкон бермоқда, инсониятнинг ахборотлар ресурсларига бўлган ижтимоий ва шахсий эҳтиёжларини қониқтиришини таъминламоқда.

АҚШнинг Вашингтон штати Сиетл шаҳрида бўлиб ўтган Буилд 2017 конференциясининг илк кунида Microsoft компанияси булутли технологиялар, сунъий интеллектни такомиллаштириш соҳасидаги сўнгги ютуқлар ва ИТ соҳасидаги бошқа муваффақиятли ишланмаларни намойиш этди. Azure булутли хизматидан фойдаланиб, Буюмлар Интернети (Internet of Things) қурилмаларини бошқаришнинг мутлақо янги усулини яратгани — компаниянинг муҳим ютуқларидан бири бўлган. Компанияда яратилган ***Azure IoT Edge*** иловаси нафақат уй шароитларида, янада кенгроқ чегараларда — офис, корхона ва ишлаб чиқаришда Буюмлар Интернети қурилмаларининг ҳаракатини бошқаришнинг уникал имкониятини тақдим этади. Ушбу консепция «ақлли» буюмларнинг кўплаб функцияларини бошқариш имкониятини берадиган «булутли шаҳар» яратиш томон тобора ҳаракат қилавериш кераклигини тақозо этади. (5.3.1- расм.)

Ақлли тармоқ – (инглизча: smart network) маълумотларни узатишдан ташқари мураккаб ахборот хизматларининг ранг-баранг турларини тақдим қилувчи коммуникация тармоғи.

«***SMART технология***» (ақлли технология) ва «***Буюмлар интернети***» каби атамаларнинг пайдо бўлиши эса Интернетдан фойдаланишни энди нафақат инсонлар, балки, буюмлар ҳам «уддалайдиган» замонга қадам қўйилмоқда. “**SMART**” (ақл-идрокли, технологик мукаммал) айни пайтда технология оламида кенг қўлланилаётган ибора (қисқартма сўз) бўлиб, уни дастлаб 1965 йилда ***Паул Ж Меер***, сўнгра 1981 йили ***Георге Т. Доран*** ўз илмий ишларида

қўллаганлар.[Википедия]

Дастлаб “SMART – тузилиш” концепцияси янги материалга ўтиш, материалларнинг янги хусусиятларидан фойдаланиш, электроника ва ахборот технологиялари соҳасида мувафаққиятлар каби тенденсиялар билан мустаҳкамланадиган аерокосмик технология контекстида қўлланилган.

SMART – “Specific” (ўзига хос), “Measurable” (ўлчаб бўладиган), “Attainable” (эришиб бўладиган), “Relevant” (долзарб), “Time-bound” (аниқ муддатли) инглизча сўзларининг бош ҳарфлари билан ифодаланган.

Республикамиз етакчи олимларидан А.А. Абдуқодиров Смарт – технологиясига оид тушунчалар, мақсадларни қўйишдаги ифодаси, моҳияти, хоссаси ва унинг асосий тамойиллари тўғрисида батафсил маълумот бериб ўтган. Жумладан: “Смарт – технологиялар – ўзаро таъсир ва тажриба алмашиш негизида протседураларга узатиладиган, авваллари ахборот ва билимларга асосланган технологиялардир..... «Смарт» нинг таянч хоссаси атроф муҳит билан ўзаро таъсир этиш ва унга мослашиш қобилиятидир. Унинг ушбу хусусияти мустақил қийматга эга ва шаҳар, университет, таълим, технология, жамият ва кўпгина бошқа категорияларга қўлланиши мумкин.

SMART – бу тизим ёки жараённинг ҳусусияти бўлиб, атроф муҳит билан ўзаро муносабатларда ўзини намоён қилади ва тизимга қобилиятини қайта ишлашга; ташқи муҳитдаги ўзгаришларга дарҳол жавоб; ўзгарувчан шароитга мослашиш; мустақил тараққиёт ва ўзини ўзи бошқариш; натижаларни самарали бажариш кабиларга имкон беради.”

SMART – технологияларнинг асосини бугунги кунда **IoT (Internet of things)** – буюмлар интернети ташкил этмоқда. Буюмлар интернети бу – махсус электроника, дастурий таъминот, сенсорлар, қабул қилувчи ва узатувчи қурилмаларнинг ўзаро маълумот алмашинувидан иборат тармоқ тизими билан жиҳозланган сунъий интелект ёрдамида масофадан бошқарилувчи маиший техникалар, транспорт воситалари, эшик-деразалар, қўриқчи тизимлар ва бошқалар. IoT технология тадқиқотчиларига камроқ қувват сарфлайдиган ва деярли ҳар қандай турдаги қурилмага уланиши мумкин бўлган кичикроқ ва арзонроқ симсиз тизимларни ишлаб чиқиш учун куч беради.

“Интернет – буюмлар” (баъзан “буюмлар интернети” ёки “интернет ашёлари” деган атама ҳам ишлатилади) инглиз тилидан олинган Internet of Things, IoT бўлиб—бир-бири билан ёки ташқи муҳит билан ўзаро таъсирлашув учун ичига жойлаштирилган технологиялар билан жиҳозланган, иқтисодий ва ижтимоий жараёнларни қайта қура оладиган ҳодиса каби тармоқларни ташкил этишни кўриб чиқадиган, ҳаракат ва операциялар ичидан инсон иштироки заруриятини инкор этадиган, физик жараёнлар ҳисоблаш тармоғи консепцияси ҳисобланади.

Ҳозирда буюмлар интернети мултисервисли тармоқлар консепциясининг бир бўлагига айланди. Бундай тармоқлар чекланмаган хизматларни сифатини кафолатлаган ҳолда мижозларга етказиш имконини беради. Шуни назарда тутган ҳолда мултисервисли тармоқлардан фойдаланиш долзарб масалалардан биридир. Айнан шундай мултисервисли хизматлар кейинги авлод тармоқлари (NGN)да амалга ошади. Ҳозирги кунда NGN нинг таркибий қисмига —барча жойларда сенсорли тармоқлар - USN (Ubiquitous Sensor Networks) тушунчаси кириб келди.

Интернет ашёларни, бизни ўраб турган барча предметлар ва қурилмалар (уй асбоблари ва жиҳозлари, кийим-кечак, маҳсулотлар, автомобиллар, саноат

қурилмалар ва бошқалар) миниатюрали (кичик ўлчамли) идентификацион ва сенсорли (сезгир) қурилмалар билан жиҳозланган деб тасаввур қилиш мумкин. У ҳолда улар билан зарур алоқа каналлари бўлганида нафақат бу объектларни ва уларнинг параметрларини фазода ва вақт бўйича кузатиш мумкин бўлади, балки уларни бошқариш, улар ҳақидаги маълумотларни умумий - ақлли планетага киритиш мумкин бўлади. Оддийроқ айтганда, Интернет ашёлар бу компютерлар, датчиклар (сенсорлар) ва ижрочи қурилмаларнинг (актуаторларнинг) IP (Internet Protocol) интернет протоколдан фойдаланиш орқали ўзаро боғлайдиган глобал тармоқ ҳисобланади.

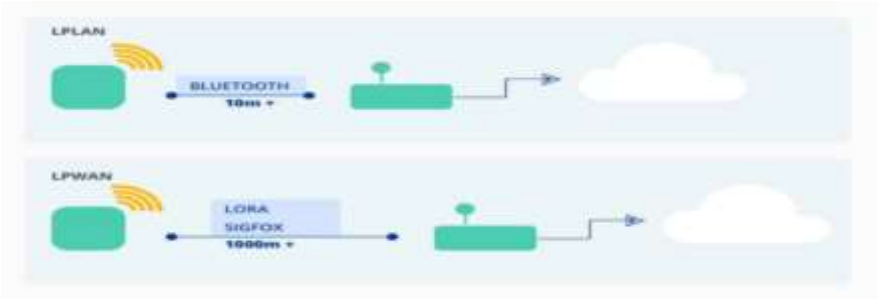
2.2. LPWAN технологияси

Cisco IBSG - тармоқ жиҳозларини ва дастурларини ишлаб чиқарувчи жаҳонда етакчи АҚШ компаниясининг ҳисоботига кўра 2008-2009 йилларда интернетга уланган буюмлар сони ер юзидаги одамлар сонидан ошиб кетган, 2015 йилда 25 миллиардга этган бўлса, 2020 йил охирига бориб эса бундай буюмлар сони 50 миллиардга етиши кутилмоқда.

Булардан кўриниб турибдики, бугунги кунда “Буюмлар интернети” инсон фаолиятининг кўплаб соҳаларида қўлланилмоқда. «Ақлли музлаткичлар», «Уйни ақлли ёритиш» ва бошқа «ақлли» сифати билан аталувчи маиший техникалар ҳаётимизни янада энгиллаштириб, ташвишларимизнинг бир қисмини улар зиммасига юклашга имконият яратади. Ҳозир бундай қурилмаларда телефондагидек оддий сим-картадан фойдаланилади. Микроелектроникани ривожлантириш, микрокон-троллерлар юқори иш фаолиятини таъминлаш ва энергия сарфини камайтириш, микросхема нархини пасайтириш – буларнинг барчаси янги йечимлар ва технологияларни ишлаб чиқиш ва жорий қилиш имконини беради. Бироқ эндиликда **LPWAN** (Low-power Wide-area Network - инглизча, кам қувватли кенг полосали тармоқ деб аталган сўзнинг қисқартмаси.) — базавий станция билан доимий алоқада бўлиб туриш учун қимматли ампер-соатларни сарфламайдиган, кичикроқ ҳажмдаги маълумотларни узоқ масофаларга узата оладиган олис радиусда таъсир кучига эга энергиядан самарали фойдаланадиган тармоқ устида фаол иш олиб борилмоқда. LPWAN - «Узоқ радиусли харакатдаги энергоеффектли тармоқ» - ҳисоблагич, ўлчаш ва сенсор қурилмалар ўртасида маълумотлар йиғиш ҳамда тарқатиш амалларини бажарувчи олис радиусли симсиз тармоқ технологияси.

Унинг кўпгина авзалликлари мавжуд:

- Кам қувват сарфи ва бунинг натижасида манба узоқ муддат хизмат қилади;
- Охирги қурилмалар (терминал) тармоқ технологиясини харид қилишнинг нархи арзонлиги;
- Катта ҳудудга хизмат қилиши;
- Узатилаётган ахборотнинг юқори даражада ҳимояланганлиги.



2.1 – расм. LPWAN технологияси

2000-йилларда Sigfox LPWAN ни қувват талаблари ва уяли алоқа учун лицензиялаш харажатларига юқори самарали aLTErнатива сифатида оммалаштирди. Француз стартапи Cycleo бир нечта жозибали кам қувватли IP яримўтказгичларни ишлаб чиқди ва Semtech уларни 2012 йилда ўзининг кам қувватли RF портфелини мустаҳкамлаш учун сотиб олди. Semtech энди LoRa протоколи ёрдамида баъзи базавий IP-ларни бошқаради, бу ҳақиқатан ҳам уяли бўлмаган LPWAN протоколи бўлди, гарчи Sigfox яқинда янги глобал кенгайтмани эълон қилди.

2.2 – расм. LPWAN технологиясининг ривожланиш босқичлари.

Йирик уяли алоқа операторлари ва 3GPP, глобал уяли алоқа стандартлари ташкилоти, Sigfox ва Cycleo (Semtech) IoT LPWAN ихтисослашган тармоқларини яратганидан мамнун эмас эдилар, кўплаб саноат мижозларини жалб қила бошлаган бозорни уяли алоқа операторларини LPWAN бозоридан ажратиб қўйдилар. 3GPP LTE-Cat M1 ва NB-IoT (тор тармоқли IoT) стандарт лицензияланган тармоқли ичида ишлайдиган LPWAN уяли сифатида стандартлаштириш ва оммалаштиришни бошлади.

IoT уяли тармоқлари деярли ўн йил давомида ёритилмаган LPWANлар сифатида ишлаб чиқилган IoT тизимлари учун тобора оммалашиб бормоқда, аммо LoRaWAN ҳамон кенгайиб бормоқда. Семтеч - аниқ потентсиал ноаниқлик билан, 2019 йилга келиб LPWANларнинг 40 фоизи LoRa-да ишлади. (кейинчалик LoRa-га ўтамиз).

5Г LPWAN-нинг бутун манзарасини намойиш этишга тайёр. Бу паст кечикиш, кам қувват истеъмоли ва юқори маълумот узатиш тезлигини ваъда қилади –бу илгари эришиб бўлмайдиган комбинация. 3GPP шунингдек 5G технологиясига

лицензиясиз тармоқларда, хусусан 3,5 гигагерцли, 5 гигагерцли ва 60 гигагерцли частоталарда ишлашга рухсат беришни кўриб чиқмоқда. Бу LPWAN нурланмайдиган тармоқларига қўшимча таъсир кўрсатади. Бироқ, 3GPP ҳозирда стандартларни ишлаб чиқишни якунламоқда. Verizon ва AT&T компаниялари биринчи 5G тармоқларини синовдан ўтказа бошлаганлари сабабли, ҳали кўп нарса кўрилмоқда.

LPWAN ушбу даражага эришади, чунки уларнинг IoT қурилмалари вақти-вақти билан ёки камдан-кам ҳолларда фақат кичик маълумот тўпламларини - статус янгиланишлари, ҳисоботларни ва бошқаларни ташқи триггердан уйғонганидан ёки олдиндан дастурлаштирилган вақтдан кейин юборадилар. Бироқ, LPWAN уяли тармоғининг пайдо бўлиши билан, қуйида жадвалда кўрсатилгандек, "паст куч" ва "глобал тармоқ" ни аниқлашда кўпроқ мослашувчанлик мавжуд. (4.3-расм)

	Cat-1	Cat-0	e-MTC	NB-IOT	EC-GSM	LoRa	Sigfox
Specification	3GPP	3GPP	3GPP	3GPP	3GPP	Open	Private
Spectrum	Licensed	Licensed	Licensed	Licensed	Licensed	Unlicensed	Unlicensed
Channel BW	1.4MHz - 20MHz	1.4MHz - 20MHz	1.4MHz	180MHz	200MHz	7.8 - 500 KHz	200KHz
System BW	1.4MHz - 20MHz	1.4MHz - 20MHz	1.4MHz	180KHz	1.4MHz	125KHz	UL: 100dB DL: 600dB
Peak Data Rate	UL: 5Mbps DL: 10Mbps	UL: 1Mbps DL: 2Mbps	UL: 1Mbps DL: 800kbps	UL: 204.8 kbps DL: 234.7 kbps	UL: 74kbps DL: 74kbps	180bps ~ 37.5kbps	140 (Devices) 50000 (BTS)
Max. # of Messages/day	unlimited	unlimited	unlimited	unlimited	unlimited	50000(BTS)	14dBm
Device Peak Tx Power	23dBm	23dBm	23dBm	26dBm	26dBm	14dBm	14dBm
MCL (Maximum Coupling Loss)	144dB	144dB	156dB	164dB	164dB	UL: 156dB DL: 168(SF12, BW7.8) 132(SF6, BW125)	UL: 156dB DL: 147dB
Device Power Consumption	Medium	Medium	Low-Medium	Low	Low	Low-Medium	Low

2.3- расм. LPWAN даражалари

Ҳар бир технологияда чекловлар мавжуд. Аниқроқ айтганда, ҳеч қандай технология фойдаланиш ҳолатига боғлиқ эмас. Юқорида тавсифланган стсенарийлар учун LPWAN-лар жуда яхши, аммо улар тез-тез маълумотларни узатишни ва катта ҳажмларни талаб қиладиган ҳолатлар учун мос эмас. Одатда LPWAN-лар 300 бит / 50 кбит/с гача бўлган пакетларни олиб юрадилар. 56 кбит/с ёки dial-up Интернетни эслайсизми. Кўп LPWAN-ларга қараганда кўпроқ маълумот узатиш линиялари орқали узатилади.

LPWAN-лар ҳам муаммоларга дуч келиши мумкин, чунки улар кўпинча лицензиясиз диапазонларда ишлайди: саноат, илмий ва тиббий ("ISM") ҳукуматлар очиқ қолдирадиган полигонлар. Одатда ISM диапазонлари 915 МГц, 2,4 ГHz ва 5 ГHz ни ўз ичига олади. LPWAN эчимлари кўпинча ИСМ 902-928 МГц диапазонида ишлайди - фақат ГHz чегарасидан паст. Очиқ ҳавода ишлайдиган LPWAN қурилмаси - масалан, бинонинг ёки миноранинг тепасида, бу ГHz пастки

диапазонида кучсиз сигналларни юборадиган, юқори ГНz чегарасидан юқори ишлайдиган юқори энергияли сигналларнинг шовқини пайдо бўлиши мумкин.

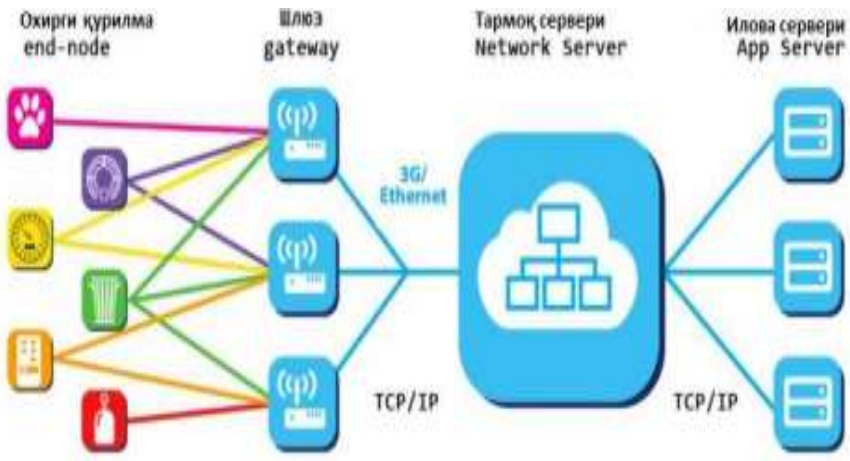
Бутун дунёда LPWAN нинг бир нечта тижорат тармоқлари мавжуд: Sigfox, «STRIJ», LoRaWAN асосида қурилган тармоқлар. Ривожланишнинг турли босқичларида янги технология ва стандартлар ишлаб чиқилган ва тадбиқ қилинган. Улар: eMTC, NB-IoT, EC-GSM-IoT, Weightless. LPWAN нинг асосий технологиялари таркибига кирувчи LoRaWAN технологиясини таҳлил қиламиз.

LoRaWAN стандарти техник хусусиятлари очиқ ҳисобланиб, тармоқни кенгайтириш учун ишлаб чиқарувчи ва ҳамкорлар томонидан ҳеч қандай чекловлар ва қандайдир шартномаларни тузишни талаб қилмайди. Шу ва бошқа омиллар LoRaWAN технологиясини танлашга бўлган эҳтиёжни оширди.

LoRaWAN (Long Range Wide-Area Networks) – бу катта радиусли кенг полосали тармоқлар деб таржима қилиниб, OSI нинг канал даражасидаги MAC протоколи ҳисобланади. LoRaWAN тармоғи оддий архитектурали «юлдуз» топологиясида қурилган бўлиб, тармоқ боғламалар кам қувват сарф қилувчи (10 йилгача хизмат қилувчи оддий батарейка), маълумот алмашиш учун катта бўлмаган тезликда лекин узоқ масофаларга (қишлоқ ҳудудларда 15 км гача, зич қурилган шаҳар ҳудудида 5 км гача) алоқа ва кам сарф харажатли охирги қурилмалар (терминаллар) билан характерланади.

LoRa технологияси паст частотали лицензиясиз частота диапозонида, спекторни кенгайтиришга асосланган (Spread Spectrum Modulation, SSM) ва тўғридан тўғри хатоларни тузатиш (Forward Error Correction, FEC) орқали чизиқли частота ўзгаришига (Chirp Spread Spectrum, CSS) асосланган модуляциялардан фойдаланади. Радиочастоталар бўйича давлат комиссияси қарорига мувофиқ, технологиялар хусусиятини ҳисобга олган ҳолда ва LoRaWAN ускунасида амалга ошириш имкониятидан келиб чиқиб частоталар режаси ишлаб чиқилди.

LoRaWAN тармоғи учун 125 кГц кенгликдаги 864-865 МГц частота диапазони (ишчи сикл 0,1% гача) ва 868,7-869,2 МГц га тенг эттита частота канали аниқланди. LoRaWAN тармоғи тузилиши қуйидаги 4.4-расмда келтирилган: Охирги қурилмалар (end-node), база станцияси (шлюзлар), тармоқ сервери, (МҚТТ-сервери), иловалар серверлардан (ORS сервери, SCADA-тизими, GIS сервери) иборат бўлади.



2.4 – расм. LoRaWAN тармоғининг тузилиши

Маълумотларни қайта ишлаш ва фойдаланувчи интерфейсини ташкил

қилишда маълумотлар оқими даражасида SCADA-тизимини ва геоинформатсион тизимларни интегратсия қилиш орқали амалга оширилади.

LoRaWAN тармоғи квартира ва умумий яшаш уйлари сув ҳисоблагичларидан, электр энергиясидан, газ ҳисоблагичларидан маълумотларни йиғиш ва узатиш жараёнини самарали автоматлаштиради.

LoRaWAN асосида яратилган ечимлар ҳаётимизнинг турли соҳаларида қўлланилиши мумкин, янги хизматларни яратиш, яъни аввалироқ, мос келувчи технологияларнинг қимматлиги ёки мавжуд эмаслиги туфайли умуман кўриб чиқилмаган хизматларни яратиш мумкин бўлди. Агросаноат комплекси, уй-жой коммунал хўжалиги, ишлаб чиқариш сектори, логистика ва омборхона, экологик хавфсизлик хизмати, соғлиқни сақлаш - буларнинг барчаси LPWAN нинг потенсиал истеъмолчилари ҳисобланади.

Шу билан бирга LoRaWAN технологияси локал ечимларни жойлаштириш учун муваффақиятли ишлатилиши мумкин. Ечимларни амалга оширишнинг иқтисодий самараси аниқ - бу тезкор жойлаштириш, ўрнатишнинг соддалиги, ташқи электр таъминоти тармоқларига уланмасдан қурилма тўлиқ ажралганлиги, ахборотнинг юқори хавфсизлиги ва арзон нархлар ҳисобланади. Бу технологияларни таълим тизимига бир қатор ривожланган мамлакатларда кенг жорий этилмоқда.

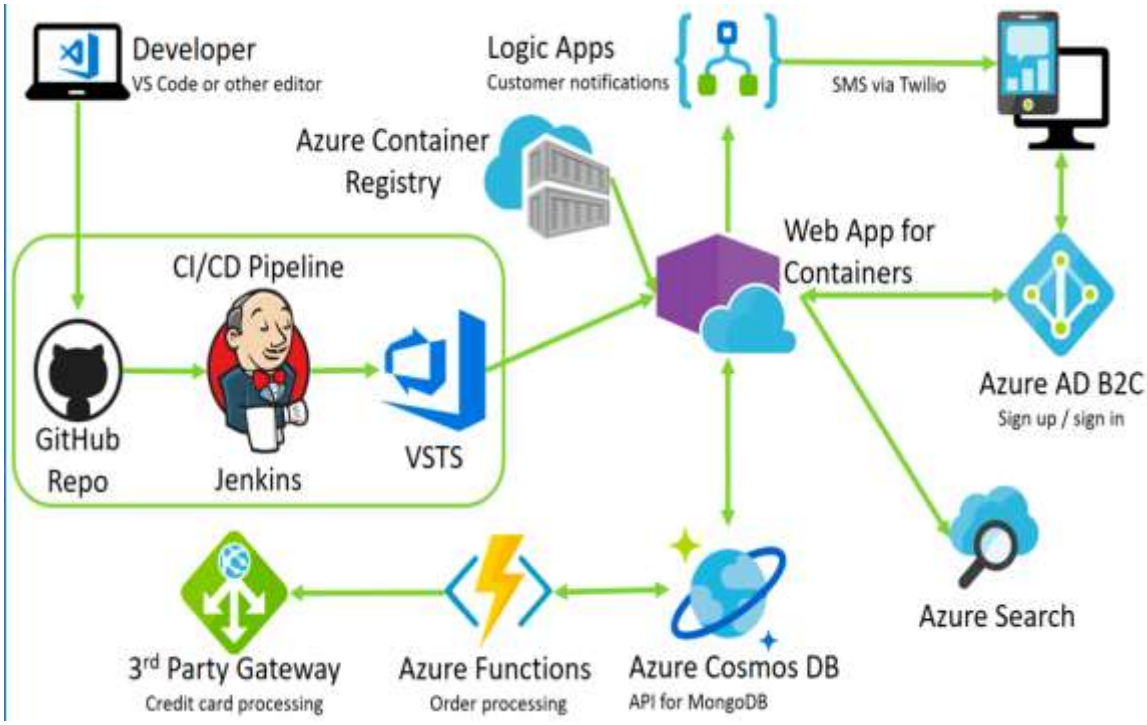
LoRaWAN тизимларининг асосий хусусиятлари:

- Узоқлик (> 5 км шаҳар,> 10 км шаҳар атрофи,> 80 км кўриш линияси)
- Батарея қуввати муддати (10 йил)
- Арзон нархлар (<$ 5 / модул)
- Маълумот узатишнинг паст тезлиги (0,3 бит / с - 50 кбит / с, кўпинча ~ 10 кБ / кун)
- Маҳаллийлаштиришни қўллаб-қувватлаш
- Икки томонлама
- Хавфсиз
- Лицензиясиз спектрларда ишлайди.

Барселонадаги Mobile World Congress 2019 - Бутунжаҳон мобил конгрессда Хитойнинг машҳур Huawei компанияси Huawei Enterprise йўналиши «Рақамли платформа», «ҳар қандай нуқтадан фойдаланиш имконияти» ва «ҳамма ерда ишлатиладиган интеллектуал тўплам ва маълумотларга қайта ишлаш» каби учта кўргазма майдонида тўртта флагман маҳсулотни намойиш қилди. Сунъий интеллект технологияси асосидаги ечимлар ва маҳсулотлар сингари ўзининг илғор технологиялари ҳамда манфаатли ва ишончли экотизимлардан ташқари, Huawei энтерприсе шаҳар транспорт тизимида ва чакана савдода сунъий интеллектдан фойдаланиш вариантларини тақдим этди.

Рақамли платформа: Ушбу майдонда булут, Интернет буюмлари ва маълумотларни тармоқда сақлашга оид all-flash каби илғор рақамли ечимлар, маълумотлар, бизнесдаги ўзаро алоқа ва охир оқибатда рақамли ўзгаришини тезлаштирувчи янги технологияларни адаптив татбиқ этиш жараёнини йўлга қўйиш учун қай тарзда Huawei Digital Platform рақамли платформасига интеграция қилиниши кўрсатилди. Бу ерда дунёдаги энг тезкор All Flash MTS OceanStore Dorado серияси, жумладан молия, саноат ва нефт соҳаларида рақамли ўзгаришларни тезлаштириш имконини берувчи ўрта ва юқори нарх

диапазонларидаги қурилмалар, шунингдек, OceanStore Dorado3000 V3 янги базавий ечими таништирилди. Бундан ташқари, Huawei Enterprise йўналиши шаҳарни янада интеллектуал бошқариш, коммунал хизматлар сифатини ошириш ва соҳани ривожлантириш учун интернет буюмлар, катта ҳажмли маълумотлар, географик маълумотлар, видео ва конвергент алоқаларни бирлаштирувчи ақлли шаҳарнинг рақамли платформасини кўрсатиб беради.



2.5- расм. Azure булутли хизмати тизими

Ҳар қандай нуқтадан фойдаланиш ва унинг имкониятлари CloudEngine16800 сунъий интеллект асосидаги MTM (маълумотларни таҳлил қилиш маркази) учун жаҳондаги илк коммутатор эканлигини кўрсатиб беради. У сунъий интеллектнинг (СИ) ҳисоблаш қувватини 50 % дан 100 % га, IPOS (сониясига кириш-чиқиш операциялари сони) маълумотлар омборини 30 % га оширади ва соҳа бўйича ўртача катталикни беш марта оширувчи коммутаторнинг самарадорлигини таъминлайди. Стендда 2019-йилда барча ссенарийлар учун янгиланган LAN Wi-Fi 6 янги ечими тақдим этилди. Wi-Fi соҳасида энг самарали ечим жаҳонда илк тижорий кира олиш нуқтаси Wi-Fi 6 ва унинг энг кенг қамровли портфолиоси Wi-Fi 6 ларни ўз ичига олади, уларга офислар учун AP7650 (ақлли антенна), чакана савдо учун AP7060DN (IoT-карта) ва таълим учун AP8660 (учталик радиочастоталар) киради. У Пудун, Шанхай (Shanghai Pudong Education Bureau) таълим бюроларида ва Хитойдаги Фудан университети «симсиз ақлли кампус»да (Wireless Smart Campus) йўлга қўйилган.

2.3. NB-IoT технологияси.

Мобил алоқанинг кейинги авлоди 5G жорий этилиши билан IoT хизматидан ташқари, катта эътибор тўғридан тўғри IoT технологиясига, жумладан, M2M

(Machine to Machine) ва MTC/eMTC (Machine Type Communications/enhanced MTC), бундан ташқари тор полосали LTE – M, NB – IoT (Norrowband IoT) ва EC-GSM (Extended Coverage GSM) технологияларга қаратилмоқда.

Юқорида санаб ўтилган технологиялардан IoT хизматларини тақдим қилишдан олдин, унга махсус талаб қўйилади: кам сарф харажат ва охирги қурилманинг электр манбаи узоқ муддат ишлаши (10 йилгача).

Солиштириш учун 2.1- жадвалга қаранг.

2.1-жадвал

Кўрсаткичлар (параметрлар)	LTE- M	NB- IoT (LTE)	EC - GSM	5G
Масофаси, км	<11	<15		
Уланишдаги минимал йўқотиш, дб	156	164		
Канал полосаси, МГц	14	0,2		-
Маълумот узатиш тезлиги	<1Мбит/с	<150Кбит/с	<10Кбит/с	<1Мбит/с
Манбанинг ишлаш муддати	>10			

Шулардан кенг тарқалгани, тор паласали NB–IoT технологияси ҳисобланади. Энг асосийси LTE тармоқ архитектура базаси қамраб олинган барча ҳудудларда NB–IoT ни қуриш мумкин бўлади. NB–IoT технологиясини амалий қўлланилишидаги барча саволлар, унинг техник жиҳатлари, хусусан частота режалаштирилиши ва радиовоситалар билан электромагнит мослашуви билан боғиқ бўлади.

NB–IoT нинг техник хусусиятларининг бир нечтасини қуйида келтириб ўтамиз:

- Радиорухсат усули: линиядан пастга (downлинк) 15 кГц частота фарқи билан (12 ташувчи) OFDMA усули; линиядан тепага (уплинк) 15 кГц частота фарқи билан (12 ташувчи) ва 3,75 кГц частота фарқи билан (48 ташувчи) SC-FDMA усули;

- Устувор фойдаланувчи радиочастоталар полосаси: 2100 МГц (банд 1), 1800 МГц (банд 3), 900 МГц (банд 8), 800 МГц(банд 20) ва 700 МГц (банд 28). Шунингдек 3GPP стандартида 450 МГц (банд 31) радиочастота полосасини қўшилиши кутилмоқда;

- Дуплекс: Частотали ярим дуплекс FDD-HD (Half-Duplex) режимини қўллаб қувватлайди, Вақт бўйича дуплекс TDD ни қўллаб қувватламайди;

- NB-IoT канал ташкил қилиш 3 вариантда амалга оширилади, булар ички —фаол LTE канал полосаси (in-band), ҳимояланган LTE канал полосаси (guard-band) ва алоҳида/мустақил канал (standalone)/ NB-IoT нинг канал кенглиги:180 кГц (in-band, guard-band) ёки 200 кГс (standalone);

- Нурланиш қуввати; абонент қурилмаси учун UE (User Equipment)- 20dBm (class 5) ёки 23dBm (class 3); База станцияси учун BS (Base Station)- in-band ва guard-band режимида умумий қуввати LTE ва NB-IoT каналлар орасида тақсимланади ва LTE канал кенглиги 10МГц, 15МГц ва 20МГц бўлганда NB-IoT битта ташувчи частотаси ошиши мумкин. NB-IoT учун динамик диапазон 6 дБ ни ташкил қилади.

Частота режалаштирилишида (частота тавсиясида) қуйидаги шартлар

ўрганилади:

1. Частота ўқида 100 кГц ни ташкил қилувчи растр канал;

2. NB-IoT учун пастга DL(downlink) ва юқорига UL(uplink) частота канал тавсияси қуйидагича:

F DL = F DL_low + 0,1 (N DL – N Off-DL) + 0,0025 (2M DL + 1);

F UL = F UL_low + 0,1 (N UL – N Off-UL) + 0,0025 (2M UL);

Бу ерда F DL, F UL, N Off-DL va N Off-UL лар 3GPP TS 36.101, TS 36.104; жадвалидаги параметрлар, N DL ва N UL – радиочастота каналининг абсалют номери (0-262143 диапозон номери); M DL ва M UL – оддий LTE каналидан NB-IoT каналига силжиши.

M DL: {-10; -9; -8; -7; -6; -5; -4; -3; -2; -1; -0,5; 0; 1; 2; 3; 4; 5; 6; 7; 8; 9}

M UL:{-10; -9; -8; -7; -6; -5; -4; -3; -2; -1; 0; 1; 2; 3; 4; 5; 6; 7; 8; 9}

NB-IoT нинг стандалоне режимида фақатгина M DL = -0,5 ва M UL = 0 тавсиясидан фойдаланади. Қолган иккита режимда бу тавсиядан фойдаланмайди.

NB-IoT нинг бошқа радиовоситалар билан электромагнит мослашувчанлиги NB-IoT технологияси бир нечта турдаги тизимлар билан жумладан, тор полосали стандалоне, кенг полосали in-band ва аралаш гуард-банд режимида бўлади. Бунинг барчаси бошқа радиовоситалар билан электромагнит мослашиши бир хил шартда бўлмайди. NB-IoT технологиясини қўллашда, электромагнит мослашиши ҳақида гап кетганда қуйидаги ҳолатларни белгилаймиз:

1. Қуйидаги келтирилган технологиялар билан NB-IoT каналларини эММ ни таъминлашда қўшимча шартларни киритишга ҳожат йўқ:

- LTE–eMTC – EMM томонидан қараганда бу LTE эквивалент стандарти ҳисобланади.
- EC GSM – GSM нинг эквивалент стандарти ҳисобланади.
- NB-IoT – LTE (in-band) канал полосасида у спектрал москасини ўзгартиришни таклиф қилмайди.

2. Юқорида келтирилгандек, 200 кГц фарқи сабаб, талаб бажарилмайдиган бунақанги бир нечта ҳолатларда, 5 МГц ни ташкил етувчи LTE канал кенглиги қачонки, ҳимояланган полосада NB-IoT каналлар аралашмасида алоҳида ўрганиш талаб этилишини қўшимча қилиш мумкин.

3. NB-IoT аралаш каналлар орасидаги сифат кўрсаткичлари бошқа технологиялар кўрсаткичлари билан қуйидагича амалга оширилади:

- 5% дан ошмаган йўқотиш зарурати;
- Сигнал/шовқин нисбати 1 дБ дан ошмаслиги зарурати.

Ўтказилган изланишлар натижаси шуни кўрсатадики, NB-IoT каналларидан фойдаланишларида LTE канали стандартлаштирилган полосали (in-band) ни жойлаштирилишида ҳеч қандай ўлчовлар талаб этилмайди, шунингдек, NB-IoT канали ҳимояланган полосаси (guard-band) ни жойлаштирилишида LTE канал кенглиги 5 МГц дан катта бўлиши талаб қилинади.

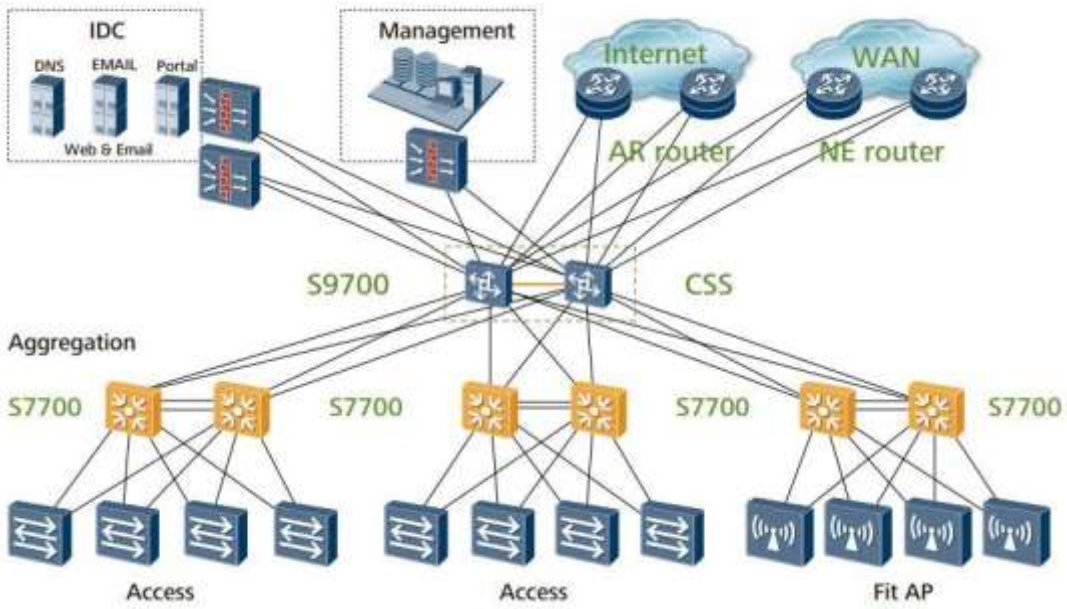
NB-IoT нинг мустақил канали (standalone) дан фойдаланишида 900 МГц дапазон частотада, GSM, UMTS ва LTE каналларининг тавсия қилинган частота фарқини сақлашни талаб қилади.

Huawei S7706 Smart Campus коммутатори

C7700 сериядаги коммутаторлар – бу келажак авлод корпоратив тармоқларига мўлжалланган юқори даражали интеллектуал йўналтиргичлардир. C7700

конструкцияси Huawei коммутациясининг кўп даражали интеллектуал технологияларига асосланади, MPLS VPN каби трафик таҳлили, H-QoS комплекс сиёсатлари, кўп манзилли жўнатмаларни бошқариш, хавфсизлик ва юкламаларни мувозанатлаш ҳамда 4 даражали коммутасион хизматлар каби вазифаларни бажаради.

Унинг яна муҳим имкониятларидан бири, кампус тармоғида ёки маълумотларни қайта ишлаш марказида симсиз алоқани бирлаштиришни таъминлаш учун базавий ёки агрегат тугун ҳолатда функсияланиши мумкин. C7700 овозни, видео ва маълумотларни узатиш хизматлари, шу билан бирга ташкилотларга иқтисодий очиқ тармоқ қуришга ёрдам бериш каби хизматларни таклиф қилади.



4.6 – расм. *Huawei S7706 Smart Campus коммутаторида тармоқ тузилмаси*

Бутун дунё бўйлаб интеллектуал тўплам ва маълумотларни қайта ишлаш ушбу доирада жаҳонда биринчи дастурий аниқланадиган Huawei X серияли камералари қай тарзда ссенарий асосидаги талаб, ўз-ўзини таҳлил қилиш ва адаптив таълим бўйича ссенарийларни аниқлаш ҳисобига бутун дунё бўйлаб интеллектуал тўплам ва маълумотларни қайта ишлаши намойиш қилинган. Huawei SI функционали кучи бир қатор бизнес-ссенарийлар учун турли соҳаларда фойдаланиш усулларининг кўплигида ўз аксини топган.

DHL ва Huawei биргаликда логистик операциялар самарадорлигини ошириш, шунингдек логистиканинг тўлиқ секторига ёрдам бериш учун Huawei IoT технологиялари асосида инқилобий Smart Logistics Solution кўп ссенарийли ечимини ишлаб чиқишди. Huawei ва Италиядаги Сардиния шаҳри ақлли шаҳарни ривожлантириш учун рақамли платформадан фойдаланмоқда.

Рақамли трансформация илғорлари билан кучларни бирлаштириб Huawei Enterprise йўналиши турли соҳаларда фаолият юритадиган мижозлар ва ҳамкорларга рақамли трансформациялар соҳасида илғор ишланмалари ҳақида фикр алмашишларини таклиф қилди. Кўплаб фикрлар ва ссенарийларни тақдим этган Huawei Enterprise ўзининг мижозларига улар рақамли бизнес-инқилобнинг иштирокчиларига айланишлари, шунингдек янгича фойдаланиш йўлларини ишлаб

чиқишда уларни руҳлантириш учун адаптив ва интеллектуал асосни яратишда ёрдам беришга уринмоқда.

2.4. IoT - буюмлар интернети соҳасида хавфсизлик масалалари

Охирги пайтларда ахборот хавфсизлиги масаласига тегишли бўлган барча тадбирларда энг кўп муҳокама қилинаётган асосий масалалардан бири бу “буюмлар интернети” ҳисобланади. Айнан ушбу технология ўтган йили ҳам ушбу соҳа мутахассислар ақлини кўпроқ эгаллаб, турли оммавий ахборот воситаларидаги янгиликларда тез-тез учраб турди. Экспертларнинг фикрича ушбу тенденсия келгусида ҳам пастламайди. Шу сабабли, ушбу мақоламизда “буюмлар интернети” номи остида қўлланиладиган технологиялар томонидан айни пайтда этказилиши мумкин бўлган долзарб хавфлар кўриб чиқилади.

Интернетга чиқиши мавжуд бўлган кўп сонли қурилмалар бузилишдан этарли даражада ҳимояланмаган бўлади. Уларнинг кўпчилигига бир хил пароллар ўрнатилган бўлиб, баъзиларида кўпчиликка маълум бўлсада, бироқ тузатилмаган заифликлар мавжуд. “Ақлли” буюмларни ишлаб чиқарувчилар аксарият ҳолатларда хавфсизлик масалаларига бефарқлик муносабатида бўлади, фойдаланувчиларнинг эса, уйидаги ҳар бир буюм билан шуғулланишга вақти бўлмайди. Бундай вазият эса фожеавий оқибатларга олиб келади. Ўтган йили “нарсалар интернети” билан боғлиқ ҳодисалар орасида энг овоза бўлгани Мираж ботнети бўлди. У деярли бутунлай обрўсизлантирилган IoT-қурилмалардан ташкил топган бўлиб, тарихдаги энг йирик ДДоС-ҳужумларга сабаб бўлди. Қонунбузарлар фаолиятининг асосий мазмуни, IoT-қурилмаларни бошқаришда кўп фойдаланадиган соддалаштрилган Линух версияси бошқарувидаги қурилмаларга кириб борадиган троян дастуридан фойдаланишдан ташкил топган. Бунда бузиб кириш ҳаракатининг ўзи унчалик мураккаб эмас бўлиб чиқди дастур бор-йўғи 61 та дефолтли логинлар ва пароллар комбинатсиясини тўлиқ териш усули орқали қурилмага киришни қўлга киритган. Бироқ обрўсизлантирилган қурилмаларнинг умумий сони 493 мингдан ошган эди. Уларнинг орасида терморегуляторлар, совутгичлар ва тостерлар каби “ақлли буюмлар” ҳам мавжуд эди. Мираж ботнетидан DDoS -ҳужумлар чўққига чиққан вақтда уларнинг тезлиги бир сонияда бир террабайтгача этган. DNS операторига уюштирилган ҳужумда ушбу ботнетдан фойдаланиш, ҳужумни қайтариш учун қўлланилган тезкор тадбирларга қарамасдан таниқли бир қатор хизматларга киришда муаммолар туғдирди, булар жумласига Twitter, GitHub, Soundcloud ва Spotify хизматлари киради.

Ҳар кунлик ҳаётимизга юксак технологияларнинг кириб келиши янгидан-янги хавфларни тақдим қилади. Яқингача қонунбузарларнинг фаоллиги ахборот хавфсизлиги билан чекланган бўлса, ҳозирда хавф остига одамларнинг ҳаёти ва соғлиги қолмоқда. Ҳозирча булар ҳавотирли таҳмин ҳисобланади, бироқ ҳаётий реаллик IoT-қурилмалар билан ишлашда жисмоний хавфсизлик ҳақида бугундан қайғуришга мажбур қилмоқда. Энг долзарб масала – кун сайин “ақлли” бўлиб бораётган автомобиллар ҳисобланади. Бугунги кунда автоном машиналар Гонконг, Дубай, АҚШнинг бир қатор штатлари ва Европанинг баъзи мамлакатларида кўча кезиб юрибди. Аммо бундай автоном автомобиллар баъзида халокатга учрайди, масалан, Тесла автопилотининг ишидаги носозликлар билан боғлиқ нохуш ҳодисалар кўп муҳокамага учрайдиган ҳолат бўлди. Ушбу ҳодисалар учун

жавобгарликни ўз зиммасига автомобил эгаси олиши керакми ё унинг ишлаб чиқарувчисими, буни ҳали аниқлаш зарур. Автопилот тизимини ҳисобга олмаган ҳолда ҳам, биламизки, замонавий автомобил турли юқори технологияли модуллар билан, бошқарув датчиклари ва воситалари билан жиҳозланган, улар, табиийки, дистанцион бошқарувга эга, шу жумладан интернет орқали ҳам.

Борган сари, автомобиллардаги муаммолар ҳақида янгидан-янги хабарлар тарқалмоқда, улар машиналарнинг механизмлари билан эмас, балки, айнан дастурий таъминот билан боғлиқ. Ушбу дастурий таъминотнинг хавфсизлиги, ҳудди маиший IoT-қурилмаларининг ҳолатидагидек ҳали анчагина иш талаб қиладиган аҳволда. Ушбу муаммо турли ишлаб чиқарувчиларга тегишли: масалан, ўтган йилнинг кузида General Motors компанияси дастурий таъминотдаги хатоликлар туфайли 3 миллиондан ортиқ автомобилларни қайтариб олишга мажбур бўлди, ушбу хатоликлар хавфсизлик ёстиқчаси ва хавфсизлик камарининг носозликлари билан боғлиқ бўлган. Шунингдек, Volkswagen консерни билан содир бўлган жанжал ҳақидаги овоза кенг тарқалди, бунда автомобилларга зарарли моддаларни чиқаришнинг реал кўрсаткичларини пасайтириб кўрсатувчи дастур ўрнатилган. Бундан ташқари, автомобилларни “компютерлаштириш” сабабли уларни масофали бузиш имкони мавжуд бўлди. Шу йўл билан тадқиқотчилар ва хакерлар Chrysler, Tesla, Mitsubishi компанияларига тегишли ва бир қанча бошқа русумдаги автомобилларга авторизатсияланмаган кириш ҳуқуқини қўлга киритишди. Агар автомобилларни бузиш – унчалик қўрқинчли туюлмаса, у ҳолда тиббиёт соҳасидаги ишлар умуман ўзгача аҳволда. Юксак технологиялар тиббиёт ходимларига катта имкониятлар тақдим этади, телемедитсинадан тортиб, то диагностика ва даволашнинг замонавий усулларигача. Бироқ бу ерда ҳам хавфсизлик масаласи ҳал қилинмаган. Тиббиёт техникасини ишлаб чиқарувчи мутахассислар кўпинча ёвуз ниятлиларнинг аралашиш эҳтимолини эътибордан четда қолдирадилар. Ахборот хавфсизлигининг экспертлари телемедицинага оид сервислар ва техник воситаларни таҳлил қилиб, ҳавотирли хулосага келдилар – касал ва шифокор орасидаги боғланиш аксарият ҳолатларда заиф ҳисобланади. Ушбу муаммони шифрлашни қўллаган ҳолда бартараф этса бўлади, бироқ, телемедитсина учун аллақачон заиф шифрланмаган протоколли асбоблардан фойдаланилмоқда. Сурункали оғир касалликлари бўлган одамлар эгнида олиб юрувчи қурилмалар уларнинг соғлиги учун алоҳида хавф туғдиради, булар инсулин помпалари ва кардиостимуляторлар. Заиф симсиз узаткичлар кардиостимуляторлар ва дефибрилляторларга топшириқ юбориши мумкин, қурилмаларнинг кўпчилиги эса 830 волтгача бўлган токни генератсия қила олиши мумкин. Кўпчилик давлатларда бундай қурилмаларнинг сифати учун тўғридан-тўғри жавоб берадиган мутасадди идоралар мавжуд эмас.

Кенгайиб бораётган “буюмлар интернети”га оид бўлган яна бир масала, бу фойдаланувчиларнинг ғайрирасмийлиги масаласидир. Гап шундаки, “ақлли” қурилмалар ўз эгалари тўғрисида анчагина миқдорда маълумот тўплайди. Қурилмалар эгалари ҳақида, уларнинг ишлаб чиқарувчилари ҳам айнан нимани билишлари устидан деярли назорат қилиб бўлмай қолди.

Ноқулай, бироқ оптимистик ссенарийда ушбу маълумотлар реклама берувчиларга сотилиши мумкин. Аммо ушбу маълумотлар қонунбузарлар қўлига тушиб қолса вазият бошқа кўриниш олиши турган гап. Бундай қурилмалардан олинган маълумотлар фойдаланувчининг максимал даражадаги тўлиқ ва батафсил

“портрети”ни шакллантириб бериши мумкин. Бугунги куннинг ўзида Шодан хизмати ёрдамида анча кенг миқдордаги веб-камералардан видео томоша қилиш мумкин. Фойдаланувчилар аллақачон ушбу хизмат орқали банклар, коллеж ва мактабларни, полиция ходимларининг бузилган камераларидан трансляцияларни, хусусий уйлар ва беби-мониторлар “кузатуви” даги ухлаётган кўп сонли ёш болаларни томоша қилиш йўлларини аниқлаб топганлар.

Бундан ташқари, кўпчилик фойдаланувчилар бу вазият билан боғлиқ бўлган давлатнинг ўз фуқаролари устидан кузатиб юриш ҳолатларининг кўпайиб кетишидан ҳавотирдалар. Кўп давлатларнинг махсус хизматлари таҳмин қилинаётган қонунбузарларни асоссиз кузатувга олганликлари ва рақамли соҳадаги ваколатларидан ҳаддан ортиқ фойдаланганликлари сабабли танқид остида кўп қолмоқдалар. Бу борада уйларимиздаги “ақлли” қурилмаларимиз анчагина катта бўлган ҳажмдаги маълумотларни тақдим этмоқда. Мисол тариқасида АҚШнинг Арканзас штатида содир бўлган воқеани келтириб ўтамиз. Хонадон эгаси томонидан Амазон компаниясидан сотиб олинган ақлли колонка мудхиш қотилликнинг “гувоҳи”га айланди. Тергов олиб борувчилар ушбу қотилликни хонадон соҳиби содир этган деб ҳисобламоқдалар. Амазон эчо колонкаси овозли бошқарувга эга ва мувофиқ равишда уйда рўй бераётган барча нарсаларни эшитади ва ёзиб олади. Колонкадан ташқари политсия ашёвий далил сифатида “ақлли уй”нинг бошқа қурилмаларидан ҳам фойдаланган: термостат, сигнализатсия тизими ва сув ўлчагичдан.

“Интернет буюмлар” билан боғлиқ муаммолар барчага маълум, бироқ уларнинг йечимини тезлик билан топишга ҳозирча имкон мавжуд эмас. Бунга қарамай, бу йўналишда силжишлар кузатилмоқда. Яқиндан бошлаб давлатлар ушбу мавзу билан жиддий шуғуллана бошладилар. Масалан, Россияда 2017 йилда индустриал интернетга оид норматив-ҳуқуқий базани яратиш бўйича ҳаракатлар бошлаб юборилди. Жумладан, ускуналар ва дастурий таъминот даражасида маълумотларни тўплаш инфратузилмасига талаблар ишлаб чиқилган ва маълумотларни тўплаш, ишлов бериш ва сақлаш тартиблари белгиланган. Америка ҳукумати ҳам борган сари IoT-қурилмаларига тегишли муаммолар билан кўпроқ шуғуллана бошлаган. Хусусан, АҚШнинг Ички хавфсизлики вазири ва Ички хавфсизлик департаменти ишлаб чиқарувчиларни қурилмаларни хавфсизликларини, юқорида келтириб ўтилган DNS-провайдерга уюштирилган DDoS -ҳужумдан сўнг максимал даражада таъминлашларига чақирдилар.

2017 йилда Тошкент шахрида «ICTWEEK Uzbekistan – 2017» ахборот-коммуникация технологиялари ҳафталиги доирасида Халқаро электралоқалар иттифоқининг «IoT» буюмлар интернети соҳаси кибер хавфсизлигининг муҳим масалаларига бағишланган ҳудудий семинар ўтказилди.

Ўзбекистон Ахборот технологиялари ва коммуникацияларни ривожлантириш вазирлиги ҳамда Халқаро электралоқалар иттифоқи томонидан ташкил этилган тадбирда Ўзбекистон, Молдова, Украина, Қозоғистон, Россиядан олим ва мутахассислар, «Cisco», «ZTE», «Huawei», «Microsoft», «Softline» компаниялари вакиллари иштирок этдилар. Илмий-техник тараққиёт интернет-технологияларидан фойдаланиш кўламини кенгайтириш имконини беради. Ҳозирги вақтда электр жиҳозларининг сўнгги моделларига интернет тармоғига уланиш имконини берувчи ускуна ва мосламалар ўрнатилмоқда. Бу жиҳозларни лойиҳалаш ва фойдаланишда ахборот хавфсизлигини таъминлаш мажбурий талаблардан биридир. Шу жиҳатдан

Ўзбекистонда электрон ускуна ва тизимлар кибер хавфсизлигини ошириш юзасидан салмоқли ишлар амалга оширилмоқда. Семинарда кибер хавфсизлик масалаларида давлат ва халқаро ҳамкорликнинг аҳамияти хақида сўз юритилди. Ахборот хавфсизлиги бутун дунёда АКТ барқарор ривожланишининг муҳим тамойилларидан бири экани тан олинган. Ҳар бир давлатда кибер таҳдидларга қарши курашувчи механизм ва ташкилотлар шакллантирилган ёки шакллантирилмоқда.

Президентимизнинг 2017 йил 29 августдаги «Ахборот-коммуникатсия технологиялари соҳасида лойиҳа бошқаруви тизимини янада такомиллаштириш чора-тадбирлари тўғрисида"ги қарорига мувофиқ, Ўзбекистонда Ахборот хавфсизлиги ва жамоат тартибини таъминлашга кўмаклашиш маркази ташкил этилди. Марказнинг вазифаси ахборот хавфсизлигига рахна солаётган замонавий таҳдидлар ҳақида маълумот йиғиш, уларни таҳлил қилиш ва сақлаш, давлат ташкилотларининг ахборот тизимлари, маълумотлар захираси ва базасига ноқонуний киришнинг олдини олишга қаратилган самарали ташкилий ва дастурий-техник ечимларни қабул қилиш бўйича таклиф ва тавсиялар ишлаб чиқишдир. Зеро, ҳеч қандай чегара мавжуд бўлмаган интернет оламидаги кибержиноятлар тобора халқаро тус олмоқда. Бу таҳдидларга қарши курашиш учун Марказий Осиё давлатлари орасида биринчи бўлиб Ўзбекистон ахборот ва коммуникация технологиялари соҳасида халқаро хавфсизлик тизимига қўшилди.

Назорат саволлари:

1. SMART технология ҳақида маълумот беринг.
2. IoT (Internet of things) – буюмлар интернети нима?
3. NB-IoT технологиясини тушинтиринг.
4. Azure IoT Edge иловасининг вазифаси нимада?
5. IoT - буюмлар интернети соҳасида хавфсизлик масалалари нималардан иборат?

Адабиётлар ва Интернет сайтлари:

1. Эшмурадов А.М., Абдужалилов Ж.А. “Интернет тармоқлари ва хизматлари” фанидан ўқув-услубий мажмуа. – Тошкент: ТАТУ. 2016.
2. Олифер Виктор, Наталия Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Сн-Петербург: Издательство ПИТЕР, 2016, 992 с.
3. Douglas E. Comer. Computer Networks and Internets (6th Edition). Pearson. USA, 2015. 672 p.
4. Компьютерные сети и технологии. http://www.xnets.ru/
5. http://www.network.xsp.ru/
6. https://iot.ru/

3-маъруза. Компьютер тармоқларида ахборотни ҳимоя қилиш усуллари. Криптография усуллари. Симметрик криптотизимлар. Очиқ калитли шифрлаш. Хеш функция.
(2 соат)

Режа:

3.1. Тармоқда ахборотни ҳимоя қилишнинг асосий воситалари
3.2. Криптография усуллари. Симметрик криптотизимлар.
3.3. Очиқ калитли шифрлаш.
3.4. Хеш функция.

Таянч иборалар: *криптография, симметрик криптотизимлар, очиқ калитли шифрлаш, хеш функция.*

3.1. Тармоқда ахборотни ҳимоя қилишнинг асосий воситалари.

Умумий ахборот кенглигининг яратилиши ва шахсий компьютерларнинг амалий жиҳатдан кенг қўлланилиши ва компьютер тизимлари ва тармоқларининг татбиқ этилиши ахборотни ҳимоя қилиш муаммосини ечиш зарурлигини келтириб чиқаради.

Ахборотни ҳимоя қилиш деганда замонавий компьютер тизимларида ва тармоқларида узатилаётган, сақланаётган ва қайта ишланаётган ахборотнинг ишончлилигини ва бутунлигини тизимли таъминлаш мақсадида турли хил воситаларни ва усулларни ишлатиш, чораларни кўриш ва тадбирларни ўтказиш тушунилади.

Ахборотни ҳимоя қилиш - бу:

– ахборотнинг физик бутунлигини таъминлаш, яъни ахборот элементларини тўсиқларга учрашига ва йўқолишига йўл қўймаслик;

– ахборот бутунлигини сақлашда унинг элементларини алмаштиришга (модификацияга) йўл қўймаслик;

– мос ваколатларга эга бўлмаган шахслар ёки жараёнлар томонидан тақиқланган ахборотни олинишига йўл қўймаслик;

– егаларига узатилаётган ресурслар фақатгина томонлар келишган шартларга мос равишда ишлатилишига ишонч ҳосил қилиниши керак.

Глобал тармоқларнинг ривожланиши ва ахборотларни олиш, қайта ишлаш ва узатишнинг янги технологиялари пайдо бўлиши билан Интернет тармоғига ҳар хил шахс ва ташкилотларнинг эътибори қаратилди. Кўплаб ташкилотлар ўз локал тармоқларини глобал тармоқларга улашга қарор қилишган ва ҳозирги пайтда WWW, FTP, Gophes ва бошқа серверлардан фойдаланишмоқда. Тижорат мақсадида ишлатилувчи ёки давлат сири бўлган ахборотларнинг глобал тармоқлар бўйича жойларга узатиш имкони пайдо бўлди ва ўз навбатида, шу ахборотларни ҳимоялаш тизимида малакали мутахассисларга эҳтиёж туғилмоқда.

Глобал тармоқлардан фойдаланиш бу фақатгина «қизиқарли» ахборотларни излаш эмас, балки тижорат мақсадида ва бошқа аҳамиятга молик ишларни бажаришдан иборат. Бундай фаолият вақтида ахборотларни ҳимоялаш воситаларининг йўқлиги туфайли кўплаб талофотларга дуч келиш мумкин.

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, видеоконференсия 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.

Ахборот хавфсизлиги бўйича йўл қўйиладиган кенг тарқалган ўнта хатолар:

a) Стикерларда пароллар;
b) Компьютерни ишлаш пайтида қаровсиз қолдириш;
c) Бегона компьютерларда элестрон почта иловаларини очиш;
d) Паролнинг ёмон тузилиши (ҳайвонлар, автомобиллар номлари, исмлар);
e) Портатив компьютерлардан эркин фойдаланиш;
f) Маҳмадоналик;
g) Ишга солиш ва ўйнаш;
h) Қайд этилмаган хавфсизликни бузиш;

i) Хавфсизлик тизими бўйича янгиланишларни ўрнатишни доим кейинга қолдириш;

j) Ташкилот ичидаги хавфларга эътиборсизлик.

Ҳозирги кунда ахборот-коммуникатсия тизимларига бўладиган тахдидлар, руҳсатсиз тизимга кириш ҳолатлари турли хил йўллар билан амалга оширилишига жавобан хавфсизликни таъминлаш турли хил усуллар ва воситалар ёрдамида амалга оширилмоқда.

Ахборот хавфсизлиги таъминлашнинг биринчи ва энг асосий воситаси бу – фойдаланувчиларни идентификациялаш ва аутентификациядан ўтказишдир.

Идентификация – фойдаланувчининг рўйхат ёзуви (логин) ни киритиши. Фойдаланувчининг тизимдаги логини орқали у ҳақидаги барча керакли ахборотларга: унинг шахси; тизимдаги руҳсат даражаси; тизимдаги фаолияти тарихи ва бошқалар эга бўлиш мумкин.

Аутентификация – бу фойдаланувчининг шахсини тасдиқлаши. Одатда бу жараён махфий сўз (парол) орқали амалга оширилади. Яъни фойдаланувчи дастлаб тизимга ўзининг калит сўзини киритади ва сўнг шу калит сўз ростдан ҳам унга тегишли эканлигини махфий сўз орқали тасдиқлайди.

Идентификация ва аутентитификация воситалари бирлашиши ҳам мумкин. Бу ерда барчамиз учун маълум бўлган хизмат гувоҳномасини келтириш мумкин. Унда шахснинг идентификацияси учун исми, фамилияси, мансаби (ва бошқа маълумотлар), аутентификация учун эса унинг сурати келтирилганлигини айтишимиз мумкин. Шуни алоҳида таъкидлаш керакки аутентификация ва идентификация воситаларининг ўзи ҳақиқийликни тасдиқловчи белгиларга эга бўлиши мумкин. Мисол учун гувоҳномадаги муҳр, имзо ёки унинг ҳимоясини сақловчи бошқа қалбакилаштиришдан ҳимояловчи воситалар.

Агар фойдаланувчи бу жараёнлардан муваффақиятли ўтса, у ахборот тизимига киришига ва унга берилган ваколат даражасида исталганча фойдаланиш ҳуқуқига эга бўлади.

Ҳозирги вақтда ахборот–ҳисоблаш тизимларида фойдаланувчиларни аутентификация ва идентификациялашнинг усулларини қуйидаги асосий гуруҳларга бўлиш мумкин:

– фойдаланувчидан қандайдир махсус ахборотни сўраш (масалан, логин ёки парол);

– фойдаланувчидан қандайдир махсус тавсияга ёки хусусиятга эга бўлган ашёни сўраш (масалан, smart-card, USB-token ва бошқалар);

– аутентификация қилинаётган ахборот фойдаланувчи танасининг муҳим қисми (масалан, бармоқ излари ёки бошқа биометрик маълумотлар).

Демак, идентификация ва аутентификация ёрдамида тизимга кириш ҳуқуқини олиш мумкин. Энди фойдаланиш чегарасини белгиловчи мантиқий бошқарув воситаси ишга тушади. Уларнинг вазифаси ҳам фойдаланишга руҳсат берувчи физик воситалар кабидир. Фойдаланишга руҳсат беришнинг мантиқий бошқарув воситалари ҳам фойдаланувчиларни тизимда сақланаётган у ёки бу ахборот бўлимига мурожаатини назорат қилади. Фойдаланишга руҳсат беришни мантиқий бошқаруви – бу ахборотни бутунлиги ва маҳфийлигини таъминлаб берадиган кўп фойдаланувчили тизимнинг асосий механизмидир.

Тармоқ хавфсизлиги – бу тармоқдаги маълумотларни ҳимоялаш чора-тадбирлари бўлиб, улар: руҳсат этилмаган мурожаатдан ҳимоялаш; тизимнинг

меъёрида ишлашига тасодифан ёки атайлаб таъсир қилишдан ҳимоялаш; тизим таркибий қисмларига зарар этказишдан сақлашдан иборат.

3.2. Криптография усуллари. Симметрик криптотизимлар.

Ҳозирги вақтда криптография деганда ҳар қандай шаклдаги, яъни дискда сақланадиган сонлар кўринишида ёки компютер тармоқларида узатиладиган хабарлар кўринишидаги ахборотни яшириш тушунилади. Криптографияни рақамлар билан кодланиши мумкин бўлган ҳар қандай ахборотга нисбатан қўллаш мумкин. Махфийликни таъминлашга қаратилган криптография кенгроқ қўлланилиш доирасига эга. Аниқроқ айтганда, криптографияда қўлланиладиган усулларнинг ўзи ахборотни ҳимоялаш билан боғлиқ бўлган кўп жараёнларда ишлатилиши мумкин. Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди.

Ахборотларни бошқалар ўқишидан сақлаш мақсадида махсус калит ёрдамида кодлаштириш ***криптография*** деб аталади. Криптография узоқ йиллар давомида харбий мақсадларда қўлланилиб келинган.

Очиқ матнни P харфи билан белгилаймиз. Бу матн файли, тасвир, махсус товуш ёки ҳ.к. бўлиши мумкин. Бу ахборотлар компютерда иккилик код кўринишида ифодаланади. Шифрланган текст S харфи билан белгиланади. Шифр матннинг ҳажми баъзан очиқ матн ҳажмига тенг бўлиши мумкин. Шифрланган матн компютер тармоғи каналлари бойлаб узатилиши ёки хотирада сақланиши мумкин. Шифрлаш функцияси E ни қуйидагича ёзиш мумкин:

E(R)=S

Шифрни очиш функциясини D ҳарфи билан белгиласак,

D (S)=R

D (E(R))=R

Криптография қуйидаги масалаларни ечилишини таъминлаши керак.

Аутентификация - қабул қилувчи шунга ишонч ҳосил қилиши керакки маълумот аниқ бир юборувчидан бўлиши шарт. Бошқа бир ном билан ёлғон маълумот юборилмаслиги керак;

Бутунлик - узатиш пайтида ахборот ўзгармаслиги;

Инкор қилмаслик - маълумотни юборувчи ўзи эканини тасдиқлаши.

XX асрнинг охири ва XXI асрнинг бошларида кишилик жамиятида ахборотнинг аҳамияти кескин равишда ортиб кетди. Инсоннинг ҳар бир соҳадаги фаолиятини такомиллаштириш ва осонлаштиришга қаратилган замонавий жамиятда ахборот маҳсулот ёки хом ашё сифатида борган сари катта қийматга эга бўлиб бормоқда.

Кейинги йилларда компютер саноатининг ривожланиши ва инсон ҳаётига тобора чуқурроқ кириб бориши натижасида ахборотни ишлаб чиқариш, сақлаш, қайта ишлаш, таҳлил қилиш, узатишга бўлган эҳтиёж ортиб бормоқда. Оқибатда ана шу ахборотларнинг хавфсизлигини таъминлаш информатиканинг энг долзарб муаммоларидан бирига айланиб улгурди. Компютернинг тармоқ технологияларининг жадал ривожланиши эса бу муаммонинг аҳамиятини янада ошириб юборди.

Ахборотларни криптографик усулда ҳимоя қилиш юзага келган муамммоларни ҳал қилишда муҳим ўрин тутади. Ахборотларни криптографик

ҳимоя қилишда уларнинг мазмунини яшириш ёки бегоналар томонидан фойдаланишнинг олдини олиш мақсадида ахборот махсус функционал акслантириш ёрдамида бир кўринишда бошқа кўринишга ўтказилади. Бу амалнинг турли усулларини ишлаб чиқиш учун амалий математиканинг янги бир йўналиши-криптография юзага келди ва ривожланиб бормоқда.

Криптография — бу ахборотларни криптографик ҳимоя қилишнинг турли модел ва методлари, алгоритмлари, дастурий ва техник воситаларини ишлаб чиқиш ҳамда бундай ҳимоя самарасини баҳолашни ўрганувчи фан ҳисобланади.

Криптография ҳақидаги маълумотларни унинг атамашунослигига оид айрим терминлар мазмунини очиб беришдан бошлаймиз.

Ахборотларни ҳимоя қилиш — бу тармоқдаги алоқа ҳамда ахборотларнинг узлуксизлиги, яхлитлиги ва маҳфийлигини таъминловчи барча восита ва амаллар мамуаси бўлиб, носозликлардан асровчи восита ва функцияларни ўз ичига олмайди. Ахборотларни ҳимоя қилиш криптография, криптоанализ (криптотаҳлил) ва компютерларга руҳсатсиз киришдан сақлаш каби бўлимларни ўз ичига олади.

Криптография – амалий математиканинг бир бўлими бўлиб, ахборотларни мазмунини яшириш ёки рухсатсиз фойдаланишдан асраш мақсадида ахборотларни бир кўринишдан бошқа кўринишга ўтказиш учун мўлжалланган моделлар, методлар, алгоритм, дастурий ва техник воситаларни ўрганади.

Криптосистема - бу ахборотларни криптографик алмаштирилишини дастурий, техник ёки дастурий-техник усуллар ёдамида амалга оширувчи тизимдир.

Криптоанализ (криптотаҳлил) — бу амалий математиканинг битта бўлими бўлиб, кирувчи ёки чиқувчи сигналлардан фойдаланиб махфий параметрларни аниқлаб олиш (яширин матнни очиш) мақсадида криптосистемаларни таҳлил қилишга қаратилган усул, модел, алгоритм, дастурий ва техник воситаларни ўрганади.

Юқоридаги маълумотлардан кўриниб турибдики, криптоанализ математик маънода криптографияга тескари бўлган масалалар билан шуғулланади. Криптография ва криптоанализ биргаликда янги фан — ***криптологияни*** ташкил қилади.Криптология тарихини уч босқичдан иборат деб ҳисоблаш мумкин.

Биринчи босқич - (енг қадимги даврлардан то 1949 йилгача) тор доирадаги, ҳусусий хамда содда ҳисоблашлардан иборат криптографик ва криптотаҳлил алгоритмлари билан ҳарактерланади ва табиийки, компютерлардан фойдаланишни назарда тутмайди. Бу босқични кўпинча компютерларгача бўлган давр деб аталади.

Иккинчи босқич - (1949-1976) амалиётчи математик К. Шенноннинг “Маҳфий тизимларда боғланиш назарияси” номли илмий ишининг чоп этилиши билан бошланади. Бу даврда ЭҲМ лардан фойдаланган ҳолда криптологик изланишлар кенг миқёсда олиб борилди. Криптология математик фанга айланди. Аммо, бу фан меваларидан фақат дипломатик ва ҳарбий ташкилотларнинг алоқа хизмати фойдалангани учун, криптология "ёпиқ" (маҳфий) фан бўлиб қолди.

Учинчи босқич - (1976 йилдан ҳозирги давргача) криптология очиқ фанга айланди. Бу жараён америкалик математик У. Диффи, М. Хеллманларнинг "Криптографиядаги янги йўналишлар" илмий ишининг чоп этилишидан бошланди. Бу ишда “маҳфий” маълумотларни “ёпиқ калитларсиз”, яъни очиқ усулда узатиш мумкинлиги (К. Шеннон ишларидан айнан шу жиҳати билан фарқланади)

кўрсатилди. Бу босқичда криптографик усуллар амалиётда оммавий равишда қўллана бошланди. Бу ҳолатни банк ишида, компютер тармоқларида (масалан, Интернет да) ва бошқа бир қатор соҳаларда кузатиш мумкин бўлди. Масалан, АҚШ да бир йилда криптологияга 15 млрд. долларгача маблағ сарф қилинади.

Криптология информатиканинг фанининг ривожланишига ҳам катта таъсир кўрсата бошлади. Замонавий криптология математиканинг эҳтимоллар назарияси, математик статистика, алгебра, сонлар назарияси, алгоритмлар назарияси, ҳисоблашларнинг мураккаблиги каби соҳалари билан чамбарчас боғланган. Шифрлаш жараёнини автоматлаштириш учун шифрлаш қурилмаси деб аталувчи махсус ва ўта кучли компютерлар ишлаб чиқилди. Ғарбий мамлакатларда ***B-CRYPT, IBM-4755, Datacryptor*** каби шифрлаш қурилмаларидан кенг фойдаланилади. Криптология тарихига оид айрим малумотларни келтириб ўтамиз.

Месопотамияда олиб борилган ареологик қазиш ишларида эрамиздан аввалги XX асрга мансуб бўлган энг қадимий шифрланган матнлардан бири топилди. У сопол тахтачага ўйиб ёзилган бўлиб, сопол идишларни бўяш учун ишлатиладиган бўёқнинг ретсепти ҳақидаги матн бўлиб чиқди. XVII асрда кардинал Ришеле томонидан дунёда биринчи бўлиб, шифрлаш хизмати ташкил қилинди. Ньютон, Эйлер, Лейбнитс, Гаусс, Кардано каби буюк математиклар ҳам бевосита криптология билан шуғулланганлар. Криптологияда қуйидаги атамалар қабул қилинган.

Хабарлар фазоси RT — барча мумкин бўлган хабарларнинг ***pt*** фазоси. Шунингдек хабарларни белгилаш учун ***m*** (message)дан ҳам фойдаланилади.

Калитлар фазоси K. Хар бир $к \in K$ калит *RT* фазодаги бирор E_k (encryption) ва унга тескари D_k (decryption) алмаштиришни белгилайди. ***Шифрланган хабарлар фазоси ST*** – барча шифрланган ct (ciphertext) ct = Ek(pt) матнларни ўз ичига олади.

Одатда криптосистемага қуйидаги талаблар қўйилади: 1) $E_k(pt)$, $D_k(ct)$ лар осон ҳисобланадиган бўлиши лозим; 2) ***к*** ни билмай туриб, ***ct*** маълум бўлган тақдирда ҳам ***pt*** ни топишнинг иложи бўлмасин.

Классик криптосистемаларда ***к*** маҳфий калит $E_к$ ва $D_к$ акслантиришни белгилаб беради. Бунда қуйидаги айниятнинг ўринли бўлиши талаб қитлинади: $D_k(E_k(pt)) = D_k(ct)=pt$. Криптоанализ бўйича мутахассиснинг асосий вазифаси ана шу калитни қидиришдан иборат. У қуйидаги кўринишларда шифрланган матнга ҳужум қилиши мумкин:

1) фақат шифрланган матн маълум (ciphertext only attack);

2) шифрланган ва шифрланмаган матнлар маълум (known plaintext attack);

3) $(pt,E_k(pt))$ жуфтликни аниқлаш имконияти мавжуд ва бу эрда *pt* – криптоаналитик томонидан танланади (chosen plaintext attack).

Ахборотларни криптографик ҳимоя қилишда, яъни ахборотларни очиқ ва ёпиқ усулларда криптографик шифрлашнинг турли алгоритмлари мавжуд бўлиб, уларнинг асосини математика фанининг турли соҳаларида ишлаб чиқилган механизмлар ташкил қилади. Қуйидаги 5.1-жадвалда ана шундай алгоритмларнинг айримларини ва уларнинг математик асоси келтирилган.

5.1-жадвал

Шифрлаш алгоритми	***Алгоритмнинг математик асоси***
GOST-28147-89	Саноқ системалари, бўлиш муносабатлари, даражага кўтариш, иккилик саноқ системасида амаллар бажариш, мулоҳазалар алгебраси, муносабатлар, ўрин алмаштиришлар, сонлар назарияси
Ryukzak	Векторлар алгебраси, қолдиқли бўлиш амали, группа, ҳалқа, майдон, иккилик саноқ системаси, мулоҳазалар алгебраси, муносабатлар, ўрин алмаштиришлар, сонлар назарияси
El-Gamal	Туб сонлар, логарифм, қолдиқлар назарияси, модул бўйича кўпайтириш
DES	Саноқ системалари, акслантиришлар, ўрин алмаштиришлар, мулоҳазалар алгебраси, муносабатлар, ўрин алмаштиришлар, сонлар назарияси
RIJNDAEL	Саноқ системалари, бўлиш муносабатлари, даражага кўтариш, иккилик саноқ системасида амаллар бажариш, мулоҳазалар алгебраси,
RSA	Тенгламалар ечимларининг мавжудлиги. Бўлиш муносабатлари, туб сонлар, туб кўпайтувчиларга ажратиш, халқа, мулоҳазалар алгебраси, муносабатлар, ўрин алмаштиришлар, сонлар назарияси.

Жадвалдан кўриниб турибдики, ахборотларни криптографик усул билан ҳимоя қилиш учун алгебранинг мулоҳазалар алгебраси, муносабатлар, ўрин алмаштиришлар, сонлар назариясига оид ва бошқа маълумотларидан кенг фойдаланилади.

Криптографик тизим, ё қисқача, криптотизим шифрлаш ҳам шифрни очиш алгоритмлари, бу алгоритмларда ишлатиладиган калитлар, шу калитларни бошқарув тизими ҳамда шифрланадиган ва шифрланган матнларнинг ўзаро боғланган мажмуасидир.

Криптотизимдан фойдаланишда матн эгаси шифрлаш алгоритми ва шифрлаш калити воситасида аввало дастлабки матнни шифрланган матнга ўгиради. Матн эгаси уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқарув тизимига ҳожат ҳам бўлмайди) сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса сақлаб қўйилган ахборотнинг бутунлигига ишонч ҳосил бўлади. Акс ҳолда ахборот бутунлиги бузилган бўлиб чиқади. Агар шифрланган матн ундан қонуний фойдаланувчига (олувчига) мўлжалланган бўлса у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан унга аввалдан маълум бўлган шифр очиш калити ва алгоритми воситасида дастлабки матнга айлантирилади.

Бунда калитни қандай ҳосил қилиш, алоқа қатнашчиларига бу калитни

махфийлиги сақланган ҳолда етказиш, ва умуман, иштирокчилар орасида калит узатилгунга қадар хавфсиз алоқа каналини ҳосил қилиш асосий муаммо бўлиб туради. Бунда яна бошқа бир муаммо – аутентификация муаммоси ҳам кўндаланг бўлади. Чунки: Дастлабки матн (хабар) шифрлаш калитига эга бўлган кимса томонидан шифрланади. Бу кимса калитнинг ҳақиқий эгаси бўлиши ҳам, бегона (мабодо криптотизимнинг сири очилган бўлса) бўлиши ҳам мумкин. Алоқа иштирокчилари шифрлаш калитини олишганда у чиндан ҳам шу калитни яратишга ваколатли кимса томонидан ё тажовузкор томонидан юборилган бўлиши ҳам мумкин.Бу муаммоларни турли криптотизимлар турлича ҳал қилиб беради. Криптотизимда ахборотни шифрлаш ва унинг шифрини очишда ишлатиладиган калитларнинг бир-бирига муносабатига кўра улар бир калитли ва икки калитли тизимларга фарқланадилар. Одатда барча криптотизимларда шифрлаш алгоритми шифр очиш алгоритми билан айнан ё бироз фарқли бўлади. Криптотизимнинг таъбир жоиз бўлса "қулфнинг" бардошлилиги алгоритм маълум бўлган ҳолда фақат калитнинг ҳимоя хоссаларига, асосан калит ахборот миқдори(битлар сони)нинг катталигига боғлиқ деб қабул қилинган. Шифрлаш калити шифр очиш калити билан айнан ё улардан бири асосида иккинчиси осон топилиши мумкин бўлган криптотизимлар симметрик(синонимлари: махфий калитли, бир калитли) криптотизим деб аталади. Бундай криптотизимда калит алоқанинг иккала томони учун бир хил махфий ва икковларидан бошқа ҳеч кимга ошкор бўлмаслиги шарт. Бундай тизимнинг хавфсизлиги асосан ягона махфий калитнинг ҳимоя хоссаларига боғлиқ. Симметрик криптотизимлар узоқ ўтмишга эга бўлса-да, улар асосида олинган алгоритмлар компютерлардаги ахборотларни ҳимоялаш зарурати туфайли баъзи давлатларда стандарт мақомига кўтарилдилар. Масалан, АҚШда маълумотларни шифрлаш стандарти сифатида 56 битли калит билан ишлайдиган DES(Data Encryption Standart) алгоритми 1977 йилда қабул қилинган. Россия (собиқ СССР)да унга ўхшаш стандарт (ГОСТ 28147-89) сифатида 128 битли калит билан ишлайдиган алгоритм 1989 йилда тасдиқланган. Булар дастлабки ахборотни 64 битли блокларга бўлиб алоҳида ёки бир-бирига боғлиқ ҳолда шифрлашга асосланганлар.

Симметрик (махфий) калитли шифрлаш системаси. Симметрик шифрлаш алгоритмида қуйидаги усуллардан кенг фойдаланилади:

1. Ўрин алмаштириш шифри
2. Силжитиш шифри.

Ўрин алмаштириш шифри оддий шифрлаш ҳисобланиб, бу усулда сатр ва устундан фойдаланилади. Чунки шифрлаш жадвал асосида амалга оширилади. Биринчи бўлиб, шифрлаш жадвалидан (XIV асрнинг охирларида) дипломатик муносабатларда, харбий соҳаларда ахборотни муҳофазалашда фойдаланилган.

Ўрин алмаштириш шифри. Алмаштириш (подстановка) усулларининг моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит символлари билан маълум қоида бўйича алмаштиришдан иборатдир. Энг содда усул сифатида **тўғридан-тўғри алмаштиришни** кўрсатиш мумкин.

3.3. Очиқ калитли шифрлаш.

Криптографик система қанчалик мураккаб ва ишончли алгоритмга асосланган бўлмасин, унинг амалий қўлланишида келиб чиқадиган нозик масала, яъни

криптосистемалардан фойдаланувчиларга калитларни тақсимлаш масаласи муҳим бўлиб қолаверади. Ҳақиқатан ҳам, ахборотлар тизимида махфий алоқани таъминловчи криптографик система фойдаланувчиларининг ўзаро алоқаси учун калит уларнинг бири орқали яратилган бўлиб, иккинчисига махфий ҳолда етказилиши лозим бўлади. Бундан келиб чиқадики, умуман олганда, калитни етказиш (узатиш) учун ҳам яна бошқа криптосистемадан фойдаланишга тўғри келади. Бу масалани ечиш учун классик ҳамда замонавий фан ва техника ютуқларига, хусусан, алгебра фани ютуқларига асосланган ҳолда очиқ калитли криптосистемалар яратиш йўналиши вужудга келди. Очиқ калитли криптосистемаларнинг моҳиятини қуйидагилар ташкил этади:

1. Ахборотлар тизими криптосистемасидан фойдаланувчиларнинг ҳар бири маълум қоида билан боғланган иккита калитни яратади (тузади).

2. Бу тузилган (яратилган) калитлардан бири очиқ эълон қилинади, иккинчиси эса сир (махфий) сақланади.

3. Дастлабки очиқ калит билан шифрланиб, тегишли фойдаланувчига узатилади, бунда шифрланган матнни (криптограммани) бу очиқ калит билан дешифрлаш имконияти йўқ, яъни шифрланган матнни бу очиқ калит билан очиш имконияти йўқ.

4. Узатилган (етказилган) криптограмма фақат криптограмманинг ҳақиқий эгасигагина маълум бўлган иккинчи махфий калит билан дешифрланади.

Очиқ калитли криптосистемалар тескариси мавжуд бўлмаган ёки тескарисини ҳозирги замонавий фан ва техника ютуқларидан фойдаланган ҳолда қопланмайдиган даражада жуда катта моддий сарф-харажатлар билан ҳамда керагидан кўп вақт сарфлаш билан аниқланадиган функцияларга ёки алгоритмларга асосланади. Шундай функциялар ёки алгоритмларни қуйидаги хоссага эга бўлиши мақсадга мувофиқ: берилган x қийматда $f(x$ функциянинг қиймати y етарли даражада осон ҳисобланади, аммо бирор номаълум x қийматда функциянинг қиймати $y=f(x)$ маълум бўлса, x қийматни топишнинг ҳам моддий жиҳатдан ҳам вақт нуқтаи назаридан этарли даражадаги имконияти йўқ.

Очиқ калитли криптосистемалар алгоритмлари уларнинг асосини ташкил этувчи бир томонли функциялар билан фарқланади. Аммо ҳар қандай бир томонли функция ҳам очиқ калитли криптосистемалар яратиш учун ва улардан амалдаги ахборотлар тизимида махфий алоқа хизматини ўрнатиш алгоритмини қуриш учун қулайлик туғдирмайди.

Бир томонли функцияларни аниқлаш таърифида назарий жиҳатдан тескариси мавжуд бўлмаган функциялар эмас, балки берилган функцияга тескари бўлган функциянинг қийматларини ҳисоблаш амалий жиҳатдан мақсадга мувофиқ бўлмаган функциялар тушунилиши таъкидланган эди. Шунинг учун маълумотнинг ишончли муҳофазасини таъминловчи очиқ калитли криптосистемаларга муҳим бўлган қуйидаги талаблар қўйилади:

1. Дастлабки очиқ матнни шифр матн кўринишида ўтказиш бир томонли жараён ва шифрлаш калити билан шифрматнни очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрматнни дешифрлаш учун этарли эмас.

2. Очиқ калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-харажатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажарилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.

Очиқ калитли шифрлаш алгоритмларидан ахборотлар тизимида маълумотларнинг махфийлигини таъминлашда замонавий илғор услуб сифатида фойдаланиб келинмоқда. Очиқ калитли криптосистемаларни яратишнинг РСА алгоритми жоҳон стандарти сифатида қабул қилинган. Бу ҳақида кейинги бўлимларда алоҳида тўхталамиз.
Умуман олганда, замонавий очиқ калитли криптосистемалар қуйидаги типдаги акслантиришларга (функцияларга) таянади:

1. Катта сонларни туб кўпайтувчиларга ёйиш.
2. Чекли сонли майдонларда логарифмларни ҳисоблаш.
3. Алгебраик тенгламаларнинг илдизларини ҳисоблаш.

Шу ерда таъкидлаш лозимки, очиқ калитли криптосистемалар алгоритмларидан қуйидаги мақсадларда фойдаланилади:

1. Сақланувчи ва узатиладиган маълумотларнинг махфийлиги муҳофазасини таъминловчи мустақил восита сифатида.
2. Калитлар тақсимотининг муҳофазасини таъминловчи восита сифатида.

Очиқ калитли криптосистемалар алгоритмлари анъанавий криптосистемалар алгоритмларига нисбатан мураккаб бўлиб, ундан кўпроқ калитларни тақсимлашда фойдаланилади. Сўнгра катта ҳажмдаги маълумотларни узатишда соддароқ бўлган системалардан фойдаланилади.

3. Аутентификация, яъни маълумотларнинг ҳақиқийлигини аниқлаш услублари воситаси сифатида.

3.4. Хеш функция.

Хеш функциялар – ихтиёрий узунликдаги кириш маълумотини чиқишда белгиланган узунликдаги хеш қийматга айлантириб берувчи бир томонлама функцияларга айтилади. Хеш функциялар криптография ва замонавий ахборот хавфсизлиги соҳасида маълумотларни тўлалигини текширишда фойдаланилади. Электрон тўлов тизимлари протоколларида ҳам истемолчи картаси маълумотларини банк-емитентга тўлиқ етказиш учун фойдаланилади. [16]

Хеш функция- ихтиёрий узунликдаги М-маълумотни фиксирланган узунликга сиқиш ёки иккилик саноқ системаси ифодаланган маълумотларни фиксирланган узунликдаги битлар кўринишидаги қандайдир конбинацияси деб аталувчи функция.

Таъриф. Хеш-функция деб, ҳар қандай

h: X→ Y

осон ҳисобланувчи ва ▿M –маълумот учун h(M) = H фиксирланган узунликга эга бўлган функцияга айтилади.

Берилган М-маълумотнинг h(M) –хеш қийматини топиш учун аввало маълумот бирор «m» -узунликдаги блокларга ажратилиб чиқилади. Агар М-маълумот узунлиги «m» -га каррали бўлмаса, у ҳолда охирги тўлмай қолган блок «m»- узунликга олиндан келишиб олинган махсус усулда бирор символ ёки белги (масалан “0” ёки “1”) билан тўлдирилиб чиқилади. Натижада ҳосил қилинган М-маълумот блокларига:

$M= \{ M_1, M_2 ,.....M_н)$

қуйидагича сиқишни (сверткани) ҳисоблаш протседураси қўлланилади:

$H_0 =$▿ ,

$H_i = f(M_i, H_{i-1})$, i =1,2,.....n

h(M)= H_n ;

бу ерда v-қандайдир фиксирланган бошланғич вектор.

Мисол сифатида қуйидаги кенг тарқалган:

$f(M_i, H_{i-1}) = E_k(M_i \oplus H_{i-1})$ i =1,2,.....n

хеш-функцияни келтириб ўтиш мумкин.

Бу ерда E-симметрик шифрлаш алгоритми (масалан DES, GOST 28147-87, AES –FIPS 197 ва ҳакоза), k- эса шифрлаш алгоритми махфий калити, $H_0 = 0$, $\oplus$ - XOR (mod 2 бўйича мос битларни қўшиш) амали.

Хеш функциялар турлари

Оддий хеш функциялар: Adler-32, CRC, FNV, Murmur2, PJW-32, TTH, Jenkins hash.

Криптографик хеш функциялар: CubeHash, BLAKE, BMW, ECHO, FSB, Fugue, Grøstl, JH, Hamsi, HAVAL, Keccak (SHA-3), Kupyna, LM-хеш, Luffa, MD2, MD4, MD5, MD6, N-Hash, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320, SHA-1, SHA-2, SHABAL, SHAvite-3, SIMD, Skein, Snefru, SWIFFT, Tiger, Whirlpool, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.

Калит ҳосил қилувчи хеш функциялар: bcrypt, PBKDF2, scrypt.

Криптографик хеш функцияларнинг эса қуйидаги турлари мавжуд:

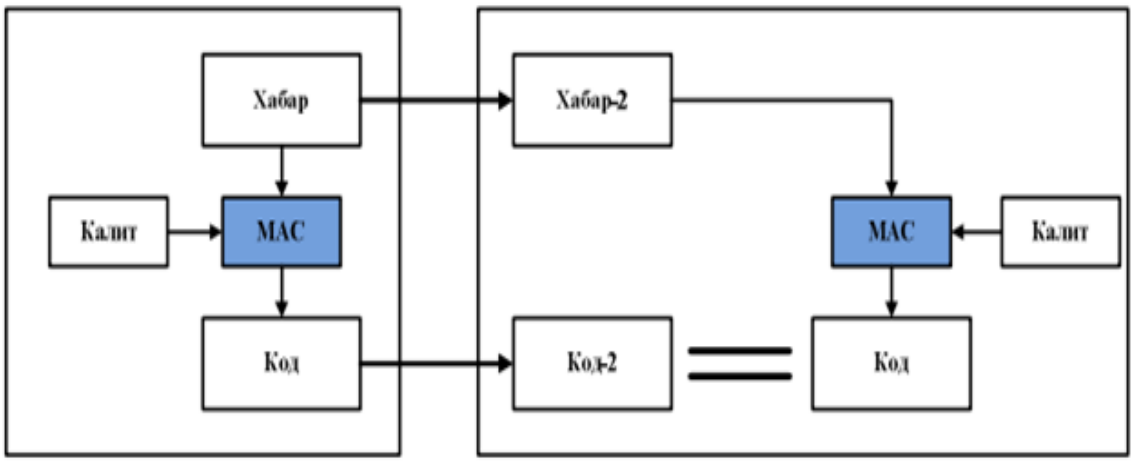
калитли хеш функция; 2) калитсиз хеш функция..

Калитли хеш функциялар симметрик шифрлаш алгоритми тизимларида қўлланилади. Калитли хеш функциялар берилган маълумот аутентификацияси коди (message authentication code (MAC)) деб ҳам юритилади. Ушбу код бир-бирига ишончи мавжуд фойдаланувчиларга берилган маълумотининг ҳақиқийлиги ва тўлалигини кафолатини қўшимча воситаларсиз таъминлаш имкониятини туғдиради [16].

Калитсиз хеш функциялар хатоларни топиш коди (modification detection code(MDC)) ёки manipulation detection code, massage integrrity code(MIC) деб аталади. Ушбу код қўшимча воситалар (масалан: ҳимояланган алоқа тармоғи, шифрлаш ёки ЭРИ алгоритмлари) ёрдамида берилган маълумот тўлалигини кафолатлайди. Бу турдаги хеш функциялардан бир-бирига ишонч билдирувчи ва ишончи бўлмаган томонлар фойдаланишлари мумкин.

Одатда калитсиз хеш функциялардан қуйидаги хоссаларни қаноатлантириши талаб қилинади: 1) бир томонлилик; 2) коллизияга бардошлилик; 3) хеш қийматлари тенг бўлган иккита маълумотни топишга бардошлилик.

Биринчи шарт бажарилганда, берилган хеш қийматга эга бўлган маълумотни топишнинг мураккаб эканлигини, иккинчи шарт бажарилганда бир хил хеш қийматга эга бўлган маълумотлар жуфтини топишнинг мураккаб эканлигини, учинчи шарт хеш қиймати маълум бўлган берилган маълумот учун хеш қиймати шунга тенг бўлган иккинчи маълумотни топишнинг мураккаб эканлигини билдиради.



3.1-расм. MAC тизимлари

Масалан, назорат йиғиндини топувчи SRC хеш функцияси чизиқли акслантириш бўлади ва шунинг учун ҳам бу учта шартдан биронтасини ҳам қаноатлантирмайди.

Маълумотларни узатишда ёки сақлашда уларнинг тўлалигини назоратлашда ҳар бир маълумотнинг хеш қиймати (бу хеш қиймат маълумотни аутентификация қилиш коди ёки “имитоқўйиш”-маълумот блоклари билан боғлиқ бўлган қўшимча киритилган белги дейилади) ҳисобланилади ва бу қиймат маълумот билан бирга сақланилади ёки узатилади. Маълумотни қабул қилган фойдаланувчи маълумотнинг хеш қийматини ҳисоблайди ва унинг хеш қиймати билан солиштиради. Агар таққослашда бу қийматлар мос келмаса, маълумот бутунлиги бузилганлигини англатади. “Имитоқўйиш”лар ҳосил қилиш учун фойдаланиладиган хеш функциялар назорат йиғиндисидан фарқли равишда маълумотни сақлаш ва узатишда рўй берадиган тасодифий хатоларни аниқлабгина қолмасдан, рақиб томонидан қилинган актив ҳужумлар тўғрисида ҳам огоҳлантиради. Бузғунчи хеш қийматни осонлик билан ўзи ҳисоблаб топа олмаслиги ва муваффақиятли имитация қилиши ёки маълумотни ўзгартира олмаслиги учун хеш функция 70 бузғунчига маълум бўлмаган махфий калитга эга бўлиши керак. Бу махфий калит фақатгина маълумотни узатувчи ва қабул қилувчи томонларга маълум бўлиши керак. Бундай хусусиятга эга хеш функцияларга калитли хеш функциялар дейилади. Калитли хеш функциялар ёрдамида ҳосил қилинадиган “имитоқўйиш”лар имитация (impersonation) туридаги ҳужумларда қалбаки маълумотларни ҳосил қилишга (fabrication) ва “ўзгартириш” (substitution) туридаги ҳужумларда узатиладиган маълумотни модификатсия (модификатион) қилишга йўл қўймасликда фойдаланилади.

Маълумот манбаининг аутентификациялаш масаласи ахборот- коммуникатсия тизимларининг бир-бирига ишонмайдиган икки томони орасида маълумот алмашинувида юзага келади. Бу масалани ҳал қилишда иккала томон ҳам биладиган махфий калитдан фойдаланиб бўлмайди. Бу ҳолатда маълумотнинг манбаини аутентификация қилишга имкон берадиган электрон рақамли имзо схемаси қўлланилади. Бунда одатда фойдаланувчининг махфий калитига асосланган имзо қўйишдан олдин хатолик кодини аниқловчи хеш функция ёрдамида маълумот сиқилади. Бу ҳолда хеш функция махфий калитга эга бўлмайди ҳамда у фиксирланган бўлиши ва ҳаммага маълум бўлиши мумкин. Унга қўйилган асосий талаб имзоланган ҳужжатни ўзгартириш ҳамда бир хил хеш қийматга эга

бўлган иккита ҳар хил маълумотни танлаш имконияти йўқлигининг кафолатидир. Агар бир хил хеш қийматга эга бўлган иккита ҳар хил маълумот мавжуд бўлса, бу маълумотлар жуфти коллизия ҳосил қилади дейилади.

Хеш функцияларда коллизия – иккита ҳар хил маълумотдан бир хил хеш қиймат ҳосил бўлиб қолиши. Коллизиянинг олдини олиш йўлларидан бири бу хеш жадвал ҳисобланади. Хешлаш алгоритмларининг бардошлилиги ха хавфсизлилиги коллизияга чидамлилиги билан аниқланади.

Хешлаш алгоритмларининг замонавий криптографиядаги тутган ўрни жуда муҳимдир ва ундан ҳозирда кенг кўламда фойдаланилади. Янги хеш алгоритмлар хам яратилмоқда. Янги хеш алгоритмлар коллизияга бардошли, хеш қийматнинг тез ҳисоб-китоб қила олиши ва.ҳ.к хусусиятларга эга бўлади.

Хеш функциялар асосан, электрон рақамли имзо (ЭРИ)да, Torrent, DC Hub, Операцион системаларда ва файлларнинг бутунлилигини ёки ўзгартирилганлигини назорат қилиш учун фойдаланилади. Ахборот бутунлигини назорат қилишнинг кўпроқ мақбул бўлган методларидан бири хеш-функциядан фойдаланиш ҳисобланади.

Email clients		Apple Mail · Claws Mail · Enigmail · GPG (Gpg4win) · Kontact · Outlook · p≡p · PGP · Sylpheed · Thunderbird
Secure Messaging	**OTR**	Adium · BitlBee · Centericq · ChatSecure · climm · Jitsi · Kopete · MCabber · Profanity
	SSH	Dropbear · lsh · OpenSSH · PuTTY · SecureCRT · WinSCP
	TLS & SSL	Bouncy Castle · BoringSSL · Botan · cryptlib · GnuTLS · JSSE · LibreSSL · MatrixSSL · NSS · OpenSSL · mbed TLS · RSA BSAFE · SChannel · SSLeay · stunnel · wolfSSL
	VPN	Check Point VPN-1 · Hamachi · Openswan · OpenVPN · SoftEther VPN · strongSwan · Tinc
	ZRTP	CSipSimple · Jitsi · Linphone · Ring · Zfone
	P2P	Bitmessage · RetroShare · Tox
	DRA	Matrix · OMEMO (Conversations · Cryptocat · ChatSecure) · Proteus · Signal Protocol (Google Allo · Facebook Messenger · Signal · TextSecure · WhatsApp)
Disk encryption (Comparison)		BestCrypt · BitLocker · CipherShed · CrossCrypt · Cryptoloop · DiskCryptor · dm-crypt · DriveSentry · E4M · eCryptfs · FileVault · FreeOTFE · GBDE · geli · LUKS · PGPDisk · Private Disk · Scramdisk · Sentry 2020 · TrueCrypt (History) · VeraCrypt
Anonymity		GNUnet · I2P · Java Anon Proxy · Tor · Vidalia · RetroShare · Ricochet
Cryptographic file systems		Freenet · Tahoe-LAFS
Educational		CrypTool
Related topics		Outline of cryptography · Timeline of cryptography · **Hash functions** (Cryptographic hash function · List of hash functions) · S/MIME

3.2-расм. Криптографик хеш функциялар ишлатилиши

Хеш-функциянинг қийматини унинг калитини билмасдан туриб қалбакилаштириб бўлмайди, шу сабабли хешлаш калитини шифрланган кўринишда ёки жиноятчининг «қўли етмайдиган» жойдаги хотирада сақлаш керак.

CRC32 (Cyclic redundancy check – Даврий камчиликни текширувчи код)

компютер қурилмаларида, яъни тармоқ қурилмалари ва доимий хотирадаги маълумотларни хавфсизлигини таъминлашда яъни ўзгартирилмаганлигини доимий равишда текшириб борадиган оддий хеш функция ҳисобланади. CRC32 халқаро стандарти CRC32-IEEE 802. Бу алгоритм жуда тез ишлагани билан, криптохавфсизликни тўлиқ таъминлай олмайди. Шунга қарамасдан кенг қўлланилади чунки, ишлатилиши жуда оддий ва тез. 32-бит хеш-код одатда 8 та символдан иборат 16 лик саноқ системасида ифодаланади. Бу алгоритм криптографик ҳисобланмайди.

MD4 хешлаш алгоритми RSA Data Security, Inc. Ronald L. Rivest томонидан ишлаб чиқилган. MD4 аралашган алгоритм ҳисобланади, энди ишончсиз ҳисобланади. Бу алгоритм (32-бит протсессорлари учун) тез ва peer-to-peer тармоғи эдонкей 2000 Қўшма Алгоритм ҳаш коди 32 та символдан иборат бўлган белгилар билан ўн олтилик сони RFC 1320. тасвирланган ҳисоблаш ишлатилади.

Хеш функциялар таҳлили

	Xeshlanadigan matn uzunligi	Kirish blokining uzunligi	Xesh qiymat uzunligi	Har bir blokni xeshlash qadamlari soni
GOST R 34.11-94	Ixtiyoriy	256	256	19
MD 2	Ixtiyoriy	512	128	1598
MD 4	Ixtiyoriy	512	128	72
MD 5	Ixtiyoriy	512	128	88
SHA-1	$<2^{64}$	512	160	80
SHA-256	$<2^{64}$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80
STB 1176.1 – 99	Ixtiyoriy	256	142≤L≤256	77
O'z DSt 1106 : 2006	Ixtiyoriy	128, 256	128, 256	16b+74, 16b+46, Bu erda b-bloklar soni

MD5 хеш функцияси алгоритми Massachusets технология институти профессори Роналд Ривест томонидан 1992 йилда ишлаб чиқилган. Бу алгоритмда кирувчи маълумот узунлиги ихтиёрий бўлиб, хеш қиймат узунлиги 128 бит бўлади. MD5 хеш функцияси алгоритмида кирувчи маълумот 512 битлик блокларга ажратилиб, улар 16 та 32 битлик қисм блокларга ажратилади ва булар устида амаллар бажарилади. Фараз қилайлик, бизга узунлиги b бит бўлган, бу ерда b – ихтиёрий номанфий бутун сон, маълумот берилган бўлсин ва бу маълумотнинг битлари қуйидагича: *m0m1…m(b-1)*

SHA-1 хеш функцияси алгоритми. Кафолатланган бардошлиликка эга бўлган хешлаш алгоритми SHA (Secure Hash Algorithm) АҚШнинг стандартлар ва технологиялар Миллий институти (NIST) томонидан ишлаб чиқилган бўлиб, 1992 йилда ахборотни қайта ишлаш федерал стандарти (RUB FIPS 180) кўринишида нашр қилинди. 1995 йилда бу стандарт қайтадан кўриб чиқилди ва SHA -1 деб номланди (RUB FIPS 180-1). SHA алгоритми MD4 алгоритмига асосланади ва унинг тузилиши MD4 алгоритмининг тузилишига жуда яқин. Бу алгоритм DSS стандарти асосидаги электрон рақамли имзо алгоритмларида ишлатиш учун

мўлжалланган. Бу алгоритмда кирувчи маълумотнинг узунлиги 264 битдан кичик бўлиб, хеш қиймат узунлиги 160 бит бўлади. Киритилаётган маълумот 512 битлик блокларга ажратилиб қайта ишланади.

Хеш қийматни ҳисоблаш жараёни қуйидаги босқичлардан иборат: ***1-босқич. Тўлдириш битларини қўшиш.***

Берилган маълумот узунлиги 512 модул бўйича 448 билан таққосланадиган (маълумот узунлиги ≡ 448 mod 512) қилиб тўлдирилади. Тўлдириш ҳамма вақт, ҳаттоки маълумот узунлиги 512 модул бўйича 448 билан таққосланадиган бўлса ҳам бажарилади. Тўлдириш қуйидаги тартибда амалга оширилади: маълумотга 1 га тенг бўлган битта бит қўшилади, қолган битлар эса 0 лар билан тўлдирилади. Шунинг учун қўшилган битлар сони 1 дан 512 тагача бўлади.

2- босқич. Маълумотнинг узунлигини қўшиш.

1-босқичнинг натижасига берилган маълумот узунлигининг 64 битлик қиймати қўшилади.

3- босқич. Хеш қиймат учун буфер инициализация қилиш.

Хеш функциянинг оралиқ ва охирги натижаларини сақлаш учун 160 битлик буфердан фойдаланилади. Бу буферни бешта 32 битлик A, B, C, D, E регистрлар кўринишида тасвирлаш мумкин. Бу регистрларга 16 лик саноқ системасида қуйидаги бошланғич қийматлар берилади:

A=0x67452301, B=0xEFCDAB89, C=0x98BADCFE, D=0x10325476,
E=0xC3D2E1F0.

Кейинчалик бу ўзгарувчилар мос равишда янги *a*, *b*, *c*, *d* ва *e* ўзгарувчиларга ёзиб олинади. ***4- босқич.*** *Маълумотни 512 битлик блокларга ажратиб қайта ишлаш.*

Бу хеш функциянинг асосий сикли қуйидагича бўлади: for ($t = 0; t < 80; t$++){ $temp = (a <<< 5) + ft(b, c, d) + e + Wt + Kt$; $e = d$; $d = c$; $c = b <<< 30$; $b = a$; $a = temp$; }, Бу ерда <<< - чапга циклик суриш амали. *Kt* лар 16 лик саноқ системасида ёзилган қуйидаги сонлардан иборат:

$$K_t = \begin{cases} \mathbf{5A827999}, & t = 0,\ldots,19, \\ \mathbf{6ED9EBA1}, & t = 20,\ldots,39, \\ \mathbf{8F1BBCDC}, & t = 40,\ldots,59, \\ \mathbf{CA62C1D6}, & t = 60,\ldots,79. \end{cases}$$

$f_t(x, y, z)$ функциялар эса қуйидаги ифодалар билан аниқланади:

$$f_t(\mathbf{x},\mathbf{y},\mathbf{z}) = \begin{cases} \mathbf{X} \wedge \mathbf{Y} \vee \neg\mathbf{X} \wedge \mathbf{Z}, & \mathbf{t} = 0,\ldots,19, \\ \mathbf{X} \oplus \mathbf{Y} \oplus \mathbf{Z}, & \mathbf{t} = 20,\ldots,39,\ 60,\ldots,79, \\ \mathbf{X} \wedge \mathbf{Y} \vee \mathbf{X} \wedge \mathbf{Z} \vee \mathbf{Y} \wedge \mathbf{Z}, & \mathbf{t} = 40,\ldots,59. \end{cases}$$

Wt лар кенгайтирилган маълумотнинг 512 битлик блокининг 32 битлик қисм блокларидан қуйидаги қоида бўйича ҳосил қилинади:

$$W_t = \begin{cases} M_t, & t = 0,\ldots,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1, & t = 16,\ldots,79. \end{cases}$$

Асосий сикл тугагандан кейин *a*, *b*, *c*, *d* ва *e* ларнинг қийматлари мос равишда

A, B, C, D ва E регистрлардаги қийматларга қўшилади ҳамда шу регистрларга ёзиб қўйилади ва кенгайтирилган маълумотнинг кейинги 512 битлик блокини қайта ишлашга ўтилади.

5- босқич. ***Натижа***. Маълумотнинг хеш қиймати A, B, C, D ва E регистрлардаги қийматларни бирлаштириш натижасида ҳосил қилинади.

Бугунги жамият тараққиёти инсоният тафаккурининг махсули бўлган ривожланган илм-фан ютуқларига асосланган техника ва технологиялар билан бир қаторда, кенг маънода, ахборотларнинг муҳим аҳамиятга эгалиги орқали хам белгиланади. Фаолият мақсадларининг турлича бўлиши табиий равишда ахборотлардан турли мақсадларда фойдаланиш асосларига сабаб бўлади. Шунинг учун бугунги, ахборотларни сақлаш ва узатиш тизимлари бир томондан такомиллашиб мураккаблашган ва иккинчи томондан ахборотдан фойдаланувчилар учун кенг қулайликлар вужудга келган даврда, ахборотларни мақсадли бошқаришнинг қатор муҳим масалалари келиб чиқади. Бундай масалалар қаторига катта хажмдаги ахборотларнинг тез ва сифатли узатиш хамда қабул қилиш, ахборотларни ишончлилигини таъминлаш, ахборотлар тизимида ахборотларни бегона шахслардан(кенг маънода) мухофаза қилиш каби кўплаб бошқа масалалар киради. Юқоридаги келтирилган асосли мулохазалардан келиб чиқиб, ахборотларни асли холидан ўзгартирилган холда, яъни шифрланган холда, сақлаш ва узатиш масалаларининг муҳим эканлигига шубха йўқдир.

Хеш функциялар асосан маълумотнинг бутунлилигини таъминлашда яъни ахборот хавфсизлигини таъминлашда кенг кўламда қўлланилади. Шунинг учун ҳам хеш функцияларнинг замонавий криптография тутган ўрни жуда муҳимдир.

Назорат саволлари:

1. Тармоқ хавфсизлиги ҳақида маълумот беринг.
2. Тармоқ хавфсизлигига таҳдидлари қандай тоифаларга бўлинади?
3. Ахборот хавфсизлиги бўйича йўл қўйиладиган кенг тарқалган ўнта хатоларни санаб беринг.
4. VPN (Virtual Private Network) виртуал хусусий тармоқ ҳақида маълумот беринг.
5. Port scanning нима?
6. IPsec протоколидан нима учун фойдаланилади?
7. Фойдаланишни бошқариш орқали хавфсизлик ҳақида маълумот беринг.
8. Рақамли имзолар нима?
9. Очиқ калитли шифрлаш нима?
10. Хеш функциялар турларини санаб беринг.
11. SHA-1 хеш функцияси алгоритми ҳақида нималарни биласиз?
12. Хеш функциялар қўлланилиши ва ахборот хавфсизлигидаги ўрнини белгиланг.

Адабиётлар ва Интернет сайтлари:

1. Эшмурадов А.М., Абдужалилов Ж.А. “Интернет тармоқлари ва хизматлари” фанидан ўқув-услубий мажмуа. – Тошкент: ТАТУ. 2016.

2. Олифер Виктор, Наталия Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Сн-Петербург: Издательство ПИТЕР, 2016, 992 с.
3. Douglas E. Comer. Computer Networks and Internets (6th Edition). Pearson. USA, 2015. 672 p.
4. Компьютерные сети и технологии. http://www.xnets.ru/
5. http://www.network.xsp.ru/
6. https://iot.ru/

4-маъруза. Тармоқда маълумотлар хавфсизлигининг ускунавий ва дастурий таъминоти.
(2 соат)

Режа:

4.1. Ipsec (Internet protocol security) хавфсизлик протоколи.
4.2. VPN (Virtual Private Network) виртуал хусусий тармоқ.
4.3. Ахборот тармоғи хавфсизлиги қурилмалар ва дастурий таъминоти.
4.4. Тармоқлараро экраннинг пакетларни филтрлаш қоидалари.

ТАЯНЧ ИБОРАЛАР: *Ipsec (Internet protocol security), тармоқлараро экран, VPN (Virtual Private Network).*

4.1. Ipsec (Internet protocol security) хавфсизлик протоколи.

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) руҳсатсиз 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 компьютерларнинг 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.

Тармоқ хавфсизлиги тармоқ компьютер тизимларига таъминлаш учун қўлланиладиган технологик ва бошқарувчилик амалларини ўз ичига олади:

– Қулайлиги
– Бутлиги
– Исталмаган фойдаланишлар, зарарлантириш, ўзгартириш ёки йўқотишга қарши тармоқни бошқарувчи ахборотнинг махфийлиги.

Ахборотнинг махфийлиги: Ахборотдан фақатгина руҳсатга эга фойдаланувчилар фойдаланишлари мумкинлигини таъминлайди. Фойдаланувчининг эркин фойдаланиш ҳуқуқини Идентификация ва Аутентификация қилиш билан бошқариш учун қуйидагилардан фойдаланиш талаб қилинади:

– Идентификация ПИН-Кодлари
– Интеллектуал карточкалар, контактсиз карточкалар
– Биометрик кўрсаткичлар
– Хавфсизликка таҳдид ва заиф жойлар
– Хатолар ва камчиликлар
– Фирибгарлик ва ўғрилаш
– Физик ва инфратузилмали таъминотни йўқотиш
– Хакер ва бузғунчи
– Зарарли код ва дастурий таъминот
– Хорижий ҳукуматнинг жосуслик ҳаракатлари

Ҳар қандай ташкилот Интенетга уланганидан сўнг, ҳосил бўладиган қуйидаги муаммоларни ҳал этишлари шарт:

– ташкилотнинг компьютер тизимини хакерлар томонидан бузилиши:
– Интернет орқали жўнатилган маълумотларнинг ёвуз ниятли шахслар
– томонидан ўқиб олиниши;
– ташкилот фаолиятига зарар етказилиши.

Интернет лойиҳалаш даврида бевосита ҳимояланган тармоқ сифатида ишлаб чиқилмаган. Бу соҳада ҳозирги кунда мавжуд бўлган қуйидаги муаммоларни келтириш мумкин:

– маълумотларни йенгиллик билан қўлга киритиш;
– тармоқдаги компьютерлар манзилини соҳталаштириш;
– TCP/IP воситаларининг заифлиги;
– кўпчилик сайтларнинг нотўғри конфигурацияланиши;
– конфигуратсиялашнинг мураккаблиги.

Глобал тармоқларнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб бўлмоқда, бу эса ўз навбатида ахборотлар хавфсизлигига тахдид солиш эҳтимолининг ошишига олиб келмоқда. Узоқ, масофалар билан ахборот алмашиш зарурияти ахборотларни олишнинг қатъий чегараланишини талаб этади. Шу мақсадда тармоқларнинг сегментларини ҳар хил даражадаги ҳимоялаш усуллари таклиф этилган:

– эркин кириш (масалан: WWW-сервер);
– чегараланган киришлар сегменти (узоқ масофада жойлашган иш жойига хизматчиларнинг кириши);
– ихтиёрий киришларни ман этиш (масалан, ташкилотларнинг молиявий локал тармоқлари).

Интернет глобал ахборот тармоғи ўзида ниҳоятда катта ҳажмга эга бўлган ахборот ресурсларидан миллий иқтисоднинг турли тармоқларида самарали

фойданишга имконият туғдиришига қарамасдан ахборотларга бўлган хавфсизлик даражасини оширмоқда. Шунинг учун ҳам Интернетга уланган ҳар бир корхона ўзининг ахборот хавфсизлигини таъминлаш масалаларига катта эътибор бериши керак. Ушбу тармоқда ахборотлар хавфсизлигининг йўлга қўйилиши ёндашуви қуйида келтирилган:

Локал тармоқларнинг глобал тармоқга қўшилиши учун тармоқлар ҳимояси администратори қуйидаги масалаларни ҳал қилиши лозим:

— локал тармоқларга глобал тармоқ, томонидан мавжуд хавфларга нисбатан ҳимоянинг яратилиши;

— глобал тармоқ фондаланувчиси учун ахборотларни яшириш имкониятининг яратилиши;

Бунда қуйидаги усуллар мавжуд:

— кириш мумкин бўлмаган тармоқ манзили орқали;

— Ping дастури ёрдамида тармоқ пакетларини тўлдириш;

— руҳсат этилган тармоқ манзили билан тақиқланган тармоқ манзили бўйича бирлаштириш;

— таъқиқланган тармоқ протаколи бўйича бирлаштириш;

— тармоқ бўйича фойдаланувчига парол танлаш;

— REDIREST туридаги ICMP пакети ёрдамида маршрутлар жадвалини модификациялаш;

— RIR стандарт бўлмаган пакети ёрдамида маршрутлар жадвалини ўзгартириш;

— DNS споофингдан фойдаланган ҳолда уланиш.

4.2. VPN (Virtual Private Network) виртуал хусусий тармоқ.

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.

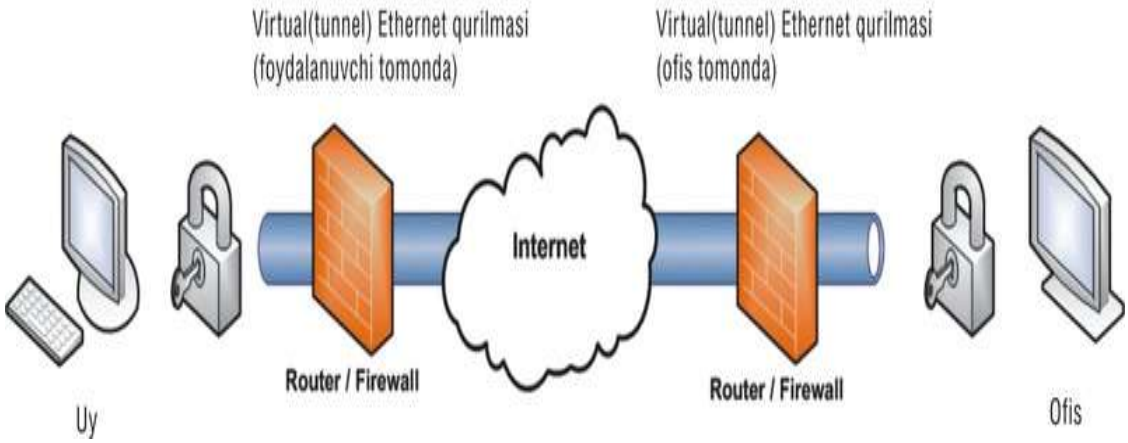
VPN технологиясининг афзаллиги. Локал тармоқларни умумий VPN тармоғига бирлаштириш орқали кам харажатли ва юқори даражали ҳимояланган тунелни қуриш мумкин. Бундай тармоқни яратиш учун сизга ҳар бир тармоқ қисмининг битта компьютерига филиаллар ўртасида маълумот алмашишига хизмат қилувчи махсус VPN шлюз 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 компьютерга оддий усулда узатилади. Буларнинг барчаси фойдаланувчи учун умуман сезилмас даражада амалга ошади ҳамда локал тармоқда ишлашдан ҳеч қандай фарқ қилмайди. Эавесдроппинг ҳужумидан фойдаланиб, тингланган ахборот тушунарсиз бўлади.

Бундан ташқари, VPN алоҳида компьютерни ташкилотнинг локал тармоғига қўшишнинг ажойиб усули ҳисобланади. Тасаввур қиламиз, хизмат сафарига

ноутбукингиз билан чиққансиз, ўз тармоғингизга уланиш ёки у йердан 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.

Руҳсатсиз киришни аниқлаш тизими (IDS) ёрдамида тизим ёки тармоқ хавфсизлик сиёсатини бузиб киришга ҳаракат қилинган усул ёки воситалар аниқланади. Руҳсатсиз киришларни аниқлаш тизимлари деярли чорак асрлик тарихга эга. Руҳсатсиз киришларни аниқлаш тизимларининг илк моделлари ва прототиплари компьютер тизимларининг аудит маълумотларини таҳлиллашдан фойдаланган. Бу тизим иккита асосий синфга ажратилади. Тармоққа руҳсатсиз киришни аниқлаш тизими (Network Intrusion Detection System) ва компьютерга руҳсатсиз киришни аниқлаш тизимига (Host Intrusion Detection System) бўлинади.



4.1- расм. VPN тармоқ тузилмаси.

IDS тизимлари архитектураси таркибига қуйидагилар киради:

• ҳимояланган тизимлар хавфсизлиги билан боғлиқ ҳолатларни йиғиб таҳлилловчи сенсор қисм тизими;

• сенсорлар маълумотларига кўра шубҳали ҳаракатлар ва ҳужумларни аниқлашга мўлжалланган таҳлилловчи қисм тизими;

• таҳлил натижалари ва дастлабки ҳолатлар ҳақидаги маълумотларни йиғишни таъминлайдиган омборхона;

• IDS тизимини конфигурациялашга имкон берувчи, IDS ва ҳимояланган тизим ҳолатини кузатувчи, таҳлил қисм тизимлари аниқлаган можароларни кузатувчи бошқарув консоли.

Тармоққа руҳсатсиз киришни аниқлаш тизими (NIDS) ишлаш тамойили қуйидагича:

1. Тармоққа кириш ҳуқуқига эга бўлган трафикларни текширади;

2. Зарарли ва руҳсатга эга бўлмаган пакетларга чеклов қўяди.

Санаб ўтилган хавфсизлик босқичларини қўллаган ҳолда эавесдроппинг таҳдидига қарши самарали тарзда ҳимояланиш мумкин.

DOS (Denial-of-service) тармоқ ҳужумнинг бу тури хизмат қилишдан воз кечиш ҳужуми деб номланади. Бунда ҳужум қилувчи легал фойдаланувчиларнинг

тизим ёки хизматдан фойдаланишига тўсқинлик қилишга уринади. Тез-тез бу ҳужумлар инфратузилма ресурсларини хизматга руҳсат сўровлари билан тўлиб тошиши орқали амалга оширилади. Бундай ҳужумлар алоҳида ҳостга йўналтирилгани каби бутун тармоққа ҳам йўналтирилиши мумкин. Ҳужумни амалга оширишдан олдин обект тўлиқ ўрганилиб чиқилади, яъни тармоқ ҳужумларига қарши қўлланилган ҳимоя воситаларининг заифлиги ёки камчликлари, қандай операцион тизим ўрнатилган ва объект иш фаолиятининг энг юқори бўлган вақти. Қуйидагиларни аниқлаб ва текшириш натижаларига асосланиб, махсус дастур ёзилади. Кейинги босқичда эса яратилган дастур катта мавқега эга бўлган серверларга юборилади. Серверлар ўз базасидаги рўйхатдан ўтган фойдаланувчиларга юборади. Дастурни қабул қилган фойдаланувчи ишончли сервер томонидан юборилганлигини билиб ёки билмай дастурни ўрнатади. Айнан шу ҳолат минглаб ҳаттоки, миллионлаб компьютерларда содир бўлиши мумкин. Дастур белгиланган вақтда барча компьютерларда фаоллашади ва тўхтовсиз равишда ҳужум қилиниши мўлжалланган обектнинг серверига сўровлар юборади. Сервер тинимсиз келаётган сўровларга жавоб бериш билан овора бўлиб, асосий иш фаолиятини юргиза олмайди. Сервер хизмат қилишдан воз кечиб қолади.

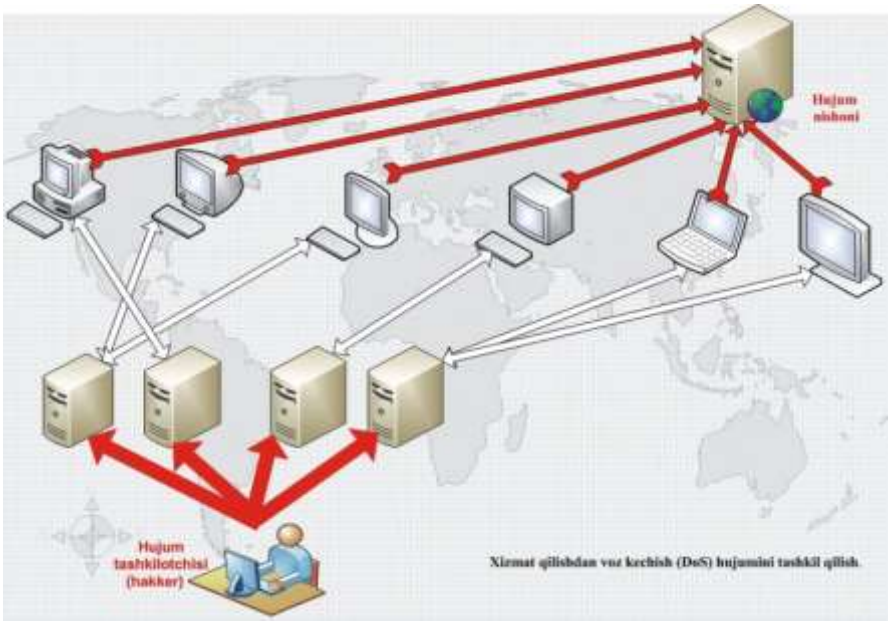
Хизмат қилишдан воз кечиш ҳужумидан ҳимояланишнинг энг самарали йўллари қуйидагилар:

- тармоқлараро экранлар технологияси (Firewall);
- IPsec протоколи.

Тармоқлараро экран ички ва ташқи периметрларнинг биринчи ҳимоя қурилмаси ҳисобланади. Тармоқлараро экран ахборот-коммуникация технология (АКТ) ларида кирувчи ва чиқувчи маълумотларни бошқаради ва маълумотларни филтрлаш орқали АКТ ҳимоясини таъминлайди, белгиланган мезонлар асосида ахборот текширувини амалга ошириб, пакетларнинг тизимга киришига қарор қабул қилади. Тармоқлараро экран тармоқдан ўтувчи барча пакетларни кўради ва иккала (кириш, чиқиш) йўналиши бўйича пакетларни белгиланган қоидалар асосида текшириб, уларга руҳсат бериш ёки бермасликни ҳал қилади. Шунингдек, тармоқлараро экран икки тармоқ орасидаги ҳимояни амалга оширади, яъни ҳимояланаётган тармоқни очиқ ташқи тармоқдан ҳимоялайди.

Ҳимоя воситасининг қуйида санаб ўтилган қулайликлари, айниқса, пакетларни филтрлаш функцияси DoS ҳужумига қарши ҳимояланишнинг самарали воситасидир. Пакет филтрлари қуйидагиларни назорат қилади:

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



4.2- расм. Хизмат қилишдан воз кечиш (DoS) ҳужумини ташкил қилиш

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

• лойиҳалашдаги хатоликлар ёки камчиликлар — тармоқлараро экранларнинг ҳар хил технологиялари ҳимоялана-ётган тармоққа бўладиган барча суқилиб кириш йўлларини қамраб 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 спетсификацияланган хусусиятлар амалга оширилганлигига ишонч ҳосил қиладиган синов ўтказишнинг умумий методологияси мавжуд эмас;

• қўллашдаги (эксплуатациядаги) камчиликлар — тармоқлараро экранларни бошқариш, уларни хавфсизлик сиёсати асосида конфигуратсиялаш жуда мураккаб ҳисобланади ва кўпгина вазиятларда тармоқлараро экранларни нотўғри конфигурациялаш ҳоллари учраб туради. Санаб ўтилган камчиликларни IPsec протоколидан фойдаланган ҳолда бартараф этиш мумкин. Юқоридагиларни умумлаштириб, тармоқлараро экранлар ва IPsec протоколидан тўғри фойдаланиш орқали DoS ҳужумидан етарлича ҳимояга эга бўлиш мумкин.

Port scanning ҳужум тури одатда тармоқ хизматини кўрсатувчи компьютерларга нисбатан кўп қўлланади. Тармоқ хавфсизлигини таъминлаш учун кўпроқ виртуал портларга эътибор қаратишимиз керак. Чунки портлар маълумотларни канал орқали ташувчи воситадир. Компьютерда 65 536та стандарт портлар мавжуд. Компьютер 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. Агар дераза очиқлигини ўғри пайқаса, уйга кириш осон бўлади. Ҳаккер ҳужум қилаётган вақтда порт очиқ ёки фойдаланилмаётганлиги ҳақида маълумот олиши учун Портларни текшириш ҳужумидан фойдаланади.

Бир вақтда барча портларни таҳлил қилиш мақсадида хабар юборилади, натижада реал вақт давомида фойдаланувчи компьютернинг қайси портини

ишлатаётгани аниқланади, бу эса компьютернинг нозик нуқтаси ҳисобланади. 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) fayl almashish protokoli;
- Port #35: Хусусий printer server;
- Port #80: HTTP traffic (Hypertext Transfer Transport Protocol) гипермatн алмашиш протоколи;
- Порт #110: ПОП3 (Пост Оффисе Протосол 3) E-mail portokoli.

Hujum turlari	Himoya vositalari
Axborotni uzatish jarayonida hujum qilish orqali, eshitish va o'zgartirish (*Eavesdropping*)	IPSec (*Internet protocol security*) protokoli. VPN (*Virtual Private Network*) virtual xususiy tarmoq IDS (*Intrusion Detection System*) ruxsatsiz kirishlarni aniqlash tizimi
Xizmat ko'rsatishdan voz kechish (*Denial-of-service*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*) IPSec (*Internet protocol security*) protokoli.
Portlarni tekshirish (*Port scanning*)	Tarmoqlararo ekranlar texnologiyasi (*Firewall*)

4.3- расм.

Портларни текшириш ҳужумига қарши самарали ҳимоя йечими 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.

4.3. Ахборот тармоғи хавфсизлиги қурилмалар ва дастурий таъминоти.

Интернетда мавжуд электрон тўловлар хавфсизлигини таъминлаш ҳозирги кунда Интернетда кўпгина ахборот марказлари мавжуд, масалан, кутубхоналар, кўп соҳали маълумотлар базалари, давлат ва тижорат ташкилотлари, биржалар, банклар ва бошқалар. Интернетда бажариладиган электрон савдо катта аҳамият касб этмоқда. Буюртмалар тизимининг кўпайиши билан ушбу фаолият яна кескин ривожланади. Натижада, ҳаридорлар бевосита уйдан ёки офисдан туриб, буюртмалар бериш имконига эга бўлишади. Шу боис ҳам, дастурий таъминотлар ва аппарат воситалар ишлаб чиқарувчилар, савдо ва молиявий ташкилотлар ушбу йўналишни ривожлантиришга фаол киришишган.

Ахборот тармоғи хавфсизлиги қурилмалар, дастурий таъминот, маълумотлар ва ходимларни ҳимоялашни ўз ичига олади.

Ахборот тармоқлари хавфсизлигини таъминлаш ва уларни бошқаришни оптималлаштирувчи бир қанча дастурий маҳсулотлар мавжуд. Масалан: Opsview

Core; StoneGate SSL VPN; Kerio Control; OpenMediaVault ва бошқалар. Корпоратив тармоқлар учун бугунги кунда энг оммабоп ва қулай тизимлардан бири бу Kerio Control ҳисобланиб, унда қуйидаги имкониятлар мавжуд:

- интернет тармоғига хавфсиз мурожаатни амалга ошириш;
- тезликка чегара қўйиш, шунингдек фақат керакли ресурсга мурожаатни таъминлаш орқали харажатларни камайтириш;
- интернетдан фойдаланишни назорат қилиш орқали ходимлар иш самарадорлигини ошириш;
- турли реклама, спам, ва вируслардан ҳимоялаши ва бошқалар.

Керио компаниясига 1997 йилда асос солинган бўлиб, у интернет тармоғида маълумотлар билан ишлаш ва алмашиш билан боғлиқ кенг турдаги дастурий маҳсулотларни тақдим этади.

Kerio Control – бу ахборот хавфсизлигини таъминловчи комплекс ечимдир. У тармоқлараро экран (Firewall), маршрутизатор, ҳужум олдини олиш тизими (IPS), антивирус ва бошқа функцияларни ташкил топган. Шунингдек, протоколлар назоратини юритади, пакетлар ҳолатини аниқлайди, локал тармоқ манзилларини ташқи тармоққа йўналтиради dNAT- dynamic Network Address Translation), DHCP (Dynamic Host Configuration Protocol) сервери вазифасини бажаради, HTTPS протоколини назорат қилади. Тизим Sophos антивируси билан таъминланган ҳамда URL манзилларни филтрлайди, Active Directory ва Open Directory билан интеграцияни таъминлайди, IP манзилларнинг “қора рўйхат”ини ҳамда Emerging Threats қоидалар базасини юритади.

Ҳозирги кунда Интернетда кўпгина ахборот марказлари мавжуд, масалан, кутубхоналар, кўп соҳали маълумотлар базалари, давлат ва тижорат ташкилотлари, биржалар, банклар ва бошқалар. Интернетда бажариладиган электрон савдо катта ҳамият касб этмоқда. Буюртмалар тизимининг кўпайиши билан ушбу фаолият яна кескин ривожланади. Натижада, ҳаридорлар бевосита уйдан ёки офисдан туриб, буюртмалар бериш имконига эга бўлишади. Шу боис ҳам, дастурий таъминотлар ва аппарат воситалар ишлаб чиқарувчилар, савдо ва молиявий ташкилотлар ушбу йўналишни ривожлантиришга фаол киришишган.

Ҳаридор, кредит картаси соҳиби, бевосита тармоқ орқали тўловларни бажариш учун ишончли ва ҳимояланган воситаларга эга бўлиши лозим. Ҳозирги кунда SSL (Secure Socket Layer) ва SET (Secure Electronic Transactions) протоколлари ишлаб чиқилган:

• SSL протоколи маълумотларни канал даражасида шифрлашда қўлланилади;

• SET хавфсиз электрон транзактсиялари протоколи якинда ишлаб чиқилган бўлиб, фақатгина молиявий маълумотларни шифрлашда қўлланилади.

SET протоколининг жорий этилиши бевосита Интернетда кредит карталар билан тўловлар сонининг кескин ошишига олиб келади.

SET протоколи қуйидагиларни таъминлашга кафолат беради:

• ахборотларнинг тўлиқ махфийлиги, чунки фойдаланувчи тўлов маълумотларининг ҳимояланганлигига тўлиқ ишонч ҳосил қилиши керак;

• маълумотларнинг тўлиқ сақланиши, яъни маълумотларни узатиш жараёнида бузилмаслигини кафолатлаш. Буни бажариш омилларидан бири рақамли имзони қўллашдир;

• кредит карта сохибининг ҳисоб рақамини аудентификатсиялаш, яъни

электрон (рақамли) имзо ва сертификатлар ҳисоб рақамини аудентификатсиялаш ва кредит карта соҳиби ушбу ҳисоб рақамининг ҳақиқий эгаси эканлигини тасдиқлаш;

• тижоратчини ўз фаолияти билан шугулланишини кафолатлаш, чунки кредит карта соҳиби тижоратчининг ҳақиқийлигини, яъни молиявий операцсиялар бажаришини билиши шарт. Бунда тижоратчининг рақамли имзосини ва сертификатини қўллаш электрон тўловларнинг амалга оширилишини кафолатлайди.

«Secure Touch» такомиллаштирилган датчик

«Secure Touch» такомиллаштирилган датчик – чакана савдо ва катта бизнес каби кўп ҳаракатлар амалга ошириладиган шароитларда фойдаланиш учун яратилган модулли янгилик.

Ушбу мослама мураккаб қурилмалар ягона ШК орқали уланишлари ва ишлашларига имкон беради ва битимлар катта фойдаланувчилар базасида бажариладиган ҳолатларда фойдаланиш мумкин. Такомиллаштирилган «Secure Touch» датчиги қуйидагилар учун йечимларни кўзда тутади:

– Чакана Савдо учун ҳақ тўлаш,
– Вақт ва мавжудлик.

ПК «Secure Touch»

ПК «Secure Touch» бармоқ изларини аниқлаш учун фойдаланиш осон, арзон, у компьютер ва тармоқдан фойдаланишни бошқариш учун кучайтирилган ҳимояни таъминлайди.

Йўқотилиши, ўғриланиши ёки ёддан чиқарилиши мумкин бўлган Идентификация кодларидан фарқли равишда бармоқ излари билан аутентификация фақатгина руҳсатга эга фойдаланувчилар компьютер ва тармоқдан фойдаланишларини кафолатлайди

Шифрлаш ахборотни ўзгартириш ва руҳсатга эга бўлмаган фойдаланувчилардан мазмунини яшириш йўли билан унинг махфийлигига амал қилиш жараёни ҳисобланади. Ишончсиз канал, мисол учун симсиз тармоқ ва Интернет орқали ахборот узатишда фойдаланилади ва у қуйидагиларга асосланади:

– Алгоритмга,
– Калитга,
– Тармоқни ҳимоялаш моделига.

Брандмауерлар

Брандмауер ташкилот тармоғига ташқаридан фойдаланиш ва бузиб киришнинг олдини олади ва тармоқ заифлигини хавфсизликка ҳужумлардан камайтиради. Кириш ва чиқиш пакетлари ушлаб қолинади, таҳлил қилинади ва руҳсат этилади/сараланади (четлатилади). Хавфсизлик сиёсатидан келиб чиқиб, брандмауер маълумотларни ўтказиш мумкинлигини ҳал қилади. У ишончсиз ташқи тармоқ ва ички тармоқ ўртасида шлюз бўлиб хизмат қилади.

Брандмауер фойдаланишни бошқариш қурилмаси сифатида:

– Кераксиз трафикни тўсади;
– Кириш трафикларини янада ишончли тизимларга йўналтиради;
– Заиф тизимларни Интернет орқали фойдаланишлардан яширади;

– Идора тармоғига қабул қилинадиган ва узатиладиган трафикни текширишни таъминлайди;

– Тизимнинг номи, тармоқ топологияси, тармоқ қурилмалари турлари ва фойдаланувчини ички аниқлаш каби ахборотларни Интернетдан яширади;

– Стандарт қўшимчага қараганда янада кучли аутентификатсияни таъминлайди.

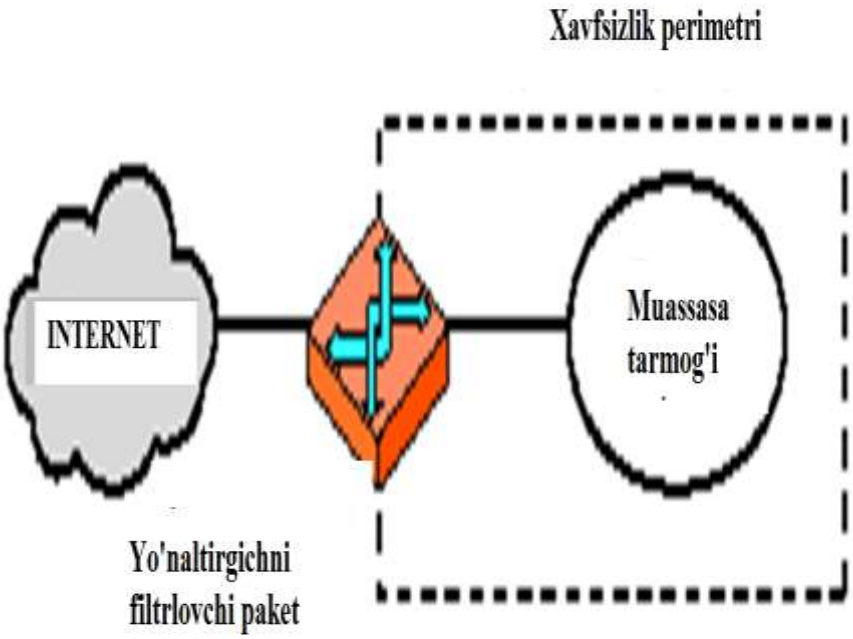
Брандмауер қуйидагиларни ўз ичига олади:

– Маршрутизаторга киритилган дастурий таъминот;

– Ажратилган компьютер, ҳост ёки ҳостлар тўплами созлашлар, айниқса тармоқдан ташқаридаги ҳостлардан келиб чиқадиган хавф туғдирадиган протоколлар ёки хизматлардан сайтни ёки тармоқни ҳимоялаш учун. Ташқи бузғунчиларга корпоратив тармоққа киришларига тўсқинлик қилади.

Брандмауерлар – пакетли фильтрлар

Брандмауерлар филтрлар сифатида тўсиқ қўйиш/руҳсат этиш учун филтрлар сифатида созланиши мумкин, бунда: IP-манзиллар; Домен номлари; Портлар; Алоҳида сўзлар ва иборалар; Кириш/чиқиш трафигини таҳлил қилиш йўли билан.



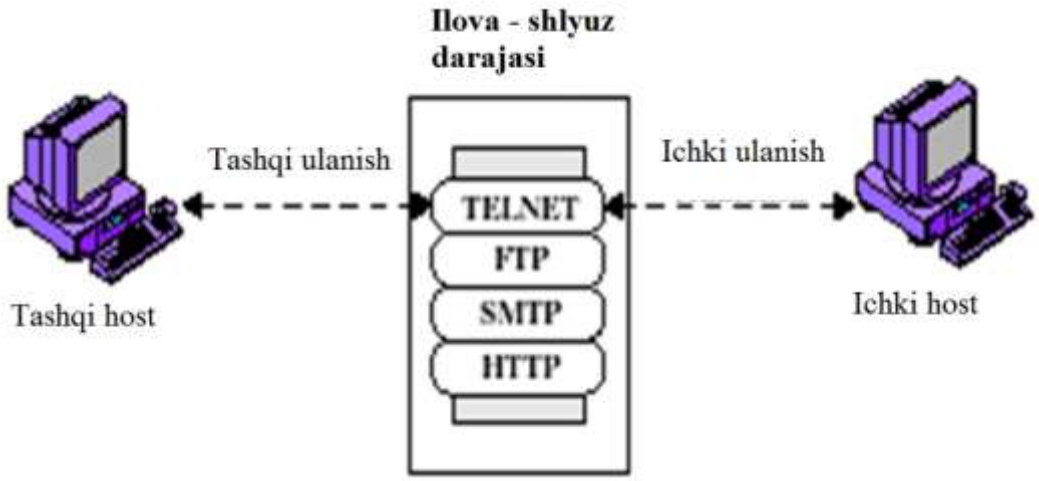
4.4. – расм.

Брандмауерлар турлари:

– Пакетли филтр ёки сараловчи филтрлар;

– Илова шлюзлар ёки прокси-серверлар.

Ушбу ҳимоя тармоқ қурилмаларини қўллаш ҳимоялаш сиёсати ва ташкилотда татбиқ этилган қоидалар тўпламига боғлиқ бўлади.



4.5. - расм. Илова – шлюз даражаси

4.4. Тармоқлараро экраннинг пакетларни филтрлаш қоидалари.

Автоматлаштирилган тизимларда тармоқ технологиялари асосида ишловчи иловалардан кенг фойдаланиш, технологияларининг ривожланиши тармоқ ресурслари ҳимоясига ва хавфсизлигини таъминлаш билан боғлиқ аввал маълум бўлмаган янги кўринишдаги хавфсизлик муаммоларни кўндаланг қўймоқда. Ушбу муаммолар сабаб замонавий компьютер тизимлари ва тармоқларида ҳимоянинг бирламчи ташкил этувчиси сифатида аппарат-дастурий йечимга эга бўлган тармоқлараро экран технологиясидан кенг фойдаланилмоқда.

Шу сабабли тармоқлараро экран асосида тармоқ трафигини филтрлаш жараёнида фойдаланиладиган махсус филтрлаш қоидалари гуруҳини созлашни ва қўллашни тўғри ташкил этиш, тармоқ трафиги билан боғлиқ хавфсизлик муаммоларини бартараф этишда энг ишончли йечимларидан бири эканлигини кўрсатмоқда.

Тармоқ трафигини филтрлаш, тармоқдаги турли сатҳларида амалга оширилиши мумкин. Ҳар бир сатҳга маълум бир филтрлаш қоидалари гуруҳи мос келади. Ҳар бир гуруҳнинг филтрлаш қоидалари жорий сатҳ боғланишига мос протокол пакетларининг сарлавҳа параметрлари берилади.

Шундай қилиб, тармоқлараро экранда пакетлар сарлавҳасининг таркибий қисми бўлган маълумотлар асосида пакетли филтрлаш амалга ошитрилади.

Тармоқлараро экранда қуйидаги қоидалар гуруҳи мавжуд:

– MAC-қоида – Ethernet кадрлар сатҳидаги филтрлаш қоидалари;
– ARP -қоида – ARP ва RARP пакетларини филтрлаш қоидалари;
– IP-қоида – IPv4 протоколи пакетларини филтрлаш қоидалари.
– IP-қоидаларида TCP, UDP ва ICMP пакетларини қайта ишлаш учун қўшимча пакетлар мавжуд. Бу гуруҳга қисқа тармоқ ҳужумларини қайтариш, абонентларни блоклаш ва бошқалар учун ўзига хос вақтинчалик IP-қоидалар ҳам киради;
– IPX-қоида – IPX пакетларини фильтрлаш қоидалари;
– AP-қоида – амалий сатҳ филтрлаш қоидалари.

Қоидаларни тузишда қоидани маълум вақт интервалига ва VLAN идентификаторига боғлашга имкон берувчи — VLAN -гуруҳлар ва “Вақт

интерваллари” махсус тузилмаларидан фойдаланилади.

Ҳар қандай филтрлаш қоидаси қуйидагича кўринишда бўлади:

– IF (қоидалар параметри) – THEN (қоидалар ҳаракати), яъни пакетнинг етиб келган сарлавҳаси қоида параметрларига тўғри келса, пакетга қоидада кўрсатилган ҳаракат қўлланилиши лозим.

– Бунда пакет устида қуйидаги ҳаракатлар амалга оширилишига йўл қўйилади:

– ўтказиш (accept) – чиқувчи филтрлаш интерфейсига ёки филтрлашнинг кейинги сатҳига (MAC-қоидалар учун) пакетни узатади;

– юбориш (pass) – кейинги филтрлаш сатҳларини айланиб ўтган ҳолда чиқувчи филтрлаш интерфейсига пакетни узатади (тармоқлараро экран ичида);

– ўчириш (drop) – пакетни кейинги ўтишига таъқиқ қўйиш.

Пакетли филтрлаш режимида пакетларни қайта ишлаш 2 босқичда амалга оширилади:

1) MAC-қоидалар бўйича филтрлаш;

2) Кейинги сатҳ қоидалари бўйича филтрлаш (ARP, IP ва IPX -қоидалари).

Биринчи навбатда тармоқлараро экранни филтрловчи интерфейси томонидан қабул қилинган ҳар бир пакетни филтрлаш MAC-қоидаларига мувофиқ Ethernet кадрлар сатҳида ишланади. Агар пакетга пакет ўчирилиши белгиланган қоида қўлланилса, унда пакет ҳеч қаерга узатилмасдан, уни қайта ишлаш тўхтатилади. Агар пакетга пакетни ўтказиш белгиланган қоидаси қўлланилса, унда бу пакет уни ўтказиш ёки ўчириш тўғрисидаги сўнгги қарор қабул қилувчи филтрлашнинг кейинги сатҳига берилади. Агар пакетга юбориш қоидаси қўлланилса, унда бу пакетни фильтрлаш процедураси тўхтатилади ва пакет чиқувчи интерфейсга берилади.

Фильтрлашнинг кейинги сатҳида пакетга жорий Ethernet-кадрда инкапсуляцияланувчи протокол тоифасига боғлиқ ҳолда ARP, IP ва IPX -қоидаларнинг мос келувчи ҳолатларидан бири қўлланилади.

Назорат саволлари:

1. Хавфсизликка таҳдид ва заиф жойлар ҳақида маълумот беринг.
2. Брандмауерлар фильтрлар сифатида қандай ишлайди?
3. Брандмауерлар – пакетли фильтрлар нима?
4. Хавфсиз электрон почта
5. Ҳужум воситаларига қайсилар киради?
6. Ipsec (Internet protocol security) хавфсизлик протоколлари
7. Ахборот тармоғи хавфсизлиги қурилмалар ва дастурий таъминот
8. ПК «Secure Touch» нима?
9. Тармоқлараро экраннинг пакетларни филтрлаш қоидалари

Адабиётлар ва Интернет сайтлари:

1. Эшмурадов А.М., Абдужалилов Ж.А. “Интернет тармоқлари ва хизматлари” фанидан ўқув-услубий мажмуа. – Тошкент: ТАТУ. 2016.

2. Олифер Виктор, Наталия Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник. – Сн-Петербург: Издательство ПИТЕР, 2016, 992 с.
3. Douglas E. Comer. Computer Networks and Internets (6th Edition). Pearson. USA, 2015. 672 p.
4. Компьютерные сети и технологии. http://www.xnets.ru/
5. http://www.network.xsp.ru/

5-маъруза. Киберхавфсизлик вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш.
(2 соат)

Режа:

5.1. Киберхавфсизликнинг фундаментал тушунчалари.
5.2. Киберхавфсизлик сиёсати ва уни бошқариш.
5.3. Хавф-хатарларни бошқариш.
5.4. Ҳужум инцидентлари ва уларга қарши реакция.

Таянч иборалар: *Киберхавфсизлик, Конфиденциаллик, Яхлитлик, Фойдаланувчанлик, Маълумотлар хавфсизлиги, Дастурий таъминотлар хавфсизлиги, Ташкил этувчилар хавфсизлиги, Алоқа хавфсизлиги, Тизим хавфсизлиги, Инсон хавфсизлиги, киберхавфсизлик рисклари, Рискларни идентификация қилиш, Ҳодиса, Инцидент , Ҳужум, ИТРМ модели.*

“Агар сиз сирингизни шамолга айтсангиз, уни дарахтларга айтгани учун шамолни айбламанг”.
Каҳлил Гибран

5.1. Киберхавфсизликнинг фундаментал тушунчалари.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатъий регламентланган динамик технологик жараёнга айтилади.

Киберхавфсизлик ҳозирда кириб келган янги тушунчалардан бири бўлиб, унга турли берилган турли таърифлар мавжуд.

- Хусусан, **CSEC2017 Joint Task Force (CSEC2017 JTF)** киберхавфсизликка қуйидагича таъриф берган: ***киберхавфсизлик*** *– ҳисоблашга асосланган билим соҳаси бўлиб, бузғунчилар мавжуд бўлган шароитда амалларни кафолатлаш учун ўзида технология, инсон, ахборот ва жараённи мужассамлаштирган.*
- У *хавфсиз компьютер тизимларини яратиш, амалга ошириш, таҳлил қилиш ва тестлашни* **ўз ичига олади**.
- Киберхавфсизлик таълимнинг **мужассамлашган** билим соҳаси бўлиб,

қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқаришни **ўз ичига олади**.

• Тармоқ бўйича фаолият юритаётган ***Cisco*** ташкилоти эса киберхавфсизликка қуйидагича таъриф берган: ***Киберхавфсизлик*** *– тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти.*

• Ушбу киберхужумлар одатда *махфий ахборотни бошқариш, алмаштириш ёки йўқ қилишни; фойдаланувчилардан пул ундиришни; ёки нормал иш фаолиятини узуб қўйишни* **мақсад қилади**.

• Ҳозирги кунда самарали киберхавфсизлик чораларини амалга ошириш *инсонларга қараганда қурилмалар сонининг кўплиги* ва *бузғунчилар салоҳиятини ортиши натижасида* **амалий томондан мураккаблашиб** бормоқда.

5.1-расм. Киберхавфсизлик кимларга керак.

Киберхавфсизликни **фундаментал терминларини** қараб чиқамиз:

• ***Конфиденциаллик***

– Тизим маълумоти ва ахборотига фақат **ваколатга эга субъектлар** фойдаланиши мумкинлигини таъминловчи қоидалар.

– Мазкур қоидалар ахборотни фақат қонуний фойдаланувчилар томонидан **“ўқилишини”** таъминлайди.

• ***Яхлитлик (бутунлик)***

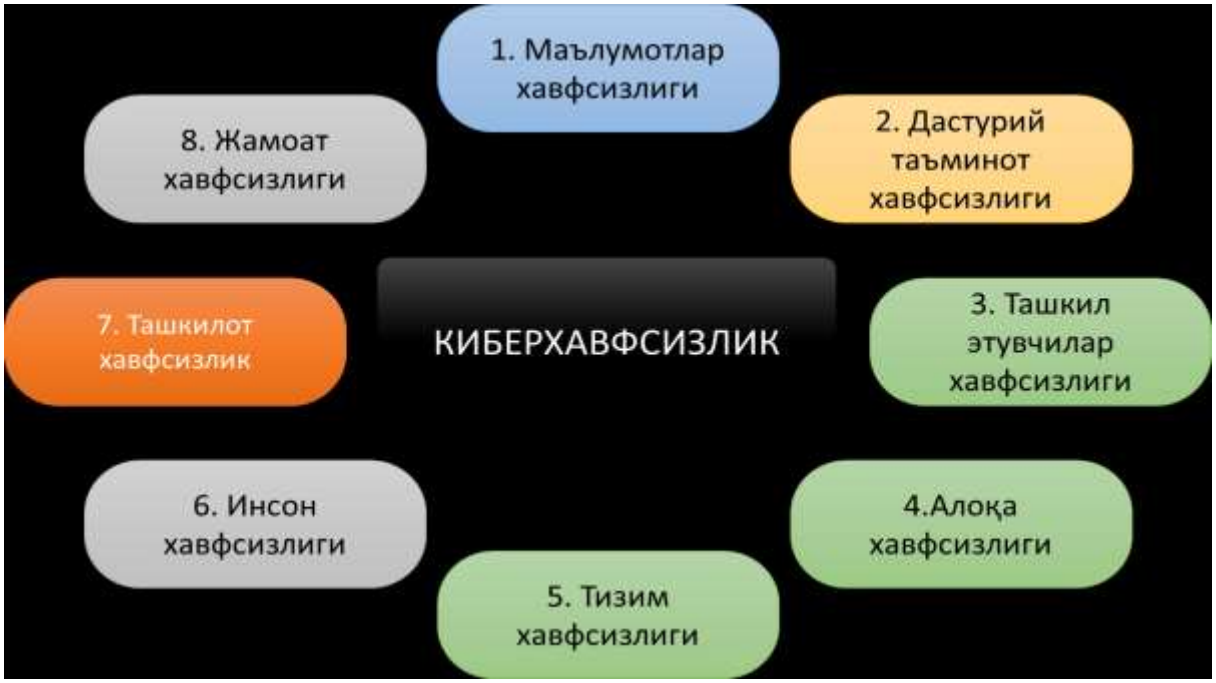
– Маълумотни аниқ ва ишончли эканлигига ишонч ҳосил қилиш.

– Яъни, ахборотни рухсат этилмаган ўзгартиришдан ёки **“ёзиш”** дан ҳимоялаш.

• ***Фойдаланувчанлик***

– Маълумот, ахборот ва тизимдан фойдаланишнинг мумкинлиги.

– Яъни, рухсат этилмаган **“бажариш”** дан ҳимоялаш.



5.2-расм. Киберхавфсизликнинг билим соҳалари.

• **“Маълумотлар хавфсизлиги”** билим соҳаси **маълумотларни сақлашда, қайта ишлашда** ва **узатишда** ҳимояни таъминлашни мақсад қилади.

– Мазкур билим соҳаси ҳимояни тўлиқ амалга ошириш учун **математик** ва **аналитик алгоритмлардан** фойдаланишни талаб этади.

• “**Дастурий таъминотлар хавфсизлиги**” билим соҳаси фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи **дастурий таъминотларни ишлаб чиқиш** ва **фойдаланиш жараёнига** эътибор қаратади.

• “**Ташкил этувчилар хавфсизлиги**” билим соҳаси катта тизимларда интеграллашган ташкил этувчиларни **лойиҳалаш, сотиб олиш, тестлаш, анализ қилиш** ва **техник хизмат кўрсатишга** эътибор қаратади.

– Тизим хавфсизлиги ташкил этувчилар хавфсизлигидан фарқ қилади.

– Ташкил этувчилар хавфсизлиги улар *қандай лойиҳаланганлиги, яратилганлиги, сотиб олинганлиги, бошқа таркибий қисмларга уланганлиги, қандай ишлатилганлиги* ва *сақланганлигига* боғлиқ.

• “**Алоқа хавфсизлиги**” билим соҳаси ташкил этувчилар ўртасидаги **алоқани ҳимоялашга** этибор қаратиб, ўзида *физик* ва *мантиқий* уланишни бирлаштиради.

• “**Тизим хавфсизлиги**” билим соҳаси **ташкил этувчилар, уланишлар** ва **дастурий таъминотдан** иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади.

– Тизим хавфсизлигини тушуниш учун нафақат, *унинг таркибий қисмлари* ва *уланишини тушунишни*, балки *бутунликни* ҳисобга олишни талаб қилади.

• “**Инсон хавфсизлиги**” билим соҳаси *киберхавфсизлик билан боғлиқ инсон ҳатти ҳаракатларини ўрганишдан* ташқари, *ташкилотлар (масалан, ходим)* ва *шахсий ҳаёт шароитида шахсий маълумотларни* ва *шахсий ҳаётни ҳимоя қилишга* эътибор қаратади.

• “**Ташкилот хавфсизлиги**” билим соҳаси ташкилотни *киберхавфсизлик таҳдидларидан ҳимоялаш* ва *ташкилот вазифасини муваффақиятли бажаришини* мададлаш учун рискларни бошқаришга эътибор қаратади.

• “**Жамоат хавфсизлиги**” билим соҳаси у ёки бу даражада жамиятда таъсир кўрсатувчи киберхавфсизлик омилларига эътибор қаратади.

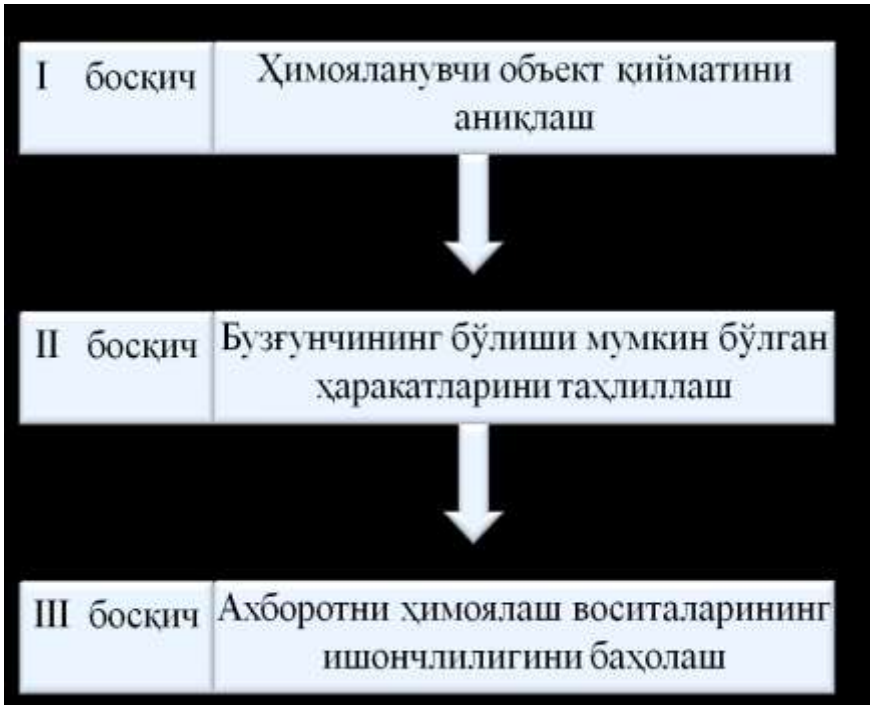
– *Кибержиноятчилик, қонунлар, ахлоқий муносабатлар, сиёсат, шахсий ҳаёт* ва *уларнинг бир-бири билан муносабатлари* ушбу билим соҳасидаги асосий тушунчалар.

5.3-расм. Хавфсизлик муаммолари.

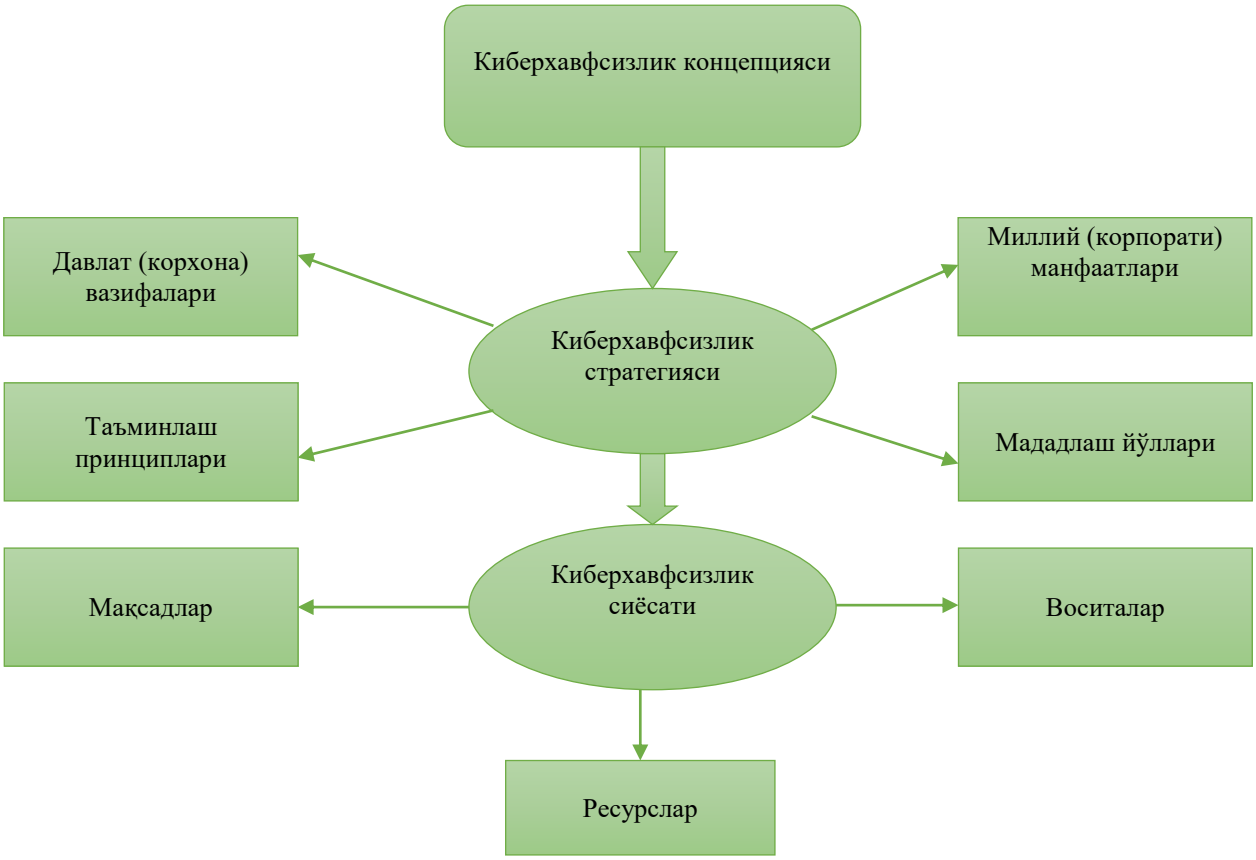
5.2. Киберхавфсизлик сиёсати ва уни бошқариш.

Киберхавфсизлик концепцияси – ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари.

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади.



5.4-расм. Ахборот химояси концепциясини ишлаб чиқиш босқичлари



5.5-расм. Киберхавфсизлик концепцияси схемаси.

Киберхавфсизлик сиёсати бу – ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режа ҳисобланади.

У хавфсизликни таъминлашнинг барча дастурларини режалаштиради.

Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт.

Ташкилотнинг амалий хавфсизлик сиёсати қўйидаги бўлимларни ўз ичига олиши мумкин:

- умумий низом;
- паролларни бошқариш сиёсати;
- фойдаланувчиларни идентификациялаш;
- фойдаланувчиларнинг ваколатлари;
- ташкилот ахборот коммуникацион тизимини компьютер вируслардан ҳимоялаш;
- тармоқ уланишларини ўрнатиш ва назоратлаш қоидалари;
- электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати қоидалари;
- ахборот коммуникацион тизимлар хавфсизлигини таъминлаш қоидалари;
- фойдаланувчиларнинг хавфсизлик сиёсатини қоидаларини бажариш бўйича мажбуриятлари ва ҳ.к.лар

5.3. Хавф-хатарларни бошқариш.

Киберхавфсизлик рискларини аниқлашнинг умумий тавсифини қраб чиқамиз. Риск номақбул воқеа - ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради.

Рискни аниқлаш қуйидаги тадбирлардан иборат:

- рискларни аниқлаш;
- рискларни идентификация қилиш;
- рискларни таҳлил қилиш;
- рискларни баҳолаш.

Рискларни аниқлаш ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди. Рискни аниқлаш кўпинча икки (ёки ундан кўп) итерациядан фойдаланиб ўтказилади.

Рискларни аниқлашнинг мақсад ва вазифалари асосида рискларни аниқлашга ўз ёндашувини танлаш ташкилотнинг ўзига боғлиқ.

Активларнинг баҳоси, оқибатларнинг ҳар бир турига тааллуқли бўлган заифликлар ва таҳдидларнинг даражалари, ҳар бир комбинация учун 0 дан 8 гача бўлган шкала асосида рискнинг тегишли ўлчовини идентификациялаш мақсадида, жадвал шаклига (матрицага) келтирилади (5.1 (а)-жадвал). Қийматлар матрицага структураланган тарзда киритилади.

5.1(а)-жадвал.

Рисклар ўлчовларини идентификациялаш матрицаси

	Таҳдиднинг юзага келиш 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 риск 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 риск 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 риск 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.

Рискларнинг берилган шкаласи қуйидагича оддий умумий рейтинги учун ҳам акс эттирилиши мумкин:

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

5.1(b)- жадвал.

Рисклар умумий рейтингининг матрицаси

	Инцидент сценарийси эҳтимоллиги	Жуда паст (эҳтимоллиги жуда кам)	Паст (эҳтимоллиги кам	Ўртача (мумкин бўлган)	Юқори (эҳтимоллиги бўлган)	Жуда юқори (тез-тез учраб турадиган)
Актив баҳоси	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

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

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

Активларни аниқлашда ахборот тизими фақат аппарат ва дастурий воситалардан иборат эмаслигини назарда тутиш керак. Активларни аниқлаш рискларни баҳолаш учун етарли ахборот таъминланадиган тегишли деталлаштириш даражасида амалга оширилиши зарур. Активларни аниқлашда фойдаланиладиган деталлаштириш даражаси рискларни баҳолаш вақтида

тўпланган ахборотнинг умумий ҳажмига таъсир этади. Бу даража рискларни баҳолашнинг кейинги итерацияларида янада деталлаштирилиши мумкин.

5.4. Ҳужум инцидентлари ва уларга қарши реакция.

Киберхавфсизлик соҳасидаги фактлар:

1. Кучли пароль кўп ҳужумларни бартараф этиши мумкин.
2. Янги восита (дастурий-аппарат) хавфсиз ҳисобланмайди.
3. Энг яхши дастурий воситалар заифликларни ўз ичига олади.
4. Булутли технология тўлиқ хавфсиз эмас.
5. Хакералар-булар ҳама вақт ҳам жиноятчи эмас.

Компьютер ва компьютер тармоқларида **компьютер хавфсизлиги инцидентларини бошқариш** ўз ичига мониторинг ва хавфсизлик ҳодиса-воқеаларини, ҳамда бу ҳодиса-воқеаларга тўғри жавобларни қайтаришни қамраб олади. Инцидентни бошқариш дастур ҳисобланиб маълум бир жараённи аниқлаб беради ва амалга оширади.

Ҳодиса - шахс ёки ишчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир.

Ҳодисанинг учта асосий тури мавжуд:

Нормал. Нормал ҳодиса критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.

Ҳодисаларни кенгайиши ва кўпайиши (Эскалация). Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.

Авариявий ҳодиса. Авариявий ҳодиса шахс хавфсизлиги ва соғлигига таъсир кўрсатади.

Инцидент - бу стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.

Инцидентга жавоб қайтариш гуруҳи. Хавфсизлик инциденти координатори инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир. Координатор командани ташкил этиб, ташкил этилган команда ўз ичига инцидентни баҳоловчи ва қарор қабул қилувчи шахсларни қамраб олади.

Инцидентни тергов қилиш - бу инцидент ҳолатини тергов қилиш ҳаракатидир. Ҳар бир инцидент тергов этишни талаб қилиши ёки унга кафиллик бериши керак бўлади. Шу билан бирга тергов қилинадиган ресурслар, яъни тиббий воситалар, номуносиб тармоқлар ва карантин қилинган тармоқлар фавқулодда инцидентларга тез ва самарали рухсат бериш учун фойдали ҳисобланади.

Инцидентга жавоб қайтариш - бу хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир. Бунинг мақсади вазиятни тўғрилаш, яъни тизимни бузилишини чеклаш ва бузилган тизимни тиклаш вақти ва маблағини камайтиришдир.

Инцидент бошқарувчисини вазифалари ва мажбуриятлари:

– муносиб ваколатлардан фойдаланиш учун ҳар қандай авария /

носозликларни билиш;

– етарли ахборот йиғиш ва тизимни таҳлил этиш учун қайта тиклайдиган командани шакллантириш;

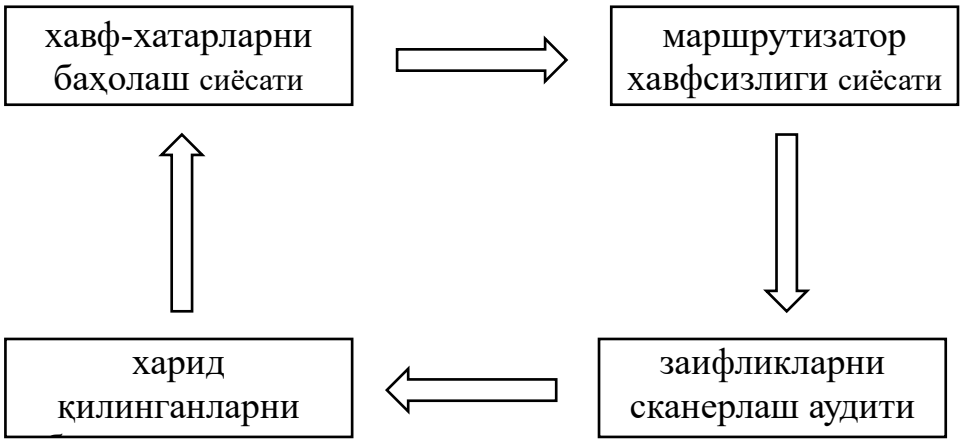
– инцидентни умумий ҳолатини сақлаш;

– функционал имкониятларни билиш (Core Network);

– командани юқори сатҳга кўтариш (приоритет бериш) учун қўлланмадан фойдаланиш.

Ҳужум инцидентларини бошқариш тизими

Ташкилот фаолиятида ахборотни ҳимоялаш учун қўйидаги моделни келтириш мумкин: **ИТРМ**. Бу модел 4та жараённи ўз ичига олади. Булар:



5.6-расм. ИТРМ модели.

Келтирилган 4 та жараён ҳам танқидий (критик) муҳим ҳисобланади. Тизимда бу жараёнларнинг бирортасини йўқлиги ёки яхши ишмаслиги корхона ёки ташкилот ахборот ресурслари ҳимояланганлигига катта зарар етказади. Ахборот хавфсизлиги инцидентларни бошқаришда бу жараёнларнинг ичидан фақат мониторинг жараёнини кўпроқ кузатиш мумкин.

Кўп ташкилот ва корхоналарда **ахборот хавфсизлиги инцидентларни бошқариш жараёни** қуйидагича қурилади:

- компьютер инциденти ҳақида ахборот олиш;
- қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш;
- ҳолатни таҳлил этиш;
- сабабларни аниқлаш;
- профилактик тадбирлар ўтказиш.

Инцидентларини бошқариш жараёни самарадорлиги қўйидагиларга боғлиқдир:

❑ ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши;

❑ инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги;

❑ олинган натижаларнинг ҳақиқийлиги.

Инцидентини бошқариш тизимини қуриш концепцияси ва структурасини қараб чиқамиз.

Ахборот хавфсизлиги инцидентини бошқариш тизими архитектураси қуйидаги асосий компоненталарни ўз ичига олади:

1. Интеграллашган платформа.
2. Аудит ва мониторингни аппарат-дастурий воситалари.
3. Ахборотни ҳимоялашнинг аппарат-дастурий воситалари.
4. Ахборот хавфсизлиги инцидентлари ҳақида ахборот омбори.
5. Ҳисоботларни генерациялаш воситалари ва аналитик асбоблар.
6. Воситаларни бошқариш ва интерфейсни тўғрилаш.

Интеграллашган платформа тизимнинг ядроси ҳисобланади. Бу тизим тузилишидаги ҳамма компоненталарни битта умумий функцияга боғлаб беради.

Интеграллашган платформа қўйидагилардан таркиб топган:

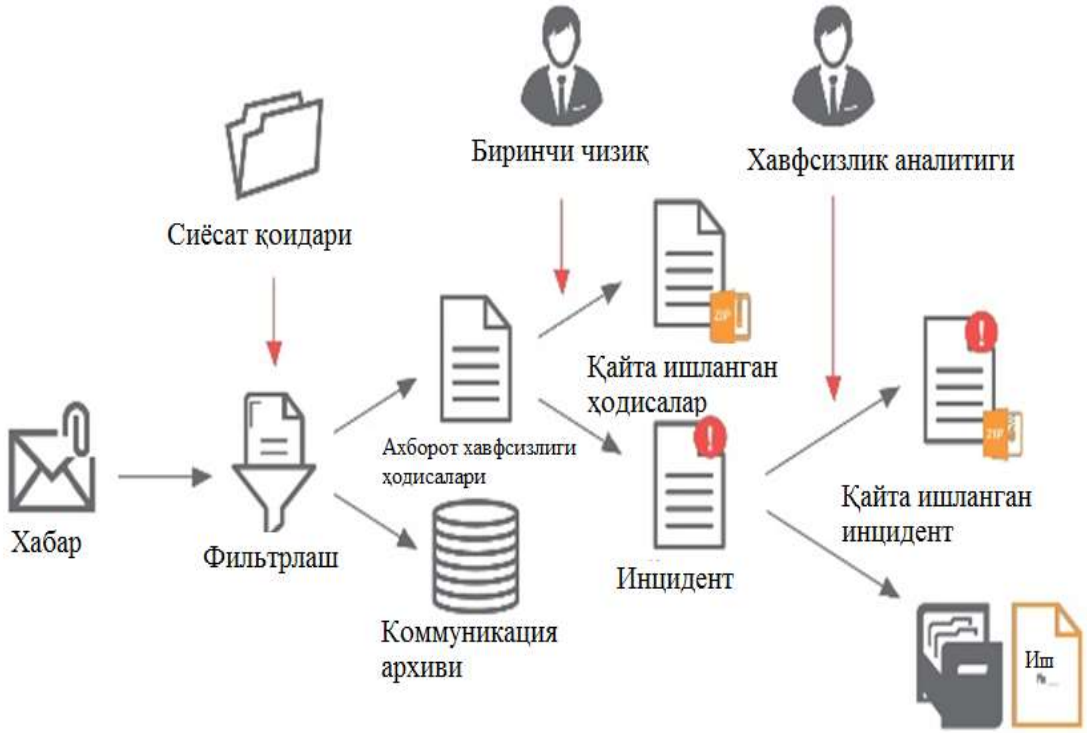
1. Маълумотларни йиғишни таъминловчи мониторинг ва аудит воситалари учун интерфейс.
2. Ахборот хавфсизлиги инцидентлари оқибатини локализациялаш мақсадида конфигурацияни тезкор ўзгартиришдаги ахборот ҳимояси воситалари интерфейси
3. Ҳисоботларни генерациялаш воситалари ва аналитик функциялардан фойдаланишдаги хизматлар.

Аудит ва мониторингни аппарат-дастурий воситалари - ташкилот ахборот тизимини қайта ишлаш, йиғиш ва протоколлаштиришни амалга оширувчи воситалардир. Бу воситаларга қуйидагилар киради: ўрнатилган воситалар (иловалар, операцион тизим воситалари, тармоқ қурилмалари, ҳимоя воситалари ва автоматлаштирилган тизимлар) ва махсус воситалар (аудит, хавфсизлик сканерлари, дастурий агентлар, сенсорлар, ахборот йиғувчи қурилмалар).

5.7-расм. Аудит ва мониторингни аппарат-дастурий воситалари.

Ахборотни ҳимоялашнинг аппарат-дастурий воситалари:

1. Firewalls
2. IDS/IPS
3. Switch Level 3
4. Ахборот хавфсизлигини таъминлаш усул ва воситалари (дастурий воситалар).



5.8-расм. Инцидентлар ахборот омбори.

Назорат саволлари:

1. Киберхавфсизлик тушунчасини изоҳлаб беринг.
2. Хавфсизлик муаммоларини санаб ўтинг.
3. Киберхавфсизлик сиёсати нима?
4. Киберхавфсизлик рискларини аниқлашни тавсифлаб беринг?
5. Инцидентга жавоб қайтариш гуруҳи қандай шакллантирилади?
6. Инцидентларини бошқариш жараёни самарадорлиги нималарга боғлиқдир?
7. Аудит ва мониторингни дастурий-аппарат воситаларини изоҳлаб беринг?

Адабиётлар ва интернет сайтлари:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.
3. https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-basics

IV БЎЛИМ

АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

IV. АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

1 – амалий машғулот. Шифрлаш алгоритмлари (4 соат)

Ишнинг мақсади: Шифрлаш алгоритмлари асосида ахборотни махфийлигини таъминлаш**.**

Масаланинг қўйилиши: ўрганилган шифрлаш усуллари асосида берилган топшириқлар бажарилсин.

Ишни бажариш учун намуна

Симметрик шифрлаш усуллари фойдаланилган алмаштириш турига кўра ўрин алмаштириш ва ўрнига қўйиш усулларига бўлинади. Ўрин алмашиниш шифрларига очиқ матн белгилари махфий калит билан бирор алгоритм бўйича тартиби ўзгартирилади. Ўрнига қўйиш усулларида эса очиқ матн белгилари бошқа алфавит белгиларига алмаштирилади.

Содда ўрин алмаштириш усуллари

Ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокини матрицага қатор бўйича ёзишни, ўқишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин.

Ўрин алмаштириш шифри оддий шифрлаш ҳисобланиб, бу усулда қатор ва устундан фойдаланилади. Чунки шифрлаш жадвал асосида амалга оширилади. Бу ерда калит (К) сифатида жадвалнинг устун ва қатори хизмат қилади. Матн (T_0) символларининг ўлчамига қараб NxM жадвали тузилади ва очиқ матнни (T_0) устун бўйича жойлаштирилиб чиқилади, қатор бўйича ўқилиб шифрланган матнга (T_1) эга бўлинади ва блокларга бўлинади.

Масалан, «Ахборот хавфсизлиги жадвали» матни шифрлансин.

T_0=Ахборот хавфсизлиги жадвали;

К = 5x5; В=5;

А	О	Ф	И	Д
Х	Т	С	Г	В
Б	Х	И	И	А
О	А	З	Ж	Л
Р	В	Л	А	И

T_1=АОФИД_ХТСГВ_БХИИА_ОАЗЖЛ_РВЛАИ

Усулнинг криптотурғунлиги блок узунлигига (матрица ўлчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8x8) учун калитнинг $1,6 \bullet 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси $1,4 \bullet 10^{26}$ га етиши мумкин.

Йўналишли ўрин алмаштириш синфидаги шифрларнинг қўлланилиши амалда кўп тарқалган. Бундай шифрлаш алгоритмлари бирор геометрик шаклга асосланган бўлади. Очиқ маълумот блоклари геометрик шаклга бирор траектория

(узлуксиз из) бўйича жойлаштирилади. Шифрмаълумот эса бошқа траектория бўйича ҳосил қилинади. Геометрик шакл сифатида (*n* x *m*) ўлчамли жадвал олиб, унинг биринчи сатри бошидан бошлаб очиқ маълумот белгиларини чапдан ўнгга кетма-кет жойлаштириб, сатр тугагач иккинчи сатрга, очиқ маълумот белгиларини ўнгдан чапга кетма-кет жойлаштириб, бу сатр тамом бўлгач, кейинги сатрга олдингисига тескари йўналишда жойлаштирилади ва ҳоказо. Охирида тўлмай қолган сатр ячейкалари очиқ маълумот алфавитидан фарқли бўлган белгилар билан тўлдирилади. Сўнгра, очиқ маълумотни жойлаштириш тартибидан фарқли бўлган бирор йўналиш танлаб олиниб, шу йўналиш асосида шифрмаълумот ҳосил қилинади. Шифрмаълумот ҳосил қилиш йўналиши калит вазифасини бажаради. Мисол сифатида "*йўналишли ўрин алмаштириш шифрлаш алгоритми*" жумласини шифрлашни (4x10) –ўлчамли жадвал асосида қўйидагича амалга ошириш мумкин:

12	3	4	5	6	7	8	9	10	
					и				*ў*
					л				*р*
					ф				*и*
..					*р*				*а*

Бу жадвал устунлари кетма-кетликларини аралаштирган ҳолда (бундай аралаштиришларнинг умумий сони 10!=3628800 та бўлади), масалан, 72968411035 тартиб (калит) билан "*шароўтиииалилфрлнлгааштйир.ўршаншмлмии*" шифрмаълумотни ҳосил қилинади. Шифрмаълумотни ҳосил қилиш жараёнини жадвалнинг сатрлари ўринларини ёки ҳар бир устунлари сатрларини алоҳида алмаштиришлар билан яна ҳам мураккаблаштириш мумкин. Сатрлар, устунлар ва алоҳида олинган сатр устунларини ёки алоҳида олинган устун сатрларини шифрлаш жараёни босқичларида ўзгартириб туриш билан яна ҳам мураккаб бўлган шифрлаш алгоритмларини ҳосил қилиш мумкин.

Содда ўрнига қўйиш усуллари

Шифрлаш алгоритмлари очиқ маълумот алфавити белгиларини шифрмаълумот белгиларига акслантиришдан иборат эканлиги такидланди. Акслантиришлар функциялари (калит деб аталувчи номаълум) параметрга боғлиқ ҳолда: жадвал ва аналитик ифода кўринишларида берилиши мумкин. Ўрнига қўйиш шифрлаш алгоритмларининг дастлабки намуналари бўлган тарихий шифрлаш алгоритмларининг деярли ҳаммаси жадвал кўринишида ифодаланади. Ўрнига қўйиш шифрлаш алгоритмларининг умумий хусусиятини ҳисобга олиб, бу синфдаги алгоритмларни жадвал кўринишда қуйидагича ифодалаш мумкин:

Очиқ маълумот алфавити (кириллча белгилар)	А	Б	...	...	Я
Шифр маълумот алфавити (иккилик саноқ системаси белгилари)	$x_0^0 x_1^0 x_2^0 x_3^0 x_4^0$	$x_0^1 x_1^1 x_2^1 x_3^1 x_4^1$	...	...	$x_0^{31} x_1^{31} x_2^{31} x_3^{31} x_4^{31}$

Кириллча алфавит белгилари сони 32 та, шу 32 та ҳар хил белгиларни битлар билан ифодалаш учун беш бит кифоя, яъни $2^5 = 32$. Келтирилган жадвалдан фойдаланиб, кириллча алфавитда ифодаланган очиқ малумот белгиларини уларга мос келувчи иккилик саноқ системасидаги беш битлик белгиларга алмаштириб шифрмаълумот ҳосил қилинади, яъни $x_i^j \in \{0;1\}$. Агарда, келтирилган жадвалда очиқ маълумот алфавити белгиларига шифрмаълумот алфавитининг қандай беш битлик белгилари мос қўйилганлиги номаълум бўлса, бу жадвал калит бўлиб, шифрмаълумотдан очиқ маълумотни тиклаш масаласи мураккаблашади. Бундай шифрлаш жараёнини ифодаловчи алгоритмнинг калитларининг умумий сони 32! бўлиб, ушбу $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Стирлинг формуласига кўра қуйидагича

$$32! = \left(\frac{32}{2,7}\right)^{32} \sqrt{2 \cdot 3,14 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} = 2^{96} \cdot 2^3 \cdot \sqrt{2} > 2^{99}$$

ҳисобланади. Бундай ҳолат эса калитни билмаган ҳолда дешифлаш жараёнини амалга оширишни жиддий мураккаблаштиради.

Аффин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аниқланади: *E(x)=ax+b (modm)*, бу ерда a, b - бутун сонлар бўлиб, калитлар ҳисобланади, 0≤a, b<m. *m* – алфавит узунлиги.

Дешифрлаш жараёни қуйидаги формула асосида амалга оширилади: $D(E(x)) = a^{-1}(E(x) - b)modm$. Бу ерда a^{-1} modm бўйича a га тескари бўлган сон.

Лотин алфавити фойдаланилганда у қуйидагича рақамланади:

										0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

Шифрлаш. Ушбу усулда маълумотларни шифрлаш учун “ATTACK AT DAWN” очиқ матни олиниб, калит сифатида a=3 ва b=4 олинди. Алфавит узунлиги m=26 га тенг. Бу ҳолда шифрлаш функцифсининг умумий кўриниши қуйидагича бўлади:$y = E(x) = (3x + 4)mod26$. Юқоридаги жадвалга асосланиб қуйидагини олиш мумкин:

Хабар	A	T	T	A	C	K	A	T	D	A	W	N
	0	19	19	0	2	10	0	19	3	0	22	13

Шифрлашнинг умумий кўриниши эса қуйидагича бўлади:

Хабар	A	T	T	A	C	K	A	T	D	A	W	N
x	0	19	19	0	2	10	0	19	3	0	22	13
3x+4	4	61	61	4	10	34	4	61	13	4	70	43
(3x+4)mod26	4	9	9	4	10	8	4	9	13	4	18	17
Шифр матн	E	J	J	E	K	I	E	J	N	E	S	R

Дешифрлаш жараёни. Дешифрлаш формуласи $D(y) = a^{-1}(y - b)modm$ га тенг бўлиб, $a^{-1} = 9$, b=4 ва m=26 га тенг бўлади.

Шифр матн	E	J	J	E	K	I	E	J	N	E	S	R
	4	9	9	4	10	8	4	9	13	4	18	17

Дешифрлашнинг умумий кўриниши эса :

Шифрматн	E	J	J	E	K	I	E	J	N	E	S	R
y	4	9	9	4	10	8	4	9	13	4	18	17
9(y-4)	0	45	45	0	54	36	0	45	81	0	126	117
9(y-4)mod26	0	19	19	0	2	10	0	19	3	0	22	13
Хабар	A	T	T	A	C	K	A	T	D	A	W	N

Частотавий таҳлил усули

Частотавий, яъни статистик характеристикалар усулида симметрик ёки носимметрик криптотизим криптотаҳлилчиси шифрматндаги белгилар, ҳарфлар, сўзларнинг такрорланишлари сонини (частоталарини) ҳисоблаб, очиқ матн қайси тилда ёзилганини аниқлайди. Сўнгра эса, шифрматн шифр белгилари параметрларини очиқ матн қайси тилда ёзилган бўлса, шу тилнинг параметрлари билан солиштиради. Масалан, инглиз тилида **E** ҳарфи частотаси юқори, шифрматнда **L** ҳарфи частотаси юқори. Шифрматндаги **L** ҳарфини **E** ҳарфи билан алмаштирилади, яъни шифрматн ва очиқ матн ёзилган тил частоталарини камайиш тартибида ёзиб, тартиби тўғри келган белгилар ўзаро алмаштирилади. Кейин шифрматн биграмма, триграмма ва **k**-граммаларининг такрорланишлар сонини топиб, очиқ матн ёзилган тил биграмма, триграмма ва **k**-граммалари билан мос ҳолда алмаштиради. Биграмма, триграмма, **k**-грамма дэганда, матнда иккита, учта ва **k**-та белгининг кетма-кет келиши тушунилади. Масалан, инглиз тилида **th**, **in**, **is**, **er**, **he**, **en**, биграммалари, рус тилида **ст**, **но**, **ен**, **то**, **на** биграммалари, **сто, ено, нов, тов, ова** триграммалари кўп учрайди. Қуйидаги жадвалда инглиз тили ҳарфларининг пайдо бўлишининг нисбий частотаси келтирилган (40 000 та сўз ичида).[1]

Ҳарф	Сони		Ҳарф	Частотаси
E	21912		E	12.02
T	16587		T	9.10
A	14810		A	8.12
O	14003		O	7.68
I	13318		I	7.31
N	12666		N	6.95
S	11450		S	6.28
R	10977		R	6.02
H	10795		H	5.92
D	7874		D	4.32
L	7253		L	3.98
U	5246		U	2.88
C	4943		C	2.71

[1] Stamp Mark. Information security: principles and practice. 24 – c.

M	4761		M	2.61
F	4200		F	2.30
Y	3853		Y	2.11
W	3819		W	2.09
G	3693		G	2.03
P	3316		P	1.82
B	2715		B	1.49
V	2019		V	1.11
K	1257		K	0.69
X	315		X	0.17
Q	205		Q	0.11
J	188		J	0.10
Z	128		Z	0.07

Юқорида айтиб ўтилган принциплар ҳозирги кунда кенг тарқалган паролларни танлаш бўйича дастурларда қўлланилади. Паролларни танлаш бўйича дастур аввало эҳтимоллиги катта бўлган паролларни танлайди. эҳтимоллиги кичик бўлган паролларни кейинга олиб қўяди.

A5/1 оқимли шифрлаш алгоритми

A5/1 шифрлаш алгоритмида дастлабки калитнинг узунлиги 64 битни ташкил этиб, у қуйидиги учта регисторга қиймат қилиб берилади:[1]

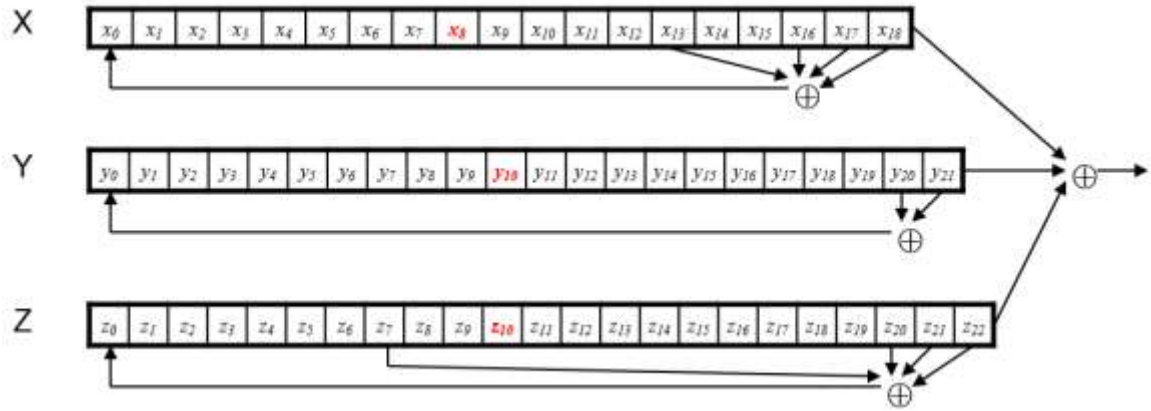
- ✓ X: 19 bit (x_0,x_1,x_2, ...,x_{18})
- ✓ Y: 22 bit (y_0,y_1,y_2, ...,y_{21})
- ✓ Z: 23 bit (z_0,z_1,z_2, ...,z_{22})

Ҳар бир қадамда: m = maj(x_8, y_{10}, z_{10}) ҳисобланади

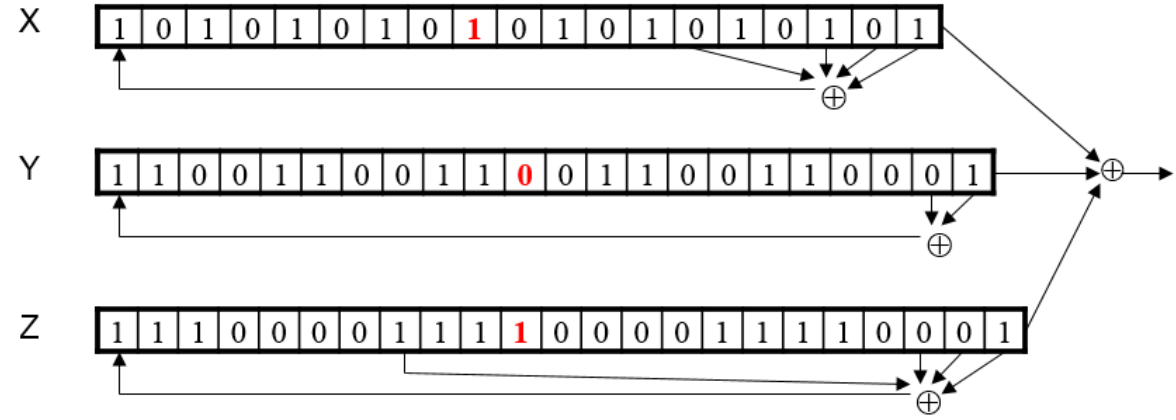
- ○ **масалан**: maj(0,1,0) = 0 ва maj(1,1,0) = 1
- ✓ агар $x_8 = m$ га тенг бўлса, у ҳолда X регистор қийматлари
- ○ $t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$
- ○ $x_i = x_{i-1}$ for i = 18,17,…,1 va $x_0 = t$
- ✓ агар $y_{10} = m$ га тенг бўлса, у ҳолда Y регистор қийматлари
- ○ $t = y_{20} \oplus y_{21}$
- ○ $y_i = y_{i-1}$ for i = 21,20,…,1 and $y_0 = t$
- ✓ агар $z_{10} = m$ га тенг бўлса, у ҳолда Z регистор қийматлари
- ○ $t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$
- ○ $z_i = z_{i-1}$ for i = 22,21,…,1 and $z_0 = t$
- ✓ **натижавий калит кетма-кетлиги** $x_{18} \oplus y_{21} \oplus z_{22}$ га тенг бўлади.

Бу амаллар қуйидаги расмда ифодаланган:

[1] Stamp Mark. Information security: principles and practice. 53 – c.



Масалан қуйидаги кўрсатилган ҳол учун:



$m = \text{maj}(x_8, y_{10}, z_{10}) = \text{maj}(\mathbf{1},\mathbf{0},\mathbf{1}) = \mathbf{1}$ га тенг бўлади. Натижада X регистор силжийди, Y регистор силжимайди ва Z регистор силжийди. Ўнг томондаги битлар XOR амал бўйича қўшилади ва $0 \oplus 1 \oplus 0 = 1$ қиймат олинади.

Ушбу усулда бир циклда бир бит калит ҳосил қилинади.

DES шифрлаш алгоритми

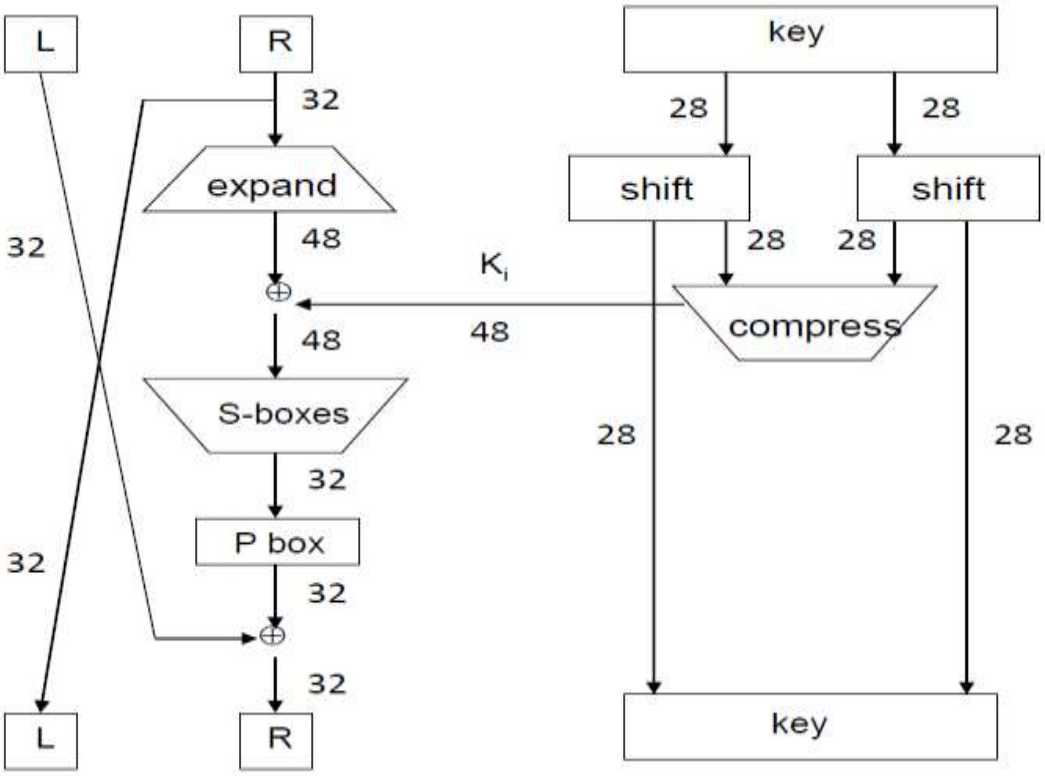
DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ) “Миллий Стандартлар Бюроси” томонидан 1977 йилда эълон қилинган. 1980 йилда АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” бу алгоритмни давлат ва савдо-сотиқ молияси соҳасидаги маҳфий бўлмаган, аммо муҳим бўлган маълумотларни руҳсат этилмаган жисмоний ва юридик шаҳслардан муҳофаза қилинишида шифрлаш алгоритми сифатида қўллаш стандарти деб қабул қилди. [1]

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.

Шифрлаш жараёни 64 битли очиқ маълумот блокларини алгоритмда берилган *IP* –жадвал бўйича ўрин алмаштириш, унинг натижасини дастлабки 56 битли калитдан алгоритмда келтирилган жадваллар билан битларнинг ўринларини алмаштириш, циклик суриш ва баъзи битларни йўқотиш акслантиришларидан

[1] Stamp Mark. Information security: principles and practice. 58 – c.

фойдаланиб ҳосил қилинадиган 48 битли раунд калитлари ҳамда асосий акслантиришлари билан 16 марта шифрлаш, шифрлаш натижаси блоки битларини берилган IP^{-1} –жадвал бўйича ўринларини алмаштиришдан иборат (2.1-расм).



2.1-расм. DES алгоритмининг 1 раунди

DES шифрлаш алгоритмида фойдаланилган муҳим хавфсизлик хусусиятларидан бири бу S – жадвалдир. Бу жадвалда кирувчи қиймат 6 битни ташкил этиб, чиқишда 4 битга ўзгаради. DES алгоритми содда криптографик ўзгартиришлардан иборат бўлиб, шифрлашда ва дешифрлашда катта тезликга эга.

DES алгоритмида фойдаланилган E кенгайтириш жадвали

- Киришда 32 бит

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

- Чиқишда 48 бит

31	0	1	2	3	4	3	4	5	6	7	8
7	8	9	10	11	12	11	12	13	14	15	16
15	16	17	18	19	20	19	20	21	22	23	24
23	24	25	26	27	28	27	28	29	30	31	0

DES да фойдаланилган S жадваллар

Кирувчи 6 бит маълумот , 101011

(0,5) (1,2,3,4)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Чиқишда, 1001

Р жадвал:

- Киришда 32 бит

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

- Чиқишда 32 бит

15	6	19	20	28	11	27	16	0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8	18	12	29	5	21	10	3	24

RSA алгоритми

1976 йилда Диффи ва Хеллман ўзларининг «Криптологияда янги йўналиш» илмий ишларида бир томонли функция сифатида $y = g^a \bmod n$ ифода билан аниқланган дискрет даражага кўтариш функциясини таклиф қилиб, $a = \log_g y \bmod n$ ифодадаги дискрет логарифмни ҳисоблашнинг амалий жиҳатдан мураккаблигига асосланган эди. 1978 йилда эса, Массачусетс технология институтининг олимлари: Р.Л. Ривест, А. Шамир, Л. Адлман, ўзларининг илмий мақоласида биринчи бўлиб маҳфий услубли ва ҳақиқатан ҳам бир томонли бўлган функцияни таклиф этдилар. Бу мақола «Рақамли имзоларни қуриш услублари ва очиқ калитли криптосистемалар» деб аталиб, кўпроқ аутентификация масалаларига қаратилган. ҳозирги кунда, бу юқорида номлари келтирилган олимлар таклиф этган функцияни, шу олимларнинг шарафига RSA бир томонли функцияси дейилади. Бу функция мураккаб бўлмай, унинг аниқланиши учун, элементар сонлар назарясидан баъзи маълумотлар керак бўлади.[1]

Мисол: Учта ҳарфдан иборат бўлган “CAB” маълумотини шифрлаймиз.

Биз қулайлик учун кичик туб сонлардан фойдаланамиз Амалда эса мумкин қадар катта туб сонлар билан иш кўрилади.

1. Туб бўлган p=3 ва q=11 сонларини танлаб оламиз.
2. Ушбу $n=pq$=3*11=33 сонини аниқлаймиз.

Сўнгра, $\varphi(33) = (p-1)(q-1) = 2 \cdot 10 = 20$ сонини топамиз, ҳамда бу сон билан 1 дан фарқли бирор умумий бўлувчига эга бўлмаган e сонини, мисол учун e=3 сонини, оламиз.

3. Юқорида келтирилган (24) шартни қаноатлантирувчи d сонини $3d$=1 (mod 20) тенгликдан топамиз. Бу сон d= 7
4. Шифрланиши керак бўлган «CAB» маълумотини ташкил этувчи

[1] Stamp Mark. Information security: principles and practice. 95 – c.

ҳарфларни: A→1, B→2, C→3 мосликлар билан сонли кўринишга ўтказиб олиб, бу маълумотни мусбат бутун сонларнинг, кетма-кетлигидан иборат деб қараймиз. У ҳолда маълумот (3,1,2)кўринишда бўлади ва уни {e;n}={3;33} очиқ калит билан $f_z(x) = x^3 (\mathrm{mod}33)$ бир томонли функция билан шифрлаймиз:

x=3 да ШМ1=(3^3)(mod33)=27,
x=1 да ШМ2=(1^3) (mod33)=1,
x=2 да ШМ3=(2^3) (mod33)=8.

5. Бу олинган шифрланган (27,1,8) маълумотни маҳфий {*d;n*}={7;33} калит билан $f_z^{-1}(y) = y^7 (\mathrm{mod}33)$ ифода орқали дешифрлаймиз:

y=9 да ОМ1=(27^7) (mod33)=3,
y=1 да ОМ2=(1^7) (mod33)=1,
y=29 да ОМ3=(8^7) (mod33)=2.

Шундай қилиб, криптотизимиларда RSA алгоритмининг қўлланиши қуйидагича: ҳар бир фойдаланувчи иккита етарли даражада катта бўлмаган *p* ва *q* туб сонларни танлайдилар ва юқорида келтирилган алгоритм бўйича *d* ва *e* туб сонларини ҳам танлаб олади. Бунда *n=pq* бўлиб, {*e;n*} очиқ калитни {*d;n*}эса маҳфий калитни ташкил этади. Очиқ калит очиқ маълумотлар китобига киритилади. Очиқ калит билан шифрланган шифрматнни шу калит билан дешифрлаш имконияти йўқ бўлиб, дешифрлашнинг маҳфий калити фақат шифр маълумотининг хақиқий эгасига маълум.

Топшириқ

1. A5/1 шифрлаш алгоритмида қуйидаги қийматлар билан 5 бит кетма – кетлик ҳосил қилинг:

$X = (x_0, x_1, ..., x_{18}) = (1010101010101010101)$
$Y = (y_0, y_1, \cdot\cdot, y_{21}) = (1100110011001100110011)$
$Z = (z_0, z_1, ..., z_{22}) = (11100001111000011110000)$

2. Цезар усулида қуйидиги шифрни очинг ва калитни аниқланг:

CSYEVIXIVQMREXIH

3. Қуйида берилган шифрматнни частоталар усули бўйича таҳлил қилинг ва очиқ матнни топинг:

GBSXUCGSZQGKGSQPKQKGLSKASPCGBGBKGUKGCEUKUZKGGBSQEI
CACGKGCEUERWKLKUPKQQGCIICUAEUVSHQKGCEUPCGBCGQOEVSHUNS
UGKUZCGQSNLSHEHIEEDCUOGEPKHZGBSNKCUGSUKUASERLSKASCUGBS
LKACRCACUZSSZEUSBEXHKRGSHWKLKUSQSKCHQTXKZHEUQBKZAENNS
UASZFENFCUOCUEKBXGBSWKLKUSQSKNFKQQKZEHGEGBSXUCGSZQGKG
SQKUZBCQAEIISKOXSZSICVSHSZGEGBSQSAHSGKHMERQGKGSKREHNKIH
SLIMGEKHSASUGKNSHCAKUNSQQKOSPBCISGBCQHSLIMQGKGSZGBKGCG
QSSNSZXQSISQQGEAEUGCUXSGBSSJCQGCUOZCLIENKGCAUSOEGCKGCEU
QCGAEUGKCUSZUEGBHSKGEHBCUGERPKHEHKHNSZKGGKAD

Назорат саволлари:

1. Ўрин алмаштириш ва ўрнига қўйиш шифрлари.
2. Модул арифметрикаси.

3. DES шифрлаш алгоритми хусусиятлари.
4. RSA алгоритми.

Адабиётлар ва интернет сайтлари:

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.

2 – амалий машғулот. Тармоқлараро экран (4 соат)

Ишнинг мақсади: Тармоқлараро экран қурилмасини ўрнатиш ва уни созлаш**.**

Масаланинг қўйилиши: Фойдаланувчи шахсий компьютерида тармоқдан бўлиши мумкин таҳдидларни олдини олиш учун шахсий тармоқлараро экран воситасини ўрнатиши ва созлаши лозим.

Ишни бажариш учун намуна

Ушбу амалий ишда шахсий тармоқлараро экранлар турига кирувчи COMODO Internet Security Firewall дастурий воситаси олиниб, уни ўрнатиш ва созлаш амалга оширилади.

Ушбу дастурий воситани ўрнатиш учун тизимдан қуйидаги ресурслар талаб этилади:

–Windows 7 (32-bit ва 64-bit версиялар) ёки Windows XP (32-bit ва 64-bit версиялар);

–Internet Explorer 5.1 ёки ундан юқори версияси;

–128 MB оператив хотира (RAM);

–210 MB қаттиқ дискдан жой.

Ушбу дастурий воситани http://www.personalfirewall.comodo.com) манзилидан олишингиз мумкин.

Дастурий воситани кўчириб олганингиздан сўнг, COMODO Internet Security 8.2.0.4508_x32 файл устида икки марта босинг. Шундан сўнг ҳосил бўлган ойнадан керакли танлов танланади.

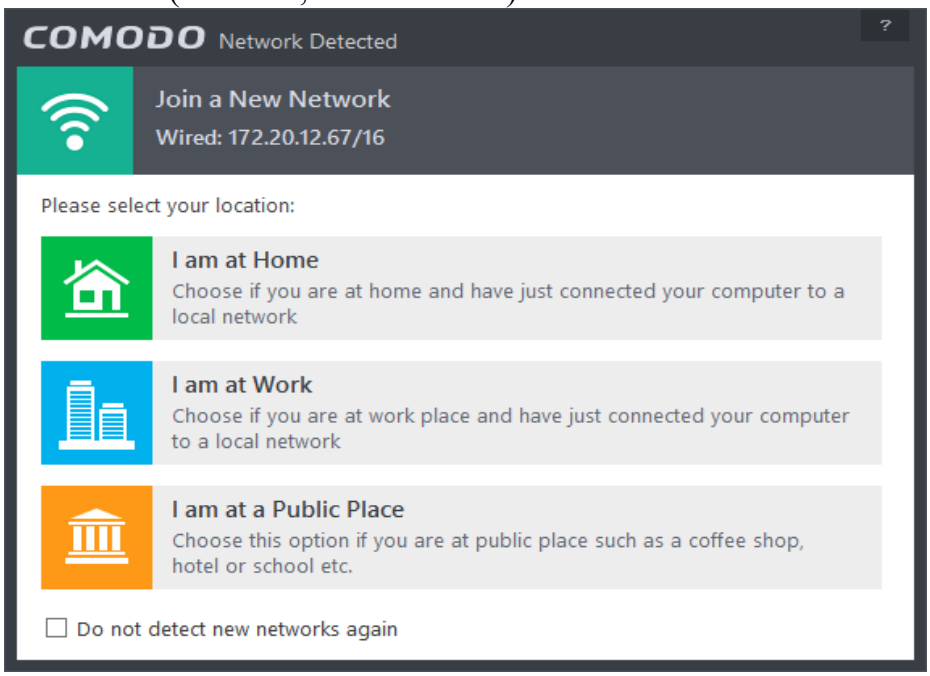
2.1 – расм. Ўрнатиш тилини танлаш

Шундан сўнг, тизим томонидан таклиф этилган келишувга ўз розилигингизни билдирасиз. Шундан сўнг дастурни ўрнатиш жараёни юкланади.

2.2 – расм. Дастур шартларини қабул қилиш

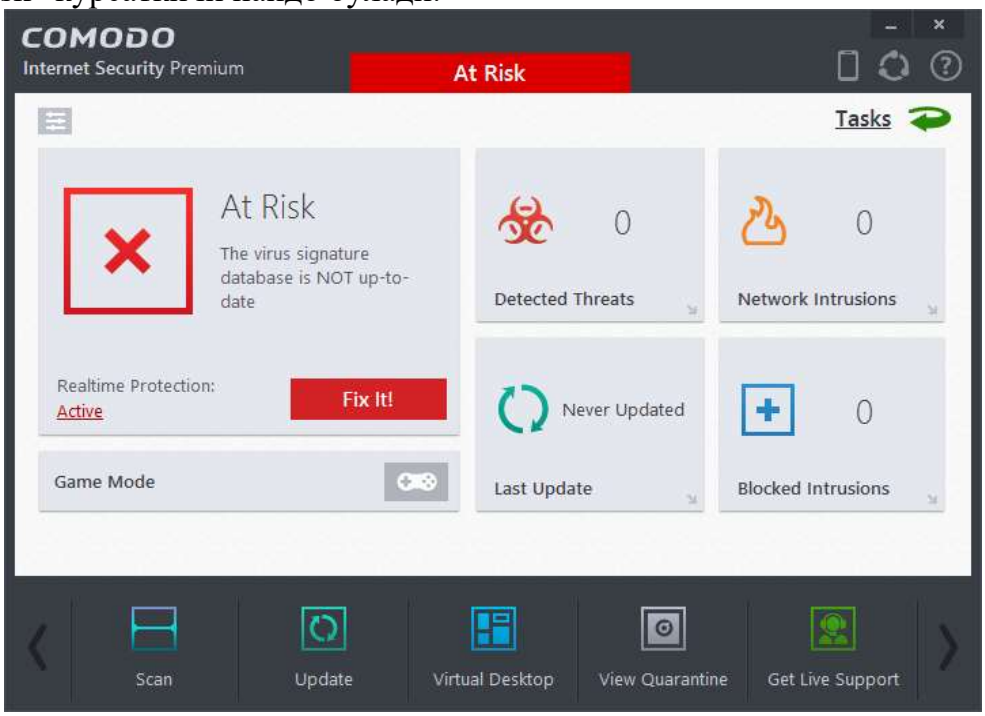
2.3 – расм. Дастурни ўрнатиш

Дастур ўрнатилгандан сўнг қуйидаги ойна ҳосил бўлади ва бу ойнадан керакли бандни танланг (масалан, I am at Home).



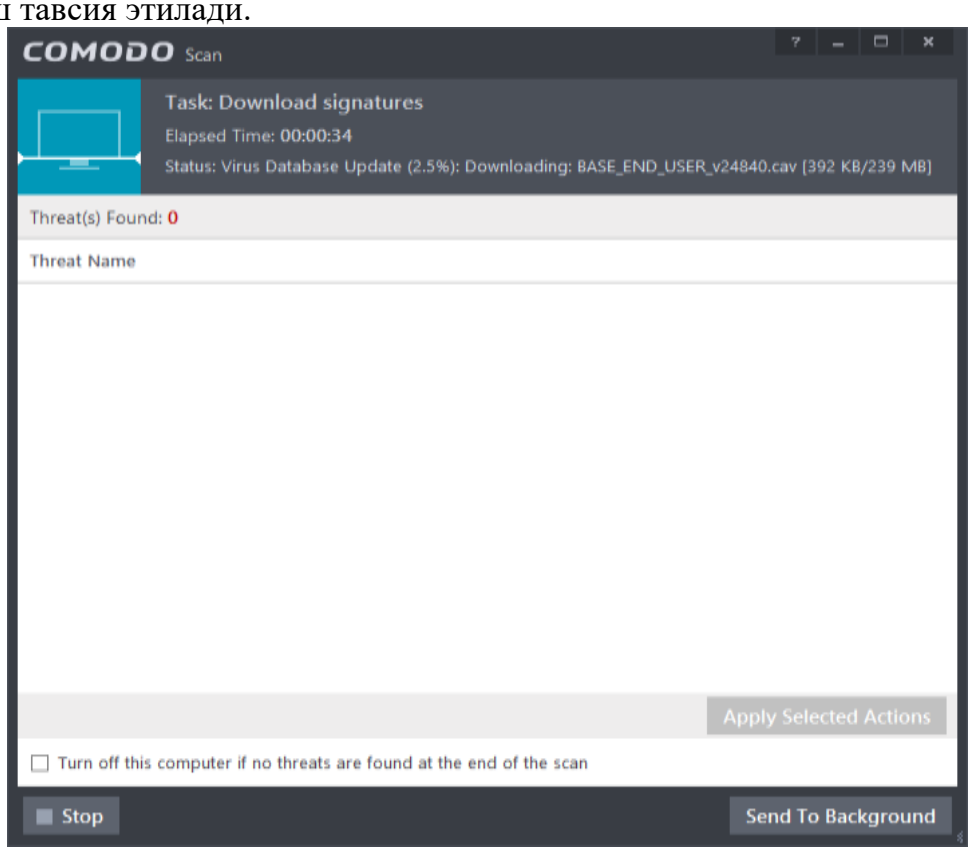
2.4 – расм. Керакли тармоқни танлаш

Шундан сўнг, дастурнинг асосий ойнаси ҳосил бўлади. Дастур янги ўрнатилгандан сўнг, интернер тармоғидан ўз базасини янгилайди. Шундан сўнг ўз ишини бошлайди. Агар дастур ўз базасини янгиламаган бўлса расмда кўрсатилгани каби “At Risk” кўрсаткичи пайдо бўлади.



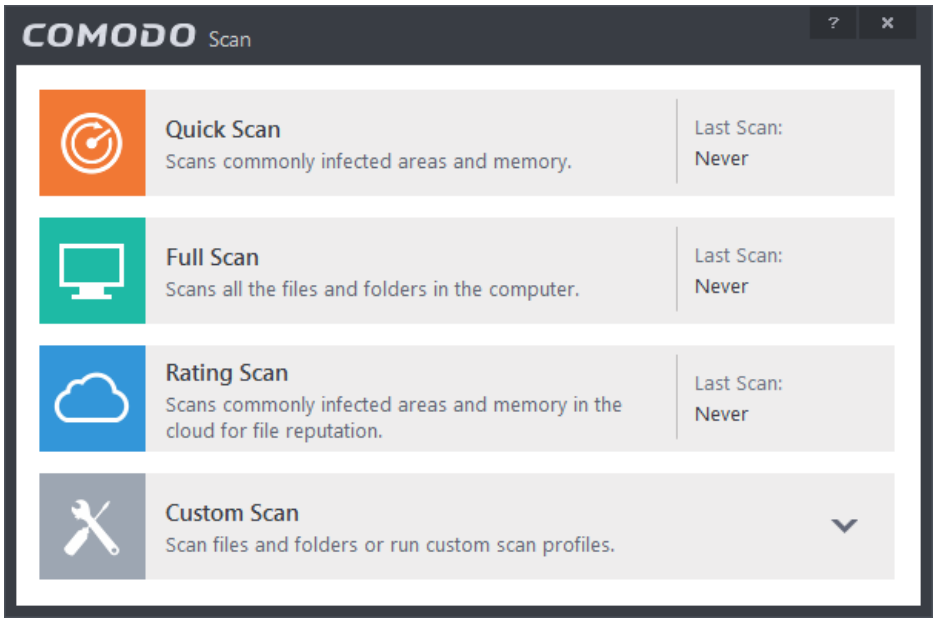
2.5 – расм. Дастурнинг асосий ойнаси

Дастурни янгилаш учун Update банди танланади ва базани юклаб олгунга қадар кутиш тавсия этилади.



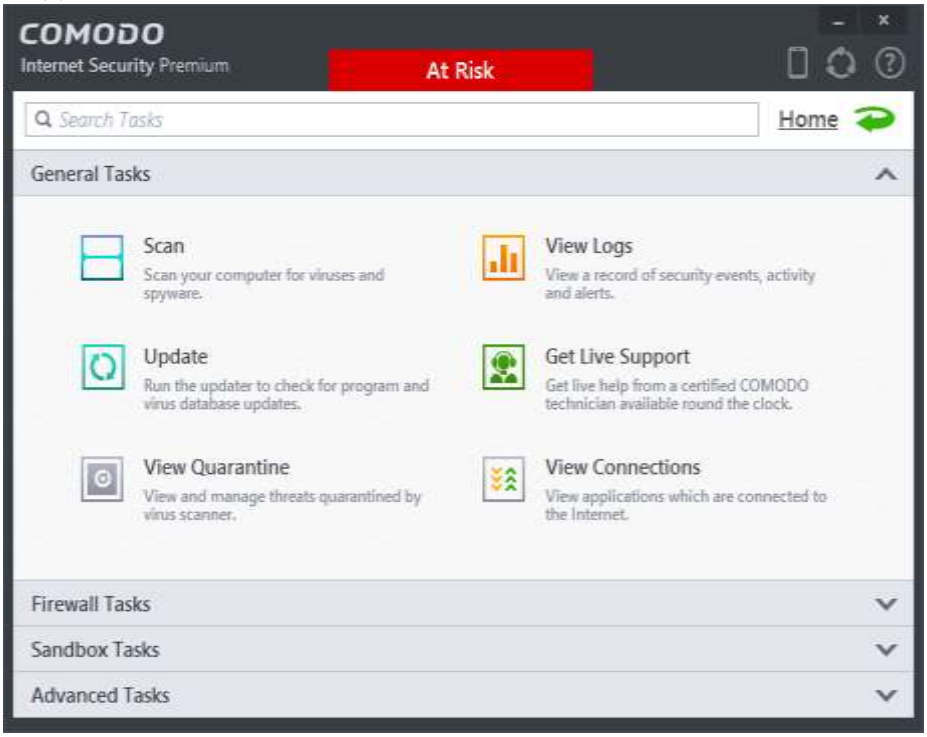
2.6 – расм. Дастурни базасини янгилаш

Тизимни текшириш учун Scan бандига ўтилади ва керакли текшириш тури танланади.



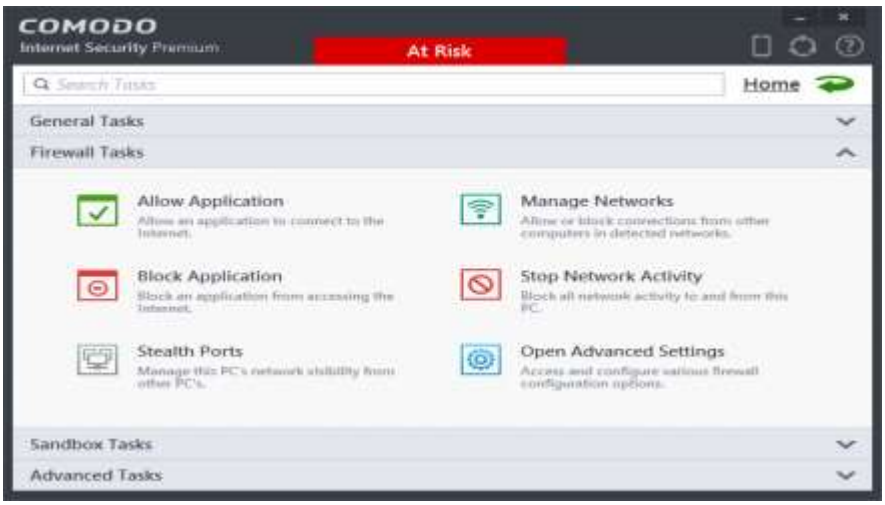
2.7 – расм. Текшириш турини танлаш

Дастурнинг асосий созланишларини амалга ошириш учун, дастурнинг асосий онасида “Tasks” банди танланади. Бу ойнада бир қанча бандлар мавжуд бўлиб, улар умумий созланишлар - “General tasks”, Тармоқлараро экран созланмалари – “Firewall Tasks”, сандбох созланмалари – “Sandbox Tasks”, кенгайтирилган созланмалар – “Advanced Tasks”. Ҳар бир бандлар ўз номига хос вазифаларни бажариб, ушбу амалий ишида тармоқлараро экранни созлаш билан яқиндан танишиб чиқилади.



2.8 – расм. Дастурнинг асосий созланишлар ойнаси

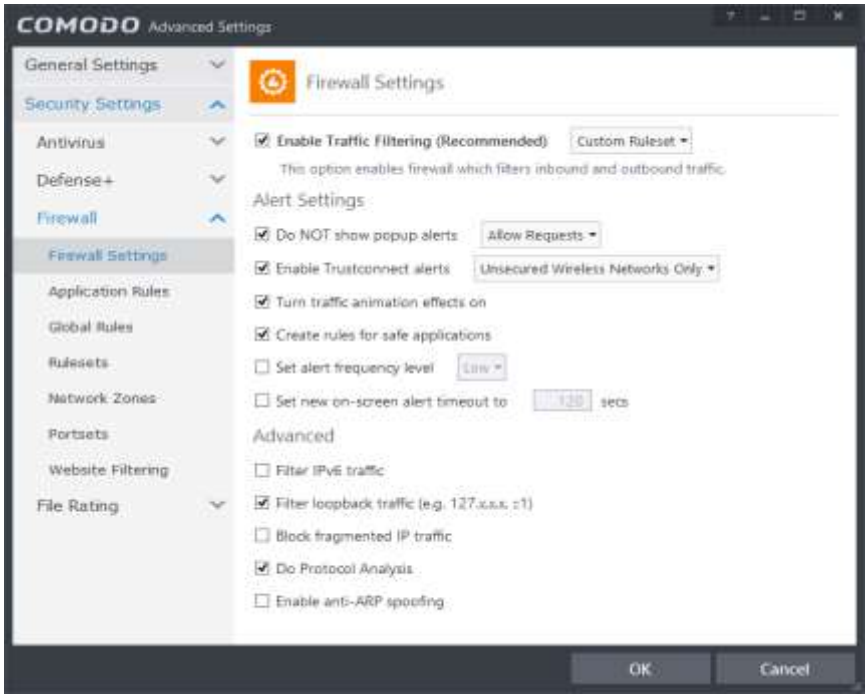
Тармоқлараро экранни бошқаришнинг ойнаси қуйидаги бандлардан иборат:



2.9 – расм. Тармоқларларо экран вазифалари

–Интернет тармоғига рухсат берилган иловалар (Allow application);
–Интернет тармоғи орқали бошқариш чекланган иловалар (Block Application);
–тармоқни бошқариш (Manage Network);
–тармоқни қулфлаб қўйиш (Stop Network Activity);
–компьютерни тармоқда бошқа компьютерларга турли кўринишда кўрсатиш (Steals Ports);
–кенгайтирилган созланишлар (Open Advanced Settings).

Ушбу саҳифада энг муҳим саналган бандлардан бири бу – кенгайтирилган бандлардир.



2.10 – расм. Тармоқлараро экран ойнаси

Ушбу ойнада тармоқлараро экранни созлашнинг кенг имкониятлари келтирилган бўлиб, бу банд орқали янги қоидаларни яратиш, қоидалар гуруҳини яратиш, иловалар учун қоидалар яратиш, веб сайтларни филтерлаш, файларни назоратлаш каби бир қатор ишларни амалга ошириш мумкин.

Топшириқ

1. Юқорида келтирилган маълумотлар асосида тармоқлараро экранни ўрнатинг ва маълумотлар базасини янгиланг.
2. Антивирус созланмаларини ўрнатинг ва анитивирус учун базани янгиланг.
3. Турли иловаларни блоклаш орқали ишламаётганига ишонч ҳосил қилинг.
4. Кенгайтирилган созланиш ойнасидан фойдаланилган ҳолда, турли қоидалар яратинг ва уларни ишлаганига ишонч ҳосил қилинг.
5. Тармоқлараро экран ишлаш вақтидаги ҳодисаларни қайд этганини Лог файлдан фойдаланиб аниқланг.
6. Барча натижаларни ҳисоботда акс эттиринг.

Назорат саволлари:

1. Тармоқлараро экранни вазифаси.
2. Шахсий тармоқлараро экран вазифаси.
3. Тармоқлараро экран турлари.
4. Тармоқлараро экранда янги қоидалар яратиш.

Адабиётлар ва интернет сайтлари:

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.

3 – амалий машғулот. Тармоқларда ахборот хавфсизлиги (4 соат)

Ишнинг мақсади: SSL ва IPSec тармоқ протоколларининг таҳлили ва улардан фойдаланиш. Симсиз тармоқ протоколларида ахборот хавфсизлигини таъминлаш.

Масаланинг қўйилиши: SSL протоколларида хавфсизлик таҳлили амалга оширилсин. Локал симсиз тармоқларда (WI-FI роутер) хавфсизлик созланмаларини амалга оширилсин.

1-қисм
Ишни бажариш учун намуна

SSL тармоқ протоколи. Transport Layer Security (TLS) дастлаб яратилган Secure Sockets Layer (SSL) протоколининг давомчиси саналиб, компьютер тармоғида алоқа хавфсизлигини таъминлаш учун яратилган ва бир нечта криптографик протоколлар ва алгоритмлардан ташкил топган. Ушбу протоколда X.509 сертификатидан фойдаланилган бўлиб, томонларни аутентификациялашда

ассиметрик шифрлаш алгоритмларидан фойдаланилади.

X.509 сертификати. Криптографияда X.509 стандарти очиқ калитли инфратузилмалар (public key infrastructure (PKI)) ва имтиёзга асосланган бошқариш инфратузилмалари (Privilege Management Infrastructure (PMI)) учун мўлжалланган.

Ушбу X.509 v3 сертификатининг тузулиши қуйидагича:

–**Certificate;**
–**Version** (версия);
–**Serial Number** (сериал рақами);
–**Algorithm ID** (алгоритм ID си);
–**Issuer** (сертификат берувчи ташкилот, эмитент);
–**Validity** (амал қилиш муддати);
–**Not Before;**
–**Not After;**
–**Subject** (сертификат олувчи ташкилот, истемолчи);
–**Subject Public Key Info** (истемолчи очиқ калит маълумоти);
–**Public Key Algorithm** (очиқ калит алгоритми);
–**Subject Public Key** (очиқ калит);
–**Issuer Unique Identifier (optional)** (эмитентнинг такрорланмас идентификатори);
–**Subject Unique Identifier (optional)** (истемолчининг такрорланмас идентификатори);
–**Extensions (optional)** (кенгайтирилган имкониятлари);
–**Certificate Signature Algorithm** (сертификатда фойдаланилган ЭРИ алгоритми);
–**Certificate Signature** (сертификат қўйилган имзо).

TLS/SSL протоколида фойдаланилган рақамли сертификатларни яратувчи, учинчи ишончли томон сифатида қатнашган ташкилотларнинг 2015 йил бошидаги кўрсаткичи қуйида кўрсатилган (3.1-жадвал):

3.1-жадвал

Рақамли сертификатларни яратувчи ташкилотлар

Ўрин	Ташкилот	Фойдаланиши	Бозордаги улуши
1.	Comodo	6.6%	33.6%
2.	Symantec Group	6.5%	33.2%
3.	Go Daddy Group	2.6%	13.2%
4.	GlobalSign	2.2%	11.3%
5.	DigiCert	0.6%	2.9%

Ҳозирда юқорида номлари келтирилган SSL/TLS протоколверсиялари амалда фойдаланилмоқда ва қуйидаги жадвалда уларнинг web саҳифаларда фойдаланиш кўрсаткичлари ва уларнинг хавфсизлик хусусияти келтирилган (3.2-жадвал).

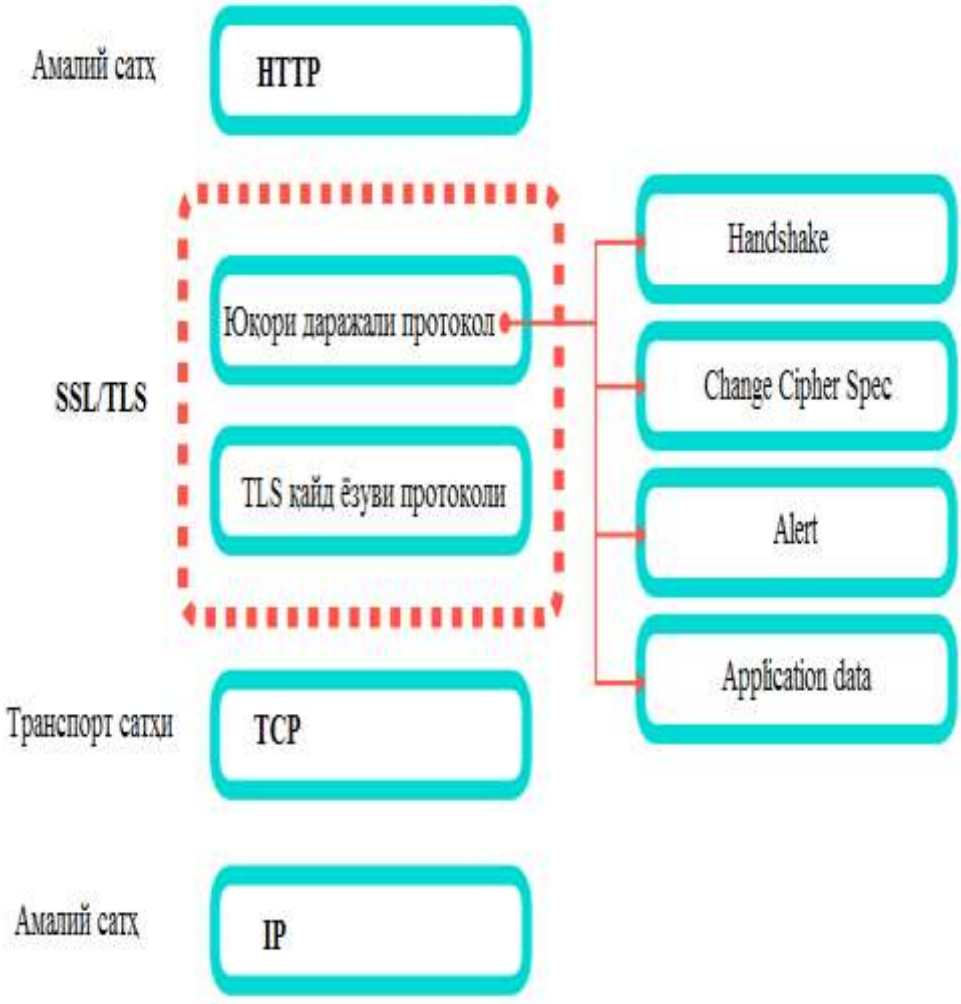
3.2-жадвал

SSL/TLS протоколларнинг хавфсизлиги таҳлили

Протокол версияси	Web саҳифаларда қўллаб қувватланиши	Хавфсизлик кўрсаткичи
SSL	14.4% (−0.5%)	Хавфсиз эмас

2.0		
SSL 3.0	47.3% (−3.1%)	Хавфсиз эмас
TLS 1.0	99.7% (±0.0%)	Алгоритм турига боғлиқ
TLS 1.1	51.5% (+1.6%)	Алгоритм турига боғлиқ
TLS 1.2	54.5% (+1.8%)	Алгоритм турига боғлиқ

Қуйидаги, 3.1-расмда SSL/TLS тармоқ протоколининг тармоқ сатҳларида жойлашуви келтирилган.



3.1-расм. SSL/TLS протоколи

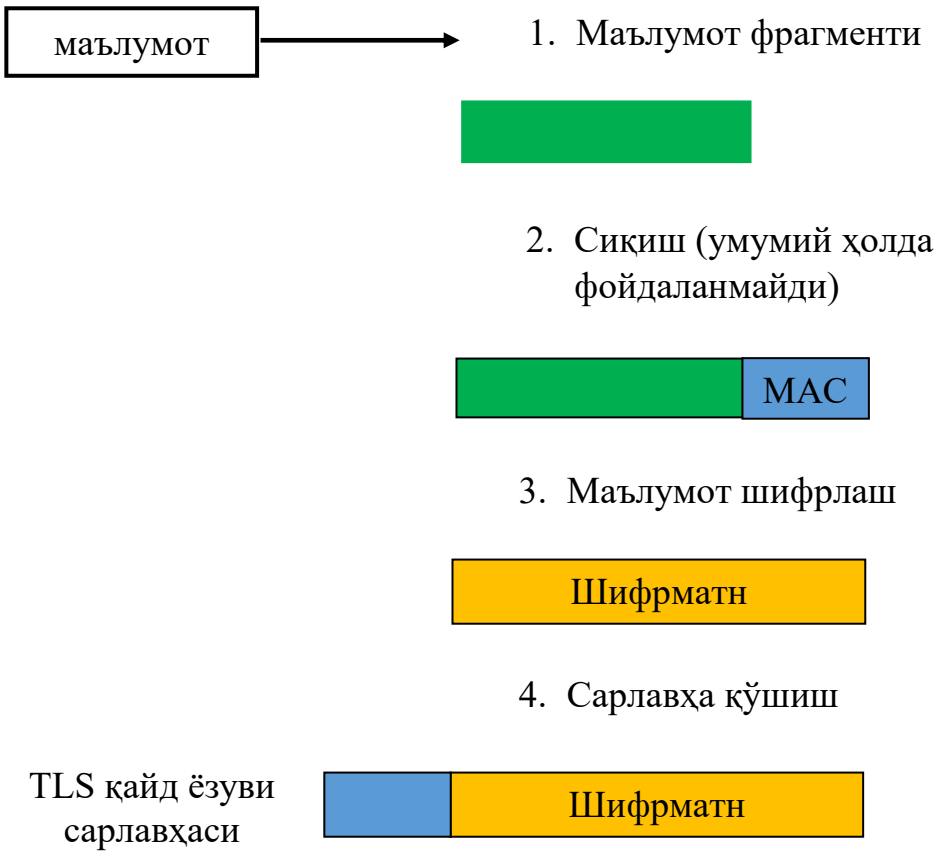
SSL/TLS сатҳининг қуйи ташкил этувчи протоколи (TLS қайд ёзуви протоколи), дастлабки маълумотни фрагментларга ажратиш, созланишга кўра фрагмент маълумотни сиқиш, сиқилган маълумотга унинг MAC қийматини қўшиш, ҳосил бўлган маълумот жуфтини шифрлаш алгоритми ёрдамида шифрлаш ва унга TLS қайд ёзуви сарлавҳасини қўшиш амалларидан ҳосил бўлади (4.2-расм).

*Юқори даражали протокол.*Ушбу протокол TLS қайд ёзуви протоколи

устида жойлаштирилган бўлиб, у тўртта протоколдан иборат. Ҳар бир протокол ўзининг махсус вазифасига эга бўлиб, улар алоҳида ёки биргаликда ҳам фойдаланилиши мумкин.

*Handshake протоколи.*Ушбу протокол ҳар икки томонда бир-бирини аутентификациялаш, фойдаланиладиган криптографик алгоритмларни келишиш ва бошқа боғланиш параметларини алмашиш имконини беради. Ушбу протокол клиент ва сервер орасида алмашинувчи тўртта хабарлар мажмуасидан иборат. Ҳар бир хабарлар мажмуаси алоҳида пакет бўлиб юборилади.

*ChangeCipherSpec Protocol:*ушбу протокол асосида алоқа канали ҳимояланади.



3.2-расм. TLS/SSL қайд ёзуви протоколи

*Alert Protocol:*ушбу хабар бериш протоколи, барча протокол натижаларини эълон қилишда фойдаланилади.

*Application Data Protocol:*ушбу протокол илова сатҳидан маълумотни олиб, уни махфий канал орқали юборишни таъминлайди.

TLS қайд ёзуви формати. Ушбу формат учта майдондан иборат бўлиб, унинг асосида юқори даражали протокол қурилади (3.6-жадвал).

–Byte 0:TLS қайд ёзуви тури.

–Bytes 1-2:TLS протокол версияси (major/minor).

–Bytes 3-4: қайд ёзувидаги маълумот узунлиги (ўзидан ташқари). Максимал қиймати 16384 бит ёки 16 Кбит.

3.3-жадвал

TLS қайд ёзуви формати

TLS қайд ёзуви тури	Версияси		Маълумот узунлиги		юқори даражали протокол
	major	minor	(bits 15..8)	(bits 7..0)	

TLS қайд ёзуви тури қуйидаги 3.4-жадвалда кенлтирилган

3.4-жадвал

Hex	**Dec**	**Тури**
0x14	20	ChangeCipherSpec
0x15	21	Alert
0x16	22	Handshake
0x17	23	Application
0x18	24	Heartbeat

Протокол версияси эса 3.5-жадвалда келтирилиб ўтилган.

3.5-жадвал

Hex	**Dec**	**Протокол версияси**
0x0300	3,0	SSL 3.0
0x0301	3,1	TLS 1.0
0x0302	3,2	TLS 1.1
0x0303	3,3	TLS 1.2

*Handshake протокол формати.*Ушбу протокол TLS протоколида асосий протоколларда бири саналиб, бу протокол орқали хавфсизлик параметрлари узатилади. Ушбу протокол орқали ўнбир турдаги хабар узатилаши мумкин (3.6-жадвал).

3.6-жадвал

Handshake протокол формати

Byte +0	Byte +1	Byte +2	Byte +3
22			
Версия		Узунлик	
Минор	Мажор	(bits 15..8)	(bits 7..0)
Хабар тури	Handshake маълумоти узунлиги		
	(bits 23..16)	(bits 15..8)	(bits 7..0)
Handshake маълумоти			

*Handshake маълумоти узунлиги.*Ушбу майдон узунлиги 3 байт бўлиб, фақат Handshake маълумоти узунлигини билдиради, сарлавҳани ўз ичига олмаган ҳолда. Битта TLS ёзишмасида бир нечта Handshake маълумоти бўлиши мумкин. Handshake протоколида хабар тури қуйидагича бўлиши мумкин (3.7-жадвал).

3.7-жадвал

Handshake протоколида хабар тури

Хабар тури		
Dec	**Hex**	**Тасниф**

0	0x00	HelloRequest
1	0x01	ClientHello
2	0x02	ServerHello
4	0x04	NewSessionTicke
11	0x0b	Certificate
12	0x0c	ServerKeyExchange
13	0x0d	CertificateRequest
14	0x0e	ServerHelloDone
15	0x0f	CertificateVerify
16	0x10	ClientKeyExchange
20	0x14	Finished

*ChangeCipherSpec протокол формати.*Ушбу протокол битта хабардан иборат бўлиб, пакетнинг шифрланганлигини билдиради. TLS протоколи бутун TLS қайд ёзуви маълумотини инкапсуциялайди.

*Alert протоколи.*Handshaking ва application туридаги протокол ўз ишини нормал ҳолатда тугатмаган ҳолда Alert протоколи орқали хабар берилади. Шунга қарамасдан, ушбу хабар ҳар бир турлаги протокол билан биргаликда юборилади. Агар ушбу хабар маълумоти “fatal error” бўлса, у ҳолда сессия зудлик билан ёпилади. Агар хабар маълумоти “warning” бўлса, у ҳолда масофадаги фойдаланувчи талабига кўра сессияни тугатиш ёки тугатмаслик танланади.

Byte +0	Byte +1	Byte +2	Byte +3
21			
Версияси		Узунлиги	
Мажор	Минор	0	2
Даража	Тасниф		

3.3-расм. Alert протоколи формати

*Даража.*Ушбу майдон Alert ни даражасини кўрсатади. Юқорида айтиб ўтилганидек, икки турдаги Alert мавжуд (3.8-жадвал).

3.8-жадвал

Коди	**Даража тури**	**Боғланиш ҳолати**
1	**warning**	Боғланиш ёки хавфсизлик ўзгарувчан бўлиши мумкин.
2	**fatal**	Боғланиш ёки хавфсизлик хавфли бўлиши мумкин, тиклиб бўлмас хатолик юз берган.

Агар жараён нормал ҳолатда ўз ишини тугатган тақдирда ҳам, бирор бир

даража тури қайтарилади. Жараённинг қандай тугаганлиги эса тасниф асосида аниқланади. Қуйида тасниф жадвали келтирилган (3.9-жадвал).

3.9-жадвал

Жараён таснифи

Коди	**Тасниф**	**Даража**	**Коди**	**Тасниф**	**Даража**
0	Close notify	warning/ fatal	49	Access denied	fatal
10	Unexpected message	fatal	50	Decode error	fatal
20	Bad record MAC	fatal	51	Decrypt error	warning /fatal
21	Decryption failed	fatal	60	Export restriction	fatal
22	Record overflow	fatal	70	Protocol version	Fatal
30	Decompression failure	fatal	71	Insufficient security	Fatal
40	Handshake failure	fatal	80	Internal error	Fatal
41	No certificate	warning/ fatal	90	User canceled	fatal
42	Bad certificate	warning/ fatal	100	No renegotiation	warning
43	Unsupported certificate	warning/ fatal	110	Unsupported extension	warning
44	Certificate revoked	warning/ fatal	111	Certificate unobtainable	warning
45	Certificate expired	warning/ fatal	112	Unrecognized name	warning /fatal
46	Certificate unknown	warning/ fatal	113	Bad certificate status response	Fatal
47	Illegal parameter	fatal	114	Bad certificate hash value	Fatal
48	Unknown CA (Certificate authority)	fatal	115	Unknown PSK identity (used in TLS-PSK and TLS-SRP)	Fatal

ApplicationData протоколи. Ушбу протокол маълумотни шифрлаб жўнатувчи протокол саналиб, маълумот ва унинг MAC қиймати биргаликда шифрланиб юборилади (3.4-расм).

Byte +0	Byte +1	Byte +2	Byte +3
23			
Версияси		Узунлиги	
Мажор	Минор	16 кб гача	
Маълумот			MAC қиймати

3.4-расм. ApplicationData протоколи

Назорат саволлари:

1. X.509 сертификати.
2. SSL протоколи тарихи.
3. SSL протоколида хавфсизлик усуллари.
4. SSL протоколида ўртага турган одам таҳдиди.

2-қисм
Ишни бажариш учун намуна

Симсиз тармоқлар одамларга симли уланишсиз ўзаро боғланишларига имкон беради. Бу силжиш эркинлигини ва уй, шахар қисмларидаги ёки дунёнинг олис бурчакларидаги иловалардан фойдаланиш имконини таъминлайди. Симсиз тармоқлар одамларга ўзларига қулай ва хохлаган жойларида электрон почтани олишларига ёки Web-сахифаларни кўздан кечиришларига имкон беради.

Симсиз тармоқларнинг турли хиллари мавжуд, аммо уларнинг энг мухим хусусияти боғланишнинг компьютер қурилмалари орасида амалга оширилишидир. Компьютер қурилмаларига шахсий рақамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахсий компьютерлар, серверлар ва принтерлар тааллуқли. Одатда уяли телефонларни компьютер қурилмалари қаторига киритишмайди, аммо энг янги телефонлар ва хатто наушниклар маълум хисоблаш имкониятларига ва тармоқ адаптерларига эга. Яқин орада электрон қурилмаларнинг аксарияти симсиз тармоқларга уланиш имкониятини таъминлайди.

Боғланиш таъминланадиган физик худуд ўлчамларига боғлиқ холда симсиз тармоқларнинг қуйидаги категориялари фарқланади:

–симсиз шахсий тармоқ (Wireless personal-area network, PAN);
–симсиз локал тармоқ (Wireless local-area network, LAN);
–симсиз регионал тармоқ (Wireless metropolitan-area network, MAN):
–симсиз глобал тармоқ (Wireless Wide-area network, WAN).

3.9-жадвал

Симсиз тармоқ усуллари

Тармоқ тури	Таъсир доираси	Амалда фойдала нилиши	Мавжуд стандартлар	Қўлланиш соҳаси
Шахсий симсиз тармоқлар	Фойдаланувчидан бевосита яқинликда	Ўртача	Bluetooth,IEEE 802.15,IRDA	Ташқи қурилмалар кабеллари нинг ўрнида
Локал симсиз	Бинолар ёки офислар орасида	Юқори	IEEE 802.11, Wi-Fi ва	Симли тармоқларни

тармоқлар			HiperLAN	мобил кенгайти риш
Регионал симсиз тармоқлар	Шаҳарлар орасида	Юқори	IEEE 802.16, ва WIMAX	Бинолар ва корхоналар ва Internet орасида белгиланган симсиз боғланиш
Глобал симсиз тармоқлар	Бутун дунё бўйича	Паст	CDPD, 2G, 2.5G, 3G, 4G	Бутун дунё бўйича интернетдан фойдаланишда

WI-FI технологиясида фойдаланилган криптографик протоколлар

Симсиз локал тармоқларда фойдланилган WI-FIтехнологиясида қуйидаги криптографик протоколлардан фойдаланилган:

–Wired Equivalent Privacy (WEP);

–Wi-Fi Protected Access (WPA) ва унинг иккинчи варианти.

Wired Equivalent Privacy (WEP) хавфсизлик алгоритми IEEE 802.11 симсиз тармоқлари учун фойдаланилиб, IEEE 802.11 стандарти 1999 йил сентябр ойидақабуд қилинган бўлиб, симсиз тармоқларда (wireless LAN) маълумотни бутунлигини, аутентификация ва тўлиқлигини таъминлашда фойдаланилади.

Ушбу протоколдп 10 ёки 26 та ўн олтилик тизимдаги калитдан фойдаланилади, ва бу калит дастлаб роутерни созлашда фойдалинилган парол билан бир хил бўлади.

Ушбу протоколда қуйидаги хавфсизлик амалиётларидан фойдаланилган:

–Аутентификациялаш;

–Маълумотни бутунлигини таъминлаш;

–Маълумот махфийлагини таъминлаш.

*WEP да аутентификациялаш.*Ушбу протоколда икки турдаги аутентификациялашдан фойдаланилади.

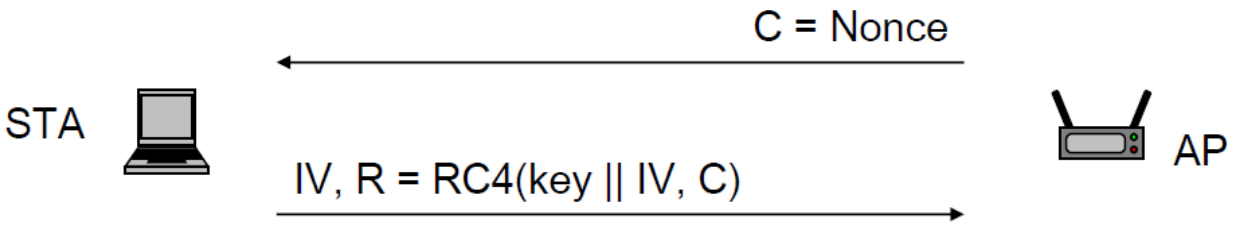
–Open System authentication;

–Shared Key authentication.

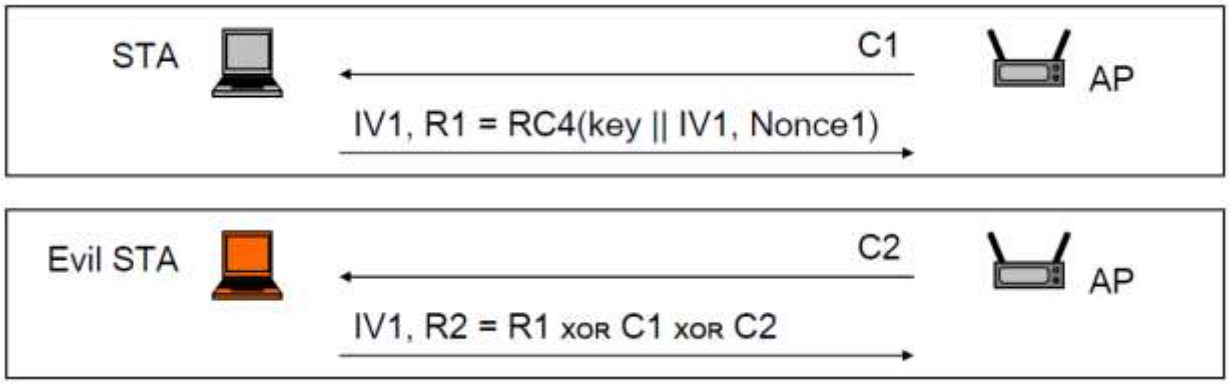
Биринчи усулда аутентификациялаш амалга оширилмай ихтиёрий фойдаланувчи серверга боғланиши мумкин. Маълумот WEP калити асосида шифрланади. Фойдаланувчи серверга боғланаши учун клиент тўғри калитга эга бўлиши керак.

Shared Key асосида аутентификациялаш усули 3.5 - расмда келтирилган бўлиб, 3.5 – расмда ушбу аутентификацияни синдириш усули келтирилган.[1]

[1] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures.



5.1 – расм. Shared Key аутентификациялаш усули



3.5 – расм. Shared Key аутентификация усулини синдириш

R2=R1 XOR C1 XOR C2 = (keystream(key || IV1) XOR C1) XOR C1 XOR C2 = keystream(key || IV1) XOR (C1 XOR C1) XOR C2 = keystream(key || IV1) XOR C2 = қониқарли жавоб.

*Маълумот махфийлагини таъминлаш***.**WEP протоколи икки хил узунликдаги калитлардан фойдаланганлиги сабабли, улар мос ҳолда WEP-40 WEP-104 деб аталади. WEP-40вариантида 40 битли (10 та ўн олтилик белги) калитдан фойдаланиб, 24 битли бошланғич вектордан (IV) фойдаланилади. WEP-104вариантида 104 битли (26 та ўн олтилик белги) калитдан фойдаланиб, 24 битли бошланғич вектордан фойдаланилади. Шифрлаш RC4 алгоритми асосида амалга оширилади (3.6-расм).

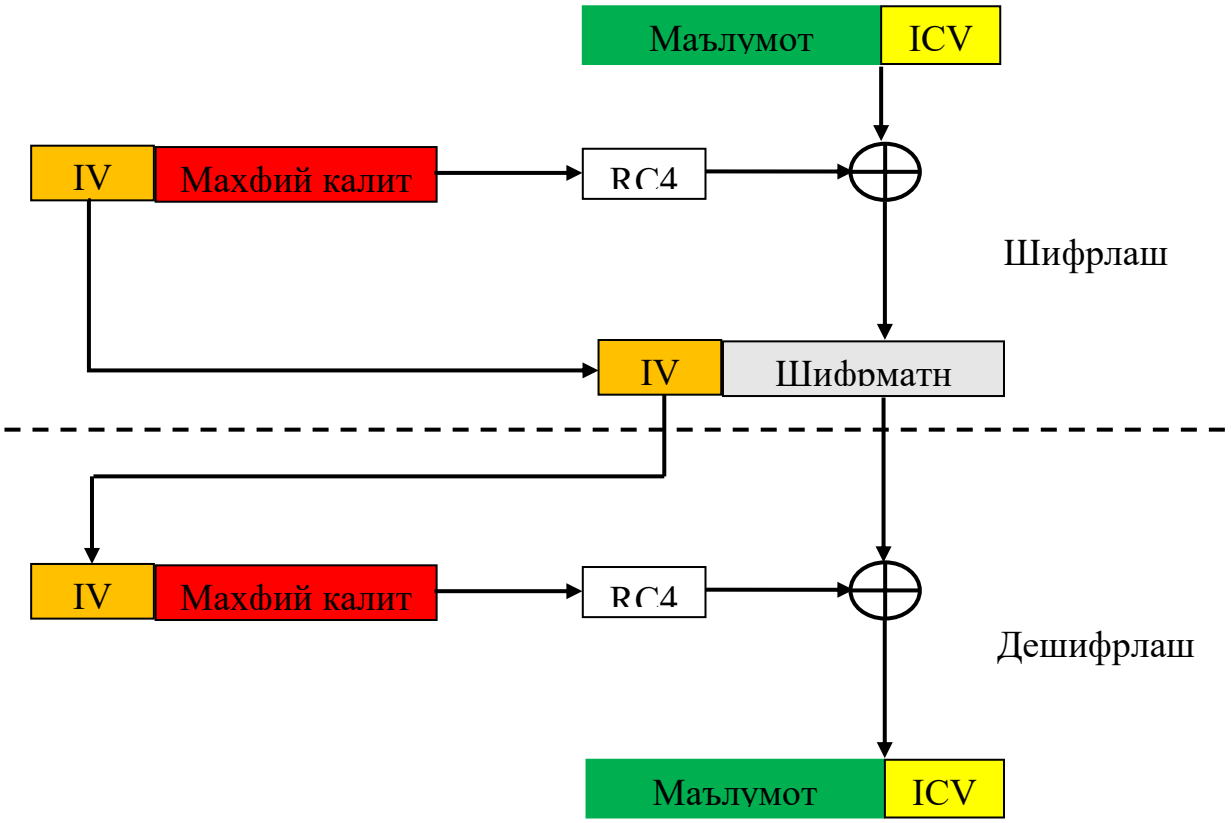
Иккинчи усулда WEP протоколида аутентификациялаш учун оддий савол-жавоб тизимидан фойдаланилган. Жараён кетма-кетлиги қуйидагича:

1. Клиент серверга (бошқарув нуқтасига) аутентификациялаш сўровини юборади.
2. Сервер фойдаланувчига тасодифий сонни юборади(r, 128 битдан катта бўлган) .
3. Фойдаланувчи ушбу сонни умумий калит (бошқарув нуқтаси пароли) билан шифрлаб юборади ($e_K(r)$).
4. Шифрматнни очиш натижасига қараб, аутентификациялашдан ўтилади ёки йўқ.

*Маълумотни бутунлигини таъминлаш.*WEP протоколида маълумот бутунлигини таъминлашда CRC-32 функциясидан фойдаланилади.

WEP протокол заифликлари. Ушбу протокол амалда фойдалниш даражаси пасайишига қуйидаги заифликлари орқали келиб чиққан ҳужумлар сабабчи бўлган.[1]

[1] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures.



3.6-расм. WEP протоколида шифрлаш

Бу ерда: IV – бошланғич вектор, ICV – маълумотнинг CRC қиймати.

1. Сервер (бошқарув нуқтасига) фойдаланувчини аутентификацияламайди.
2. Шифрлашда ва аутентификациялашда битта калитдан фойдаланилади.
3. Аутентификациялаш давомида сессия калитидан фойдаланилмайди.
4. Протокол хабарни такрорлаш ҳужумидан ҳимояланмаган.
5. Фойдаланилган IVқайта фойдаланилади ва қиймати жуду ҳам кичик:
6. 24 бит узунлик, 16.777.216 мумкин бўлган калитлар.
7. Қарийиб 17 миллион хабардан сўнг IVтакрорланади.
8. Аган тизим 11 Mbps тезликдан фойдаланса, секундига 700 та пакет юборади ва бир IV қиймати қарийиб 7 соат учун етарли бўлади.
9. Одатда барча қурилмаларда IVнолдан бошланади.
10. Баъзи заиф калитлардан фойдаланиш орқали RC4 тасодифий саналмаган калитларни ишлаб чиқаради.
11. Юқоридаги сабабга кўра, амалда RC4 орқали ҳосил қилинган калитнинг дастлабки 256 байти олинмайди. Аммо WEP бундай эмас.

Юқорида келтирилган сабабларга кўра, амалда WEP протоколидан фойдаланиш тавсия этилмайди.

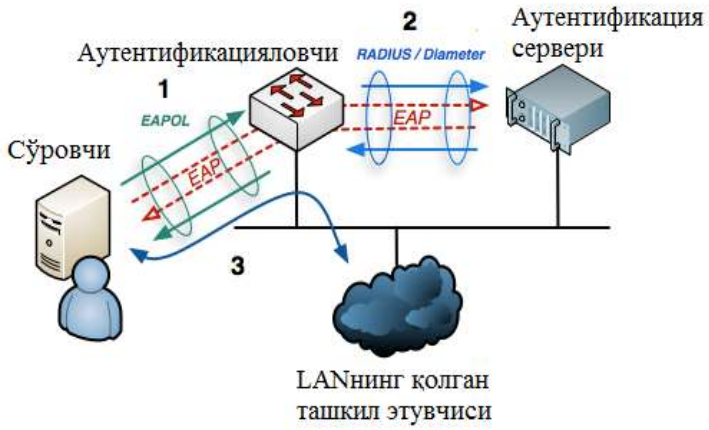
WPA протоколи. 2003 йилда Wi-Fi AllianceWEP протоколи Wi-Fi Protected Access (WPA) билан алмаштирлганин элъон қилди. 2004 йилда WPA ва WPA2 протоколини ўз ичига олган 802.11i стандарти ишлаб чиқилди. Ушбу ишлаб чиқилган протоколлар WEP протоколига қараганда хавфсиздир. Қурилмалар ушбу протоколлардан фойдаланиш учун уларни аппарат томондан янгилаш шарт.

WPA протоколи WEP протоколида мавжуд заифликларни бартараф этиш учун ишлаб чиқилган бўлиб, унда Temporal Key Integrity Protocol (TKIP) протоколидан

фойдаланилади. WEP протоколида 40 битли ёки 104 битли калитлардан фойдаланилган бўлса, WPA протоколида ҳар бир пакет учун алоҳида ҳосил қилинган калитлардан фойдаланилади. WEP протоколи заиф деб топилгандан сўнг, вақтинчалик қурилмаларни янгилашга қадар фойдаланиш учун бардошли протокол керак эди. TKIPпротоколи WEPпротоколи асосида қурилган бўлиб, WEP протоколи қурилмалари учун мосдир.

Маълумотни бутунлигини таъминлаш алгоритмлари сифатида фойдаланилган CRC тизимлари ўрнига эса “Michael” деб номланувчи маълумотни бутунлигини текширувчи алгоритмдан фойдаланилган. MAC тизимлари юқоридаги икки тизимларга қараганда бардошли саналсада, қурилмалардан юқори имкониятларни талаб этади. “Michael” тизими MAC қараганда тезкор ва CRC мавжуд камчиликларни ўзида бартараф этган.

Аутентификациялаш. WPAпротоколида 802.1X аутентификациялаш моделидан фойдаланилади.



3.7-расм. 802.1X аутентификациялаш модели

*Маълумот махфийлиги.*TKIP протоколида шифрлаш алгоритми сифатида RC4 оқимли шифрлаш алгоритмидан фойдаланилган. TKIP протоколида фойдаланилган калитлар мажмуаси қуйидагилар.

WPA проктоколида фойдаланилган калитлар

1.	Фойдаланувчи аутентификацияланади.
2.	Аутентификация сервери “Masterkey” ни ҳосил қилади.
3.	“Master key” билан “Key Encryption Keys”лар шифрланади.
4.	“Key Encryption Keys” билан “Temporal key”шифрланади.
5.	“Temporal key” фойдаланувчи маълумотини шифрлашда ишлатилади.

“Temporal key” калитлар тўплами икки калитдан, улар 128-битли шифрлаш калити ва 64-битли Michael функцияси калитидан иборат.

Маълумотни шифрлашда RC4 оқимли шифрлаш алгоритмидан фойдаланилган бўлиб, WEP протоколидан фарқли равишда ҳар бир пакет учун алоҳида такрорланмас калитлардан фойдаланади.

WPA2 протоколи IEEE 802.11i-2004 ёки 802.11i стандартида асосида ишлаб чиқилган ва WEP, WPA (TKIP) протоколидан тамоман фарқ қилади. Ушбу

протокол ишлаши учун янгидан ишлаб чиқилган қурилма асосида ишлайди. Ушбу протоколнинг тўлиқ номи CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) деб номалиниб, унда блокли шифрлаш алгоритми саналган AES-128 шифрлаш алгоритмидан фойдаланилади.

Ушбу протоколнинг TKIP протоколидан асосий фарқи, 48-битли PN (Packet Number) майдони фойдаланилган бўлиб, унинг асосий мақсади ҳар бир пакет учун алоҳида ҳисобланиб, пакетни қайта юбориш ҳужумига қарши фойдаланилади.

WI-FI симсиз алоқа тармоқлари усуллари таҳлили

Хусусият	**Статик WEP**	**Динамик WEP**	**WPA**	**WPA 2**
Идентификациялаш	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер
Аутентификациялаш	Умумий калит	EAP	EAP ёки умумий калит	EAP ёки умумий калит
Бутунлик	CRC-32	CRC-32	64-битли MIC	CBC режими асосида MIC
Махфийлик	Статик калит	Сессия калити	TKIP асосида калит	CCMP (AES)
Калитларни тақсимлаш	Бир томонлама	Pair-wise Master Key (PMK)	PMK	PMK
Бошланғич вектор	24-бит	24-бит	56-бит	48-бит (PN)
Алгоритм	RC4	RC4	RC4	AES
Калит узунлиги	64/128	64/128	128	128, 192, 256
Талаб этиладиган структура	Йўқ	RADIUS	RADIUS	RADIUS

Назорат саволлари:

1. Симсиз тармоқ турлари.
2. WEP протоколи ва унда мавжуд заифликлар.
3. WI – FI стандартида хавфсизлик созланмаларини ўрнатиш.
4. WEP протоколида фойдаланилган криптографик алгоритмлар.

Адабиётлар ва интернет сайтлари:

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.

3. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures. School of Multimedia, Hannam University, Daejeon, Korea. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

4. http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

V БЎЛИМ

КЕЙСЛАР БАНКИ

V. КЕЙСЛАР БАНКИ

1 – кейс

1. Цезар шифрлаш усули ёрдамида шифрланган қуйидагига тенг. Унга тегишли бўлган очиқ матнни ва калитни аниқланг ? (Фақат инглиз алифбосидан, /A....Z/ фойдаланилган)
    a. VSRQJHEREVTXDUHSDQWU
    b. CSYEVIXIVQMREXIH
2. DES шифрлаш алгоритми билан танишинг ва қуйидагиларга жавоб беринг:
    a. Очиқ матн блокининг узунлиги;
    b. Шифрматн блокининг узунлиги;
    c. Калит узунлиги;
    d. Раунд калит узунлиги;
    e. Раундлар сони;
    f. S жадваллар сони;
    g. S жадвалда кирувчи ва чиқувчи маълумот узунлиги;
3. ECB ва CBC шифрлаш режимларининг афзалликлари ва камчиликларини мисоллар билан исботланг.
4. Фараз қилинг блокли шифрлаш усули қуйидаги қоида бўйича шифрлашни амалга оширади: C_0 = IV XOR E(P_0, K), C_1 = C_0 XOR E(P_1, K), C_2 = C_1 XOR E(P_2, K), ...
    a. Унга мос бўлган дешифрлаш қоидасини ёзинг;
    b. Бу режимни CBC режим билан таққослаганда афзаллик ва камчиликларни айтинг.
5. Электрон рақамли имзо учун қуйидагиларни исботланг:
    a. Қандай қилиб ва нима учун электрон рақамли имзо хабарни юборишдан тонмасликни таъминлайди ?
    b. Қандай қилиб ва нима учун электрон рақамли имзо хабар бутунлигини таъминлайди ?

2 – кейс.

1. SSL ва IPSec протоколлари тармоқда хавфсизликни таъминлаш учун фойдаланилади.
    a. SSL протоколни IPsec протоколга қараганда афзалликларини кўрсатинг.
    b. IPsec протоколни SSL протоколга қараганда афзалликларини кўрсатинг.
    c. SSL ва IPSec протоколлари орасидаги фарқни ва ўхшашликни аниқланг.
2. 4 – маърузада келтирилган SSH нинг соддалиштирилган протоколига қаранг.
    a. Қаерда ва қандай қилиб Алиса аутентификациядан ўтмоқда. Нима такрорлаш таҳдидидан ҳимояламоқда.
    b. Агар Триди пассив ҳужумчи бўлса (фақат маълумотни кузата олади), К калитни ҳисоблай олмайди. Нима учун ?
    c. Агар Триди актив ҳужумчи бўлса (хабар ҳам юбора олади), у К калитни ҳисоблай олади. Нима учун бу калит билан протоколни буза олмайди ?
    d. Охирги хабарни К калит билаг шифрлашдан мақсад нима?

3. Фараз қилинг WEP протоколи қуйидагича ўзгартирилди. Ҳар бир пакетни шифрлашда К калитдан фойдаланилади. К калит аутентификацияда фойдаланилган калит билан бир хил.
    a. Бу яхши фикрми ёки йўқ. Асосланг.
    b. Бу усул WEP да фойдаланилган K_{IV}=(IV, K) усулга қараганда бардошлими ёки йўқ.

4. Wireshark ёки ихтиёрий тармоқ снифферидан фойдаланиб, SSL тармоқни тутиб олинг ва уни таҳлил этинг.
5. IPSec протоколининг AH ва ESP режимлари орасидаги фарқни тушунтиринг.

VII БЎЛИМ

ГЛОССАРИЙ

VII. ГЛОССАРИЙ

Тушунча ўзбек тилида	Тушунчанинг таърифи	Тушунча инглиз тилида
Компьютер тизими	ахборотни ўлчаш, унинг шаклини ўзгартириш ва ишлаш учун мўлжалланган, функционал жиҳатидан бирлаштирилган ҳамда истъемолчига, яъни фойдаланувчига у талаб қиладиган кўринишда ахборотни (маълумотни) тақдим этадиган тизим	Computer system
Компьютер тармоғи	алоқа каналлари ёрдамида маълумотларни тармоқланган ягона тизимига уланган компьютерлар ва терминаллар тўплами	Computer network
PAN	шахсий тармоқ, компьютер қурилмаларининг симсиз тармоғи.	PERSONAL-AREA NETWORK
LAN	локал тармоқ, чегараланган соҳадаги компьютерларни бирлаштириш имкониятини беради.	LOCAL-AREA NETWORK
CAN	кампус тармоқ, ўзаро яқин биноларда жойлашган локал тармоқларни бирлаштириш учун мўлжалланган.	CAMPUS-AREA NETWORK
MAN	шаҳар каби катталикдаги географик минтақани қамраб олган алоқа тармоғи..	METROPOLITAN AREA NETWORK
WAN	давлат каби йирик географик ҳудудни ўз ичига олади.	WIDE AREA NETWORK
GAN	барча давлатлар ва континентларни бирлаштирувчи ҳамда ер шарининг ихтиёрий нуқтасидаги ахборот ресурсларига мурожаат қилиш имкониятини берувчи умумпланетар тармоқ.	Global-Area Network
OSI модели	бошқа тизимлар билан алоқа қилиш учун очиқ бўлган тизимларни бирлаштиради; еттита босқичга бўлинган	Open System Interconnection
Амалий босқич	иловалар босқичи	Application level
Презентация босқичи	ахборотни таништириш босқичи, бу босқичда ахборотни аниқланади ва ахборот форматини кўриниш	Presentation level

	синтаксисини тармоққа қулай равишда ўзгартиради, яъни таржимон вазифасини бажаради	
Алоқани ўтказиш босқичи	алоқани ўрнатади, тасдиқлайди ва тамомлайди	Session level
Транспортли босқичи	пакетларни хатосиз ва йўқотмасдан, керакли кетма-кетликда етказиб беришни амалга оширади	Transport level
Тармоқли босқичи	пакетларни манзиллаш, мантиқий номларни жисмоний тармоқ манзилига ўзгартириш, тескарига ҳам ва шунингдек, пакетни керакли абонентга жўнатиш йўналишини танлашга жавобгар	Network level
Каналли босқичи	узатиш йўлини бошқариш босқичи, стандарт кўринишдаги пакет тузишга бошлаш ҳамда тамом бўлишни бошқариш майдонини пакет таркибига жойлашишига жавобгардир	Canal level
Жисмоний босқич	узатилаётган ахборотни сигнал катталигига кодлаштиради, узатиш муҳитига қабул қилишни ва тескари кодлашни амалга оширишга жавоб беради	Physical level
TCP	тармоқдаги ахборот узатувини назорат қилиб турувчи протокол; катта ҳажмдаги ахборотларнинг жўнатиш муаммоларини хал қилади.	Transmission Control Protocol
TCP/IP	Интернет тизимида фойдаланиладиган протоколлар.	TCP/IP
IP	IP баённомада тармоқдаги ҳар бир компьютерга тўрт хоналик IP-манзил (4 байт) мос қўйилади.	Internet Protocol
Мультимедиали тармоқ	тармоқни, реал вақтда ва мураккаб уланиш конфигуратсиясини қўллаган ҳолда, кўп компонентли ахборот (овоз, мазкур видео, аудио)ларни шу компонентлар учун зарур бўлган синхронизация билан узатиш қобилияти билан изоҳланади	Multimedia network
Мултимедиали шлюз	хар хил турдаги тармоқларни бирлашиш учун мултимедиа ва бошқариш ахборотларни	Gateway

	ўзгартириш учун мўлжалланган қурилмаси	
Маршрутизатор	тармоқ пакетларини маршрутлаш билан шуғулланадиган компьютер тармоғи, яъни пакетларнинг тармоқ бўйлаб энг қисқа ҳаракат маршрутлари танлаб берилади.	Router
CGI	стандарт интерфейс бўлиб, у Web–сервер билан берилган маълумотлар ва маҳсуслашган интернет–иловалари ўртасида ахборот алмашинувини амалга оширишга имкон яратади.	Common Gateway Interfac)
NOC	Интернет тармоқлари орасида пайдо бўладиган турли хил муаммоларни хал қилувчи Интернет ҳар бир тармоғини хусусий эксплуатасион маркази.	NOC
NSFNET	IP –технологиясида ташкил қилинган миллий – илмий фонднинг хусусий тармоғи.	NSFNET
Жўнатувчи порт	майдон дейтаграмма узатган ишчи станциянинг портини кўрсатади.	Source Port
Қабул қилувчи порт	майдон пакет етказиладиган ишчи станция портини идентификациялайди.	Destination Port
UDP	фойдаланувчи дейтаграммалари протоколи	User Datagram Protocol
UDP протоколи	иловаларга мантиқий уланиш ўрнатмасдан ишончсиз маълумотлар узатиш хизматини тақдим этади	UDP
TCP протоколи	мантиқий уланиш ўрнатиб, ишончли маълумотлар узатиш хизматини тақдим этади	TCP
UDP ва TCP ларнинг асосий вазифаси	тармоқ сатхи протоколи (IP) тақдим этадиган, охирги тизимлар орасида маълумотлар алмаштириш хизмати ёрдамида, охирги тизимларда бажариладиган, жараёнлар орасида маълумотлар алмашинишини таъминлайди.	The main function of UDP and TCP
SMTP	Email нинг амалий сатх протоколи	SMTP
HTTP	WWW нинг амалий сатх протоколи	HTTP
FTP	File transfer нинг амалий сатх протоколи	FTP
NFS	Remote File server нинг амалий сатх	NFS

	протоколи	
H.323	IP telefoniya нинг амалий сатх протоколи	H.323
SIP	IMO, Skype нинг амалий сатх протоколи	SIP
TCP	Email, WWW нинг транспорт сатхи протоколи	TCP
UDP	IP telefoniya, IMO, Skype нинг транспорт сатхи протоколи	UDP
Ақлли тармоқ	маълумотларни узатишдан ташқари мураккаб ахборот хизматларининг ранг-баранг турларини тақдим қилувчи коммуникация тармоғи	smart network
SMART	1965 йилда ***Паул Ж Меер***, сўнгра 1981 йили ***Георге Т. Доран*** ўз илмий ишларида қўллаганлар.	SMART
SMART	“Specific” (ўзига хос), “Measurable” (ўлчаб бўладиган), “Attainable” (эришиб бўладиган), “Relevant” (долзарб), “Time-bound” (аниқ муддатли) инглизча сўзларининг бош ҳарфлари билан ифодаланган.	SMART
IoT	буюмлар интернети, махсус қабул қилувчи ва узатувчи қурилмаларнинг ўзаро маълумот алмашинувидан иборат тармоқ тизими билан жиҳозланган сунъий интелект ёрдамида масофадан бошқарилувчи ахборот тизимлар	Internet of things
LPWAN	базавий станция билан доимий алоқада бўлиб туриш учун қимматли ампер-соатларни сарфламайдиган, кичикроқ ҳажмдаги маълумотларни узоқ масофаларга узата оладиган олис радиусда таъсир кучига эга энергиядан самарали фойдаланадиган тармоқ	Low-power Wide-area Network
LoRaWAN	катта радиусли кенг полосали тармоқлар деб таржима қилиниб, OSI нинг канал даражасидаги MAC протоколи ҳисобланади	Long Range Wide-Area Networks
Идентификация	шахсни кимдир деб даво килиш жараёни	Identification
Аутентификация	фойдаланувчини (ёки бирор томонни) тизимдан фойдаланиш учун рухсати мавжудлигини аникдаш	Authentication

	жараёни	
Авторизация	идентификация, аутентификация жараёнларидан ўтган фойдаланувчи учун тизимда бажариши мумкин бўлган амалларга рухсат бериш жараёни	authorization
Ахборотнинг ҳимояси	бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёни	Information protection
Кодлаштириш	ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёни	Coding
Калит	матнни шифрлаш ва шифрини очиш учун керакли ахборот.	The key
Криптоанализ	калитни билмасдан шифрланган матнни очиш имкониятларини ўрганади.	Cryptanalysis
Симметрик шифр	маълумотни шифрлаш ва дешифрлаш учун бир хил калитдан фойдаланилади	Symmetric cipher
Ассимметрик шифр	шифрлаш ва дешифрлаш учун иккита калитдан фойдаланилади	Asymmetric cipher
стеганографиянинг асосий ғояси	махфий маълумотларнинг мавжудлиги ҳақидаги шубҳани олдини олиш	the basic idea of steganography
Хэш функция	ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ёки байт бирликларида) қийматга ўтказувчи функция	Hash function
Пароль	факат фойдаланувчига маълум ва бирор тизимда аутентификация жараёнидан утишни таъминловчи бирор ахборот	password
Ipsec	хавфсизлик протоколлари ҳамда шифрлаш алгоритмларидан фойдаланган ҳолда тармоқ орқали хавфсиз маълумот алмашиш имконини беради	Internet protocol security
VPN	виртуал хусусий тармоқ,	Virtual Private

	фойдаланувчилар ўртасида барча маълумотларни алмашиш бошқа тармоқ доирасида ички тармоқни шакллантиришга асосланган, ишончли ҳимояни таъминлашга қаратилган.	Network
Тармоқ сканерлари	масофавий ёки локал ташхис дастури бўлиб, у тармоқнинг турли элементларида ҳар хил заифликларни аниқлайди	Network scanners
Илова сканерлари	аниқ МББТ, Web-браузерлари ва бошқа амалий тизимларга мўлжалланган	Application scanners
Тармоқ вируслари	ўзини тарқатишда компъютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади.	Network viruses
Тармоқ ҳужуми	Компьютер тармоқлари орқали ташкилотнинг тизимига рухсатсиз таъсир кўрсатиш	Network attack
Ҳужум	заифлик орқали ахборот тизимлари хавфсизлигини бузишга оширилган ҳаракат	Attack
Заифлик	тизим хавфсизлигини бузувчи ва ошкор бўлмаган ҳодисаларга олиб келувчи камчилик, лойиҳалашдаги ёки амалга оширишдаги хатолик.	Weakness
web-ҳужумлар	web технологиялар орқали ташкилотнинг тизимига рухсатсиз таъсир кўрсатиш	web attacks
вируслар	ўзини ўзи кўпайтирадиган программа бўлиб, ўзини бошқа программа ичига, компьютернинг юкланувчи секторига ёки ҳужжат ичига бириктиради.	viruses
Тармоқ хавфсизлиги	ахборот тармоғини рухсатсиз фойдаланишдан, меъёрий ишлашига тасодифан ёки атайин аралашишдан ёки тармоқ компонентларини бузишга уринишдан эхтиёт қилувчи чоралар	Network Security
Компьютер тизими хавфсизлиги	деструктив ҳаракатларга ва ёлғон ахборотни зўрлаб қабул қилинишига олиб келувчи ишланадиган ва сақланувчи ахборотдан рухсатсиз фойдаланишга уринишларга компьютер тизимининг қарши тура	Security of computer systems

	олиш ҳусусияти	
Kerio Control	ахборот хавфсизлигини таъминловчи комплекс ечимдир. У тармоқлараро экран (Firewall), маршрутизатор, ҳужум олдини олиш тизими (IPS), антивирус ва бошқа функцияларни ташкил топган.	Kerio Control
Брандмауер	Тармоқлараро тўсиқ, «Firewall» атамасининг синоними (немис тилидан «оловли девор» деб таржима қилинади).	Brandmauer
Ахборотнинг ҳимояси	бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёни	Information protection
киберхавфсизлик	қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқариш	cybersecurity
Киберхавфсизли (Cisco ташкилоти таърифи)	тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти	Cybersecurity (Cisco definition)
Маълумотлар хавфсизлиги	маълумотларни сақлашда, қайта ишлашда ва узатишда ҳимояни таъминлашни мақсад қилади	Data security
Дастурий таъминотлар хавфсизлиги	фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи дастурий таъминотларни ишлаб чиқиш ва фойдаланиш жараёнига эътибор қаратади	Software security
Ташкил этувчилар хавфсизлиги	катта тизимларда интеграллашган ташкил этувчиларни лойиҳалаш, сотиб олиш, тестлаш, анализ қилиш ва техник хизмат кўрсатишга эътибор қаратади	Organizer security
Алоқа хавфсизлиги	ташкил этувчилар ўртасидаги алоқани ҳимоялашга этибор қаратиб, ўзида физик ва мантиқий уланишни бирлаштиради.	Communication security
Тизим хавфсизлиги	ташкил этувчилар, уланишлар ва дастурий таъминотдан иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади	System security

Инсон хавфсизлиги	киберхавфсизлик билан боғлиқ инсон ҳатти ҳаракатларини ўрганишдан ташқари, ташкилотлар (масалан, ходим) ва шахсий ҳаёт шароитида шахсий маълумотларни ва шахсий ҳаётни ҳимоя қилишга эътибор қаратади	Human security
Ташкилот хавфсизлиги	ташкилотни киберхавфсизлик таҳдидларидан ҳимоялаш ва ташкилот вазифасини муваффаққиятли бажаришини мададлаш учун рискларни бошқаришга эътибор қаратади	Organizational security
Жамоат хавфсизлиги	у ёки бу даражада жамиятда таъсир кўрсатувчи киберхавфсизлик омилларига эътибор қаратади	Public safety
Киберхавфсизлик концепцияси	ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари	The concept of cybersecurity
Киберхавфсизлик сиёсати	ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режаси	Cybersecurity policy
Риск	ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради	Risk
Рискни аниқлаш тадбирлари	Рискларни аниқлаш; рискларни идентификация қилиш; рискларни таҳлил қилиш; рискларни баҳолаш.	Risk detection measures
Рискларни аниқлаш	ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг	Risk identification

	идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди	
Рискларни идентификация қилишдан мақсад	потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади.	The purpose of risk identification
Ҳодиса	шахс ёки ишчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир	event
Нормал ҳодиса	критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.	Normal event
Ҳодисаларни кенгайиши ва кўпайиши (Эскалация)	Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.	Expansion and multiplication of events (Escalation)
Авариявий ҳодиса	шахс хавфсизлиги ва соғлигига таъсир кўрсатади.	An accident.
Инцидент	стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.	Incident
Хавфсизлик инциденти координатори	инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир.	Security Incident Coordinator
Инцидентни тергов қилиш	инцидент ҳолатини тергов қилиш ҳаракати	Investigate the incident
Инцидентга жавоб қайтариш	хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир	Responding to an incident
Инцидент бошқарувчисини	– муносиб ваколатлардан фойдаланиш учун ҳар қандай авария /	Duties and responsibilities of

вазифалари ва мажбуриятлари	носозликларни билиш; – етарли ахборот йиғиш ва тизимни таҳлил этиш учун қайта тиклайдиган командани шакллантириш; – инцидентни умумий ҳолатини сақлаш; – функционал имкониятларни билиш (Core Network); – командани юқори сатҳга кўтариш (приоритет бериш) учун қўлланмадан фойдаланиш.	the incident manager
ахборот хавфсизлиги инцидентларни бошқариш жараёни	• компьютер инциденти ҳақида ахборот олиш; • қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш; • ҳолатни таҳлил этиш; • сабабларни аниқлаш; • профилактик тадбирлар ўтказиш	information security incident management process
Инцидентларини бошқариш жараёни самарадорлиги	❑ ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши; ❑ инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги; ❑ олинган натижаларнинг ҳақиқийлиги.	The effectiveness of the incident management process
Криптографик алгоритм	– криптографик функцияларнинг бирини ҳисоблашни амалга оширувчи алгоритм	Cryptographic algorithm
Криптографик ҳимоя	- маълумотларни криптографик ўзгартириш ёрдамида ҳимоялаш.	Cryptographic protection
Криптография	–ахборот мазмунини ниқоблаш, унинг ушлаб қолиниши ва бузилиши имкониятини бартараф этиш, ахборотни рухсатсиз фойдаланишдан ҳимоялаш мақсадида маълумотларни ўзгартириш принципларини, усулларини ва воситаларини бирлаштирувчи билим соҳаси.	Cryptography
PAP	серверга уловчи пароллар системаси.	Password authentication protocol
POP	протокол «почтали офис». Хост ва	Post Office

	абонент ўртасида почта алмашуви учун ишлатилади. Абонент талаби бўйича ҳам алмашув ишлари бажарилади.	Protocol
Шифрлаш алгоритми	- шифрлаш функциясини амалга оширувчи криптографик алгоритм, блокли шифртизим ҳолида шифрлашнинг муайян режимида шифрлашнинг базавий блокли алгоритмидан фойдаланиб ҳосил қилинади.	Encryption algorithm
Шифрматн	очиқ матнни шифрлаш натижасидаги олинган матн.	Ciphertext
Alert Protocol	ушбу хабар бериш протоколи, барча протокол натижаларини эълон қилишда фойдаланилади.	*Alert Protocol*
Application Data Protocol	ушбу протокол илова сатҳидан маълумотни олиб, уни махфий канал орқали юборишни таъминлайди.	*Application Data Protocol*
TLS қайд ёзуви формати	ушбу формат учта майдондан иборат бўлиб, унинг асосида юқори даражали протокол қурилади	*TLS қайд ёзуви формати*
Тармоқлараро экран	аппарат-дастурий воситалар ёрдамида тармоқдан фойдаланишни марказлаштириш ва уни назоратлаш йўли билан тармоқни бошқа тизимлардан ва тармоқлардан келадиган хавфсизликка тахдидлардан ҳимоялаш усули	Firewall
SSL	компьютер тармоғида алоқа хавфсизлигини таъминлаш учун яратилган ва бир нечта криптографик протоколлар ва алгоритмлардан ташкил топган	Secure Sockets Layer
X.509	Криптографияда ушбу стандарти очиқ калитли инфратузилмалар (public key infrastructure (PKI)) ва имтиёзга асосланган бошқариш инфратузилмалари (Privilege Management Infrastructure (PMI)) учун мўлжалланган	*X.509*
Handshake протокол формати	Ушбу протокол TLS протоколида асосий протоколларда бири саналиб, бу протокол орқали хавфсизлик параметрлари узатилади	Handshake protocol format
Handshake	3 байт бўлиб, фақат Handshake	Handshake token

маълумоти узунлиги	маълумоти узунлигини билдиради, сарлавҳани ўз ичига олмаган ҳолда	length
ChangeCipherSpec протокол формати	Ушбу протокол битта хабардан иборат бўлиб, пакетнинг шифрланганлигини билдиради, TLS протоколи бутун TLS қайд ёзуви маълумотини инкапсуциялайди.	ChangeCipherSpec protocol format
Alert протоколи	Handshaking ва application туридаги протокол ўз ишини нормал ҳолатда тугатмаган ҳолда Alert протоколи орқали хабар берилади.	Alert protocol
ApplicationData протоколи	Ушбу протокол маълумотни шифрлаб жўнатувчи протокол саналиб, маълумот ва унинг MAC қиймати биргаликда шифрланиб юборилади	ApplicationData protocol

VIII БЎЛИМ

АДАБИЁТЛАР РЎЙХАТИ

VIII. АДАБИЁТЛАР РЎЙХАТИ

АДАБИЁТЛАР РЎЙХАТИ

I. Ўзбекистон Республикаси Президентининг асарлари

1. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. – Т.: “Ўзбекистон”, 2017. – 488 б.

2. Мирзиёев Ш.М. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. 1-жилд. – Т.: “Ўзбекистон”, 2017. – 592 б.

3. Мирзиёев Ш.М. Халқимизнинг розилиги бизнинг фаолиятимизга берилган энг олий баҳодир. 2-жилд. Т.: “Ўзбекистон”, 2018. – 507 б.

4. Мирзиёев Ш.М. Нияти улуғ халқнинг иши ҳам улуғ, ҳаёти ёруғ ва келажаги фаровон бўлади. 3-жилд.– Т.: “Ўзбекистон”, 2019. – 400 б.

5. Мирзиёев Ш.М. Миллий тикланишдан – миллий юксалиш сари. 4-жилд.– Т.: “Ўзбекистон”, 2020. – 400 б.

II. Норматив-ҳуқуқий ҳужжатлар

6. Ўзбекистон Республикасининг Конституцияси. – Т.: Ўзбекистон, 2018.

7. Ўзбекистон Республикасининг 2020 йил 23 сентябрда қабул қилинган “Таълим тўғрисида”ги ЎРҚ-637-сонли Қонуни.

8. Ўзбекистон Республикаси Президентининг 2015 йил 12 июнь “Олий таълим муасасаларининг раҳбар ва педагог кадрларини қайта тайёрлаш ва малакасини ошириш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-4732-сонли Фармони.

9. Ўзбекистон Республикаси Президентининг 2017 йил 7 февраль “Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида”ги 4947-сонли Фармони.

10. Ўзбекистон Республикаси Президентининг 2017 йил 20 апрель "Олий таълим тизимини янада ривожлантириш чора-тадбирлари тўғрисида”ги ПҚ-2909-сонли Қарори.

11. Ўзбекистон Республикаси Президентининг 2018 йил 21 сентябрь “2019-2021 йилларда Ўзбекистон Республикасини инновацион ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПФ-5544-сонли Фармони.

12. Ўзбекистон Республикаси Президентининг 2018 йил 19 февраль “Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-5349-сонли Фармони.

13. Ўзбекистон Республикаси Президентининг 2019 йил 27 май “Ўзбекистон Республикасида коррупцияга қарши курашиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-5729-сон Фармони.

14. Ўзбекистон Республикаси Президентининг 2019 йил 17 июнь “2019-2023 йилларда Мирзо Улуғбек номидаги Ўзбекистон Миллий университетида талаб юқори бўлган малакали кадрлар тайёрлаш тизимини тубдан такомиллаштириш ва илмий салоҳиятини ривожлантири чора-тадбирлари тўғрисида”ги ПҚ-4358-сонли Қарори.

15. Ўзбекистон Республикаси Президентининг 2019 йил 27 август “Олий

таълим муассасалари раҳбар ва педагог кадрларининг узлуксиз малакасини ошириш тизимини жорий этиш тўғрисида”ги ПФ-5789-сонли Фармони.

16. Ўзбекистон Республикаси Президентининг 2019 йил 8 октябрь “Ўзбекистон Республикаси олий таълим тизимини 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-5847-сонли Фармони.

17. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2019 йил 23 сентябрь “Олий таълим муассасалари раҳбар ва педагог кадрларининг малакасини ошириш тизимини янада такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги 797-сонли Қарори.

18. Ўзбекистон Республикаси Президентининг 2019 йил 21 май “«Электрон ҳукумат» тизими доирасида ахборот-коммуникация технологиялари соҳасидаги лойиҳаларни ишлаб чиқиш ва амалга ошириш сифатини яхшилаш чора-тадбирлари тўғрисида”ги ПҚ-4328-сонли Қарори.

19. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг 2020 йил 25 январдаги Олий Мажлисга Мурожаатномаси.

20. Ўзбекистон Республикаси Президентининг 2020 йил 29 октябрь “Илм-фанни 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-6097-сонли Фармони.

21. Ўзбекистон Республикаси Президентининг 2020 йил 5 октябрь “Рақамли Ўзбекистон-2030” Стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида”ги ПФ-6079-сонли Фармони.

Ш. Махсус адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.
4. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.
5. Ахмедова О.П., Хасанов Х.П., Назарова М.Ҳ., Нуритдинов О.Д.. Криптографик протоколлар. Тошкент, 2012 – 187 бет.
6. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures. School of Multimedia, Hannam University, Daejeon, Korea. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.
7. Michael Sikorski, Andrew Honig. Practical malware analysis. 2012.

IV. Интернет сайтлар

1. http:// www.mitc.uz - Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги
2. http://lex.uz – Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси
3. http://lib.bimm.uz – Олий таълим тизими педагог ва раҳбар кадрларини қайта тайёрлаш ва уларнинг малакасини оширишни ташкил этиш бош илмий-

методик маркази
4. http://ziyonet.uz – Таълим портали ZiyoNET
5. http://natlib.uz – Алишер Навоий номидаги Ўзбекистон Миллий кутубхонаси
6. http:// www.tuit.uz - Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети
7. https://iot.ru/
8. https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria
9. https://en.wikipedia.org/wiki/Common_Criteria
10. https://technet.microsoft.com/en-us/library/dd277395.aspx
11. http://ictnews.uz/api/news/78

РЕЦЕНЗИЯ

на учебно-методический комплекс, составленный доц. Ш.Гуломовым по модулю «Безопасность компьютерных сетей» для курсов повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Компьютерный инжиниринг»

Учебно-методический комплекс по модулю «Безопасность компьютерных сетей» составлен для курсов повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Компьютерный инжиниринг» и содержит в себе программу курсов, рекомендованные педагогические технологии, тексты лекций, материалы для практических занятий, кейсы, глоссарий и список рекомендованной литературы и интернет сайтов.

Программа модуля соответствует содержанию типовой программы и включает в себя введение, цели и задачи модуля, требования к знаниям, умениям, навыкам и компетенциям слушателей, рекомендации к проведению занятий, разбивка часов по темам, краткое содержание теоретических и практических занятий, список рекомендованной литературы и интернет сайтов. В теоретических материалах раскрываются такие вопросы, как компьютерные сети и их виды, протоколы компьютерных сетей, Smart технологии, IoT, методы обеспечения информационной безопасности в компьютерных сетях, методы криптографии, кибербезопасность. В практических работах описывается стратегия обеспечения безопасности компьютерной сети.

Разработанный авторами учебно-методический комплекс по модулю «Безопасность компьютерных сетей» соответствует содержанию типовой и учебной программы, часы распределены соответственно часам, указанным в учебном плане.

Подводя итог, можно сказать, что учебно-методический комплекс по модулю «Безопасность компьютерных сетей» может быть рекомендован к использованию на курсах повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Компьютерный инжиниринг», а также его можно рекомендовать к публикации.

И.о. заместителя директора по научной работе и инновациям Совместного Белорусско-Узбекского межотраслевого института прикладных технических квалификаций, к.п.н. **Л.Набиулина**

ОЛИЙ ТАЪЛИМ МУАССАСАЛАРИ ПЕДАГОГ КАДРЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА МАЛАКАСИНИ ОШИРИШ КУРСИ УЧУН ТАЙЁРЛАНГАН "КОМПЬЮТЕР ТАРМОҚЛАРИ ХАВФСИЗЛИГИ" МОДУЛИНИНГ ЎҚУВ-УСЛУБИЙ МАЖМУАСИГА

Т А Қ Р И З

Ўқув-услубий мажмуа "Компьютер тармоқлари хавфсизлиги" модули бўйича қайта тайёрлаш ва малака ошириш тингловчилари учун яратилган. "Компьютер тармоқлари хавфсизлиги" модулининг мақсади компьютер тармоқлари хавфсизлиги бўйича олий таълим муассасалари педагог кадрларининг касбий компетентлигини ошириш, модулнинг вазифалари эса олий таълим муассасалари педагог кадрларида компьютер тармоқлари хавфсизлигини таъминлаш ҳақида назарий ва амалий билимларни, кўникма ва малакаларни такомиллаштиришдан иборат деб белгиланган. Қайта тайёрлаш ва малака ошириш йўналишининг ўзига хос хусусиятлари ҳамда долзарб масалаларидан келиб чиққан ҳолда ўқув-услубий мажмуада тингловчиларнинг ушбу модул доирасидаги билим, кўникма, малака ҳамда компетенцияларига қўйиладиган талаблар асосида ўқув-услубий мажмусида берилган материаллар ушбу мақсадга йўналтирилиб, компьютер тармоқлари, ахборот хавфсизлиги ва киберхавфсизлик соҳасидаги ҳозирги кундаги замонавий усулларини ўрганиш, уларни таълим жараёнига қўллаш бўйича назарий ва амалий маълумотлар келтирилган.

Ўқув-услубий мажмуа доирасида берилаётган мавзулар таълим соҳаси бўйича педагог кадрларни қайта тайёрлаш ва малакасини ошириш мазмуни, сифати ва уларнинг тайёргарлигига қўйиладиган умумий малака талаблари, ўқув режалари ва дастурлари асосида шакллантирилган бўлиб, бу орқали олий таълим муассасалари педагог кадрларининг соҳага оид замонавий таълим ва инновация технологиялари, илғор хорижий тажрибалардан самарали фойдаланиш, киберхавфссизлик усул ва воситаларини амалиётга кенг татбиқ этиш билан боғлиқ компетенцияларга эга бўлишлари таъминланади.

Умуман олганда, "Компьютер тармоқлари хавфсизлиги" модули бўйича яратилган ўқув-услубий мажмуа барча талабларга жавоб беради ва уни ўқув жараёнида қўллаш ва чоп этиш учун тавсия этиш мумкин.

Мухаммад Ал-Хоразмий номидаги
ТАТУ "Ахборот технологиялари" кафедраси
мудири, профессор **Х.Зайнидинов**