ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ҳимояга руҳсат
МУТ ва Т кафедра мудири
доц. У.Б. Амирсаидов____
2011 й. «____» _____

«Маълумот узатишда қўлланиладиган тармоқлараро экран тахлили мавзуида

БИТИРУВ МАЛАКАВИЙ ИШИ

Битирувчи _____ О.Ф. Вафаев
имзо

Раҳбар _____ Ш.Ю. Джаббаров
имзо

Тақризчи _____ _____
имзо

ХФХ _____ У.Т. Алиев_____
имзо

Тошкент – 2011

ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ
ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Телекоммуникация факультети *МУТ ва Т* кафедраси

йўналиш *Телекоммуникация*

ТАСДИҚЛАЙМАН

Кафедра мудири_____

2011 й «_____ »_____

Талаба *Вафаев Отабек Фахриддинович* нинг

(фамилияси, исми, отасининг исми)

Маълумот узатишда қўлланиладиган тармоқлараро экран тахлили

мавзуидаги малакавий битирув ишига

Т О П Ш И Р И Қ

1. Мавзу университетнинг 2011 йил «19» 02 даги 147 – 09 сонли буйруқ билан тасдиқланган

2. Ишни ҳимояга топшириш муддати *30. 05. 2011*

3. Ишга оид дастлабки маълумотлар *Диплом олди амалиёти ва адабиётлар*

4. Ҳисоблаш–тушунтириш ёзмалар мазмуни (ишлаб чиқиладиган масалалар рўйхати)

1. *Маълумотлар узатиш тармоқлари ва ахборот хавфсизлиги муаммолари.* ***2***. *Маълумотлар узатиш тармоқларини ахборот хавфсизлигини таъминлаш тамойиллари.* ***3***. *Маълумотлар узатишда қўлланиладиган тармоқлараро экран тахлили.* ***4***. *Хаёт фаолияти хавфсизлиги*

5. График материаллар рўйҳати *Презентация*

6. Топшириқ берилган сана 24.01.2011

Раҳбар _____
имзо

Топшириқ олдим _____
имзо

7. Ишнинг айрим бўлимлари бўйича маслахатчилар:

Бўлим номи	Маслаҳатчи	Имзо, сана	
		Топшириқ берилди	Топшириқ олинди
1. Асосий қисм	Ш.Ю. Джаббаров	24.01.2011	
2. ХФХ	У.Т. Алиев	3.05.2011	

8. Ишни бажариш графиги

Т/р	Иш бўлимлари номи	Бажариш муддати	Раҳбар (маслаҳатчи) имзоси
1.	Маълумотлар узатиш тармоқлари ва ахборот хавфсизлиги муаммолари.	26.02.2011	
2.	Маълумотлар узатиш тармоқларини ахборот хавфсизлигини таъминлаш тамойиллари.	28.03.2011	
3.	Маълумотлар узатишда қўлланиладиган тармоқлараро экран тахлили	30.04.2011	
4.	Хаёт фаолияти хавфсизлиги	20.05.2011	

Битирувчи _____ 2011 йил «_____»_____
имзо

Раҳбар _____ 2011 йил «_____»_____
имзо

Ушбу битирув малакавий ишда маълумотлар узатишда қўлланиладиган тармоқлараро экран тахлили, тармоқлараро экранларнинг ишлаш хусусиятлари ва тармоқлараро экран асосидаги тармоқ химоясининг схемалари келтирилган.

Шунингдек хаёт фаолияти хавфсизлиги чоралари хам кўриб ўтилган.

В данной выпускной квалификационной работе проведен анализ внедрение межсетевых экранов для передачи данных, рассмотрены особенности функционирования межсетевых экранов и прведены схемы защиты сетей, основанных на применении межсетевых экранов.

Также рассмотрены вопросы безопасности жизнедеятельности.

In the given final qualifying work the analysis introduction of gateway screens for data transmission is carried out, features of functioning of gateway screens are considered and schemes of protection of the networks based on application of gateway screens are spent.

Also ability to live safety issues are considered.

КИРИШ

Ахборот жуда қадриятли ёки ўта муҳим бўлганлиги сабабли бундай ахборотни сақлайдиган, қайта ишлайдиган ёки узатадиган компьютер тизимларига нисбатан турли – туман ёмон ниятли ҳаракатлар мавжуддир. Масалан, бузғунчи ўзини бошқа фойдаланувчи каби кўрсатишга интилиши, алоқа каналини билдирмасдан эшитиб олиши ёки тизим фойдаланувчилари алмашаётган ахборотни ушлаб олиши ва ўзгартириши мумкин. Замонавий компьютер тизимлари ва тармоқлари (КТ ва Т), Интернет ёмон ниятли одамларга муҳим махфий ахборотни ўғирлаш, бузиш ёки халақитларга учратиш мақсадида корхона ва ташкилотларнинг ички тармоқларига кириш учун кўплаб имконият яратиб берадилар. Шу сабабли ҳозирда инсонларни ва жамиятни информацион хавфсизлик ва ахборотни ҳимоя қилишни таъминлаш муаммосини комплекс ечишни долзарб равишда кераклиги пайдо бўлмокда.

Ахборот хавфсизлигини таъминлаш муаммоси Интернетнинг ишлаш шароитларида муҳим аҳамият касб этади. Мутлоқ кўпчилик компания ва ташкилотлар бугунги кунда ўзларининг локал тармоқларини Интернетга, унинг ресурслари ва афзалликларидан фойдаланиш учун уламоқдалар. Улар Интернетни турли мақсадларда ишлатадилар, бунга электрон почта билан алмашиниш, қизиқиб қолган шахс ва ташкилотлар ўртасида ахборотларни олиш ва тарқатиш ва бошқалар киради. Бош тармоққа уланиш катта афзалликга эга, аммо бунда уланаётган локал ёки корпоратив тармоқдаги ахборот хавфсизлигини таъминлашда жиддий муаммолар пайдо бўлади. Ўзининг идеалогиясидаги очиқчилик туфайли Интернет ёмон ниятли одамларга, муҳим ва махфий ахборотни ўғирлаш, халақитларга учратиш ва бузиш мақсадида корхона ва ташкилотларнинг ички тармоқларига кириш учун кўп имконият яратиб беради. Ахборот жуда ахамиятли ёки ўта муҳим бўлганлиги сабабли бундай ахборотни сақлаётган, қайта ишлаётган ёки узатаётган компьютер тизимлари ва тармоқларига нисбатан турли хил ёмон ниятли харакатлар бўлиши

мумкин. Масалан, бузувчи одам ўзини тизимнинг бошқа фойдаланувчиси қилиб кўрсатишга интилиши мумкин, алоқа каналини билдирмасдан эшитиши ёки тармоқ фойдаланувчилари алмашаётган ахборотни ушлаб олиш ва ўзгартириши мумкин. Тизимнинг фойдаланувчиси бузғунчи бўлиши мумкин, у ўзи хақиқатда ҳам узатилмаган маълумотни улар томонидан олинганлигини тасдиқлашга интилиши мумкин. У мурожаат қилиши мумкин бўлмаган ахборотга мурожаат қилишга рухсат олиш учун ўзининг ваколатларини кенгайтиришга интилиши ёки бошқа фойдаланувчиларнинг хуқуқларини рухсат этилмаган ҳолда ўзгартириб тизимни бузишга интилиши мумкин. Шу муносабат билан, замонавий ахборотлашган жамиятда глобал ва бошқа тармоқларнинг улкан афзалликлари мавжудлиги билан бир қаторда, уларда ахборотни ҳимоя қилиш бўйича ўзига хос муаммоларни ҳам ечишга тўғри келади. Шунинг учун ахборотнинг махфийлиги ва бутунлигини таъминлаш билан боғлиқ бўлган барча керакли ишларни амалга ошириш учун самарали воситаларни яратиш ва қўллаш жуда муҳимдир.

Интернетни тадбиқ қилиниши билан жиноятлар айниқса кенг қулоч ёйди. Бу эса қонуниятлидир, негаки ШК нинг фаол ишлатилишининг биринчи ўн йиллигида компьютерларга асосан телефон тармоғи орқали уланиб олган хакерлар ёки «электрон қароқчилар» асосий хавф-хатарга эга бўлган бўлса, унда компьютер тизимларини ва тармоқларини оммавий ишлатиш даврида ахборотнинг ишончлилиги ва бутунлигини бузишга компьютер вируслари дастурлари ва Интернет глобал тармоқи орқали хавф солинмоқда.

Компьютерлар, компьютер тизимлари ва тармоқлари ахборотни сақлаш ва қайта ишлашни, уни истеъмолчиларга тақдим этишни, шу билан бирга энг замонавий ахборот технологияларини қўллашни амалга оширадиган, ахборотни қайта ишлайдиган барча автоматлаштирилган тизимларнинг асоси ҳисобланади.

1.МАЪЛУМОТ УЗАТИШ ТАРМОҚЛАРИ ВА АХБОРОТ ХАВФСИЗЛИГИ МУАММОЛАРИ

1.1. Тармоқнинг ташкил этилиши ва талаблар

Тармоқнинг ташкил этилиши. Ташкилий тузилма тармоқнинг яхлит ташкил қилинишини, яъни унинг вазифалари, элементларнинг асосий хусусиятлари ва алохида тизим ости ахборот тармоқ сегментлари сифатида қўлланиладиган унсурларнинг тузилма компонентларига бирлаштиришнинг композицион тамойилларини акс эттиради.

Тармоқ элементлари, уларнинг вазифалари ва хусусиятлари. Умумий холда хар қандай тармоқнинг элементлари пунктлар ва уларни боғловчи линиялар хисобланадилар. Тармоқ пунктлари *охирги* ва *тугун* пунктларга бўлинади.

Охирги пунктларда (ОП) (endpoints) тармоқнинг терминал ускуналари хамда ОП функционал вазифаларини белгиловчи ахборот ресурслари ва ишчи тизимлар жойлашади. Масалан, ОП тармоққа,телекоммуникацион хизматларга киришни таъминлаш ёки тармоқнинг турли сегментларини бирлаштириш учун ишлатилади. Юқоридаги иккита холатда ОП *кириш тугуни* (access node) деб аталади.

Фойдаланувчиларнинг тармоққа киришида, мувофиқ ОП терминал қурилмаси фойдаланувчи вазифасига кўра, ахборот киритиш-чиқариш хамда ахборотни қайта ишлаш функциясини бажаради.

Телекоммуникация хизматларидан фойдаланиш учун фойдаланувчининг тармоққа кириш имконини берувчи пункт-*хизмат тугуни* (service node) деб юритилади. Уларда фойдаланувчилар кириши учун абонент-тармоқ интерфейслари (User Network Interface, UNI) ва тармоқ билан ўзаро боғланиш учун хизмат тугуни интерфейси (Service Node Interface) амалга оширилган.

Турли сегментларни бирлаштирувчи ОП да чегара коммутатор, киритиш-чиқариш мультиплексори ёки турли телекоммуникацион технологиялар тармоқларини бирлаштиришда тармоқлараро ўзгартиргич (*шлюз*) вазифасини бажарувчи махсус ускуналар ўрнатилиши мумкин.

Тугун пункти (node point) ёки *тармоқ тугуни* (node) бу икки ва ундан ортиқ алоқа линиялари бирлашган пункт ва ушбу пункт маълумотлар оқими йўлида оралиқ пунктдир. Тармоқ тугунида бир пайтда ёки хар хил пайтда турли вазифалар амалга оширилади, улардан асосийси коммутация, концентрация, мультиплексорлаш ва маршрутизациядир.

Коммутация (switching)-маршрутизация схемасига мувофиқ тармоқда ахборот оқимларини тақсимлашда тугунда бирлашадиган линиялар ўртасида алоқа ўрнатиш жараёни. Коммутация оператив (алоқа сеанси мобайнида) ва узоқ муддатли (кроссли), яъни тугунда бирлашадиган линияларни кросслаш йўли билан амалга ошириладиган бўлади.

Концентрация (concentration)-линиянинг самарали юкланишини таъминлаш мақсадида қувватли чиқиш оқимига эришиш учун бир неча кириш ахборот оқимларини бирлаштиришдир.

Мультиплексорлаш (multiptxing)-линиянинг ўтказиш қобилияти ресурснинг маълум қисмини ахборот оқимининг хар бирига бериш йўли билан битта линиядан бир неча ахборот оқимларини узатишни таъминлаб беради. Ўрнатилган бу тақсимлаш узатилаётган ахборот йўқлигида хам сақланиб қолади, яъни бу ерда концентрация вазифаси мавжуд эмас.

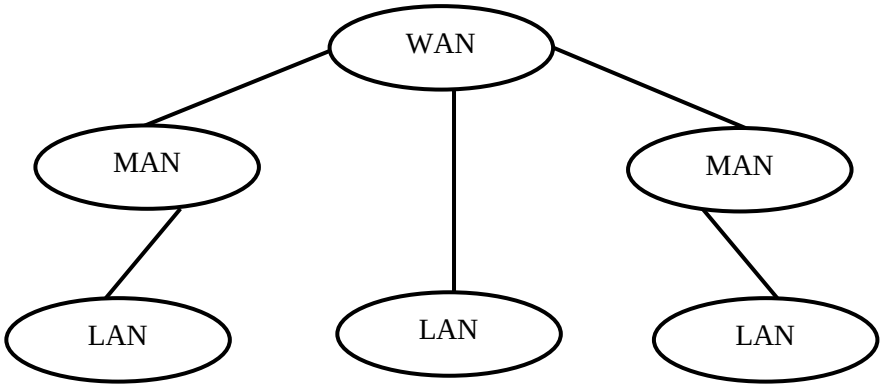
Маршрутизация (routing)-адрес ахборот ва маршрутлар трассаси жадвали асосида тармоқнинг икки пункти ўртасида йўл қидириш жараёни.

Алоқа линиялари сигнал шаклида ахборот оқимларини узатишни таъминлаб беради ва умумий холатда сигнал тарқатиш мухитини ва уни тақсимлаш режимида ишлатишга имконият берувчи ускуналар мажмуасини ўз ичига олувчи қурилмалардир. Физикавий мухит жуфт мис симлар, оптик тола,эфир бўлиши мумкин. Мухит турига боғлиқ равишда алоқа линиялари *симли* ва *симсизга* ажратилади.

Симли линияларга сигнал сунъий ташкил қилинган йўналтирувчи мухитда тарқаладиган, масалан, химояланган қобиққа эга симлар(кабель алоқа линиялари) киради. Кабель алоқа линияларида узоқ масофани таъминлаш мақсадида, маълум интервалда кучайтиргич пунктлари ташкил қилинади. Оптик толали алоқа линиялари хам симли хисобланади, уларда тарқалиш мухити сифатида диэлектрик материал, хусусан, юпқа шиша толалар ишлатилади. Уларнинг афзаллиги конструкциясида дефицит бўлган мис, алюминий, қўрғошиннинг йўқлигидир.

Тармоқ тузилмаси компонентлари. Тармоқ элементлари бирлашишнинг нисбатан мустақил тузилма компонентларга *–тармоқ сегментларига*-бирлашиши тамойиллари одатда сегмент миқёси, унинг бажараётган вазифаси, ишлатилаётган телекоммуникацион технологияси бўйича таснифланади. Тармоқни сегментациялашнинг асосий вазифаси сегмент ичидаги оқим улушини максималлаштириш ва сегментлар орасидаги оқимлар улушини камайтиришдир.

Тармоқ сегментларини миқёс тамойили асосида тасниф қилиш тармоқ иерархияси билан тасвирланади (1.1-расм):



1.1-расм. Масштаб белгисига кўра тармоқнинг иерархия сегменти

- локал тармоқ (Local Area Network, LAN), унда юкланишнинг асосий қисми кичик худуд, муассаса, саноат корхонаси ва хоказо ичида чегараланади, яъни катта бўлмаган маълум худудда жойлашган

компьютерлар тармоғи. Умумий холда битта ёки бир нечта бинолар ва битта ташкилотга тааллуқли бўлган қурилмалар мажмуаси;

- худудий (минтақавий) тармоқ (Metropolitan Area Network, MAN), йирик ахоли пункти ёки кичик минтақага хизмат қилиш учун мўлжалланган;

- йирик миқёсли худудий (глобал) тармоқ (Wide Area Network,WAN), катта худуд, давлат, континент хамда турли континентларда жойлашган LAN, MAN туридаги тармоқларни бирлаштириш учун мўлжалланган. Мазкур магистрал тармоқ узатиш мухити сифатида асосан оптик толадан фойдаланилади.

LAN, MAN, WAN тармоқларидан хар бири кичик миқёсдаги бир қатор сегментларга бўлиниши мумкин. Улар тармоқнинг мантиқий тузилмасини акс эттиради ва уларнинг хар бир сегменти умумтармоқ алмашувини шакллантиришда аниқ функционал вазифани бажаради. Хар қандай қатламда сегментлар боғлиқлиги магистраллар (магистрал сегментлар) билан таъминланади.

Охирги пунктларнинг сегмент ичида бирлашиши ва магистрал сегментларнинг амалга оширилиши *умумий коммуникацион мухит* ёки тугун ташкил қилиш йўли билан амалга оширилиши мумкин.

Умумий коммуникацион мухитни ишлатиш иқтисодий томондан фойдалидир. Бунда битта тугун тизими билан генерация қилинадиган юклама барча бошқа тизимларга юборилади, бироқ қабул қилувчи манзили бўлган битта тизим билан қабул қилинади. Умумий бўлинадиган мухитли тармоқ сегментлари мисолига шина топологияли кичик бир рангли махаллий тармоқларни хамда транспорт халқа тамойили бўйича ташкил қилинган худудий тармоқларни келтирса бўлади.

Тугун ташкил қилиш сегмент коммутацияланаётган топологияни очиқ тизимлар ўзаро боғланиш моделини (Open System Interconnection,OSI) канал ва тармоқ вазифаларга эга бўлган ускуналар тугунида жойлаштириш йўли орқали амалга оширилади. Бунда умумий коммуникацион мухитдан фарқли равишда тармоқнинг катта миқёси, юқори ишлаб чиқариш даражаси ва

ишончлилиги таъминланади, бироқ нархи ошади. Бундай тармоқларга мисол сифатида юқори тезликли махаллий тармоқларнинг магистрал сегментларини хамда радиал тугун тамойили асосида ташкил қилинган худудий тармоқларни келтирса бўлади.

Тармоқ (тармоқ сегментлари) боғловчи магистрал сифатида ташкил қилинса, таянч тармоқ (backbone network) деб аталади. Магистрал қурилишининг турли топографик вариантлари бўлиши мумкин, бунга асосланиб таянч тармоқларнинг номланиши хам турличадир, масалан: «тизма тармоқ», «транспорт халқа», «коммутацияланадиган тармоқ». Улардан хар бири аниқ вазифа доирасида чегараланган.

Таянч тармоқ ихтиёрий даражада (LAN, MAN, WAN) ташкил қилиниши мумкин, яъни тармоқнинг ишончлилиги, ишлаб чиқаришни ошириш мақсадида, тармоқнинг мантиқий сегментация вазифаси ечиладиган хамма жойда ишлатилиши мумкин. Турли даражалардаги таянч тармоқларнинг йиғиндиси тақсимланган тармоқнинг иерархик боғлиқлигини таъминлаб беради. Шуни қайд қилиш лозимки, кичик миқёсли сегментлар (LAN, MAN) учун таянч тармоғи вазифасини битта тугун бажариши мумкин. Бундай магистрал ўзгарган магистрал (collapsed backbone) ёхуд таянч тугуни (backbone node) деб номланади. Мисол тариқасида махаллий тармоқларнинг маршрутизатор ёрдамида марказий нуқтада бирлашишини келтирсак бўлади. Таянч тугун охирги пункт сегменти ёки битта даража сегментлари ўртасида юкламани қайта тақсимлайди, бу йўл билан юқорироқ даражадаги сегментнм ташкил қилади ва унинг чегара ортига йўналтириладиган оқимларни концентрация қилади.

Тақсимланган тармоқ боғлиқлик иерархиясидаги юқори даража таянч тармоғини транспорт тармоқ(transport network) деб аташади. У юкламани анча секин сегментлар бўлмиш минтақавий ва махаллий даражага узатадиган юқори тезликли тракт(сегмент) тизими кўринишида амалга оширилади.

«Транспорт тармоғи» атамаси сегментнинг масштабини эмас, балки функционаллигини акс эттиради. Бунинг натижасида транспорт тармоғи

технологияларни қўллаб ташкил қилинган катта бўлмаган худудий тармоқларнинг таянч тармоқларини аксарият холларда транспорт тармоқлари деб аталади. Барча вазиятларда сегментларнинг транспорт магистрали билан бирлашиши унинг охирги пунктлари бўлган кириш тугунларида амалга оширилади.

Функционалликни композицион тамойил сифатида қабул қилиб, *кириш тармоғи* (access network) деб транспорт тармоғига кириш пункти билан ўзаро боғланган ахборот тармоқни худудий тақсимланган охирги пунктлари трактини ташкил қиладиган сегмент ёки сегментлар йиғиндисига айтилади. Хусусан, сервис тугуни билан фойдаланувчиларнинг терминал тизимлари ўзаро таъсир қиладиган тармоқ сегменти абонент кириш тармоғи (customer access network) деб аталади.

Транспорт тармоқлари ва кириш тармоқлари функционал белгилари бўйича мустақил тузилма компонентлари, яъни телекоммуникацион тармоқнинг функционал сегменти сифатида қабул қилиниши мумкин.

Ахборот тармоғи концепциясида ахборот ва хисоблаш ресурсларига киришни тақдим этувчи ишчи тизимлар билан фойдаланувчиларни терминал тизимларнинг ўзаро таъсирини таъминлаб берувчи телекоммуникацион тармоқ сегментлари йиғиндиси *узоқлашган кириш* (remote access) сифатида тавсифланиши мумкин. Уни амалга ошириш услублари глобал алоқаларни ташкил қилиш схемалари ва ишлатилаётган дастурий махсулотлар функциялари билан ахамиятли фарқланиши мумкин.

Фойдаланувчиларга хизмат кўрсатиш платформасини ташкил қилиш хам тармоқ компонентларини вазифалари бўйича бирлаштиришга асосланган. Хизматлар кўрсатишнинг ягона платформасини ташкил қилишда хизматларни етказиб берувчи ва алока операторларини бирлаштирувчи глобал коммуникациялар сегментининг йиғиндиси *база тармоғи* (Core Network) деб аталади.

Турли ўлчамдаги (бутун тармоқдан алохида фрагментгача) технологик равишда фарқланадиган сегментлар тармоқ технологияларнинг кескин

ривожланишида ахборот тармоқларининг эволюцион ривожланиши туфайли пайдо бўлди. Бундай сегментларнинг мавжудлиги хизматлар кўрсатишнинг ягона мультисервисли платформага ўтиш даври учун хосдир. Уларни функционал-технологик белгилар бўйича таснифлаб, қуйидаги тушунчалар ишлатилади: аналог тармоқ, рақамли тармоқ, ISDN тармоғи, IP-тармоқ, SDH тармоғи, FR(Frame Relay) тармоғи, ATM тармоғи ва бошқалар.

Тармоқнинг функционал модели. Функционал модель тармоқнинг физикавий амалга оширилиши тамойилларига боғлиқ бўлмаган холда тармоқни мантиқий даражада мавхум равишда тасвирлайди. Модель элементлар сифатида кўриб чиқилаётган тармоқ функцияларининг ўзаро таъсирини акс эттиради.

Функция-мантиқий элемент бўлиб, белгиланган вазифани бажаради. Физикавий равишда функция аппарат билан ёки дастурий махсулот (функционал объект) кўринишида амалга оширилиши мумкин. Охирги холатда функцияларни *объект* деб номлаш қабул қилинган. Функцияни физикавий амалга оширишда уларни *мантиқий модул* деб аталувчи алохида функционал тизим ости бирликлар гурухига бирлаштириш мумкин.

Тармоқда бажариладиган функцияларнинг қуйидаги турлари фарқланади:

- *амалий(қўлланиш)* функциялар-фойдаланувчилар ва тармоқ маъмурияти илова объектлари;
- *хизматларни бошқариш* функциялари-хизмат компонентларидан ва улар билан боғлиқ бўлган ресурслардан хизматларни амалга оширишга имконият берувчи ва фойдаланувчини мазкур хизматлар ўзаро таъсири билан бошқариш имкониятини берадиган объектлар;
- тармоқни *маъмурий бошқарув* функциялари-хамма бошқа функциялар бошқарувини амалга оширадиган объектлар;
- *маълумотларга ишлов бериш ва сақлаш* функциялари-илова объектларини чақириш ва бошқариш, уларнинг ўзаро таъсирини хамда

маълумотларни маълумотлар базасидан олиш ёки унга жойлаштиришни таъминлаб берадиган объектлар;

- *коммутацион* функциялар-ахборот оқимларини бошқариш ва транспорт функциялари (улар коммуникацион тугунларда қайта тақсимланганда).

Тармоқ функциялари ўзаро таъсир тартиби функционал модель элементлар алоқасини белгилаб беради. Бундай ўзаро таъсирни алохида функциялар (объектлар) ёки мантиқий модуллар ўртасида тўлиқ махсуллиги *мантиқий интерфейс* деб аталади. У элементлар ўзаро таъсир қоидалари мажмуасини ва алмашилаётган ахборотни тақдим этиш форматини белгилаб беради. Бир турдаги функциялар (объектлар) ўртасидаги мантиқий интерфейс протокол деб аталади. Коммуникацион функциялар ўртасидаги мантиқий интерфейс *телекоммуникацион тармоқнинг функционал эталон нуқтаси* деб аталади.

Тармоқларда коммутация усуллари таърифи. **Коммутация жараенининг вазифаларидан бўлган – оқимлар ва керакли маршрутлар аниқлаш, махсус жадвалларда маршрутларни белгилаш, оқимларни мултиплекслаш, узатиш мухитини тақсимлаш – техникавий масалалар барча тармоқ технологиялари асоси сифатда унинг функционал хусусиятларини белгилайди.**

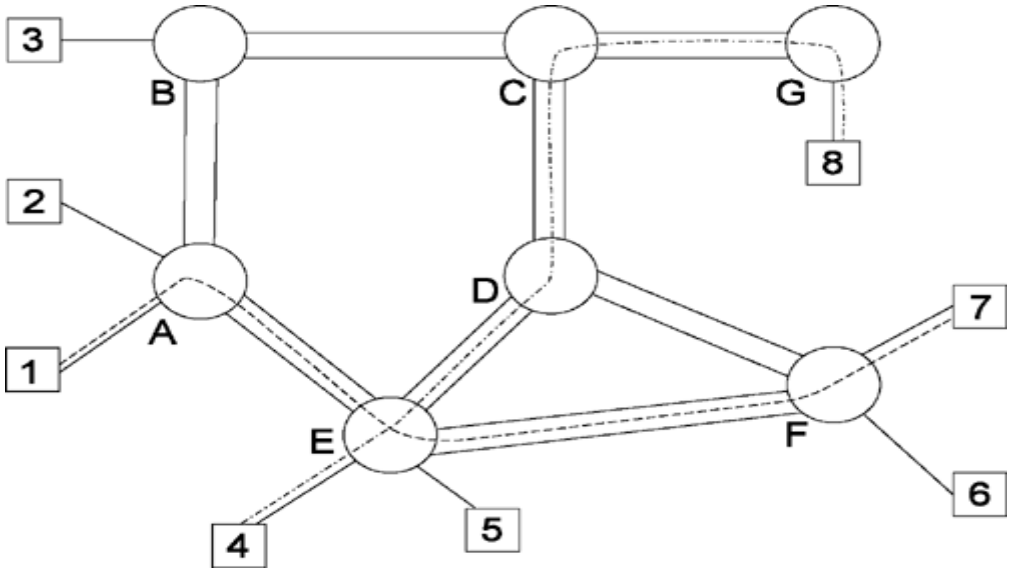
Тармоқларда иккита фойдаланувчи бири бири билан боғланиш жараенида қуйидаги асосий коммутаця усуллари мавжуд:

- **Каналлар коммутацяси *(circuit switching*);**
- **Пакетлар коммутацияси *(packet switching*);**
- **Хабарлар коммутацияси *(message switching).***

Умумий холда фойдаланувчилар боғланиши 1.2-расмда келтирилган каби бўлади, коммутация усулига кўра бажариладиган вазифалар фарқланади.

Каналлар коммутацияси тарихи дастлабки телефон тармоқларидан бошланади. Пакетлар коммутацияси 60чи йиллар охирида барпо этилиб,

биринчи компютер тармоқларида қўлланилган. Коммутация усулларнинг хар бири афзаллик ва камчиликларга эга; мутахассислар фикрига кўра, пакетлар коммутациясига асосланган тармоқ технологиялари истиқболда асосий ўрин эгаллайди.



1.2. расм Тармоқда фойдаланувчилар коммутацияси

Каналлар коммутацияси усулида тугунлар ўртасида узлуксиз физикавий канал хосил бўлиб, коммутаторлар ердамида алохида канал қисмлари кетма кет уланган бўлади: бир нечта физикавий каналлар ягона физикавий канални ташкил этади ва хар бир каналда узатиш тезлиги бир хил бўлиши шарти асосланган. Бундай ягона канал маълумот узатиш жараенидан аввал ўрнатилиши керак бўлади, ва бу канал улаш ўрнатиш жараенида фақат ушбу боғланишга хизмат қилади.

Мисол учун, расмдаги 1-тугундан 7-тугунга маълумот узатиш учун, аввал 1-тугун А-коммутаторига улаш ўрнатиш учун 7-тугун адресини белгилаган холда махсус сўров сигналини юборади. А-коммутатори ягона канал хосил қилиш учун маршрут аниқлаб, сўров сигналини кейинги коммутаторга юборади ва х.к. 7-тугун сўров белгисини олганлиги тўғрисида 1-тугунга жавоб сигналини қайтаради ва ягона канал хосил бўлганлиги

(коммутацияланганлиги) ни белгиланади; шундан сўнг 1-тугун 7-тугун билан маълумот алмашиши мумкин.

Каналлар коммутациясининг афзалликлари:

- Фойдаланувчилар аро ўрнатилган каналда маълумот узатиш тезлиги доимий ва маълум бўлади (фойдаланувчи сифатли узатишга мўлжалланган каналнинг ўтказиш қобилиятига мослаб керакли тезликни белгилаш имкониятига эга);
- Тармоқ орқали маълумот узатишда тўхталишлар даражаси паст ва доимий бўлиши (тўхталишларга сезгир реал вақтли трафик (овоз, видео)ни сифатли узатилиш имконияти).

Каналлар коммутациясининг камчиликлари:

- канал бандлигида фойдаланувчига рад эиш жавоби берилиши;
- физикавий канлларнинг ўтказиш қобилиятини самарасиз ишлатилиши (канал улаш ўратиш жараени мобайнида банд бўлади);
- аввалдан улаш ўрнатилиши туфайли маълумот узатиш жараенидан олдин шартли тўхталиш мавжудлиги.

Бу коммутация усули телефон сўзлашувларни узатишда қўлланилади.

Пакетлар коммутацияси асосан, компютер трафигини узатишга мўлжалланган бўлиб, маълумот алмашувини самарали равишда ташкил этишга имкон беради.

Пакетлар коммутациясида фойдаланувчилар аро узатилаетган хабарлар кичик қисмлар- пакетларга бўлинади. Маълумот узатиш тармоқларида пакет асосий узатиш бирлиги хисобланади. Катта хажмдаги хабарлар кичик пакетларга бўлиниши тармоқда маълумот узатиш тезлигини кескин ошишига олиб келади. Хабарлар турли узунликга эга бўлиши мумкин – бир неча байтдан ўнлаб мегабайтгача; пакетлар эса ўзгарувчан узунликга эга бўлишлари мумкин.

Хар бир пакет керакли тугунга етиб бориши учун адрес ахбороти белгиланган сарлавха қисми билан бошланади. Пакет турли қисмлардан иборат бўлиши мумкин ва қуйидагиларни ўз таркибига олиши шарт:

- узатувчини (source) ифодалайдиган манба адреси;
- узатилетган маълумотлар;
- қабул қилувчининг (destination) адреси
- тармоқ воситаларига маълумот узатилиши лозим бўлган маршрут ахбороти;
- хабарни дастлабки кўринишда тақдим этиш учун ахборот;
- узатиш аниқлигини таъминловчи хатоликлар текшириш ахбороти.

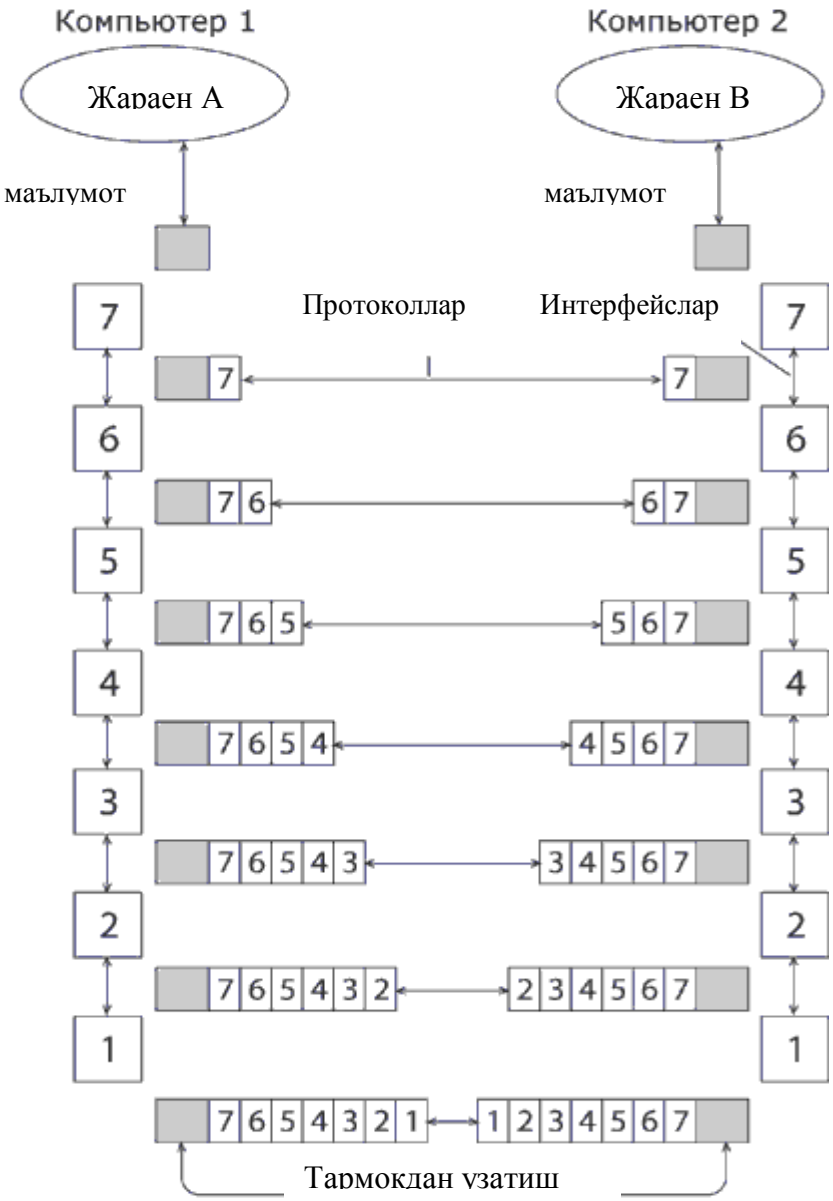
Бу қисмлар учта гурухга бўлиниб, пакетнинг сарлавха, маълумот ва трейлер қисмларини шакллайди.

Сарлавха қисми пакет узатилиши сигнали, манба адреси, макон адреси, узатишни синхронлаш кабиларни ўз ичига олган.

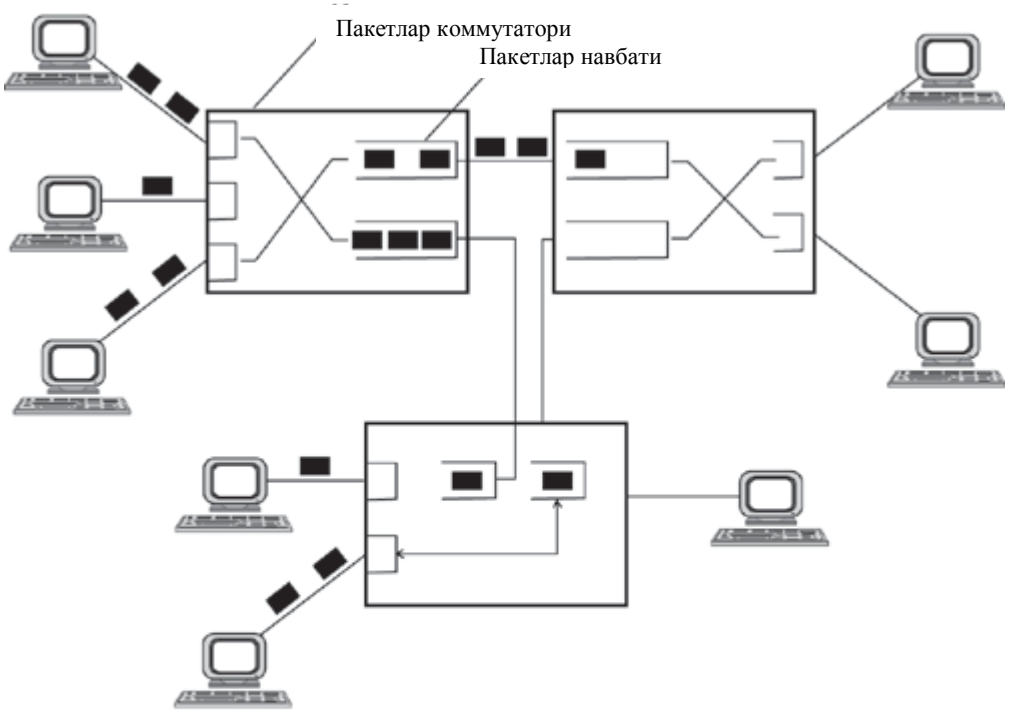
Маълумот қисми хабар таркибидаги узатишга мўлжалланган маълумолардан иборат. Тармоқ турига нисбатан бу қисм 0,5-4 Кб бўлиши мумкин.

Трейлер қисми кўп холларда хатоликларни текширишга мўлжалланган (мисол учун, Cyclic Redundancy Check циклик код ердамида текширув).
Пакет шаклланиши OSI моделининг қўлланиш поғонасида бошланади. Узатишга мўлжалланган ахборот юқори (қўлланиш поғонаси)дан қуйи поғонага етказилади ва хар бир поғона маълумот қисмига тегишли ахборот қўшади (1.3- расм)

Пакетлар тармоқ орқали мустақил ахборот блоклар сифатида узатилади. Пакетли коммутация асосидаги тармоқда коммутаторлар ички буфер хотирасига эга бўлиб, унда пакетлар вақтинча сақланилади. Коммутаторнинг чиқиш порти банд бўлган холатда, пакет бирор вақт навбат кутади ва кейинги коммутаторга узатилади (1.4 - расм). Пакетлар узатишни шундай йўсинда ташкил этиш трафик пулсациясини бартараф этишга ва тармоқнинг умумий ўтказиш қобилиятини оширишга имкон беради.
Пакетлар коммутациясида бир вақтда узатилаетган маълмотлар хажми нисбатан юқори бўлади ва узатиш тезлиги ошади.



1.3. Пакетли узатишни ташкил этиш



1.4. Пакетлар коммутациясида трафик узатилишини ташкил этиш

Сарлавхалар узатилишига вақт сарфланиши, хар бир кейинги пакетни узатишга зарур бўлган вақт, пакет буферизацияси ва коммутациясига сарфланган вақт- тармоқдан пакетни умумий узатиш вақтига таъсир кўрсатади ва тўсқинликлар манбаи бўлади.

Пакетли коммутациянинг афзалликлари:

- пулсацияли трафикни узатишда тармоқни ўтказиш қобилиятини ошириш имкониятини беради;

- фойдаланувчилар аро трафик холатини инобатга олган холда, тармоқ шароитига нисбатан физикавий каналларнинг ўтказиш қобилиятини тақсимлаш имконияти.

Пакетли коммутациянинг камчиликлари:

- коммутаторлар буферларида тўсқинликлар тармоқ холатига боғлиқ бўлганлиги сабабли фойдаланувчилар аро узатиш тезлиги ноаниқлиги;

- маълумот пакетларининг тўсқинлиги ўзгарувчанлиги;

- буферларда навбатлар ортиб кетганлиги сабабли маълумот (пакетлар) йўқолиши.

Бу камчиликларни бартараф этиш мақсадида турли усуллар қўлланилади (Quality of Service QoS каби). Бундай усуллар қўлланилиши пакетлар коммутациясини хозирги кундаги юқори тезликли тармоқлар ташкил этишда энг самарали ва истиқболли деб тан олинган.

Хабарлар коммутацияси усули ўз вазифалари бўйича пакетлар коммутациясига яқин. Бу усулда маълумотларнинг тўлиқ блоки тармоқнинг оралиқ тугунларида вақтинча сақланиб, транзит тугунлари аро узатилади. Хабар таркибидаги ахборот унинг узунлигни белгилайди.

Транзит тугунлар ўзаро боғланишда нафақат пакетли, балки каналлар коммутациси асосидаги тармоқдан фойдаланишлари мумкин. Хабар оралиқ тугунда бирир вақт сақланиши мумкин ва тармоқ бўшаши билан керакли фойдаланувчига етказилади. Бундай ишлаш принцип зарурияти юқори бўлмаган хабарлар етказилишда қўлланилади (мисол учун, электрон хат, матнли хужжат, файл) ва оралиқ «сақлаш билан узатиш» (store-and-forward) усули номини олган. Хозирги кунда хабарлар коммутацияси, асосан, пакетли коммутацияли тармоқларда, қўлланиш поғонаси хизмати сифатида фақат баъзи тезкор бўлмаган хизматлар ташкил этишда қўлланилади.

1.2. Ахборот хавфсизлигининг бузилишига олиб келувчи тахдидларнинг турлари ва уларнинг таснифи

Таъсир этиш мақсади бўйича хавфсизлик хавфини учта асосий турга фарқланади:

1. Ахборот махфийлигининг бузилиш хавфи;
2. Ахборот бутунлигининг бузилиш хавфи;
3. Тизимнинг ишлаш лаёқатлигининг бузилиш хавфи (хизмат кўрсатишдаги инкор (рад) этишлар).

Ахборот махфийлигининг бузилиш хавфи махфий ёки сирли ахборотни хавфни амалга оширишда ахборот унга мурожаат қилиши мумкин бўлмаган шахсларга маълум бўлиб қолади. Компьютер тизимида, бир тизимдан бошқасига узатилаётган ёки компьютер тизимида сақланаётган бирор ёпиқ ахборотга рухсат этилмаган мурожаат қилиш бўлганда ҳар сафар ахборот махфийлигини бузилиши ҳавфи содир бўлади.

Ахборот бутунлигининг бузилиши хавфи унинг сифати ва ишончлиги бузилишига ёки тўлиқ йўқотилишига олиб келадиган халақитларга ёки ахборотнинг ўзгаришига йўналтирилгандир. Ахборотнинг бутунлиги нияти ёмон одам томонидан кўра била туриб ҳамда тизимни ўраб турган муҳит томонидан объетив таъсирлар натижасида бузилиши мумкин. Бу ҳавф айниқса, ахборотни узатиш тизимлари, компьютер тармоқлари ва радиотехника тизимлари учун долзарбдир.

Тизимнинг ишлаш лаёқатлигини бузилиш хавфи (хизмат кўрсатишдаги инкор этишлар) маълум бир олдиндан мўлжалланган таъсирлар ёки тизимнинг ишлаш лаёқатлигини сусайтирадиган ёки унинг баъзи бир ресурсларига мурожаат қилишни блокировкалайдиган холатларни яратишга йўналтирилгандир. Масалан, тизимнинг бир фойдаланувчиси бирор хизматга мурожаат қилишга сўров берса, бошқаси эса бу мурожаат қилишни блокировкалаш бўйича характерларни амалга оширса, унда биринчи фойдаланувчи хизмат кўрсатишга рад жавобини олади.

Ресурсга мурожаат қилишни блокировкалаш доимий ва вақтинча бўлиши мумкин.

Ахборот хавфсизлигини бузиш бўйича сабаблар тасодифий ва ёмон ниятли (олдиндан мўлжалланган) бўлиши мумкин. Биринчи ҳолда бузувчи, халақит берувчи ва бошқа жараёнларнинг манбалари бўлиши мумкин:

- тасодифий ҳолатлар (ер қимирлаши, ёнгин, довул ва б.);
- тизимнинг таркибий элементларини издан чиқиши (техник бузилишлар);
- фойдаланувчилар ва хизмат кўрсатиш ходимларини хато харакатлари;

- дастур таъминотидаги хатоликлар;

- ташқи муҳит таъсири натижасида алоқа йўлидаги халақитлар ва бошқалар.

Ҳозир жаҳонда молия – банк компьютер тармоқлари олдиндан мўлжалланган хавфларга энг юқори даражада таъқиб этилади? бундай хавфларга қуйидагилар тегишлидир:

- банк хизматчилари сонига тегишли бўлмаган бегона шахсларнинг рухсат этилмаган мурожаат қилиши ва сақланаётган махфий ахборот билан танишиши;
- банк хизматчиларининг улар мурожаат қилиши мумкин бўлмаган ахборот билан танишиб чиқиши;
- дастурларни ва берилганларни рухсатсиз нусхалаш;
- махфий ахборотни ўз ичига олган магнит ташувчиларни ўғирлаш;
- чоп қилинган банк хужжатларини ўғирлаш;
- ахборотни атайлаб йўқотиш;
- банк ходимлари томонидан молиявий ҳужжатларни, ҳисобот ва маълумот базасини рухсатсиз ўзгариш;
- алоқа каналлари бўйича узатилаётган маълумотларни қалбакилаштириш;
- алоқа каналлари бўйича узатилаётган маълумотлар муаллифларини рад этиш;
- маълумотлар (ахборотни) олиш далилини рад этиш;
- олдин узатилган маълумотларни тўхтатиб қўйиш;
- вирусли ҳаракатлар келтириб чиқарган ахборотнинг бузилиши;
- магнит ташувчиларда сақланаётган архивдаги банк ахборотларини бузилиши;
- тизим ташкил этувчилари ва тугунларини ўғирланиши.

Ахборот хавфсизлигигининг асосий тахдид турлари:

1. Техник воситаларда ахборотларни сақланиши ёки рухсатсиз киришдаги қайта ишлашлар;

2. Телекоммуникация каналлари орқали узатилаётган ахборотларни техник воситалар ёрдамида тутиб олиш;

3. Қайта ишланган ахборотларни электромагнит нурланиши орқали чиқиб кетиши (тарқалиши);

4. Техник воситалар электрон қурилмалари ёрдамида ахборотларни тутиб олиш ва объектларни жорий этиш;

5. Телекоммуникация қурилмалари ишида ишдаш чиқиш ёки ахборотларни бузилиши, чақирувчи бузилишлар, махсус дастурий техник таъсирлар.

Ташкилотнинг ҳимоялаш тизимига бўлган ҳақиқий эҳтиёжини аниқлаш ва хавфсизликнинг мавжуд барча хилма-хил чораларидан кераклигини танлашда турли ёндашишлардан фойдаланилади. Бундай ёндашишлардан бири ахборот ҳимоясининг қуйидаги учта жиҳатига асосланган.

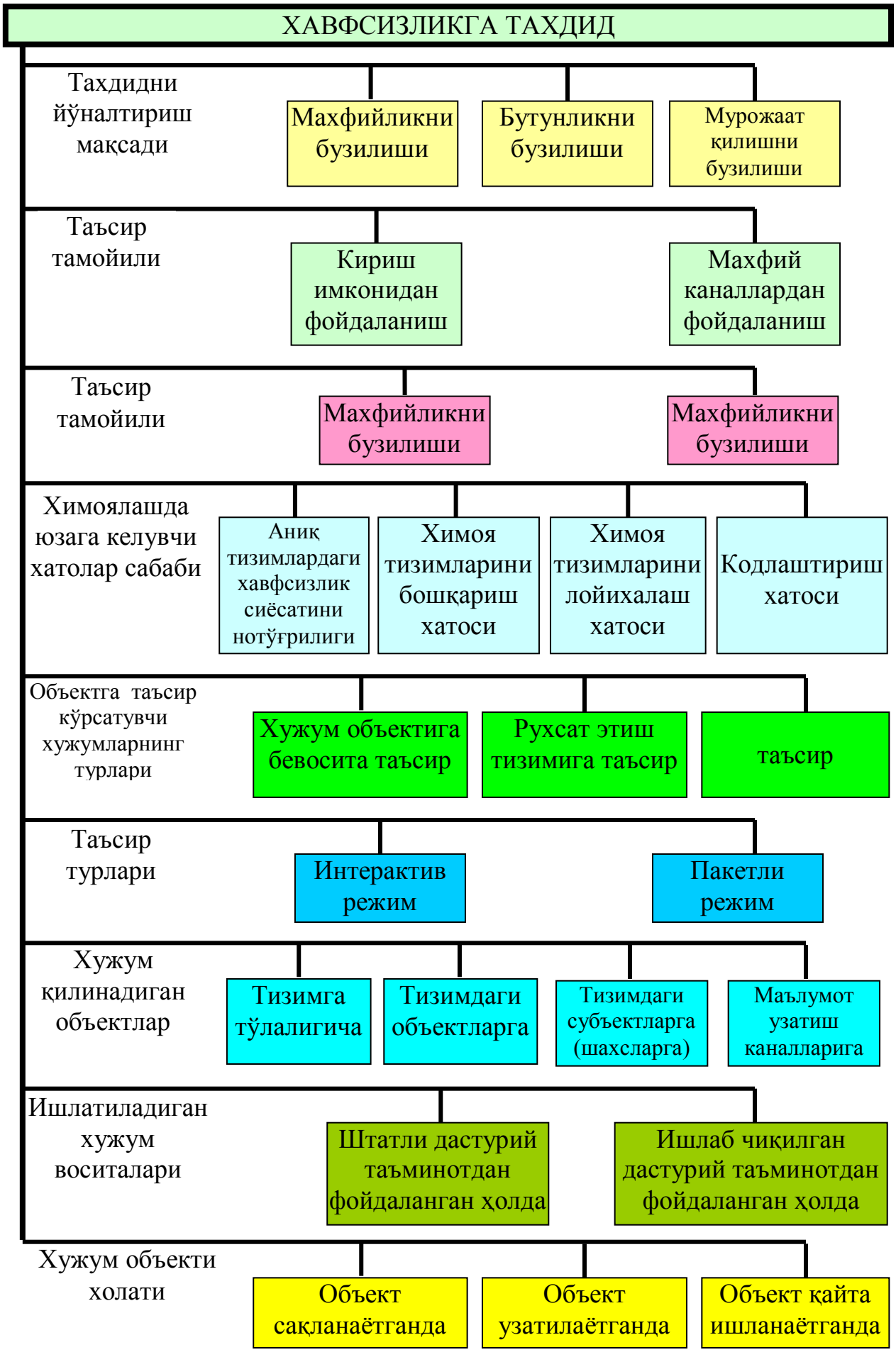
1. Ҳимоянинг бузилишлари. Корхонага тегишли ахборотни сақлаш ва ишлатиш хавфсизлигига зарар келтирувчи ҳар қандай харакатлар.

2. Ҳимоя механизми. Ҳимоянинг бузилишларини аниқлаш ва бартараф этиш, ҳамда бузилишлар оқибатини йўқотиш механизмлари.

3. Ҳимоя хизмати. Маълумотларни ишлаш тизимлари ва корхонага тегишли ахборотни ташиш хавфсизлиги савиясини кўтаришга мўлжалланган сервис хизмати.

Ҳимоянинг бузилишлари. Компьютер тизими ёки тармоғи ҳимоясини бузишга уринишларни компьютер тизимини ахборот билан таъминловчи объект сифатида кўриш орқали классификациялаш мумкин. Умумий ҳолда қандайдир манбадан (масалан, файл ёки хотира қисми) ахборот оқимининг адресатга (масалан, бошқа файл ёки бевосита фойдаланувчи) узатилиши кузатилади. Шу нуқтаи назардан қуйидаги хужумларни фарқлаш мумкин:


Кириш турлари:
-сирли маълумотларни айтиш;
-ахборотни ўғирланиши;
- рухсат этилмаган мурожаат қилиш
Хавф-хатар объектлари:
- иш олиб борилиши, холати ва таркиби хақида маълумот
Химоя йўналиши:
-хуқуқий;
-ташкилий;
- мухандис-техник.
Хавф-хатар:
-бутунлиги;
-махфийлиги;
- тўлиқлиги;
- мурожаат қилиш.
АХБОРОТ
Химоя воситалари:
-физик;
-аппаратли;
- дастурли;
-криптографик.
Хавф-хатар манбаълари:
-рақобатчилар;
-жиноятчилар;
- коррупционерлар;
-ташкилий қўмиталар.
Мақсад:
-танишув;
-модификация;
- йўқотиш.
Ахборот манбалари:
-одамлар;
-хужжатлар;
- нашриётлар;
-техник ташувчилар;
-техник воситалар;
-чиқинди (мусор)
Химоя усуллари:
-олдини олиш;
-кесиб ўтиш (чегаралаш);
- қарши ҳаракат.


ХАВФСИЗЛИКГА ТАХДИД
Тахдидни йўналтириш мақсади
Махфийликни бузилиши
Бутунликни бузилиши
Мурожаат қилишни бузилиши
Таъсир тамойили
Кириш имконидан фойдаланиш
Махфий каналлардан фойдаланиш
Таъсир тамойили
Махфийликни бузилиши
Махфийликни бузилиши
Химоялашда юзага келувчи хатолар сабаби
Аниқ тизимлардаги хавфсизлик сиёсатини нотўғрилиги
Химоя тизимларини бошқариш хатоси
Химоя тизимларини лойихалаш хатоси
Кодлаштириш хатоси
Объектга таъсир кўрсатувчи хужумларнинг турлари
Хужум объектига бевосита таъсир
Рухсат этиш тизимига таъсир
таъсир
Таъсир турлари
Интерактив режим
Пакетли режим
Хужум қилинадиган объектлар
Тизимга тўлалигича
Тизимдаги объектларга
Тизимдаги субъектларга (шахсларга)
Маълумот узатиш каналларига
Ишлатиладиган хужум воситалари
Штатли дастурий таъминотдан фойдаланган ҳолда
Ишлаб чиқилган дастурий таъминотдан фойдаланган ҳолда
Хужум объекти холати
Объект сақланаётганда
Объект узатилаётганда
Объект қайта ишланаётганда

- Узиш (разъединение);
- Ушлаб қолиш (перехват);
- Турлаш (модификация);
- Сохталаштириш (фальсификация).

Узиш (разъединение). Тизим ресурси йўқ қилинади, ахборотдан фойдаланувчанлик бузилади. Бундай бузилишларга мисол тариқасида ускунанинг ишдан чиқиши, алоқа линиясининг узилиши ёки файлларни бошқарувчи тизимнинг бузилишини кўрсатиш мумкин.

Ушлаб қолиш (перехват). Ресурсдан рухсат берилмаган фойдаланишга йўл очилади. Натижада ахборотнинг *махфийлиги (конфиденциаллиги)* бузилади. Бундай фойдаланувчилар физик шахс, дастур ёки компьютер бўлиши мумкин. Бундай бузилишларга мисол тариқасида маълумотларни ушлаб қолиш мақсадида алоқа кабелига уланиш ва файллардан ёки дастурлардан ноқонуний нусха кўчиришни кўрсатиш мумкин.

Турлаш (модификация). Ресурсдан нафақат ноқонуний фойдаланишга йўл очилади, балки ресурс бузғунчи томонидан ўзгартирилади. Натижада ахборотнинг яхлитлиги бузилади. Бундай бузилишларга мисол тариқасида файлдаги маълумотлар мазмунини ўзгартирилишини, дастурнинг вазифалари ва характеристкаларини ўзгартириш мақсадида уни модификациялашни, тармоқ орқали узатилаётган ахборотлар мазмунини ўзгартирилишини ва ҳ. кўрсатиш мумкин.

Сохталаштириш (фальсификация). Тизимга сохта объект киритилади. Натижада ахборотнинг аслига тўғрилиги бузилади. Бундай бузилишларга мисол тариқасида тармоқ орқали ясама маълумотларни узатиш ёки файлга ёзувларни қўшишни кўрсатиш мумкин.

Юқорида келтирилган бузилишлар ***пассив*** ва ***актив*** хужум атамалари бўйича классификацияланганида пассив тахдидга ушлаб қолиш (перехват) мансуб бўлса, узиш (разъединение), турлаш (модификация) ва

сохталаштириш (фальсификация) актив тахдидга мансуб эканлигини кўриш қийин эмас.

Пассив хужумлар натижасида узатилаётган маълумотлар ушлаб қолинади ёки мониторинг амалга оширилади. Бунда бузғунчининг мақсади узатилаётган ахборотни ушлаб қолишдир. Пассив бузилишларни иккита гурухга ажратиш мумкин: ахборотлар мазмунини фош этиш ва маълумотлар оқимини тахлил этиш.

Ахборотлар мазмунини фош этиш нима эканлиги маълум. Телефон орқали сухбатда, электрон почта ахборотида ёки узатилаётган файлда муҳим ёки махфий ахборот бўлиши мумкин. Табиийки, бундай ахборот билан бу ахборот мўлжалланмаган шахсларнинг танишиши мақбул эмас.

Маълумотлар оқимини тахлили мукаммалроқ хисобланади. Фараз қилайлик, биз ахборот ёки бошқа узатилувчи маълумотлар мазмунини шундай маскировка қилайликки, бузғунчи ахборотни ўз ихтиёрига киритганида ҳам ундаги ахборотни чиқариб ололмасин. Кўпинча ахборот мазмунини маскировка қилишда шифрлаш қўлланилади. Аммо, ахборот мазмуни шифрлаш ёрдамида ишончли тарзда беркитилган бўлсада, бузғунчида узатилувчи маълумотларнинг ўзига ҳос аломатларини кузатиш имконияти қолади. Масалан, узатувчини ва ахборотларни узатишга ишлатилувчи тугунларни, ахборотлар узунлигини ва уларнинг алмашинув частотасини аниқлаш мумкин. Бундай ахборот маълумотлар алмашинувидан кўзланган мақсадни аниқлашда жуда ҳам қўл келиши мумкин.

Ҳимоянинг пассив бузилишларини аниқлаш жуда қийин, чунки уларда маълумотларга қандайдир ўзгартиришлар киритиш кўзда тутилмайди. Аммо, бундай хил бузилишларни олдини олишни амалга оширса бўлади. Шу сабабли пассив бузилишлар холида эътиборни уларни аниқлашга эмас, балки уларни олдини олишга қаратиш лозим.

Актив хужумлар натижасида маълумотлар оқими ўзгартирилади ёки сохта оқимлар ҳосил қилинади. Бундай бузилишларни тўртта гурухга

ажратиш мумкин: имитация, тиклаш, ахборотни турлаш (модификациялаш), хизмат кўрсатишдаги халақитлар.

Имитация деганда объектнинг ўзини бошқа объект қилиб кўрсатиши тушунилади. Одатда имитация актив бузилишларнинг бошқа бир хилининг уриниши билан биргаликда бажарилади. Масалан, бузғунчи тизимлар алмашинаётган аутентификация маълумотларининг оқимини ушлаб қолиб сўнгра аутентификация ахборотларининг ҳақиқий кетма-кетлигини тиклаши мумкин. Бу эса ваколати чегараланган объектнинг ўзини ваколати кенгроқ объект қилиб кўрсатиши (имитация) орқали ваколатини кенгайтиришига имкон беради.

Тиклаш деганда маълумотлар блокини пассив ушлаб қолиб, кейин уни рухсат берилмаган натижани ҳосил қилиш мақсадида ретрансляция қилиш тушунилади.

Маълумотларни модификациялаш деганда рухсат берилмаган натижани ҳосил қилиш мақсадида қонуний ахборот қисмини ўзгартириш, ёки ахборот келиши кетма-кетлигини ўзгартириш тушунилади.

Хизмат кўрсатишдаги халақитлар алоқа ёки уларни бошқарувчи воситаларнинг нормал ишлашига тўсқинлик қилади. Бундай бузилишларда муайян мақсад кўзланади: масалан, объект маълум адресатга йўналтирилган барча ахборотларни тўхтатиб қолиши мумкин. Яна бир мисол, тармоқни атайин ахборотлар оқими билан ортиқча юклаш орқали ёки тармоқни ишдан чиқариш йўли билан барча тармоқ ишини блокировка қилиш.

Ҳимоянинг актив бузилишларини бутунлай олдини олиш жуда мураккаб, чунки бунга фақат барча алоқа воситаларини узлуксиз физик ҳимоялаш орқали эришиш мумкин. Шу сабабли ҳимоянинг актив бузилишларида асосий мақсад уларни оператив тарзда аниқлаш ва тездан тизимнинг ишга лаёқатлилигини тиклаш бўлиши шарт. Бузилишларнинг ўз вактида аниқланиши бузғунчини тўхтатиш вазифасини хам ўтайди, ва бу вазифани бузилишлардан огохлантириш тизимнинг қисми деб кўриш мумкин.

Ҳимоя механизмлари. Амалиётда ишлатиладиган химоя механизмларининг аксарияти криптография усулларига асосланган. Шифрлаш ёки шифрлашга яқин ахборотни ўзгартиришлар маьлумотларни химоялаш усуллари хисобланади.

1.3. Ахборот хавфсизлигини таъминлаш чораларининг таснифи

Компьютер тизимларини ахборот хавфсизлиги хавфини амалга ошириш жуда мураккаб ва хавфли оқибатлар билан боғлангандир. Уларга қуйидагилар тегишлидир:

- физик бутунликни бузиш - ахборот сифатини бузишга ёки уни тўлиқ йўқ қилишга йўналтирилган, айниқса ахборотни узатиш тизимларида ва телекоммуникация ва радиотехник тизимларнинг компьютер тармоқларида;

- рухсат этилмаган ўзгартириш - у турли хил хужжатларда, хисобларда ва маълумотлар базаларида берилганларни қалбакилашишига ёки халақитларга учрашига олиб келиши мумкин;

- рухсат этилмаган олиш - махфий ахборотни бевосита компьютер тизимларидан ва тармоқларидан уларга уланиш йўли билан ўғирлаш ёки ахборот ташувчиларни ва бошқаларни ўғирлаш билан тавсифлидир;

- рухсат этилмаган кўпайтириш - дастурларни ва берилганларни нусхалашга йўналтирилган.

1.1-жадвалда компьютер тизимлари ва тармоқларини хавфсизлиги хавфларини, уларни ташкил этувчиларига таъсир этилганда амалга оширишни асосий йўллари кўрсатилган.

1.1- жадвал

№	Таъсир этиш объектлари	Ахборот махфийлигини бузилиши	Ахборот бутунлигини бузилиши	Тизимни ишга лаёқатлигини бузилиши
1	Аппарат воситалари	Рухсат этилмаган уланиш; ресурсларни ишлатиш; ташувчиларни ўғрилаш	Рухсат этилмаган уланиш; ресурсларни ишлатиш; режимларни ўзгартириш	Режимларни рухсат этилмаган ўзгартириш; ишдан чиқариш; бузиш.
2	Дастур таъминоти	Рухсат этилмаган нусхалаш; ушлаб олиш	Рухсат этилмаган мурожаат этиш; «Троян оти» ва «Чувалчанглар» вирусларни, тадбиқ қилиш	Рухсат этилмаган халақитга учраш; ўчириш; алмаштириш
3	Маълумотлар	Рухсат этилмаган нусхалаш; ўғрилаш; ушлаб олиш.	Рухсат этилмаган халақитга учраш; ўзгартириш.	Рухсат этилмаган халақитга учраш; ўчириш; алмаштириш
4	Ходимлар	Сирни очиб қўйиш; ахборотни химоя қилиш тизими тўғрисида маълумотларни узатиш; совуққонлик.	шантаж қилиш; ходимни сотиб олиш	Иш жойидан кетиш; физик бартараф этиш.

Компьютер тизимлари ва тармоқларининг ахборот хавфсизлигини таъминлаш. Амалга ошириш усуллари бўйича компьютер тизимларининг хавфсизлигини таъминлашнинг барча чоралари қуйидагиларга бўлинадилар:

- ҳуқуқий (қонунчилик);
- ахлоқ- этикали;
- физикавий;
- аппарат - дастурли;
- технологик.

Химоя қилинаётган ахборотгача етиб бориш учун химоя қилишнинг бир неча чегараларини кетма-кет босиб ўтиш керак.

Хуқуқий. Ахборотни химоя қилишнинг бу жихати ахборотни узатишда ва қайта ишлашдан юридик меёрларга риоя қилишни зарурлиги билан боғлангандир. Ахборотни химоя қилишни хуқуқий меёрларига мамлакатда харакатда бўлган қонунлар, буйруқлар ва бошқа меёрий далолатномалар тегишлидир.

Ахлоқ - этика. Химоя қилиш талабларига риоя қилишнинг этика моменти жуда катта ахамиятга эгадир. Компьютер тизимларига мурожаат қиладиган одамлар соғлом ахлоқ - этика муҳитида ишлашлари жуда муҳимдир. Меёрлар қонунчилик томонидан тасдиқланган, лекин мажбурий ҳисобланмайди, лекин уларга риоя қилмаслик одатда инсонни шахслар гурухларини ёки ташкилотларни обрўсини пасайишига олиб келади.

Маъмурий. Барча тоифали маъмуриятлар хуқуқий меёрларини ва ижтимоий жиҳатларни ҳисобга олган ҳолда ахборотни ҳимоя қилишни маъмурий чораларини аниклайдилар. Улар қуйидагиларни назорат қиладилар:

- КТ ва Т ларининг ишлаш жараёнини;
- тизимнинг барча ресурсларини ишлатилишини;
- ходимларнинг фаолиятини;
- фойдаланувчиларнинг тизим билан ўзаро таъсирлашиш тартибини (бунда хавфсизлик хавфларини амалга ошириш имкониятини юқори даражада қийинлаштириш ёки инкор қилиш кўзда тутилади).

Маъмурий чоралар қуйидагиларни ўз ичига оладилар:

- КТ ва Т ларида ахборотни қайта ишлаш қоидаларини қайта ишлаб чиқишни;
- жиҳозларни, компьютер тизимлари ва тармоқларини, воситаларни лойихалашда ва монтаж қилишдаги ҳаракатлар тўплами (ёнғинларни,ер қимирлашларни, биноларни қўриқлашни ва ҳакозо таъсирларини иноботга олиш);

- мутахассис ва ходимларни танлаш ва тайёрлашдаги ҳаракатлар тўплами (янги ходимларни текшириш, уларни махфий ахборот билан ишлаш тартиби билан таништириш, уни қайта ишлаш қоидаларини бузганлиги учун жавобгарлик чоралари билан таништириш, ходимларни ўз мансабларидан фойдаланишдан фойда бўлмаган шароитларни яратиш ва х.к.);

- ишончли ўтиш режимини ташкил этиш;

- хужжатларни ва махфий ахборотларни ташувчиларни ҳисобга олишни, сақлашни, ишлатишни ва йўқотишни ташкил этиш;

- мурожаат қилиш чекланишларни, реквизитларини тақсимлаш (паролларни, калитларни, ваколатларни ва хок.);

- тизимдан фойдаланувчи ва ходимларнинг ишлашини устидан ёпиқ (билдирмасдан) назорат қилишни ташкил килиш.

Физик чора, ашаддий бузғунчиларни тизимнинг ташкил этувчиларига ва химоя килинаётган ахборотга кириб олишнинг мумкин бўлган йўлларида физик тўсиқларни яратиш учун махсус мўлжалланган турли кўринишдаги механик электрик ва электрон қўлланмалар ва иншоотлар тегишлидир.

Аппарат - дастурли воситалар. Уларга мустақил ёки бошқа воситалар билан биргаликда тизимларнинг ахборот хавфсизлигини таъминлайдиган қуйидаги усулларни амалга оширадиган турли хил электрон курилмалар ва махсус дастурлар кирадилар:

- тизим субъектларини идентификациялаш (англаш) ва аутентификациялаш;
- КТ ва Т ларини ресурсларига мурожаат қилишни чеклаш;
- ахборот бутунлигини назорат килиш;
- ахборот махфийлигини таъминлаш;
- тизимларда бўлаётган ходисаларни қайд этиш ва тахлил килиш;
- КТ ва Т ресурсларини ва ташкил этувчиларни заҳиралаш.

Химоя қилишнинг технологик чораси, бу берилганларни қайта ишлашнинг технологик жараёнларига органик созланадиган тадбирлар тўпламидир. Уларга қуйидагилар киради:

- ахборот ташувчиларини архив нусхаларини яратиш;

- тизимнинг ташқи хотираларида қайта ишланаётган файлларни дастаки ёки автоматик сақлаш;

- КТ ва Т лари фойдаланувчиларни махсус журналларда қайд этиш;

- фойдаланувчиларни у ёки бу ресурсларга мурожаат қилишни автоматик қайд килиш;

- барча технологик жараёнларни ва жараёнларини бажариш бўйича махсус йўриқномаларни ишлаб чиқиш.

ХУЛОСА

БМИ нинг биринчи бўлимида қуйидаги масалалар келтирилган:

- тармоқнинг ташкил этилиши ва уларга қўйиладиган талаблар, асосан тармоқнинг ташкмл этилиши, тармоқ элементлари, уларнинг вазифалари ва хусусиятлари, тармоқ тузилмалари компонентлари, тармоқнинг функционал модели, коммутация усуллари;

- ахборот хавфсизлигини бузилишига олиб келувчи тахдидларнинг турлари ва уларнинг таснифлари, химоянинг бузилишлари, пассив хужумлар, маълумотлар оқимини тахлили, ахборотлар мазмунини фош этиш, химоя механизмлари;

- ахборот хавфсизлигини таъминлаш чоралари таснифлари, компьютер тизимлари ва тармоқларининг ахборот хавфсизлигини таъминлаш ва аппарат дастурли воситалар кўриб ўтилган.

2. МАЪЛУМОТ УЗАТИШ ТАРМОҚЛАРИНИ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ТАМОЙИЛЛАРИ

2.1. Ўзаро очиқ тизимларнинг эталон моделини хавфсизлик архитектураси ахборот хавфсизлигининг хизматлари ва механизмлари

Очиқ тизимларнинг тавсифлари ва воситаларини аниқлайдиган концептуал асоси сифатида OSI (Open System Interconnection) эталон модели ишлатилади. У очиқ тизимларнинг турли ишлаб чиқарувчилар томонидан тавсия этилган тизимларнинг бир тармоқда ишлашини таъминловчи ўзаро боғланишини аниқлайди ва қуйидагиларни мувофиқлаштиради:

- қўлланиш жараёнларнинг ўзаро боғланишини;
- маълумотларни тақдим этиш шаклларини;
- маълумотлар сақланиши бир хиллигини;
- тармоқ ресурсларини бошқариш;
- маълумотлар хавфсизлиги ва ахборот ҳимоясини;
- дастурлар ва техник воситаларнинг диагностикасини.

Очиқ тизимларнинг стандарт ҳолатдаги ўзаро боғланиши қуйидагича:

1. ўзаро очиқ тизимнинг эталон модели;
2. эталон моделини қаноатлантирадиган хизматларнинг аниқ тўплами;
3. хизматлар бажарилишини таъминловчи ва уларни амалга ошириш учун ишлаб чиқилган протоколлар тўплами.

Хизмат - юқори даража компонентлари ихтиёрига бериладиган жорий даражага тегишли функционал имкониятлар тўпламидир.

Протокол - ҳар-хил техник қурилмаларда ишлатиладиган, бир хил жараёнлар орасидаги мантиқий ва процедурали боғланишни таъминловчи қоидалар тўплами.

Интерфейс - иккита қурилма ёки тизимлар ости чегарасида уларнинг тўлиқ бирга ишлашини таъминловчи қурилмалар ва процедуралар тўплами. Интерфейс электрик, механик ва функционал боғланишларни таъминлайди.

Протоколларнинг функциялари:

7–амалий поғонаси (прикладн. протокол) моделнинг энг юқори поғонаси бўлиб, қўлланиш жараёнларининг тармоқ хизматларига кириш учун имкон яратади ва қуйидагиларни таминлайди:

- очиқ тизимларни ўзаро боғланиш муҳити билан фойдаланувчиларнинг амалий дастурларни бирга ишлашини;
- ахборот алмашиш бўйича шерикларни (партнерларни) идентификациялаш;
- маълумотлар ҳажмини аниқлаш;
- конфеденциалликни таъминлаш механизмини мувофиқлаштириш;
- хизмат кўрсатиш сифатини мувофиқлаштириш;
- хизмат кўрсатиш тартибини танлашларни таъминлайди.

6–тақдим этиш поғонаси (представительн. протокол) қуйидагиларни таъминлайди:

- юборувчи ва қабул қилувчи синтаксисларни тармоққа узатиш синтаксиси билан мувофиқлаштириш;
- сўров орқали сеанс ўрнатиш ва якунлаш;
- ахборот юборишларни таъминлайди.

Тақдимот поғонаси протоколларни қайта ўзгартириш, маълумотлар трансляцияси, қўлланилаётган символлар тўпламини алмаштириш кабиларга жавоб беради.

5-сеанс поғонаси (протокол сеансовый) сеанс бошланиши ва якунланишини, транспорт тармоғи даражасида ишдан чиқиш (ишламаслик) ҳолатларида қайта улашни амалга оширишни таъминлайди.

4-транспорт поғонаси (транспортн. протокол) транспорт поғонасининг асосий вазифаси пакетларни хатосиз, дастлабки кетма-кетликда йўқотишсизларсиз кафолат билан етказиб беришдир. Бу поғонада

маълумотлар қайта тахланади: узунлари бир нечта пакетларга ажратилади, қисқа пакетлар эса бирлаштирилади. Шу орқали тармоқдан пакетларни юбориш самарадорлиги оширилади. Транспорт поғонасида қабул қилувчи томонидан маълумотлар қабул қилингани хақида тасдиқ сигнали юборилади.

Траспорт поғонаси оқимни бошқаради, хатоларни текширади, пакетларни юбориш ва қабул қилиш билан боғлиқ бўлган муаммоларни ҳал қилишда иштирок этади.

3-тармоқ поғонаси (сетевой протокол) қуйидагиларни таъминлайди:

- фойдаланаётган тармоқ ва физик муҳитларни коммутациялаш;
- маршрутизациялашга боғлиқ бўлмаган транспорт тармоқ даражаси учун ахборотларни узатилишни таъминловчи тармоқ уланишларни ўрнатиш;
- фаол ҳолда тутиш ва узиш воситаларини етгазиб бериш;
- маълумот оқимларини бошқарилишини таъминлаш;
- пакетлар жўнатилиши кетма – кетлигини тартибга солиш;
- шошилинч маълумот узатилишини таъминлаш;
- хатоларни топиш ва тузатилишини таъминлаш.

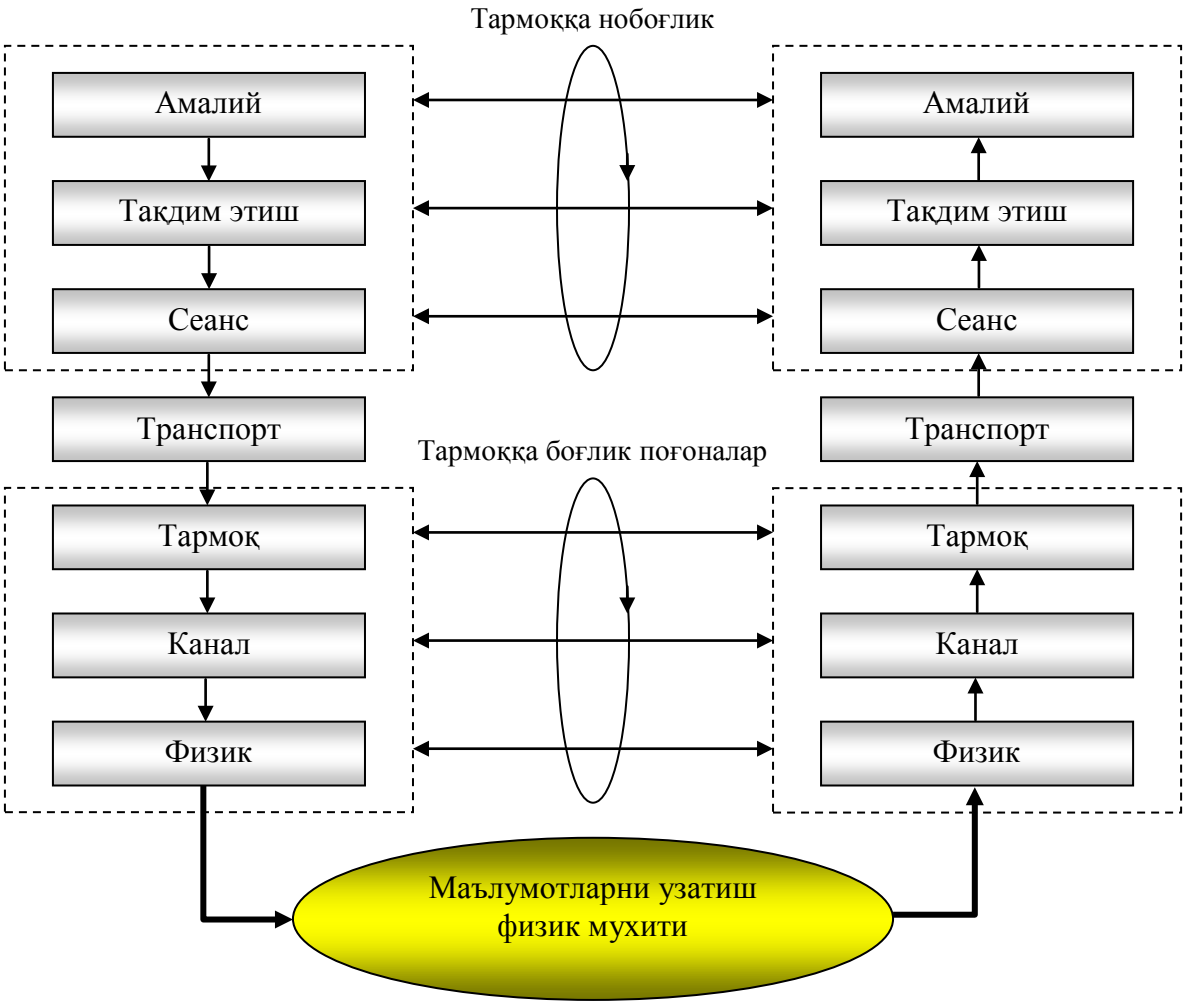
Тармоқ поғонасининг маълумотларини пакетлар деб аташ қабул қилинган. Тармоқ поғонасида 2 хил протоколлар ишлайди.

1. тармоқ протоколлари – тармоқ орқали пакетларни ҳаракатини йўлга қўяди;
2. маршрутлаш протоколлари – маршрутизатор тармоқлараро боғланишлар топологияси тўғрисида ахборот тўплайдилар.

2–канал поғонаси (канальн. пратокол) канал узатишларини ўрнатади ва узатади, кадрлар бўйича синхронизациялашни таъминлайди, хатоларни топиш ва тузатиш ахборот оқимини бошқариш, кадрлар кетма - кетлигини тартибга солишларни таъминлайди.

1-физик поғона (протокол физический) физикавий каналлар коаксиал кабель, оптик толали кабель ёки радиомуҳит орқали битлар кетма-кетлиги билан иш олиб боради. Физик поғона физик улашларни ўрнатиш, фаол ҳолатда тутиш ва ўзини механик, электрон ва процедурали

воситаларини бошқариш, битлар бўйича синхронизациялаш, битларни дуплекс ёки ярим дуплексли узатиш, икки ёки кўп нуқтали узатиш, физик даражада ишдан чиқиш холатлари тўғрисида канал даражасини огоҳлантиришларни таъминлайди.



2.1 – расм. Очиқ тизимлар ўзаро боғланиш эталон модели.

Хизмат турлари	Поғоналар					
	Физик	Канал	Тармоқ	Транспорт	Сеанс	Т
поғонали объектлар аутентификацияси			+	+		
ълумотлар манбаъи аутентификацияси			+	+		
риш йўли назорати			+	+		
ш ўрнатишли алоқа конфиденциаллиги	+	+	+	+		
ш ўрнатишсиз алоқа конфиденциаллиги		+	+	+		
ийрий танланган майдонлар фиденциаллиги						
ълумотлар оқими конфиденциаллиги	+		+			
ланишли уланиш бутунлиги				+		
ланишсиз уланиш бутунлиги			+	+		
нишнинг ажратилган майдони унлиги						
ш ўрнатишсиз боғланиш бутунлиги			+	+		
нишсиз ажратилган майдон бутунлиги						
ъбаъни тасдиқлаб рад этишлардан химоя						
азиб беришни тасдиқлаб рад этишлардан оя						

Хавфсизликни таъминлашни хизматлари ва механизмларини ўзаро боғлиқлиги

Механизм / Хизмат	Шифрлаш	Рақамли имзо	Кириш йўли назорати	Маълумот-лар бутунлиги	Алмашув аутентиф-икацияси	Марш изаци бошқа
лоғонали объектлар нтификацияси	+	+			+	
лумотлар манбаъи аутентификацияси	+	+				
риш йўли назорати			+			
ш ўрнатишли алоқа фиденциаллиги	+					
ш ўрнатишсиз алоқа фиденциаллиги	+					
ийрий танланган майдонлар фиденциаллиги	+					
лумотлар оқими конфиденциаллиги	+					+
ланишли уланиш бутунлиги	+			+		
ланишсиз уланиш бутунлиги	+			+		
нишнинг ажратилган майдони унлиги	+			+		
ш ўрнатишсиз боғланиш бутунлиги	+	+		+		
нишсиз ажратилган майдон унлиги	+	+		+		
баъни тасдиқлаб рад этишлардан оя		+		+		
азиб беришни тасдиқлаб рад шлардан химоя		+		+		

2.2. Ахборот хавфсизлигини дастурий - техникавий воситаларининг тузилиши

Химоя қилишнинг ташкилий – дастурий воситалари техник усулларга тегишли бўлади. Бундай усуллар ва воситалар етарлича ктта миқдордадир. Булар тасодифий хавфлардан анъанавий жосуслик ва қўпорувчилик, электромагнит нурланишлардан ва йўналтиришлардан КТ лари тузилмаларини рухсат этилмаган ўзгартиришлардан, рухсат этилмаган мурожаат қилишдан ахборотни химоя қилиш, криптографик усуллар, компьютер вируслари ва улар билан курашиш механизмлари ва бошқалар.

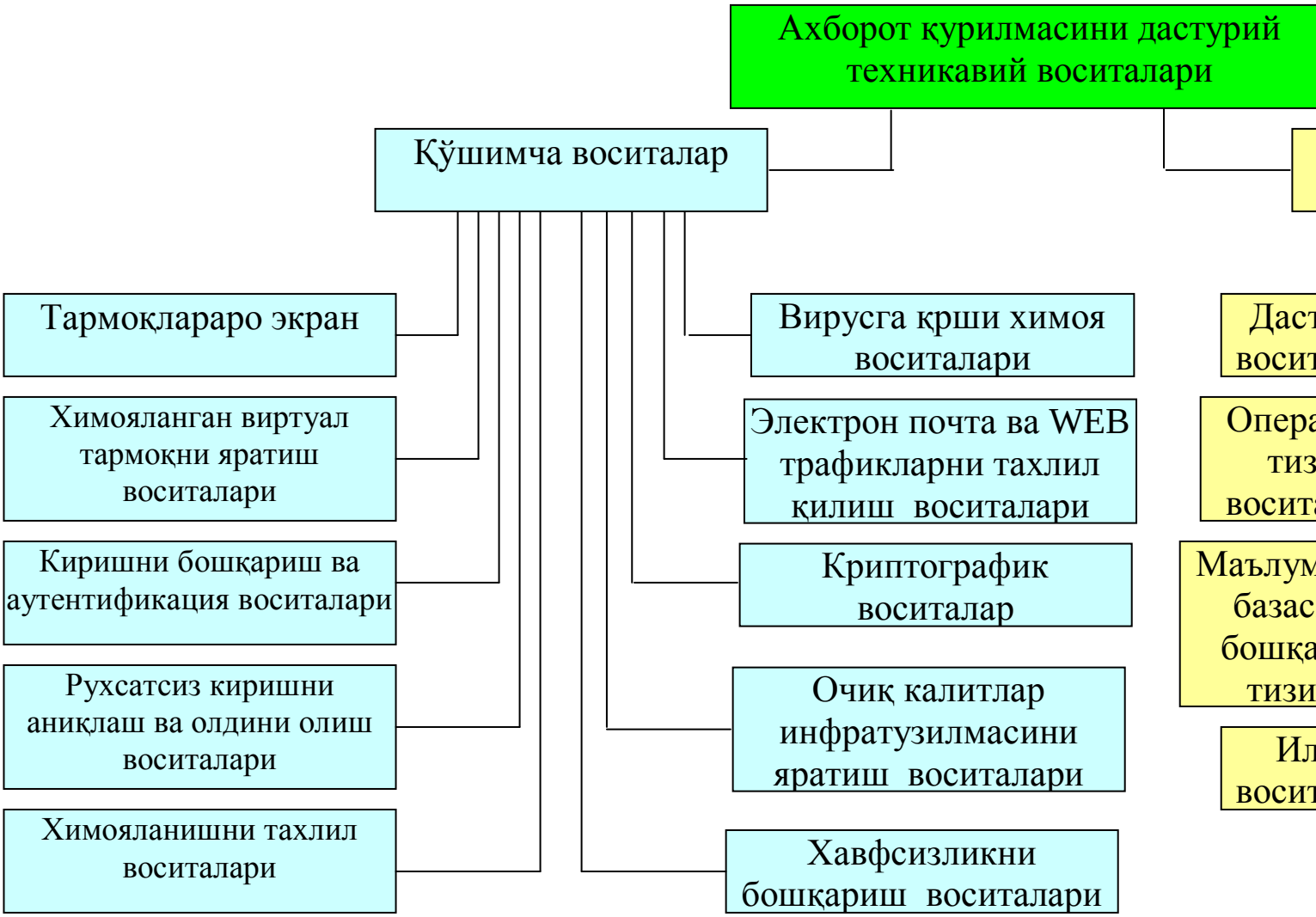
Тасодифий хавфлардан ахборотни химоя қилишга ахборотларни дубллаш, КТ ишончлилигини ошириш, ишдан чиқишларига мустахкам КТ ларини яратиш, халокатлардан ва фавқулодда холатлардан келадиган талофатларни камайтириш, нотўғри амалларни блокировкалаш билан эришилади.

Анъанавий жосусликдан ва қўпорувчиликдан ахборотни химоя қилишда КТ ларидан КТ лари ишлатилмайдиган бошқа объектларни химоя қилиш учун ишлатиладиган восита ва усуллар қўлланилади. Бу тизимнинг вазифаларига объектни қўриқлаш тизимини яратиш, КТ объектларида махфий ахборот ресурслари билан ишлашни ташкил этиш, кузатишга ва билдирмасдан эшитиб олишга хамда ходимларнинг ёмон ниятли харакатларга қарши курашиши киради.

Зарарли электромагнит нурланишдан ва йўналтиришлардан химоя қилиш хам фаол хам пассив усуллар билан амалга оширилади. Химоя қилишнинг фаол усуллари, ёмон ниятли одам томонидан ушлаб олинган хабарлардан фойдали ахборотларни қабул қилиш ва ажратиб олишни мураккаблаштирадиган, зарарли электромагнит нурланишлар ва йўналтирилишлар каналларида халақитларни яратишга қаратилгандир.

Пассив усуллар хавфли хабарни даражасининг камайишини ёки хабарларнинг ахборотланганлигини пасайишини таъминлайдилар.

КТ ларини тузилмасини рухсат этилмаган ўзгартиришлардан химоя қилиш усул ва услублари КТ ларини ишлаб чиқиш ва ишлатиш босқичларида алгоритмик, дастурли ва техник тузилмаларни химоя қилиш учун мўлжаланган. 2.2-расмда ахборот қурилмасини дастурий техникавий воситалари келтирилган.

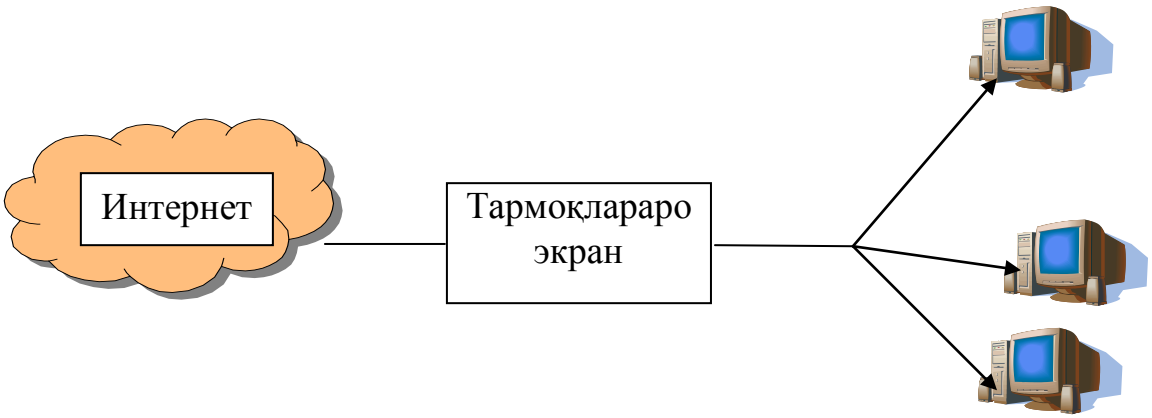


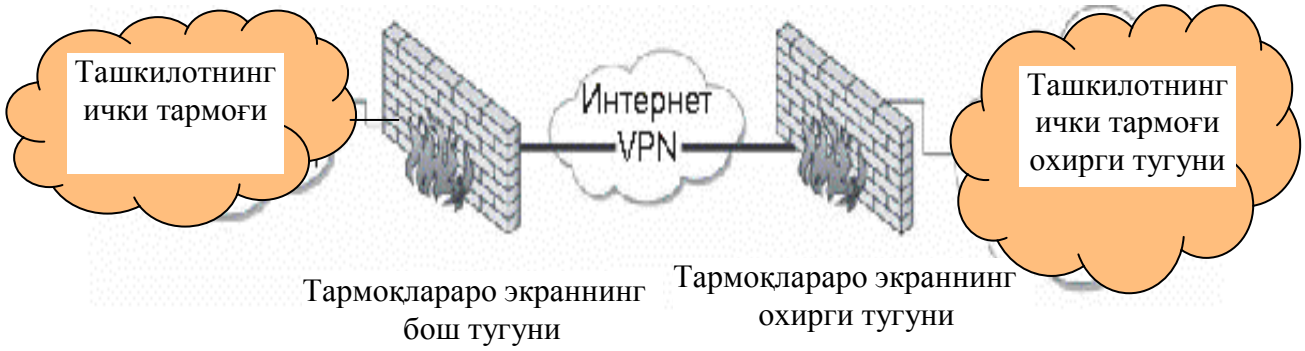
2.2-расм. Ахборот қурилмасини дастурий техникавий воситалари

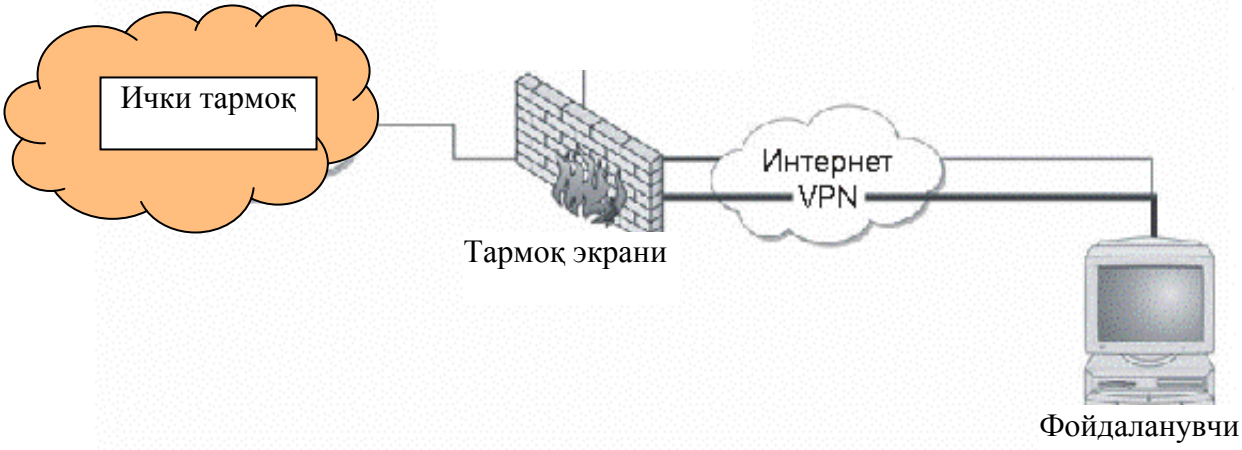
2.3. Тармоқлар оралиги экранлари

Бугун кўпгина компаниялар интернетга локал тармоққа рухсат этилмаган мурожаат қилишга тўсқинлик қиладиган махсус дастур таъминоти билан таъминланган компьютерлар – брандмауэрлар (тармоқлараро экранлар ёки fire Wall) орқали уланмоқдалар.

Локал тармоқда брандмауэрли ўрнатилишнинг асосий сабаби унинг ҳар доим чақирилмаган маехмонлардан ҳимоя қилинишидир. Ёмон ниятли одам томонидан олинган ахборот корхонанинг рақобатбардошлигини ва унинг клиентларини ишончини жиддий бузиб қўйиши мумкин. Ички тармоқлар учун энг эхтимолли хавфларни бартараф этиш бўйича бир қатор масалаларни брандмауэрлар ҳал қилиш қобилиятига эгадирлар. Компьютер мухитидан ташқарида ёнмайдиган материаллардан ва ёнғинни тарқалишига тўсқинлик қиладиган деворни брандмауэр (ёки fire Wall) деб аталади. Компьютер тармоғи мухитида тармоқлараро экран фигурали ёнғиндан ёмон ниятли одамларни ички тармоққа, ахборотни нусхалаш, ўзгартириш ёки ўчириш учун ёки бу тармоқда ишлаётган компьютерлар хотирасидан ёки ҳисоблаш қувватидан фойдаланиш учун кириб олишга интилиши тушунилади (2.3-расм) .







2.3-расм. Тармоқлараро экранни ўрнатиш чизмаси

Тармоқлараро экран (ТЭ) – тармоқлараро ҳимоя қилиш тизими бўлиб, у умумий тармоқни икки ва ундан ортиқ қисмларга ажратишга ва маълумотлар пакетларини чегара орқали умумий тармоқнинг бир

қисмидан бошқа қисмига ўтиш шартларини аниқлайдиган қоидалар тўпламини амалга оширишга имкон яратади. Қоидага кўра, бу чегара корхонанинг корпоратив (локал) тармоғи ва Интернет глобал тармоғи ўртасида ўтказилади, бироқ уни корхонанинг корпоратив тармоғи ичида ҳам ўтказиш мумкин. ТЭ ўзи орқали ҳар бир ўтаётган пакет учун қарорни, уни ўтказиш керакми ёки ташлаб юбориш керакми, қабул қилган ҳолда бутун трафикни ўтказади. ТЭ буни амалга ошира олиш учун у фильтрлашнинг қоидалар тўпламини аниқлаб олиши керак.

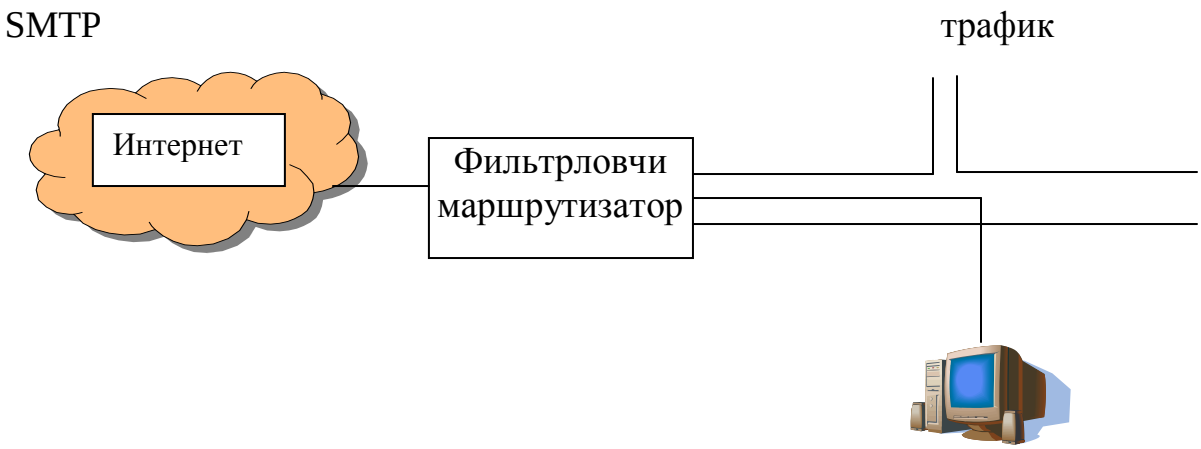
Тармоқлараро экранларнинг асосий ташкил этувчилари.

Тармоқлараро экранларнинг кўпчилик ташкил этувчиларини қуйидаги учта тоифадан биттасига киритиш мумкин:

- фильтрловчи маршрутизаторлар;
- тармоқ даражасидаги шлюзлар;
- амалий даражадаги шлюзлар.

Фильтрловчи маршрутизатор маршрутизатор ёки серверда ишлайдиган дастур кўринишига эга бўлиб, у кирувчи ва чиқувчи пакетларни фильтрлайдиган қилиб тайёрланган бўлади. Пакетларни фильтрлаш пакетларнинг TCP ва IP сарлавхаларида мавжуд бўлган ахборот асосида амалга оширилади.

Филтрлаш аниқ бир хост – компьютерлар билан ишончсиз ёки рақиб деб хисобланган тармоқларнинг ва хост – компьютерларнинг аниқ адреслари алоқаларини блоклаш учун турли кўринишда амалга ошириш мумкин. Масалан, ички тармоқ баъзи бир тизимлардан ташқари барча хост-компьютерлар билан барча ички уланишларни блоклаши мумкин. Бу тизимлар учун фақатгина маълум бир сервисларгина рухсат этилиши мумкин. (SMTP битта тизим учун, TELNET ёки FTP-бошқа тизим учун) (2.4-расм)



2.4-расм. SMTP ва TELNET трафикни фильтрлаш чизмаси

Фильтрловчи маршрутизаторларнинг ижобий сифатларига қуйидагиларни киритиш мумкин:

- нисбатан юқори бўлмаган нархи;
- фильтрлаш қоидаларини аниқлашдаги мослашувчанлик;
- пакетларни ўтишида унчалик катта бўлмаган ушланиб қолишлар.

Фильтрловчи маршрутизаторларнинг камчиликлари қуйидагилар:

- ички тармоқ Интернет тармоғидан кўриниб туради (маршрутланади);
- пакетларни фильтрлаш қоидаларини ёзиб чиқиш қийин. Бунинг учун TCP ва IP технологияларини жуда яхши билиш талаб этилади;
- пакетларни фильтрлашда тармоқлараро экранни ишлаш қобилияти бузилганда барча компьютерлар ундан кейин, тўлиқ ҳимоя қилинмаган ёки мурожаат қилиб бўлмайдиган бўлиб қолади;
- хужум қиладиган тизим IP адресини ишлатиб ўзини бошқа тизим каби кўрсатади.

Тармоқ даражасидаги шлюзни баъзида тармоқ адресларини намойиш қилиш тизими ёки OSI моделининг сеансли даражаси шлюзи деб аталади. Бундай шлюз муаллифлаштирилган клиент ва ташқи хост-компьютер ўртасидаги тўғридан - тўғри ўзаро таъсирни инкор этади.

Тармоқ даражадаги шлюз ишонган клиентни аниқ бир хизматларга сўровини қабул қилади ва сўроқланган сеансни мумкин эканлигини текширгандан кейин ташқи хост-компьютер билан уланишни ўрнатади.

Пакетларни нусхалаш ва қайта йўналтириш учун тармоқ хизматчилари деб аталадиган махсус иловалар қўлланилади, чунки улар икки тармоқ ўртасида виртуал занжир ёки канални ўрнатадилар. Кейин эса TCP/IP иловалари билан хосил қилинаётган пакетларга бу канал бўйича ўтишга рухсат беради. Аслида эса тармоқ даражасидаги кўпчилик шлюзлар мустақил махсулотлар ҳисобланмайди, балки амалий даражадаги шлюзлар билан биргаликда етказиб берилади.

Амалий даражадаги шлюз. Фильтрловчи маршрутизаторларга хос бўлган бир қатор камчиликларни бартараф этиш учун тармоқлараро экранлар TELNET ва FTP туридаги қўшимча дастур воситаларини ишлатиши керак. Бундай дастур воситалари ваколатли сервер (сервер-хизматчилар), улар бажариладиган хост- компьютерлар эса амалий даражадаги шлюз деб аталади. Амалий даражадаги шлюзлар амалий трафик бевосита ички хост – компьютерларга ўтказиб юбориладиган оддий режимга нисбатан бир қатор жиддий афзалликларга эга:

- интернет глобал тармоғидан ҳимоя қилинаётган тармоқ тузилмасининг кўринмаслиги;
- ишончли қайд қилиниши;
- нарх ва самарадорлик ўртасидаги оптимал нисбати;
- фильтрлашнинг оддий қоидалари;
- кўп сонли текширувларни ташкил этиш имконияти.

Амалий даражадаги шлюзларнинг камчиликларига қуйидагилар тегишлидир:

- фильтрловчи маршрутизаторларга нисбатан бирмунча паст унумдорлиги;
- фильтрловчи маршрутизаторларга нисбатан бирмунча юқори нархдалиги.

ХУЛОСА

Иккинчи бўлимда қуйидаги масалалар кўриб ўтилган:

- ўзаро очиқ тизимларнинг эталон моделини хавфсизлик архитектураси, ахборот хавфсизлигининг хизматлари ва механизмлари;

- ахборот хавфсизлигининг дастурий техникавий воситаларининг тузилиши;

- тармоқлар оралиги экранлари ва ўрнатиш чизмаси, тармоқлараро экранларнинг асосий ташкил этувчилари келтирилган.

3. МАЪЛУМОТ УЗАТИШДА ҚЎЛЛАНИЛАДИГАН ТАРМОҚЛАРАРО ЭКРАН ТАХЛИЛИ

3.1. Тармоқлараро экранларнинг ишлаш хусусиятлари

Тармоқлараро экран (ТЭ) - *брандмауэр* ёки *firewall системаси* деб хам аталувчи тармоқлараро химоянинг ихтисослаштирилган комплекси. Тармоқлараро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чегара орқали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи қоидалар тўпламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоғи ва Internet глобал тармоқ орасида ўтказилади. Тармоқлараро экранлар гарчи корхона локал тармоғи уланган корпоратив интратармоғидан қилинувчи хужумлардан химоялашда ишлатилишлари мумкин бўлсада, одатда улар корхона ички тармоғини Internet глобал тармокдан суқилиб киришдан химоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шарти хисобланади.

Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ хисобланувчи ташкилотнинг химояланувчи тармоғи ва ташқи ғаним тармоқ орасида жойланиши лозим (3.1-расм). Бунда бу тармоқлар орасидаги барча алоқа фақат тармоқлараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи назаридан

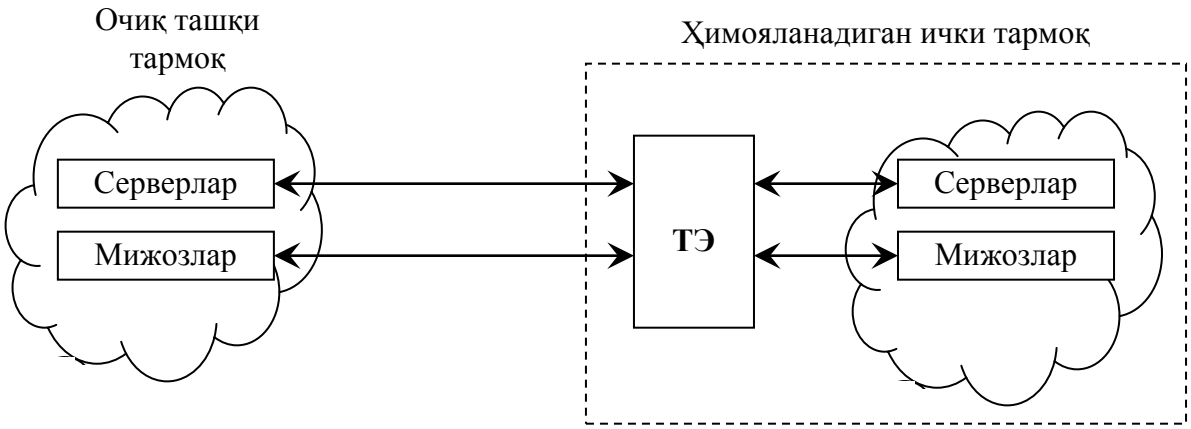
тармоқлараро экран химояланувчи тармоқ таркибига киради.

Ички тармоқнинг кўпгина узелларини бирданига химояловчи тармоқлараро экран қуйидаги иккита вазифани бажариши керак:

- ташқи (химояланувчи тармоққа нисбатан) фойдаланувчиларнинг корпоратив тармоқнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар қаторига тармоқлараро экран химояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар,

масофадаги фойдаланувчилар, хакерлар, хатто компаниянинг ходимлари киритилиши мумкин;

- химояланувчи тармоқдан фойдаланувчиларнинг ташқи ресурслардан фойдаланишларини чегаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.



3.1-расм. Тармоқлараро экранни улаш схемаси.

Хозирда ишлаб чиқарилаётган тармоқлараро экранларнинг тавсифларига асосланган холда, уларни қуйидаги асоси й аломатлари бўйича туркумлаш мумкин:

OSI модели сатхларида ишлаши бўйича:

- пакетли фильтр (экранловчи маршрутизатор – screening router);
- сеанс сатхи шлюзи (экранловчи транспорт);
- татбиқий шлюз (application gateway);
- эксперт сатхи шлюзи (stateful inspection firewall).

Ишлатиладиган технология бўйича:

- протокол холатини назоратлаш (Stateful inspection);
- воситачилар модуллари асосида (proxy);

Бажарилиши бўйича:

- аппарат-дастурий;
- дастурий;

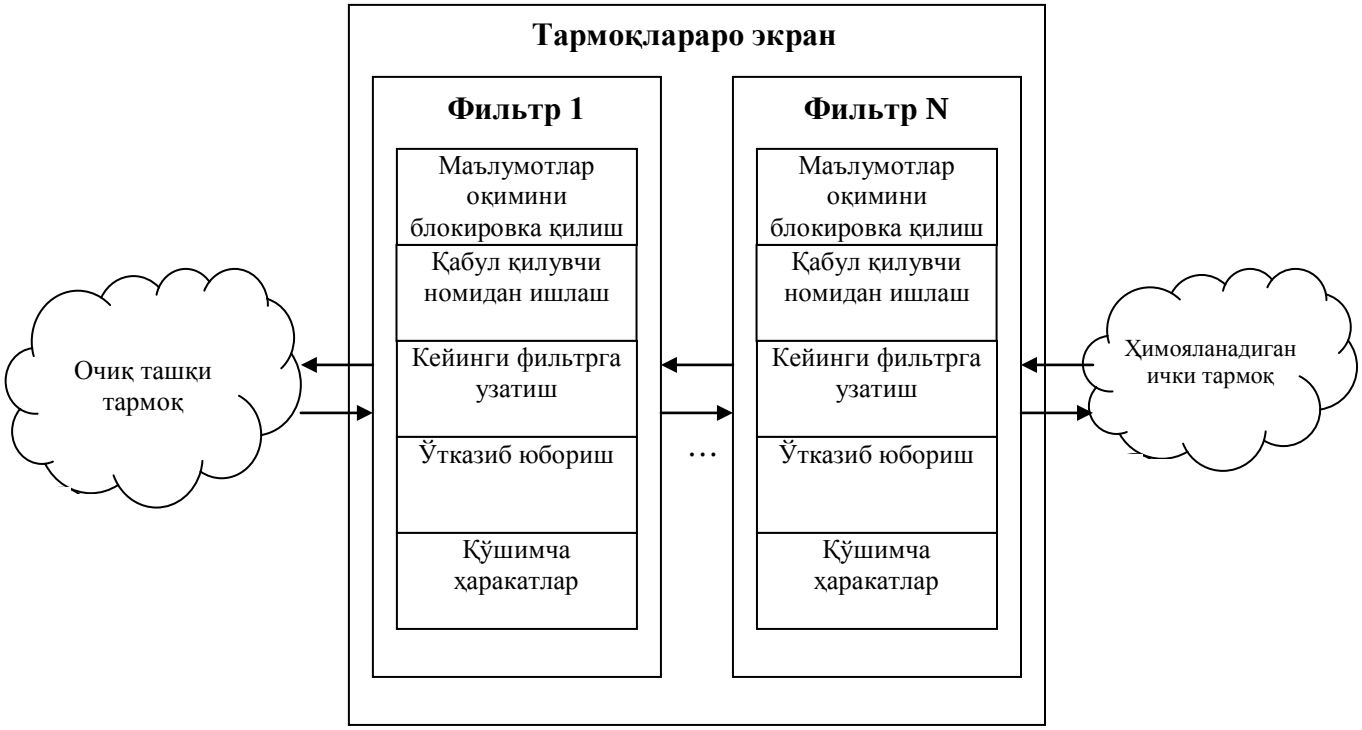
Уланиш схемаси бўйича;

- тармоқни умумий химоялаш схемаси;

- тармоқ сегментлари химояланувчи берк ва тармоқ сегментлари химояланмайдиган очиқ схема;

- тармоқнинг берк ва очиқ сегментларини алохида химояловчи схема.

Трафикларни фильтрлаш. Ахборот оқимларини фильтрлаш уларни экран орқали, баъзида қандайдир ўзгартиришлар билан, ўтказишдан иборат. Фильтрлаш қабул қилинган хавфсизлик сиёсатига мос келувчи, экранга олдиндан юкланган қоидалар асосида амалга оширилади. Шу сабабли тармоқлараро экранни ахборот оқимларини ишловчи фильтрлар кетма-кетлиги сифатида тасаввур этиш қулай (3.2-расм).



3.2-расм. Тармоқлараро экран тузилмаси.

Фильтрларнинг хар бири қуйидаги харакатларни бажариш орқали фильтрлашнинг алохида қоидаларини изохлашга аталган:

1. Ахборотни изохланувчи қоидалардаги берилган мезонлар бўйича тахлиллаш, масалан, қабул қилувчи ва жўнатувчи адреслари ёки ушбу ахборот аталган илова хили бўйича.

2. Изохланувчи қоидалар асосида қуйидаги ечимлардан бирини қабул қилиш:

- маълумотларни ўтказмаслик;

- маълумотларни қабул қилувчи номидан ишлаш ва натижани жўнатувчига қайтариш;

- тахлиллашни давом эттириш учун маълумотларни кейинги фильтрга узатиш;

- кейинги фильтрларга эътибор қилмай маълумотларни узатиш.

Фильтрлаш қоидалари воситачилик функцияларига оид қўшимча, масалан маълумотларни ўзгартириш, ходисаларни қайдлаш ва х. каби харакатларни хам бериши мумкин. Мос холда, фильтрлаш қоидалари қуйидагиларнинг амалга оширилишини таъминловчи шартлар рўйхатини аниқлайди:

- маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

- химоялашнинг қўшимча функцияларини бажариш.

Ахборот оқимини тахлиллаш мезони сифатида қуйидаги параметрлардан фойдаланиш мумкин:

- таркибида тармоқ адреслари, идентификаторлар, интерфейслар адреси, портлар номери ва бошқа мухим маълумотлар бўлган хабар пакетларининг хизматчи хошиялари;

- масалан, компьютер вируслари борлигига текширилувчи хабар пакетларининг бевосита таркиби;

- ахборот оқимининг ташқи характеристикалари, масалан, вақт ва частота характеристикалари маълумотлар хажми ва х.

Ишлатилувчи тахлиллаш мезонлари фильтрлашни амалга оширувчи OSI моделининг сатхларига боғлиқ. Умумий холда, пакетни фильтрлашни амалга оширувчи OSI моделининг сатхи қанчалик юқори бўлса, таъминланувчи химоялаш даражаси хам шунчалик юқори бўлади.

Воситачилик функцияларининг бажарилиши. Тармоқлараро экран воситачилик функцияларини *экранловчи агентлар* ёки *воситачи дастурлар* деб аталувчи махсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар хисобланади ва ташқи ва ички тармоқ орасида хабарлар пакетини бевосита узатишни тақиқлайди.

Ташқи тармоқдан ички тармоқнинг ва аксинча фойдаланиш зарурияти туғилганда аввал тармоқлараро экран компьютерида ишловчи воситачи-дастур билан мантиқий уланиш ўрнатилиши лозим. Воситачи-дастур сўралган тармоқлараро алоқанинг жоизлигини текширади ва ижобий натижада ўзи суралган компьютер билан алохида уланиш ўрнатади. Сўнгра ташқи ва ички тармоқ компьютерлари орасида ахборот алмашиш, хабарлар оқимини фильтрлашни хамда бошқа химоялаш функцияларини бажарувчи дастурий воситачи орқали амалга оширилади.

Таъкидлаш лозимки, тармоқлараро экран фильтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташқи ва ички тармоқ орасида ўзаро алоқанинг шаффофлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар оқимини фильтрлашни амалга оширмаслиги хам мумкин.

Умуман, воситачи-дастурлар, хабарлар оқимини шаффоф узатилишини блокировка қилган холда, қуйидаги функцияларни бажариши мумкин:

- узатилувчи ва қабул қилинувчи маълумотларнинг хақиқийлигини текшириш;
- ички тармоқ ресурсларидан фойдаланишни чегаралаш;
- ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;
- ташқи тармоқдан сўралувчи маълумотларни кэшлаш;
- хабарлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;
- фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- ички тармоқ адресларини трансляциялаш;

- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, хамда қайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш.

Узатилувчи ва қабул қилинувчи маълумотларнинг хақиқийлигини текшириш нафақат электрон хабарларни, балки сохталаштирилиши мумкин бўлган мигрцияланувчи дастурларни (Java, Active X Controls) аутентифкациялаш учун долзарб хисобланади. Хабар ва дастурларнинг хақиқийлигини текшириш уларнинг рақамли имзосини текширишдан иборатдир.

Ички тармоқ ресурсларидан фойдаланишни чегаралаш усуллари операцион тизим сатхида мададланувчи чегаралаш усулларидан фарқ қилмайди.

*Ташқи тармоқ ресурсларидан фойдаланишни чегарлаш*да кўпинча қуйидаги ёндашишлардан бири ишлатилади:

- фақат ташқи тармоқдаги берилган адрес бўйича фойдаланишга рухсат бериш;

- янгиланувчи ножоиз адреслар руйхати бўйича суровларни фильтрлаш ва ўринсиз калит сўзлари бўйича ахборот ресурсларини қидиришни блокировка қилиш:

- маъмур томонидан ташқи тармоқнинг қонуний ресурсларини брандмауэрнинг дискли хотирасида тўплаш ва янгилаш ва ташқи тармоқдан фойдаланишни тўла тақиқлаш.

Ташқи тармоқдан сўралувчи *маълумотларни кэшлаш* махсус воситачилар ёрдамида мададланади. Ички тармоқ фойдаланувчилари ташқи тармоқ ресурсларидан фойдаланганларида барча ахборот, proxy-сервер деб аталувчи брандмауэр қаттиқ диски маконида тўпланади. Шу сабабли, агар навбатдаги сўровда керакли ахборот proxy-серверда бўлса, воситачи уни ташқи тармоққа мурожаатсиз тақдим этади. Бу фойдаланишни жиддий тезлаштиради. Маъмурга фақат proxy-сервер таркибини вақти-вақти билан янгилаб туриш вазифаси қолади.

Кэшлаш функцияси ташқи тармоқ ресурсларидан фойдаланишни чегаралашда муваффақиятли ишлатилиши мумкин. Бу холда ташқи тармоқнинг барча қонуний ресурслари маъмур томонидан proxy-серверда тўпланади ва янгиланади. Ички тармоқ фойдаланувчиларига фақат proxy-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташқи тармоқ ресурсларидан бевосита фойдаланиш эса манн қилинади.

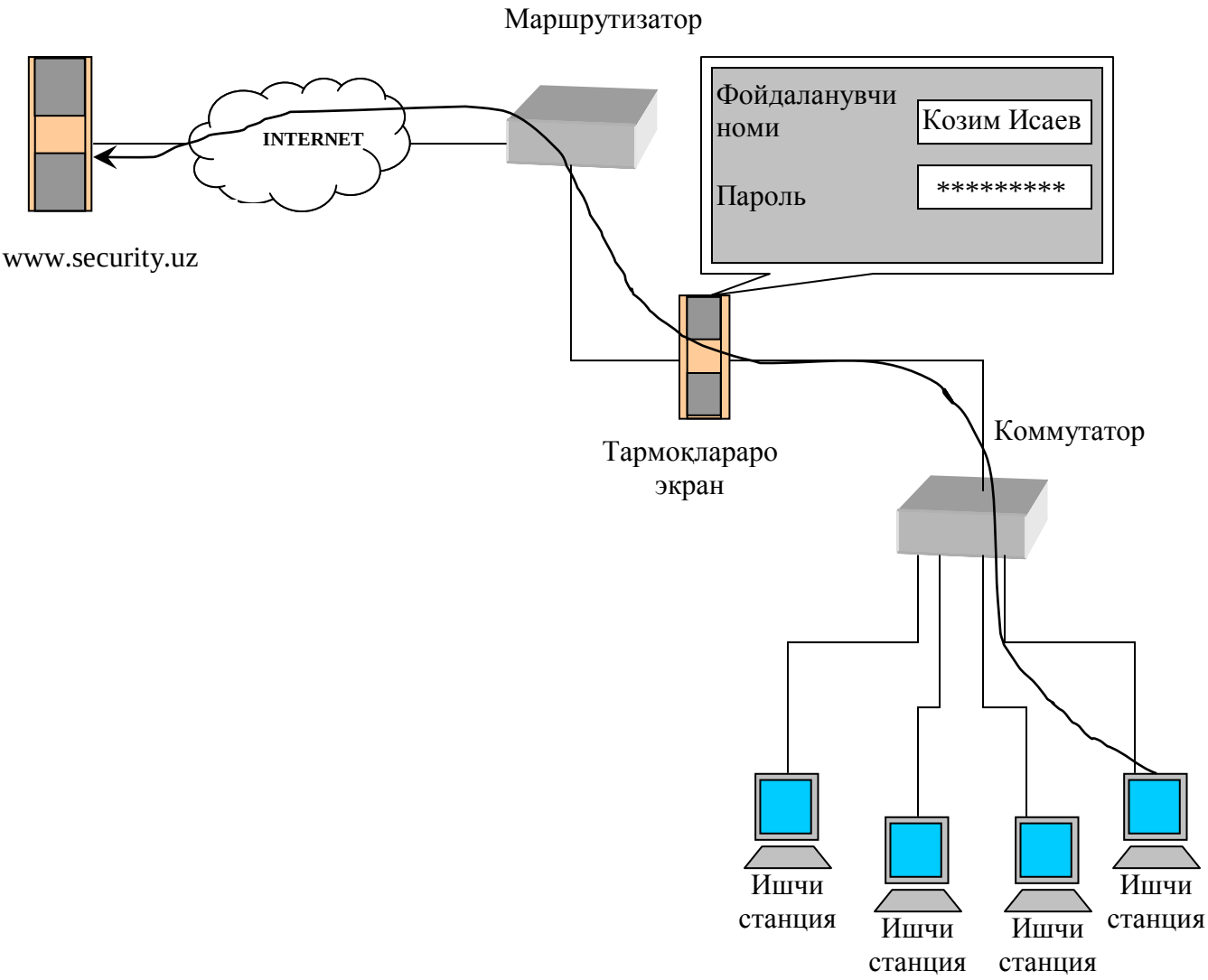
Хабарлар оқимини фильтрлаш ва ўзгартириш воситачи томонидан қоидаларнинг берилган тєплами ёрдамида бажарилади. Бунда воситачи-дастурларнинг икки хили фарқланади:

- сервис турини аниқлаш учун хабарлар оқимини тахлиллашга мўлжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

- барча хабарлар оқимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини қидириб зарарсизлантиришга ёки маълумотларни шаффоф шифрлашга мўлжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини тахлиллайди ва агар қандайдир объект берилган мезонларга мос келмаса, воситачи унинг кейинги силжишини блокировка қилади ёки мос ўзгаришини, масалан, ошкор қилинган компьютер вирусларни зарарсизлантиришни бажаради. Пакетлар таркибини тахлиллашда экранловчи агентнинг ўтувчи файлли архивларни автоматик тарзда оча олиши мухим хисобланади.

Фойдаланувчиларни идентификациялаш ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни тақдим этиш билан амалга оширилади (3.3-расм). Аммо бу схема хавфсизлик нуқтаи назаридан заиф хисобланади, чунки паролни бегона шахс ушлаб қолиб ишлатиши мумкин. Internet тармоғидаги кўпгина можаролар қисман анъанавий кўп марта ишлатилувчи паролларнинг заифлигидан келиб чиққан.



3.3–расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси

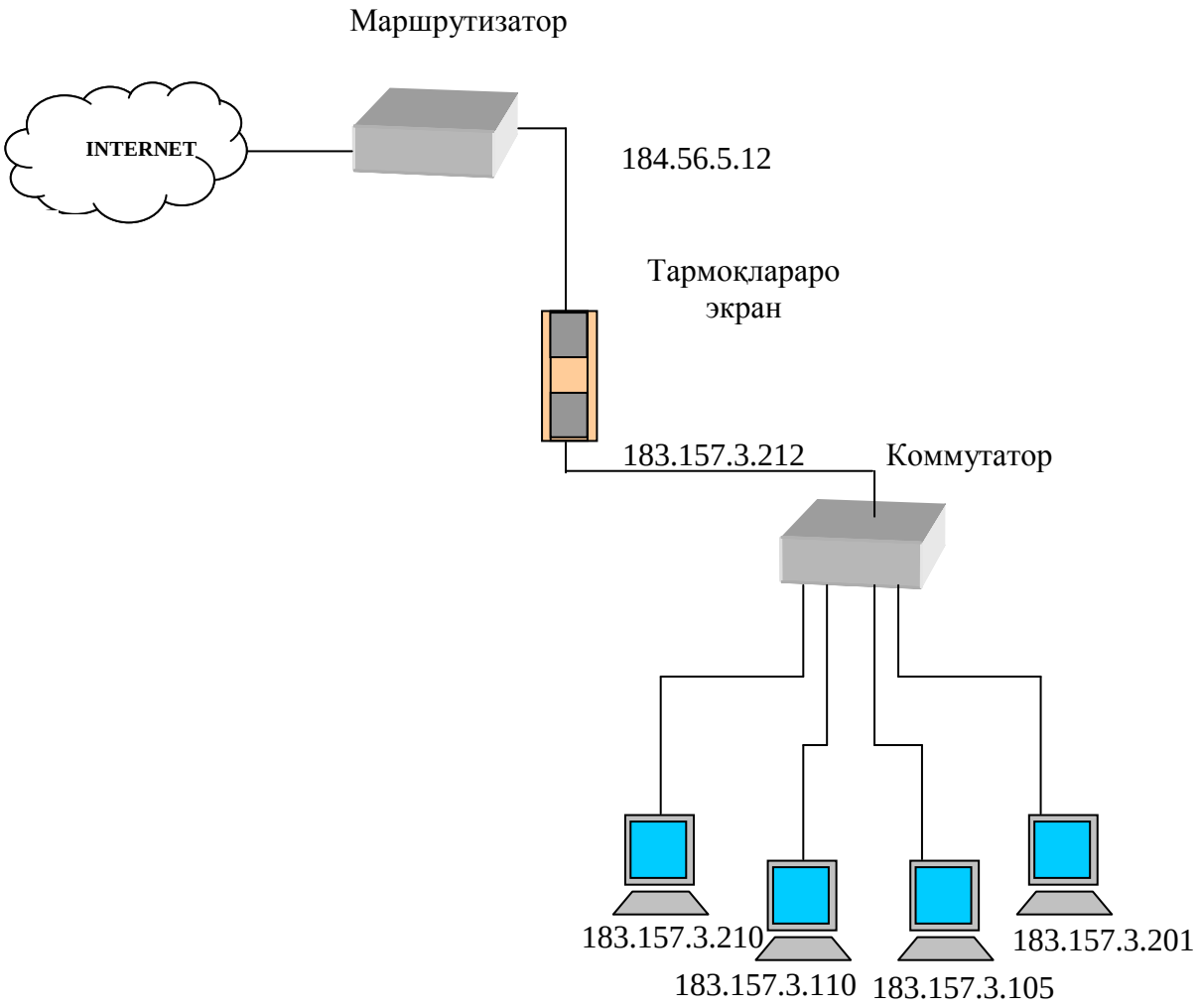
Аутентификациялашнинг ишончлироқ усули – бир марта ишлатилувчи пароллардан фойдаланишдир. Бир мартали паролларни генерациялашда аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига ўрнатилувчи қурилма бўлиб, уни ишга тушириш учун фойдаланувчи қандайдир махфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялайди ва бу ахборотни хост анъанавий парол ўрнида ишлатади. Смарт-карта ёки токен хостнинг аппарат ва дастурий таъминоти билан бирга ишлаши сабабли, генерацияланувчи парол хар бир сеанс учун ноёб бўлади.

Ишончли орган, масалан калитларни тақсимлаш маркази томонидан берилувчи рақамли сертификатларни ишлатиш хам қулай ва ишончли. Кўпгина воситачи дастурлар шундай ишлаб чиқиладики, фойдаланувчи фақат тармоқлараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгиланган вақт мобайнида ундан қўшимча аутентификацияланиш талаб этилмайди.

Тармоқлараро экранлар тармоқдан фойдаланишни бошқаришни марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва қурилмаларини ўрнатишга муносиб жой хисобланади. Гарчи кучайтирилган аутентификация воситалари хар бир хостда ишлатилиши мумкин бўлсада, уларнинг тармоқлараро экранларда жойлаштириш қулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармоқлараро экранлар бўлмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиги тармоқнинг ички тизимларига тўғридан-тўғри ўтиши мумкин.

Қатор тармоқлараро экранлар аутентификациялашнинг кенг тарқалган усулларидан бири – Kerberosни мададлайди. Одатда, аксарият тижорат тармоқлараро экранлар аутентификациялашнинг турли схемаларини мададлайди. Бу эса тармоқ хавфсизлиги маъмурига ўзининг шароитига қараб энг мақбул схемани танлаш имконини беради.

Ички тармоқ адресларини трансляциялаш. Кўпгина хужумларни амалга оширишда нияти бузуқ одамга қурбонининг адресини билиш керак бўлади. Бу адресларни хамда бутун тармоқ топологиясини беркитиш учун тармоқлараро экранлар энг мухим вазифани – ички тармоқ адресларини трансляциялашни бажаради (3.4-расм).



3.4–расм. Тармоқ адресларини трансляциялаш

Бу функция ички тармоқдан ташқи тармоққа узатилувчи барча пакетларга нисбатан бажарилади. Бундай пакетлар учун жўнатувчи компьютерларнинг IP-адреслари битта "ишончли" IP адресга автоматик тарзда ўзгартирилади.

Ички тармоқ адресларини трансляциялаш иккита усул-динамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда адрес узелга тармоқлараро экранга мурожаат онида ажратилади. Уланиш тугалланганидан сўнг адрес бўшайди ва уни корпоратив тармоқнинг бошқа узели ишлатиши мумкин. Статик усулда узел адреси барча чиқувчи пакетлар узатиладиган тармоқлараро экраннинг битта адресига доимо боғланади. Тармоқлараро экраннинг IP-адреси ташқи тармоққа тушувчи ягона фаол IP-адресга айланади. Натижада, ички тармоқдан чиқувчи барча пакетлар тармоқлараро

экрандан жўнатилган бўлади. Бу авторизацияланган ички тармоқ ва хавфли бўлиши мумкин бўлган ташқи тармоқ орасида тўғридан-тўғри алоқани истисно қилади.

Бундай ёндашишда ички тармоқ топологияси ташқи фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи қийинлашади. Адресларни трансляциялаш тармоқ ичида ташқи тармоқ, масалан Internetдаги адреслаш билан келишилмаган адреслашнинг хусусий тизимига эга бўлишига имкон беради. Бу ички тармоқнинг адрес маконини кенгайтириш ва ташқи адрес танқислиги муаммосини самарали ечади.

Ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, хамда қайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш тармоқлараро экранларнинг мухим вазифалари хисобланади. Корпоратив тармоқни химоялаш тизимининг жиддий элементи сифатида тармоқлараро экран барча харакатларни рўйхатга олиш имкониятига эга. Бундай харакатларга нафақат тармоқ пакетларини ўтказиб юбориш ёки блокировка қилиш, балки хавфсизлик маъмури томонидан фойдаланишни қоидасини ўзгартириш ва х. хам тааллуқли. Бундай руйхатга олиш зарурият туғилганда (хавфсизлик можароси пайдо бўлганида ёки суд инстанцияларига ёки ички тергов учун далилларни йиғишда) яратилувчи журналларга мурожаат этишга имкон беради.

Шубхали ходисалар (alarm) хусусидаги сигналларни қайдлаш тизими тўғри созланганида тармоқлараро экран ёки тармоқ хужумга дучор бўлганлиги ёки зондланганлиги тўғрисидаги батафсил ахборотни бериши мумкин. Тармоқдан фойдаланиш ва унинг зондланганлигининг исботи статистикасини йиғиш қатор сабабларга кўра мухимдир. Аввало. тармоқлараро экраннинг зондланишга ва хужумларга бардошлигини аниқ билиш зарур ва тармоқлараро экранни химоялаш тадбирларининг адэкватлигини аниқлаш лозим. Ундан ташқари, тармоқдан фойдаланиш статистикаси тармоқ асбоб-ускуналарига ва дастурларига талабларни

ифодалаш мақсадида хавф-хатарни тадқиқлаш ва тахлиллашда дастлабки маълумотлар сифатида мухим хисобланади.

Кўпгина тармоқлараро экранлар статистикани қайдловчи, йиғувчи ва тахлилловчи қувватли тизимга эга. Мижоз ва сервер адреси, фойдаланувчилар идентификатори, сеанс вақтлари, уланиш вақтлари, узатилган ва қабул қилинган маълумотлар сони, маъмур ва фойдаланувчилар харакатлари бўйича хисоб олиб борилиши мумкин. Хисоб тизимлари статистикани тахлиллашга имкон беради ва маъмурларга батафсил хисоботларни тақдим этади. Тармоқлараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тўғрисида реал вақт режимида масофадан хабар беришни бажариши мумкин.

Рухсатсиз харакатларни қилишга уринишларни аниқланишига бўладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огохлантирувчи сигналларни бериш белгиланиши лозим. Хужум қилинганлиги аниқланганда огохлантирувчи сигналларни юборишга қодир бўлмаган тармоқлараро экранни тармокларараро химоянинг самарали воситаси деб бўлмайди.

3.2. Тармоқлараро экранларнинг асосий компонентлари

Тармоқлараро экранлар тармоқлараро алоқа хавфсизлигини OSI моделининг турли сатхларида мададлайди. Бунда эталон моделнинг турли сатхларида бажариладиган химоя функциялари бир-биридан жиддий фарқланади. Шу сабабли, тармоқлараро экранлар комплексини, хар бири OSI моделининг алохида сатхига мўлжалланган, бўлинмайдиган экранлар мажмуи кўринишида тасаввур этиш мумкин.

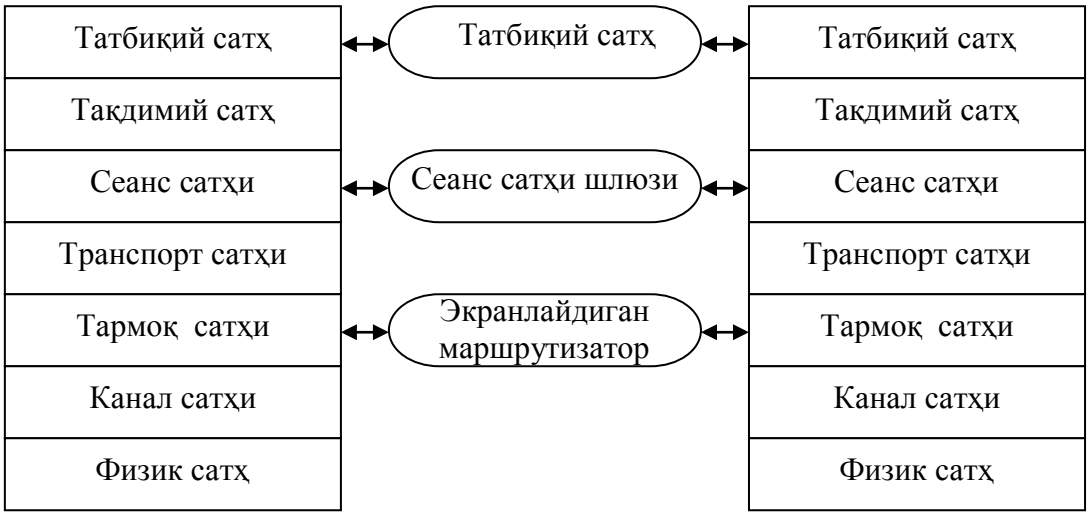
Экранлар комплекси кўпинча эталон моделнинг тармоқ, сеанс, татбиқий сатхларида ишлайди. Мос холда, қуйидаги бўлинмайдиган брандмауэрлар фарқланади (3.5-расм).

- экранловчи маршрутизатор;

- сеанс сатхи шлюзи (экранловчи транспорт);

- татбиқий сатх шлюзи (экранловчи шлюз).

Тармоқларда ишлатиладиган протоколлар (TCP/IP, SPX/IPX) OSI эталон моделига батамом мос келмайди, шу сабабли санаб ўтилган экранлар хили функцияларини амалга оширишда эталон моделининг қўшни сатхларини хам қамраб олишлари мумкин. Масалан, татбиқий экран хабарларнинг ташқи тармоққа узатилишида уларни автоматик тарзда шифрлашни, хамда қабул қилинувчи криптографик беркитилган маълумотларни автоматик тарзда расшифровка қилишни амалга ошириши мумкин. Бу холда бундай экран OSI моделининг нафақат татбиқий сатхида, балки тақдимий сатхида хам ишлайди.



3.5-расм. OSI моделининг алоҳида сатҳларида ишлайдиган тармокдараро экранлар тури

Сеанс сатхи шлюзи ишлашида OSI моделининг транспорт ва тармоқ сатхларини қамраб олади. Экранловчи маршрутизатор хабарлар пакетини тахлиллашда уларнинг нафақат тармоқ, балки транспорт сатхи сарлавхаларини хам текширади.

Юқорида келтирилган тармоқлараро экранларнинг хиллари ўзининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмауэрларнинг

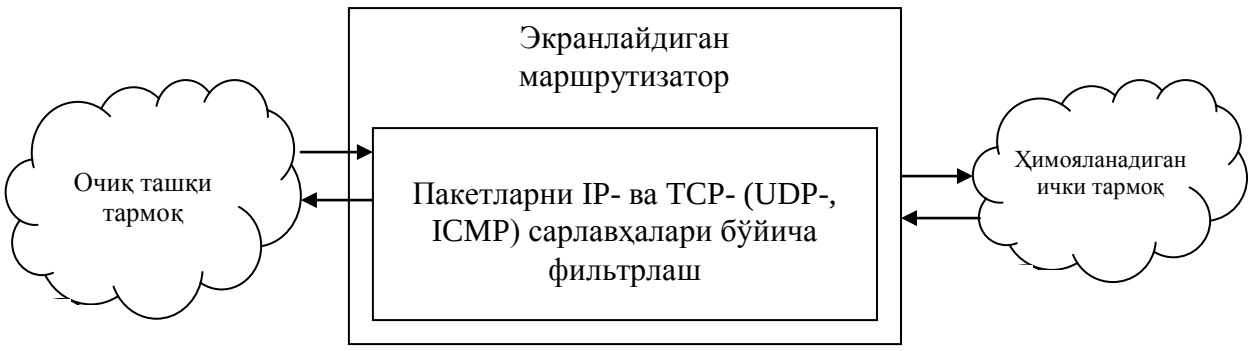
кўпчилиги ёки татбиқий шлюзлар, ёки экранловчи маршрутизаторлар бўлиб, тармоқлараро алоқанинг тўлиқ хавфсизлигини таъминламайди. Ишончли химояни эса фақат хар бири экранловчи маршрутизатор, сеанс сатхи шлюзи, хамда татбиқий шлюзни бирлаштирувчи тармоқлараро экранларнинг комплекси таъминлайди.

Экранловчи маршрутизатор (screening router) (пакетли фильтр (packet filter) деб хам аталади) хабарлар пакетини фильтрлашга аталган ва ички ва ташқи тармоқлар орасида шаффоф алоқани таъминлайди. У OSI моделининг тармоқ сатхида ишлайди, аммо ўзининг айрим функцияларини бажаришида эталон моделининг транспорт сатхини хам қамраб олиши мумкин.

Маълумотларни ўтказиш ёки бракка чиқариш хусусидаги қарор фильтрлашнинг берилган қоидаларига биноан хар бир пакет учун мустақил қабул қилинади. Қарор қабул қилишда тармоқ ва транспорт сатхлари пакетларининг сарлавхалари тахлил этилади (3.6-расм).

Хар бир пакетнинг IP- ва TCP/UDP – сарлавхаларининг тахлилланувчи хошиялари сифатида қуйидагилар ишлатилиши мумкин:

- жўнатувчи адреси;
- қабул қилувчи адреси;
- пакет хили;
- пакетни фрагментлаш байроғи;
- манба порти номери;
- қабул қилувчи порт номери.



3.6-расм. Пакетли фильтрни ишлаш схемаси

Биринчи тўртта параметр пакетнинг IP-сарлавхасига, кейингилари эса TCP-ёки UDP сарлавхасига тааллуқли. Жўнатувчи ва қабул қилувчи адреслари IP-адреслар хисобланади. Бу адреслар пакетларни шакллантиришда тўлдирилади ва уни тармоқ бўйича узатганда ўзгармайди.

Пакет хили хошиясида тармоқ сатхига мос келувчи ICMP протокол коди ёки тахлилланувчи IP-пакет тааллуқли бўлган транспорт сатхи протоколининг (TCP ёки UDP) коди бўлади.

Пакетни фрагментлаш байроғи IP-пакетлар фрагментлашининг борлиги ёки йўқлигини аниқлайди. Агар тахлилланувчи пакет учун фрагментлаш байроғи ўрнатилган бўлса, мазкур пакет фрагментланган IP-пакетнинг қисм пакети хисобланади.

Манба ва қабул қилувчи портлари номерлари TCP ёки UDP драйвер томонидан хар бир жўнатилувчи хабар пакетларига қўшилади ва жўнатувчи иловасини, хамда ушбу пакет аталган иловани бир маънода идентификациялайди. Портлар номерлари бўйича фильтрлаш имконияти учун юқори сатх протоколларига порт номерларини ажратиш бўйича тармоқда қабул қилинган келишувни билиш лозим.

Хар бир пакет ишланишида экранловчи маршрутизатор берилган қоидалар жадвалини, пакетнинг тўлиқ ассоциациясига мос келувчи қоидани топгунича, кетма-кет кўриб чиқади. Бу ерда ассоциация деганда берилган пакет сарлавхаларида кўрсатилган параметрлар мажмуи тушунилади. Агар экранловчи маршрутизатор жадвалдаги қоидаларнинг бирортасига ҳам мос келмайдиган пакетни олса, у, хавфсизлик нуқтаи назаридан, уни брака чиқаради.

Пакетли фильтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли фильтр сифатида оддий маршрутизатор, хамда кирувчи ва чиқувчи пакетларни фильтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар хар бир порт билан бир неча ўнлаб қоидаларни боғлаши ва киришда, ҳам чиқишда пакетларни фильтрлаши мумкин.

Пакетли фильтрларнинг камчилиги сифатида қуйидагиларни кўрсатиш мумкин. Улар хавфсизликнинг юқори даражасини таъминламайди, чунки фақат пакет сарлавхаларини текширадилар ва кўпгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охирги узелларни аутентификациялаш, хабарлар пакетларини криптографик беркитиш, хамда уларнинг яхлитлигини ва хақиқийлигини текшириш киради. Пакетли фильтрлар дастлабки адресларни алмаштириб қўйиш ва хабарлар пакети таркибини рухсатсиз ўзгартириш каби кенг тарқалган тармоқ хужумларига заиф хисобланадилар. Бу хил брандмауэрларни "алдаш" қийин эмас - фильтрлашга рухсат берувчи қоидаларни қондирувчи пакет сарлавхаларини шакллантириш кифоя.

Аммо, пакетли фильтрларнинг амалга оширилишининг соддалиги, юқори унумдорлиги, дастурий иловалар учун шаффофлиги ва нархининг пастлиги, уларнинг хамма ерда тарқалишига ва тармоқ хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

Сеанс сатхи шлюзи, (*экранловчи транспорт* деб хам юритилади) виртуал уланишларни назоратлашга ва ташқи тармоқ билан ўзаро алоқа қилишда IP-адресларни трансляциялашга аталган. У OSI моделининг сеанс сатхида ишлайди ва ишлаши жараёнида эталон моделнинг транспорт ва тармоқ сатхларини хам қамраб олади. Сеанс сатхи шлюзининг химоялаш функциялари воситачилик функцияларига тааллуқли.

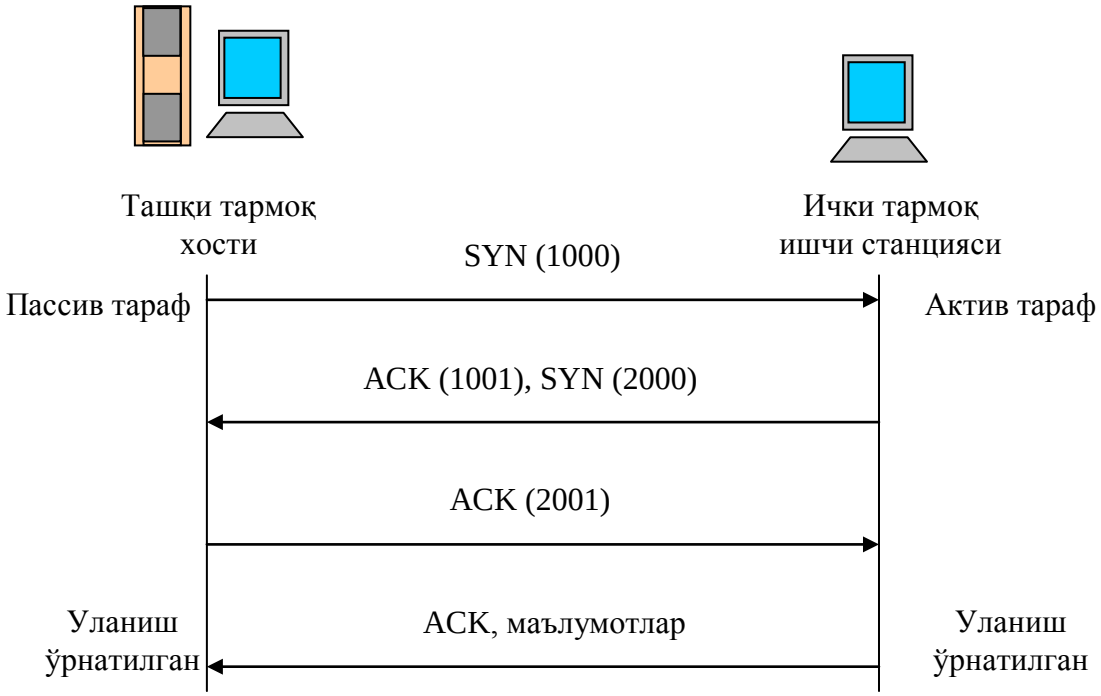
Виртуал уланишларнинг назорати алоқани квитирлашни кузатишдан хамда ўрнатилган виртуал каналлар бўйича ахборот узатилишининг назоратлашдан иборат. Алоқани квитирлашнинг назоратида сеанс сатхида шлюз ички тармоқ ишчи станцияси ва ташқи тармоқ компьютери орасида виртуал уланишни кузатиб, сўралаётган алоқа сеансининг жоизлигини аниқлайди.

Бундай назорат TCP протоколининг сеанс сатхи пакетларининг сарлавхасидаги ахборотга асосланади. Аммо TCP-сарлавхаларни тахлиллашда пакетли фильтр фақат манба ва қабул қилувчи портларининг

номерини текширса, экранловчи транспорт алоқани квиртирлаш жараёнига тааллуқли бошқа хошияларни тахлиллайди.

Алоқа сеансига сўровнинг жоизлигини аниқлаш учун сеанс сатхи шлюзи қуйидаги харакатларни бажаради. Ишчи станция (мижоз) ташқи тармоқ билан боғланишни сўраганида, шлюз бу сўровни қабул қилиб унинг фильтрлашнинг базавий мезонларни қаноатлантиришини, масалан сервер мижоз ва у билан ассоциацияланган исмнинг IP-адресини аниқлай олишини текширади. Сўнгра шлюз, мижоз исмидан харакат қилиб, ташқи тармоқ компьютери билан уланишни ўрнатади ва TCP протоколи бўйича квитирлаш жараёнининг бажарилишини кузатади.

Бу муолажа SYN (Синхронлаш) ва ACK (Тасдиқлаш) байроқлари орқали белгиланувчи TCP-пакетларни алмашишдан иборат (3.7-расм).

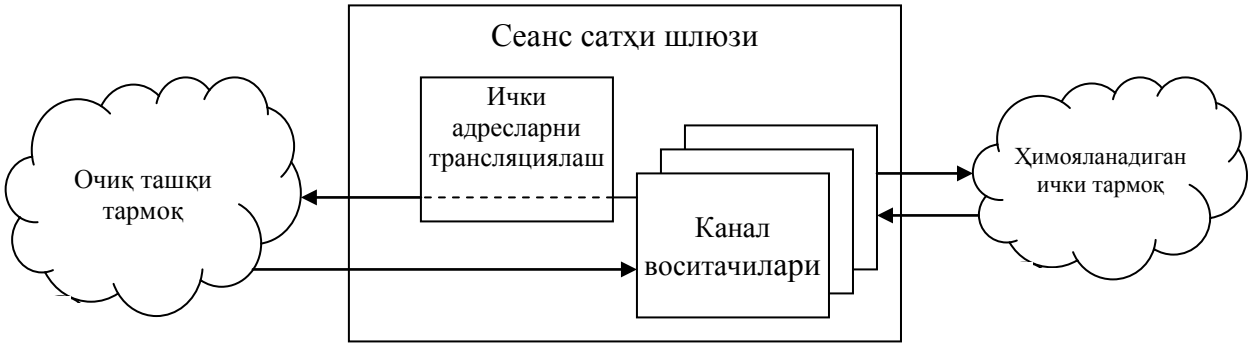


3.7–расм. TCP протоколи бўйича алоқани квитирлаш схемаси.

SYN байроқ билан белгиланган ва таркибида ихтиёрий сон, масалан 1000, бўлган TCP сеансининг биринчи пакети мижознинг сеанс очишга сўрови хисобланади. Бу пакетни олган ташқи тармоқ компьютери жавоб тариқасида ACK байроқ билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг холда 1001) сон бўлган пакетни

жўнатади. Шу тариқа, мижоздан SYN пакети олинганлиги тасдиқланади. Сўнгра, тескари муолажа амалга оширилади: ташқи тармоқ компьютери хам мижозга узатилувчи маълумотлар биринчи байтининг тартиб рақами билан (масалан, 2000) SYN пакетини жўнатади, мижоз эса уни олганлигини, таркибида 2001 сони бўлган пакетни узатиш орқали тасдиқлайди. Шу билан алоқани квиртирлаш жараёни тугалланади.

Сеанс сатхи шлюзи (3.8-расм) учун сўралган сеанс жоиз хисобланади, қачонки алоқани квиртирлаш жараёни бажарилишида SYN ва ACK байроқлар, хамда TCP-пакетлари сарлавхаларидаги сонлар ўзаро мантиқий боғланган бўлса.



3.8-расм. Сеанс сатҳи шлюзи ишлаш схемаси

Ички тармоқнинг ички станцияси ва ташқи тармоқнинг компьютери TCP сеансининг авторизацияланган қатнашчилари эканлиги хамда ушбу сеанснинг жоизлиги тасдиқланганидан сўнг шлюз уланишни ўрнатади. Бунда шлюз уланишларининг махсус жадвалига мос ахборотни (жўнатувчи ва қабул қилувчи адреслари, уланиш холати, кетма-кетлик номери хусусидаги ахборот ва х.) киритади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йўналтириб, ўрнатилган виртуал канал бўйича ахборот узатилишини назорат қилади. Ушбу назорат жараёнида сеанс сатхи шлюзи пакетларни фильтрламайди. Аммо у узатилувчи ахборот сонини назорат қилиши ва қандайдир чегарадан ошганида уланишни узиши мумкин. Бу эса, ўз

навбатида, ахборотнинг рухсатсиз экспорт қилинишига тўсиқ бўлади. Виртуал уланишлар хусусидаги қайдлаш ахборотининг тўпланиши хам мумкин.

Сеанс сатхи шлюзларида виртуал уланишларни назоратлашда *канал воситачилари* (pipe proxy) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташқи тармоқлар орасида виртуал каналларни ўрнатади, сўнгра TCP/IP иловалари генерациялаган пакетларнинг ушбу канал орқали узатилишини назоратлайди.

Канал воситачилари TCP/IPнинг муайян хизматларига мўлжалланган. Шу сабабли ишлаши муайян иловаларнинг воситачи-дастурларига асосланган татбиқий сатх шлюзлари имкониятларини кенгайтиришда сеанс сатх шлюзларидан фойдаланиш мумкин.

Сеанс сатхи шлюзи ташқи тармоқ билан ўзаро алоқада тармоқ сатхи ички адресларини (IP-адресларини) трансляциялашни хам таъминлайди. Ички адресларни трансляциялаш ички тармоқдан ташқи тармоққа жўнатилувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуқтаи назаридан сеанс сатхи шлюзи етарлича оддий ва нисбатан ишончли дастур хисобланади. У экранловчи маршрутизаторни виртуал уланишларни назоратлаш ва ички IP-адресларни трансляциялаш функциялари билан тўлдиради.

Сеанс сатхи шлюзининг камчиликлари – экранловчи маршрутизаторларнинг камчиликларига ўхшаш. Ушбу технологиянинг яна бир жиддий камчилиги маълумотлар хошиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузуқ одамларга зарар келтирувчи дастурларни химояланувчи тармоққа узатиш имконияти туғилади. Ундан ташқари, TCP-сессиясининг (TCP hijacking) ушлаб қолинишида нияти бузуқ одам хужумларини хатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатх шлюзлари мустақил махсулот бўлмай, татбиқий сатх шлюзлари билан комплектда тақдим этилади.

Татбиқий сатх шлюзи (*экранловчи шлюз* деб хам юритилади) OSI моделининг татбиқий сатхида ишлаб, тақдимий сатхни хам қамраб олади ва тармоқлараро алоқанинг энг ишончли химоясини таъминлайди. Татбиқий сатх шлюзининг химоялаш функциялари, сеанс сатхи шлюзига ўхшаб, воситачилик функцияларига тааллуқли. Аммо, татбиқий сатх шлюзи сеанс сатхи шлюзига қараганда химоялашнинг анча кўп функцияларини бажариши мумкин:

- брандмауэр орқали уланишни ўрнатишга уринишда фойдаланувчиларни идентификациялаш ва аутентификациялаш;

- шлюз орқали узатилувчи ахборотнинг хақиқийлигини текшириш;

- ички ва ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;

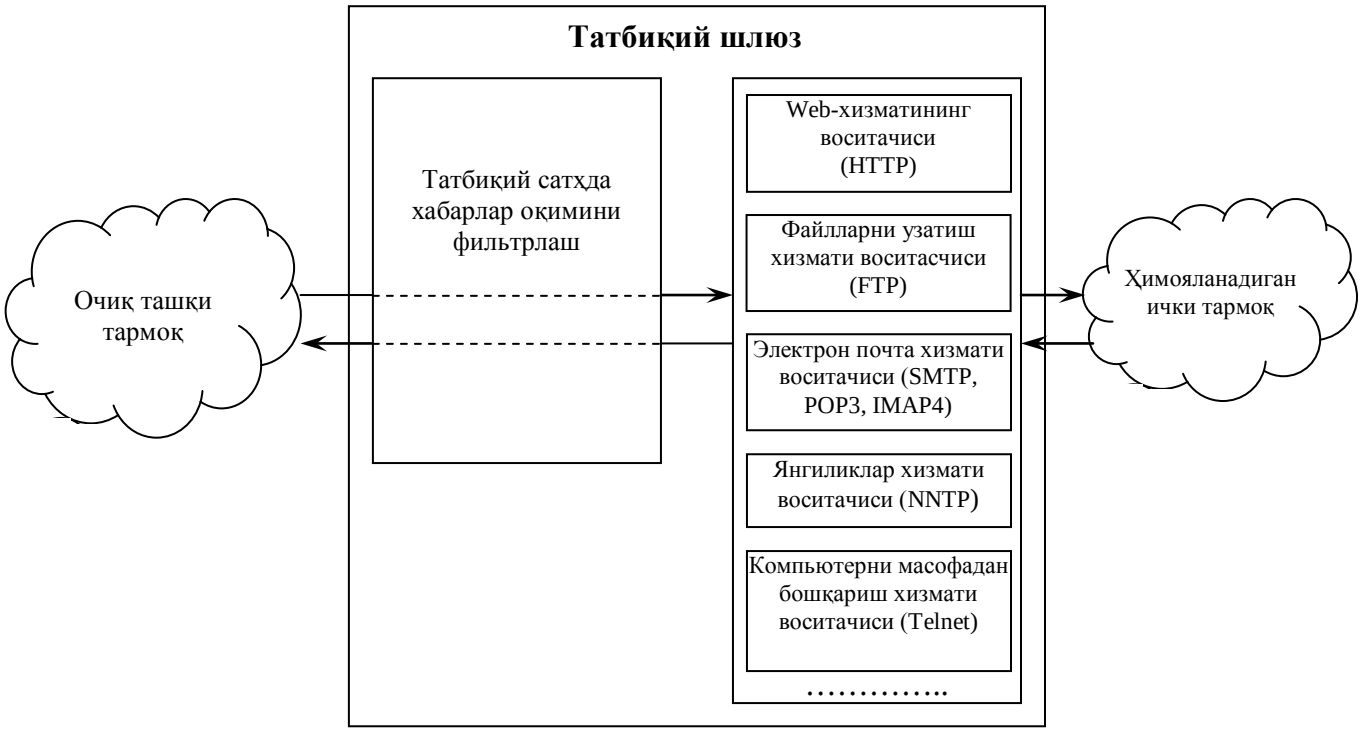
- ахборотлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;

- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, хамда қайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш;

- ташқи тармоқдан сўралувчи маълумотларни кэшлаш.

Татбиқий сатх шлюзи функциялари воситачилик функцияларига тааллуқли бўлганлиги сабабли, бу шлюз универсал компьютер хисобланади ва бу компьютерда хар бир хизмат кўрсатилувчи татбиқий протокол (HTTP, FTP, SMTP, NNTP ва х.) учун биттадан воситачи дастур (экранловчи агент) ишлатилади. TCP/IPнинг хар бир хизматининг воситачи дастури (application proxy) айнан шу хизматга тааллуқли хабарларни ишлашга ва химоялаш функцияларини бажаришга мўлжалланган.

Татбиқий сатх шлюзи мос экранловчи агентлар ёрдамида кирувчи ва чиқувчи пакетларни ушлаб қолади, ахборотни нусхалайди ва қайта жўнатади, яъни ички ва ташқи тармоқлар орасидаги тўғридан-тўғри уланишни истисно қилган холда, сервер-воситачи функциясини бажаради (3.9-расм).



3.9-расм. Татбиқий шлюз ишлаш схемаси.

Татбиқий сатх шлюзи ишлатадиган воситачилар сеанс сатхи шлюзларининг канал воситачиларидан жиддий фарқланади. Биринчидан, татбиқий сатх шлюзлари муайян иловалар (дастурий серверлар) билан боғланган, иккинчидан улар OSI моделининг татбиқий сатхида хабарлар оқимини фильтрлашлари мумкин.

Татбиқий сатх шлюзлари воситачи сифатида мана шу мақсадлар учун махсус ишлаб чиқилган TCP/IPнинг муайян хизматларининг дастурий серверлари – HTTP, FTP, SMTP, NNTP ва х. – серверларидан фойдаланади. Бу дастурий серверлар брандмауэрларда резидент режимида ишлайди ва TCP/IPнинг мос хизматларига тааллуқли химоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг махсус транслятори хизмат кўрсатади.

Ички тармоқ ишчи сервери ва ташқи тармоқ компьютери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмауэргача ва брандмауэрдан белгиланган жойгача. Канал воситачиларидан фарқли холда, татбиқий сатх шлюзининг воситачилари фақат ўзлари хизмат қилувчи

иловалар генерациялаган пакетларни ўтказади. Масалан, HTTP хизматининг воситачи-дастури фақат шу хизмат генерациялаган трафикни ишлайди.

Агар қандайдир иловада ўзининг воситачиси бўлмаса, татбиқий сатхдаги шлюз бундай иловани ишлай олмайди ва у блокировка қилинади. Масалан, агар татбиқий сатхдаги шлюз фақат HTTP, FTP ва Telnet воситачи-дастурларидан фойдаланса, у фақат шу хизматларга тегишли пакетларни ишлайди ва қолган хизматларнинг пакетларини блокировка қилади.

Татбиқий сатх шлюзи воситачилари, канал воситачиларидан фарқли холда, ишланувчи маълумотлар таркибини текширишни таъминлайди. Улар ўзлари хизмат кўрсатадиган татбиқий сатх протоколларидаги командаларнинг алохида хилларини ва хабарлардаги ахборотлани фильтрлашлари мумкин.

Татбиқий сатх шлюзини созлашда ва хабарларни фильтрлаш қоидаларини тавсифлашда қуйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жоиз вақт оралиғи, ушбу сервисга боғлиқ хабар таркибига чегаралашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва х.

Татбиқий сатх шлюзи қуйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармоқ химоясининг юқори даражасини таъминлайди;

- иловалар сатхида химоялаш кўпгина қўшимча текширишларни амалга оширишга имкон беради, натижада дастурий таъминот камчиликларига асосланган муваффақиятли хужумлар ўтказиш эхтимоллиги камаяди;

- татбиқий сатх шлюзининг ишга лаёқатлиги бузилса, бўлинувчи тармоқлар орасида пакетларнинг тўппа-тўғри ўтиши блокировка қилинади, натижада, рад қилиниши туфайли химояланувчи тармоқнинг хавфсизлиги пасаймайди.

Татбиқий сатх шлюзининг камчиликларига қуйидагилар киради:

- нархининг нисбатан юқорилиги;

- брандмауэрнинг ўзи, хамда уни ўрнатиш ва конфигурациялаш муолажаси етарлича мураккаб;

- компьютер платформаси унумдорлигига ва ресурслари хажмига қуйиладиган талабларнинг юқорилиги;

- фойдаланувчилар учун шаффофликнинг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши.

Охирги камчиликка батафсил тухталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралиқ ролини бажаради. Аввал воситачи билан уланиш ўрнатилади, сўнгра воситачи адресат билан уланишни яратиш ёки яратмаслик хусусида қарор қабул қилади. Мос холда татбиқий сатх шлюзи ишлаши жараёнида хар қандай рухсат этилган уланишни қайталайди. Натижада фойдаланувчилар учун шаффофлик йўқолади ва уланишга хизмат қилишга қўшимча харажат сарфланади.

Эксперт сатхи шлюзи. Татбиқий сатх шлюзининг фойдаланувчилар учун шаффофлигининг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши каби жиддий камчиликларини бартараф этиш мақсадида пакетларни фильтрлашнинг янги технологияси ишлаб чиқилган. Бу технологияни баъзида *уланиш холатини назоратлашли фильтрлаш* (stateful inspection) ёки эксперт сатхидаги фильтрлаш деб юритишади. Бундай фильтрлаш пакетлар холатини кўп сатхли тахлиллашнинг махсус усуллари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармоқ сатхида пакетларни ушлаб қолиш ва ундан уланишни назорат қилишда ишлатилувчи татбиқий сатх ахборотини чиқариб олиш орқали уланиш холатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоқлараро экран *эксперт сатх брандмауэри* деб юритилади. Бундай брандмауэрлар ўзида экранловчи маршрутизаторлар ва татбиқий сатх шлюзлари элементларини уйғунлаштиради. Улар хар бир пакет таркибини берилган хавфсизлик сиёсатига мувофиқ бахолайдилар.

Шундай қилиб эксперт сатхидаги брандмауэрлар қуйидагиларни назоратлашга имкон беради:

- мавжуд қоидалар жадвали асосида хар бир узатилувчи пакетни;

- холатлар жадвали асосида хар бир сессияни;

- ишлаб чиқилган воситачилар асосида хар бир иловани.

Эксперт сатх тармоқлараро экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот оқимини ишлашининг юқори тезкорлигини хамда улар орқали ўтувчи пакетларнинг IP-адресларини ўзгартирмаслигини кўрсатиш мумкин. Охирги афазаллик. IP-адресдан фойдаланувчи татбиқий сатхнинг хар қандай протоколининг бундай брандмауэрлардан хеч қандай ўзгаришсиз ёки махсус дастурлашсиз бирга ишлай олишини англатади.

Бундай брандмауэрларнинг авторизацияланган мижоз ва ташқи тармоқ компьютери орасида тўғридан-тўғри уланишга йўл қўйиши, химоянинг унчалик юқори бўлмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатхини фильтрлаш технологиясидан комплекс брандмауэрлар ишлаши самарадорлигини оширишда фойдаланилади. Эксперт сатхнинг фильтрлаш технологиясини ишлатувчи комплекс брандмауэрларга мисол тариқасида Fire Wall-1 ва ON Guardларни кўрсатиш мумкин.

3.3. Тармоқлараро экранлар асосидаги тармоқ химоясининг схемалари

Тармоқлараро алоқани самарали химоялаш учун брандмауэр тизими тўғри ўрнатилиши ва конфигурацияланиши лозим. Ушбу жараён қуйидагиларни ўз ичига олади:

- тармоқлараро алоқа сиёсатини шакллантириш;

- брандмауэрни улаш схемасини танлаш ва параметрларини созлаш.

Тармоқлараро алоқа сиёсатини шакллантириш. Тармоқлараро алоқа сиёсатини шакллантиришда қуйидагиларни аниқлаш лозим:

- тармоқ сервисларидан фойдаланиш сиёсати;

- тармоқлараро экран ишлаши сиёсати.

Тармоқ сервисларидан фойдаланиш сиёсати химояланувчи компьютер тармоқнинг барча сервисларини тақдим этиш, хамда улардан фойдаланиш қоидаларини белгилайди. Ушбу сиёсат доирасида тармоқ экрани орқали тақдим этилувчи барча сервислар ва хар бир сервис учун мижозларнинг жоиз адреслари берилиши лозим. Ундан ташқари, фойдаланувчилар учун қачон ва қайси фойдаланувчилар қайси сервисдан ва қайси компьютерда фойдаланишларини тавсифловчи қоидалар кўрсатилиши лозим. Фойдаланиш усулларига чегаралашлар хам берилади. Бу чегаралашлар фойдаланувчиларнинг Internetнинг ман этилган сервисларидан айланма йўл орқали фойдаланишларига йўл қўймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш қоидалари, хамда ташкилот локал тармоғи ташқарисидаги фойдаланувчиларнинг ишлаш шароитлари алохида белгиланиши лозим.

Тармоқлараро экран ишлаши сиёсатида тармоқлараро алоқани бошқаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг қуйидаги иккитасидан бири танланиши мумкин:

- ошкора рухсат этилмагани ман қилинган;

- ошкора ман этилмаганига рухсат берилган.

"Ошкора рухсат этилмагани ман қилинган" принципи танланганида тармоқлараро экран шундай созланадики, харқандай рухсат этилмаган тармоқлараро алоқалар блокировка қилинади. Ушбу принцип ахборот хавфсизлигининг барча сохаларида ишлатилувчи фойдаланишнинг мумтоз моделига мос келади. Бундай ёндашиш, имтиёзларни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфсизлик нуқтаи назаридан яхшироқ хисобланади. Мохияти бўйича "ошкора рухсат этилмагани ман қилинган" принципи билмаслик зарар келтириши фактини эътироф этишдир. Таъкидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш қоидалари фойдаланувчиларга маълум ноқулайликлар туғдириши мумкин.

"Ошкора ман этилмаганига рухсат берилган" принципи танланганида тармоқлараро экран шундай созланадики, фақат ошкора ман этилган тармоқлараро алоқалар блокировка қилинади. Бу холда, фойдаланувчилар томонидан тармоқ сервисларидан фойдаланиш қулайлиги ошади, аммо тармоқлараро алоқа хавфсизлиги пасаяди. Фойдаланувчиларнинг тармоқлараро экранни четлаб ўтишларига имкон туғилади, масалан улар сиёсат ман қилмаган (хатто сиёсатда кўрсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички тармоқ хакерларнинг хужумларидан камроқ химояланган бўлади. Шу сабабли, тармоқлараро экранларни ишлаб чиқарувчилари одатда ушбу принципдан фойдаланмайдилар.

Тармоқлараро экран симметрик эмас. Унга ички тармоқнинг ташқи тармоқдан ва аксинча фойдаланишни чегараловчи қоидалар алохида берилади. Умумий холда, тармоқлараро экраннинг иши қуйидаги иккита гурух функцияларни динамик тарзда бажаришга асосланган:

- у орқали ўтаётган ахборот оқимини фильтрлаш;
- тармоқлараро алоқа амалга оширилишида воситачилик.

Оддий тармоқлараро экранлар бу функцияларнинг бирини бажаришга мўлжалланган. Комплекс тармоқлараро экранлар химоялашнинг кўрсатилган функцияларининг биргаликда бажарилишини таъминлайди.

Тармоқлараро экранларни улашнинг асосий схемалари. Корпоратив тармоқни глобал тармоқларга улаганда химояланувчи тармоқнинг глобал тармоқдан ва глобал тармоқнинг химояланувчи тармоқдан фойдаланишини чегаралаш, хамда уланувчи тармоқдан глобал тармоқнинг масофадан рухсатсиз фойдаланишидан химоялашни таъминлаш лозим. Бунда ташкилот ўзининг тармоғи ва унинг компонентлари хусусидаги ахборотни глобал тармоқ фойдаланувчиларидан беркитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш химояланувчи тармоқ ресурсларидан фойдаланишнинг қатъий чегараланишини талаб этади.

Ташкилотдаги корпоратив тармоқ таркибида кўпинча химояланишнинг турли сатхли бирнечи сегментларга эга бўлиши эхтиёжи туғилади:

- бемалол фойдаланилувчи сегментлар (масалан, реклама WWW-серверлари);

- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг масофадаги узеллари ходимларининг фойдаланиши учун);

- ёпиқ сегментлар (масалан, ташкилотнинг молия локал қисм тармоғи)

Тармоқлараро экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар химояланувчи тармоқ ишлаши шароитига, хамда ишлатиладиган брандмауэрларнинг тармоқ интерфейслари сонига ва бошқа характеристикаларига боғлиқ. Тармоқлараро экранни улашнинг қуйидаги схемалари кенг тарқалган:

- экранловчи маршрутизатордан фойдаланилган химоя схемалари;

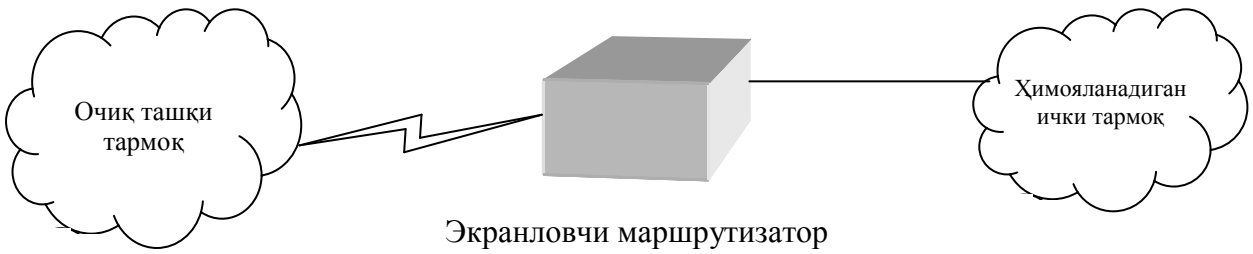
- локал тармоқни умумий химоялаш схемалари;

- химояланувчи ёпиқ ва химояланмайдиган очиқ кисм тармоқли схемалар;

- ёпиқ ва очиқ қисм тармоқларни алохида химояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган химоя схемаси.

Пакетларни фильтрлашга асосланган тармоқлараро экран кенг тарқалган ва амалга оширилиши осон. У химояланувчи тармоқ ва бўлиши мумкин бўлган ғаним очиқ тармоқ орасида жойлашган экранловчи маршрутизатордан иборат (3.10-расм).



3.10-расм. Тармоқлараро экран – экранловчи маршрутизатор

Экранловчи маршрутизатор (пакетли фильтр) кирувчи ва чиқувчи пакетларни уларнинг адреслари ва портлари асосида блокировка қилиш ва фильтрлаш учун конфигурацияланган.

Химояланувчи тармоқдаги компьютерлар Internetдан тўғридан-тўғри фойдаланаолади, Internetнинг улардан фойдаланишининг кўп қисми эса блокировка қилинади. Умуман, экранловчи маршрутизатор юқорида тавсифланган химоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йўли ва чиқиш йўли портлари номери бўйича фильтрламаса, "ошкора рухсат этилмагани ман қилинган" сиёсатини амалга ошириш қийинлашади.

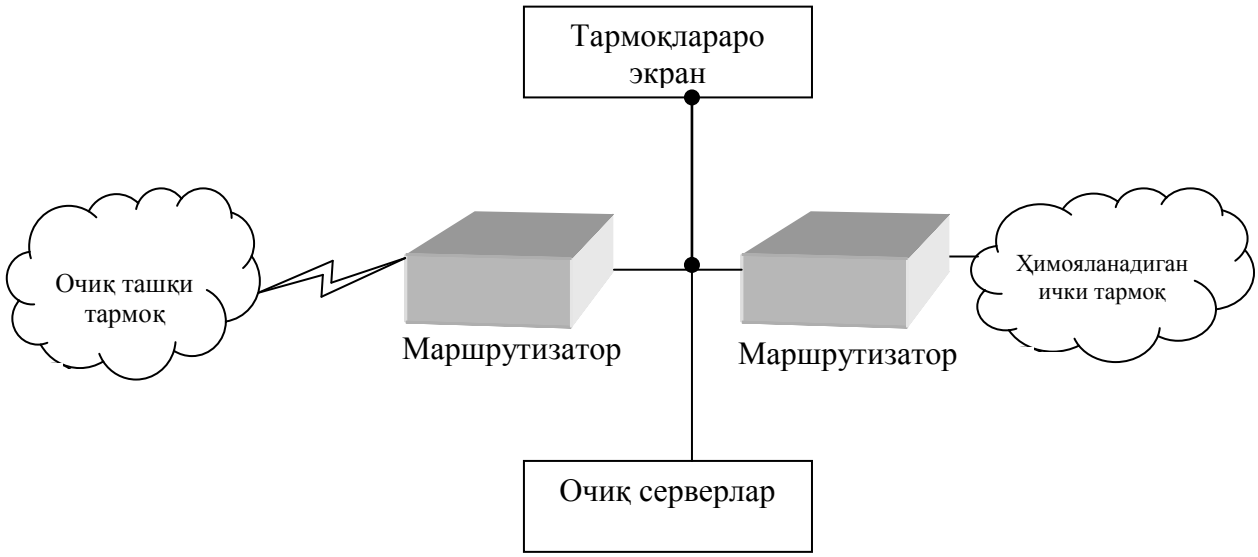
Пакетларни фильтрлашга асосланган тармоқлараро экраннинг камчиликлари қуйидагилар:

- фильтрлаш қоидаларининг мураккаблиги; баъзи холларда бу қоидалар мажмуи бажарилмаслиги мумкин;

- фильтрлаш қоидаларини тўлиқ тестлаш мумкин эмаслиги; бу тармоқни тестланмаган хужумлардан химояланмаслигига олиб келади;

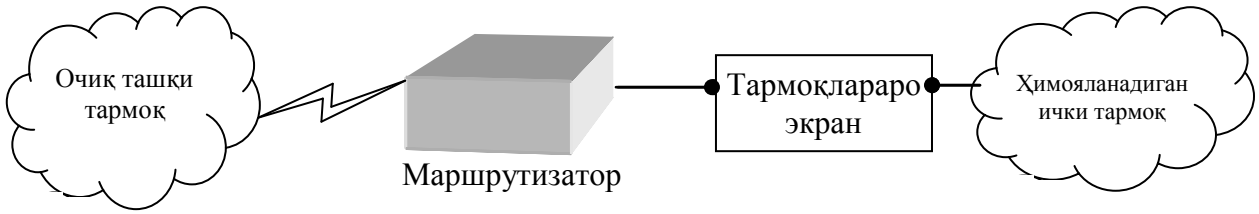
- ходисаларни руйхатга олиш имкониятининг йўқлиги; натижада маъмурга машрутизаторнинг хужумга дуч келганлигини ва обрўсизлантирилганлигини аниқлаш қийинлашади.

Локал тармоқни умумий химоялаш схемалари. Битта тармоқ интерфейсли брандмауэрлардан фойдаланилган химоялаш схемалари (3.11-расм) хавфсизлик ва конфигурациялашнинг қулайлиги нуқтаи назаридан самарасиз хисобланади. Улар ички ва ташқи тармоқларни физик ажратмайдилар, демак, тармоқлараро алоқанинг ишончли химоясини таъминлай олмайдилар.



3.11-расм. Битта тармоқ интерфейсли firewall ёрдамида локал тармоқни ҳимоялаш

Локал тармоқни умумий химоялаш схемаси энг оддий ечим бўлиб, унда брандмауэр локал тармоқни ташқи ғаним тармоқдан бутунлай экранлайди (3.12-расм).



3.12-расм. Локал тармоқни умумий ҳимоялаш схемаси

Маршрутизатор ва брандмауэр орасида фақат битта йўл бўлиб, бу йўл орқали бутун трафик ўтади. Брандмауэрнинг ушбу варианти "ошкора рухсат этилмагани ман қилинган" принципига асосланган химоялаш сиёсатини амалга оширади. Одатда маршрутизатор шундай созланадики, брандмауэр ташқаридан кўринадиган ягона машина бўлади.

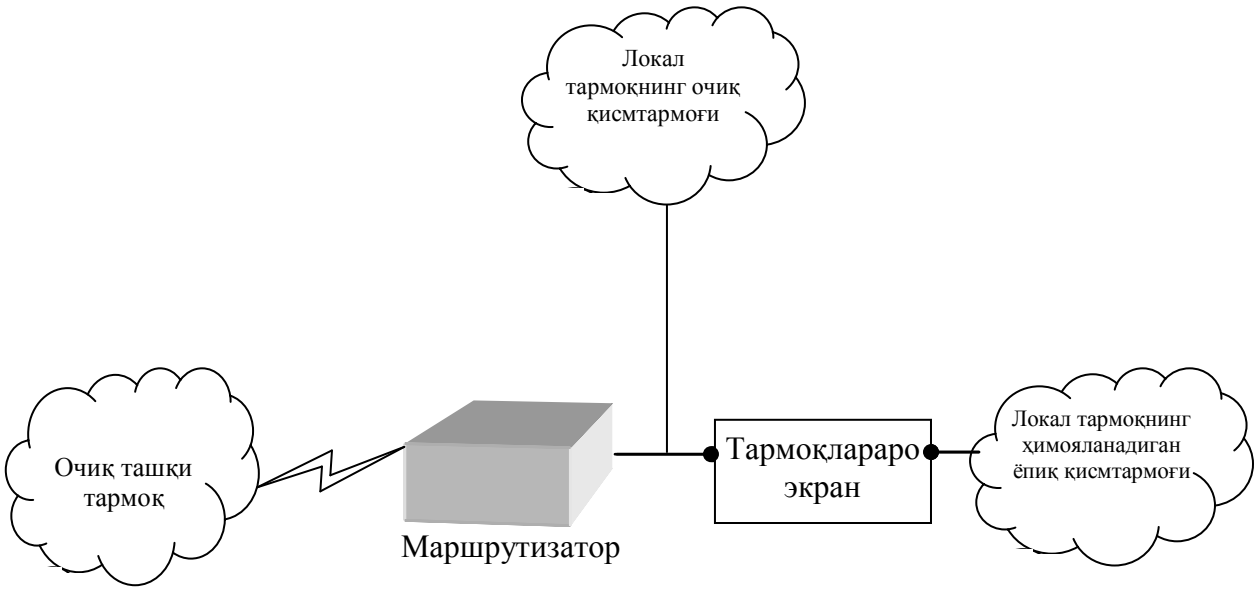
Локал тармоқ таркибидаги очиқ серверлар хам тармоқлараро экранлар томонидан химояланади. Аммо, ташқи тармоқ фойдаланаоладиган

серверларни химояланувчи локал тармоқларнинг бошқа ресурслари билан бирлаштириш тармоқлараро алоқа хавфсизлигини жиддий пасайтиради.

Тармоқлараро экран фойдаланадиган хостга фойдаланувчиларни кучайтирилган аутентификациялаш учун дастур ўранатилиши мумкин.

Химояланувчи ёпиқ ва химояланмайдиган очиқ қисм тармоқли схемалар. Агар локал тармоқ таркибида умумфойдаланувчи очиқ серверлар бўлса уларни тармоқлараро экрандан олдин очиқ қисм тармоқ сифатида чиқариш мақсадга мувофиқ хисобланади (3.13-расм).

Ушбу усул локал тармоқ ёпиқ қисмининг кучли химояланишини, аммо тармоқлараро экрангача жойлашган очиқ серверларнинг пасайган химояланишини таъминлайди.

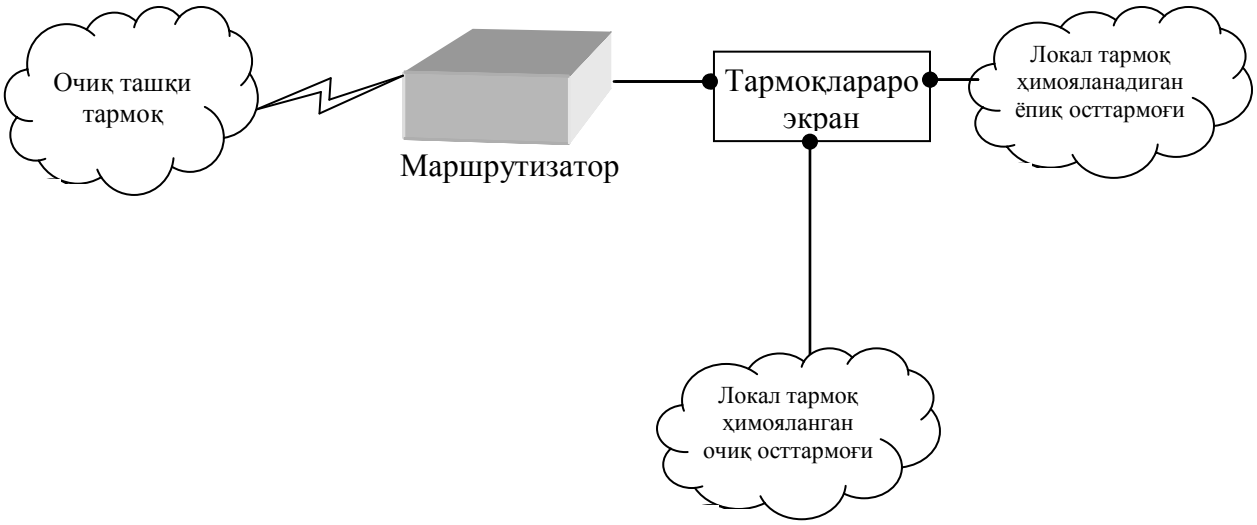


3.13-расм. Ҳимояланадиган ёпиқ ва ҳимояланмайдиган очиқ

Баъзи брандмауэрлар бу серверларни ўзида жойлаштиради. Аммо бу брандмауэрнинг хавфсизлиги ва компьютернинг юкланиши нуқтаи назаридан яхши ечим хисобланмайди. Химояланувчи ёпиқ ва химояланмайдиган очиқ қисм тармоқли схемани очиқ қисм тармоқ хавфсизлигига қўйиладиган талабларнинг бўлмаган холларида ишлатилиши

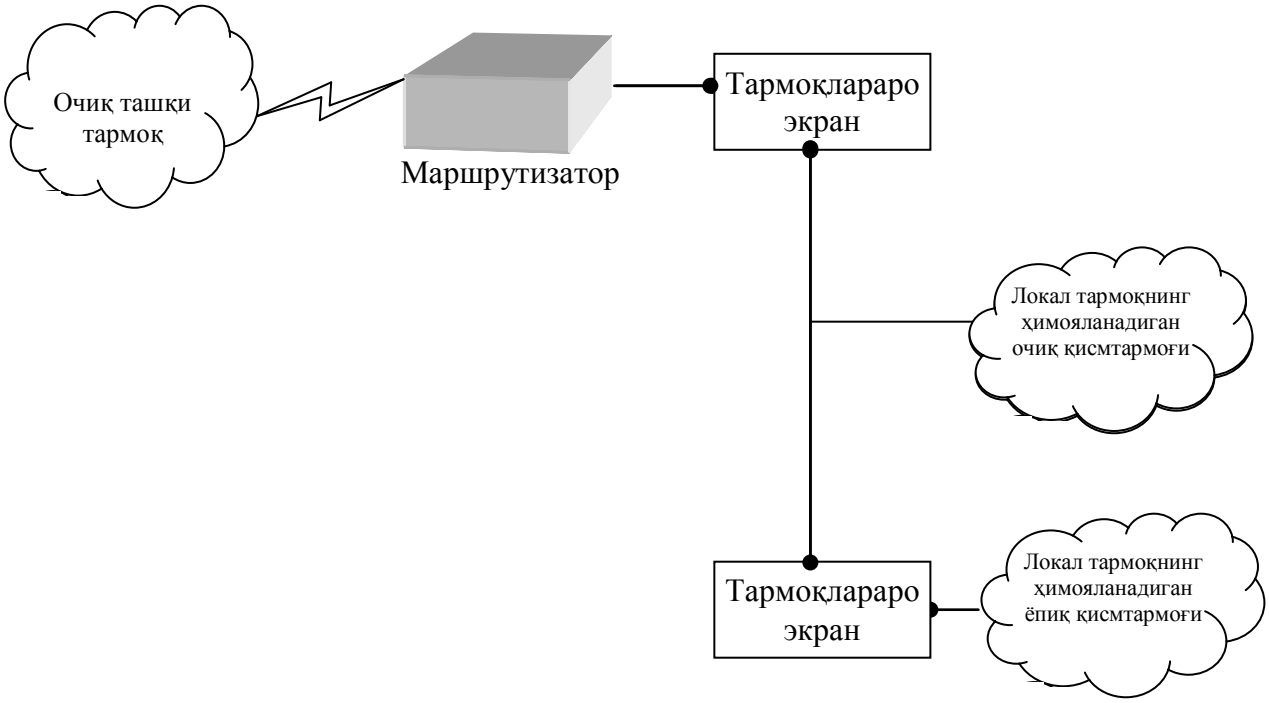
мақсадга мувофиқ хисобланади. Агар очиқ сервер хавфсизлигига юқори талаблар қўйилса, ёпиқ ва очиқ қисм тармоқларни алохида химоялаш схемаларидан фойдаланиш зарур.

Ёпиқ ва очиқ қисм тармоқларни алохида химояловчи схемалар. Бундай схемалар учта тармоқ интерфейсли битта брандмауэр (3.14-расм) ёки



3.14 -расм. Учта тармоқ интерфейсли бир брандмауэр асосида ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимоялаш схемаси

иккита тармоқ интерфейсли иккита брандмауэр (7.15-расм) асосида



3.15-расм. Иккита тармоқ интерфейсли иккита брандмауэр асосида ёпиқ ва очиқ қисмтармоқларни алоҳида ҳимоялаш схемаси

қурилиши мумкин. Иккала холда хам очиқ ва ёпиқ қисм тармоқлардан фақат тармоқлараро экран орқали фойдаланиш мумкин. Бунда очиқ қисм тармоқдан фойдаланиш ёпиқ қисм тармоқдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармоқлараро алоқа хавфсизлигининг юқори даражасини таъминлайди. Бунда хар бир брандмауэр ёпиқ тармоқни химоялашнинг алохида эшелонини хосил қилади, химояланувчи очиқ қисм тармоқ эса экранловчи қисм тармоқ сифатида иштирок этади.

Одатда экранловчи қисм тармоқ шундай конфигурацияланадики, қисм тармоқ компьютеридан ғаним ташқи тармоқ ва локал тармоқнинг ёпиқ қисм тармоғи фойдалана олсин. Аммо ташқи тармоқ ва ёпиқ қисм тармоқ орасида тўғридан-тўғри ахборот пакетларини алмашиш мумкин эмас. Экранловчи қисм тармоқли тизимни хужум қилишда, бўлмаганида химоянинг иккита мустақил чизиғини босиб ўтишга тўғри келади. Бу эса жуда мураккаб масала хисобланади. Тармоқлараро экран холатларини мониторинглаш воситалари бундай уринишни доимо аниқлаши ва тизим маъмури ўз вақтида рухсатсиз фойдаланишга қарши зарурий чоралар кўриши мумкин.

Таъкидлаш лозимки, алоқанинг коммутацияланувчи линияси орқали уланувчи масофадаги фойдаланувчиларнинг иши хам ташкилотда ўтказилувчи хавфсизлик сиёсатига мувофиқ назорат қилиниши шарт. Бундай масаланинг намунавий хал этилиши – зарурий функционал имкониятларга эга бўлган масофадан фойдаланиш серверини (терминал серверни) ўрнатиш. Терминал сервер бир неча асинхрон портларга ва локал тармоқнинг битта интерфейсига эга бўлган тизим хисобланади. Асинхрон портлар ва локал тармоқ орасида ахборот алмашиш фақат ташқи фойдаланувчини аутентификациялашдан кейин амалга оширилади.

Терминал серверни улаш шундай амалга ошириш лозимки, унинг иши фақат тармоқлараро экран орқали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурслари билан ишлаш хавфсизлигининг керакли даражасини таъминлашга имкон беради.

Терминал серверни очиқ кисм тармоқ таркибига киритилганида бундай уланиш жоиз хисобланади. Терминал серверннинг дастурий таъминоти коммутацияланувчи каналлар орқали алоқа сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошқариш модуллари серверни ўзини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш бўйича етарлича ривожланган имкониятларга эга ва қуйидаги функцияларни бажаради:

- кетма-кет портлардан, PPP протоколи бўйича масофадан, хамда маъмур консолидан фойдаланишда локал паролни ишлатиш;

- локал тармоқнинг қандайдир машинасининг аутентификациялашга сўровидан фойдаланиш;

- аутентификациялашнинг ташқи воситаларидан фойдаланиш;

- терминал сервери портларидан фойдаланишни назоратловчи руйхатни ўрнатиш;

- терминал сервер орқали алоқа сеансларини протоколлаш.

Шахсий ва тақсимланган тармоқ экранлари. Охирги бир неча йил мобайнида корпоратив тармоқ тузилмасида маълум ўзгаришлар содир бўлди. Агар илгари бундай тармоқ чегараларини аниқ белгилаш мумкин бўлган бўлса, хозирда бу мумкин эмас. Яқиндаёқ бундай чегара барча маршрутизаторлар ёки бошқа қурилмалар (масалан, модемлар) орқали ўтар ва улар ёрдамида ташқи тармоқларга чиқилар эди. Аммо хозирда тармоқлараро экран орқали химояланувчи тармоқнинг тўла хуқуқли эгаси – химояланувчи периметр ташқарисидаги ходим хисобланади. Бундай ходимлар сирасига уйдаги ёки мехнат сафаридаги ходимлар киради. Шубхасиз, уларга хам химоя зарур. Аммо барча анъанавий тармоқлараро экранлар шундай қурилганки, химояланувчи фойдаланувчилар ва ресурслар уларнинг химоясида корпоратив ёки локал тармоқнинг ички томонида бўлишлари шарт. Бу эса мобил фойдаланувчилар учун мумкин эмас.

Бу муаммони ечиш учун қуйидаги ёндашишлар таклиф этилган:

- тақсимланган тармоқлараро экранлардан (distributed firewall) фойдаланиш;

- виртуал хусусий тармоқ VPNлар имкониятидан фойдаланиш.

Тақсимланган тармоқлараро экран тармоқнинг алохида компьютерини химояловчи марказдан бошқарилувчи тармоқ мини-экранлар мажмуидир.

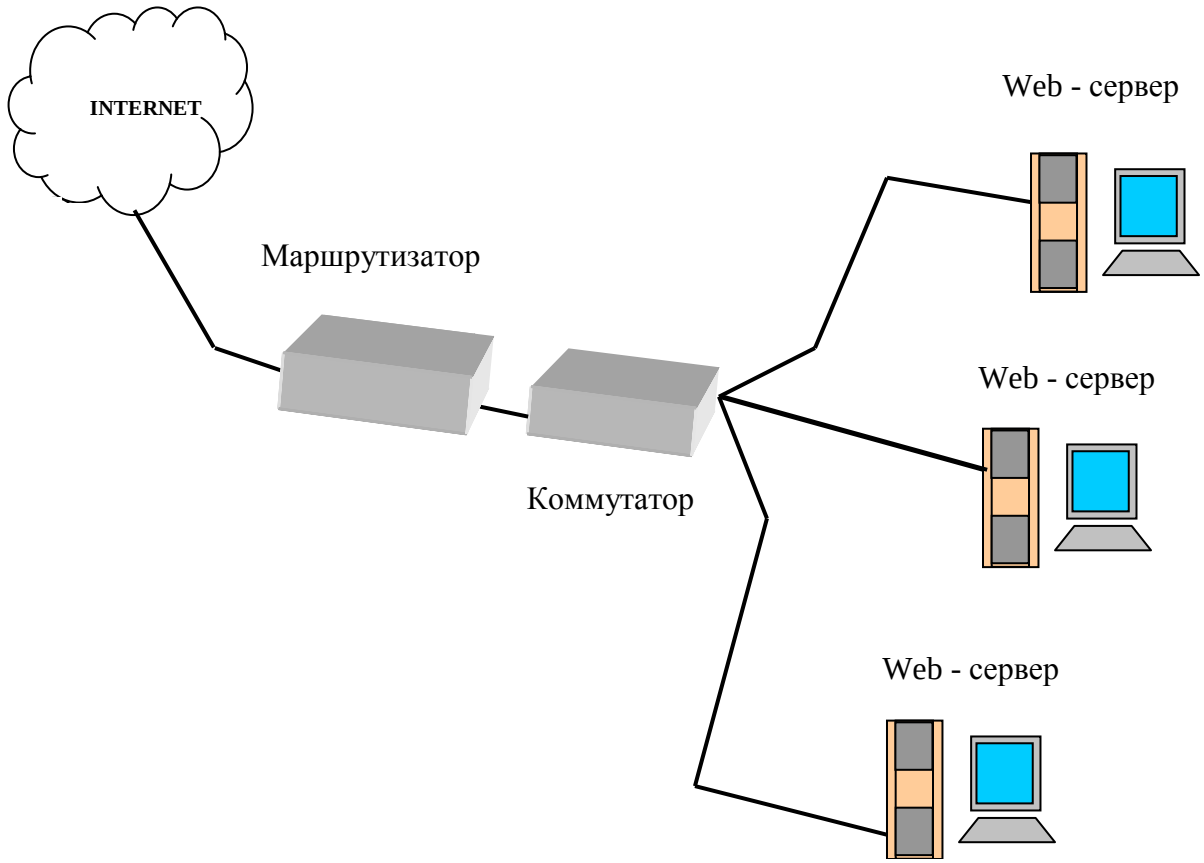
Тақсимланган брандмауэрларнинг қатор функциялари (масалан марказдан бошқариш, хавфсизлик сиёсатини тарқатиш) шахсий фойдаланувчилар учун ортиқча бўлганлиги сабабли, тақсимланган брандмауэрлар модификацияланди. Янги ёндашиш *шахсий тармоқли экранлаш технологияси* номини олди. Бунда тармоқли экран химояланувчи шахсий компьютерда ўрнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармоқли экранлаш тизими деб аталувчи бундай экран, бошқа барча тизимли химоялаш воситаларига боғлиқ бўлмаган холда бутун чиқувчи ва кирувчи трафикни назоратлайди. Алохида компьютерни экранлашда тармоқ сервисдан фойдаланувчанлик мададланади, аммо ташқи фаолликнинг юкланиши пасаяди. Натижада, шу тариқа химояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузуқ одам олдин, химоялаш воситалари синчиклаб ва қатъий конфигурацияланган, экранни босиб ўтиши лозим.

Тақсимланган тармоқлараро экраннинг шахсий экрандан асосий фарқи-тақсимланган тармоқлараро экранда марказдан бошқариш функциясининг борлиги. Агар шахсий тармоқли экранлар улар ўрнатилган компьютер орқали бошқарилса (уй шароитида қўлланишга жуда мос), тақсимланган тармоқлараро экранлар ташкилотнинг бош офисида ўрнатилган бошқаришнинг умумий консоли томонидан бошқарилиши мумкин.

Корпоратив тармоқ рухсатсиз фойдаланишдан хақиқатан хам химояланган хисобланади, қачонки унинг Internetдан кириш нуқтасида химоя воситалари хамда ташкилот локал тармоғи фрагментларини, корпоратив серверларини ва алохида компьютерлар хавфсизлигини таъминловчи ечимлар мавжуд бўлса. Тақсимланган ёки шахсий тармоқлараро экран

асосидаги ечимлар алохида компьютерлар, корпоратив серверлар ва ташкилот локал тармоқ фрагментлари хавфсизлигини таъминлашни аъло даражада бажаради.

Тақсимланган тармоқлараро экранлар, анъанавий тармоқлараро экранлардан фарқли равишда, қўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан Internet-серверларни ишончли химоялаши мумкин. Корпоратив тармоқни химоялашнинг оқилона ечими – химоялаш воситасини у химоя қилувчи сервери билан бир платформада жойлаштиришдир. 7.16-расмда корпоратив серверларни тақсимланган тармоқлараро экранлар ёрдамида химоялаш схемаси келтирилган.



3.16 -расм. Тақсимланган тармоқлараро экранлар ёрдамида корпоратив серверларни химоялаш

Анъанавий ва тақсимланган тармоқлараро экранларни қуйидаги кўрсаткичлари бўйича таққослайлик.

Самарадорлик. Анъанавий брандмауэр кўпинча тармоқ периметрии бўйича жойлаштирилади, яъни у химоянинг бир қатламини таъминлайди

холос. Агар бу ягона қатлам бузилса, тизим харқандай хужумга бардош бераолмайди. Шахсий брандмауэр операцион тизимнинг ядро сатхида ишлайди ва барча кирувчи ва чиқувчи пакетларни текшириб корпоратив серверларни ишончли химоялайди.

Ўрнатилишининг осонлиги. Анъанавий брандмауэр корпоратив тармоқ конфигурациясининг бўлими сифатида ўрнатилиши лозим. Тақсимланган брандмауэр дастурий таъминот бўлиб, саноқли дақиқаларда ўрнатилади ва олиб ташланади.

Бошқариш. Анъанавий брандмауэр тармоқ маъмури томонидан бошқарилади. Тақсимланган брандмауэр тармоқ маъмури ёки локал тармоқ фойдаланувчиси томонидан бошқарилиши мумкин.

Унумдорлик. Анъанавий брандмауэр тармоқлараро алмашишни таъминловчи қурилма бўлиб, унумдороиги (пакет/дақиқа бўйича) белгиланган чегараланишга эга. У бир-бири билан коммутацияланувчи махаллий тармоқ орқали боғланган ўсувчи сервер парклари учун тўғри келмайди. Тақсимланган брандмауэр қабул қилинган хавфсизлик сиёсатига зиён етказмасдан сервер паркларини ўсишига имкон беради.

Нархи. Анъанавий брандмауэр, одатда функциялари белгиланган, нархи етарлича юқори тизим хисобланади. Брандмауэрнинг тақсимланган махсулотлари дастурий таъминот бўлиб, анъанавий тармоқлараро экранлар нархининг 1/5 ёки 1/10 га тенг.

ХУЛОСА

Учинчи бўлимда қуйидаги масалалар кўрилган:

- тармоқлараро экранларнинг ишлаш хусусиятлари ва улаш схемалари;
- тармоқлараро экранларнинг асосий компонентлари;
- тармоқлараро экранлар асосидаги тармоқ химоясининг схемалари, шахсий ва тақсимланган тармоқ экранлари келтирилган.

УМУМИЙ ХУЛОСА

Битирув малакавий ишда қуйидаги масалалар келтирилган:

- тармоқнинг ташкил этилиши ва уларга қўйиладиган талаблар, асосан тармоқнинг ташкмл этилиши, тармоқ элементлари, уларнинг вазифалари ва хусусиятлари, тармоқ тузилмалари компонентлари, тармоқнинг функционал модели, коммутация усуллари;

- ахборот хавфсизлигини бузилишига олиб келувчи тахдидларнинг турлари ва уларнинг таснифлари, химоянинг бузилишлари, пассив хужумлар, маълумотлар оқимини тахлили, ахборотлар мазмунини фош этиш, химоя механизмлари;

- ахборот хавфсизлигини таъминлаш чоралари таснифлари, компьютер тизимлари ва тармоқларининг ахборот хавфсизлигини таъминлаш ва аппарат дастурли воситалари;.

- ўзаро очиқ тизимларнинг эталон моделини хавфсизлик архитектураси, ахборот хавфсизлигининг хизматлари ва механизмлари;

- ахборот хавфсизлигининг дастурий техникавий воситаларининг тузилиши;

- тармоқлар оралиги экранлари ва ўрнатиш чизмаси, тармоқлараро экранларнинг асосий ташкил этувчилари;

- тармоқлараро экранларнинг ишлаш хусусиятлари ва улаш схемалари;

- тармоқлараро экранларнинг асосий компонентлари;

- тармоқлараро экранлар асосидаги тармоқ химоясининг схемалари, шахсий ва тақсимланган тармоқ экранлари кўриб ўтилган.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Домарев В.В Безопасность информационных технологий: методология создания систем защиты / В.В. Домарев. – М.: СПб; Киев: DS DifSoft , 2001. - 688с
2. Петраков А.В. Основы практической защиты информации.: - М.: Радио и связь., 1999 г.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных тизимх и сетях.- М.: Радио и связь, 1999 г.
4. Кулаков М.В., Гаранин А.В., Информационная безопасность телекоммуникационных систем (технические аспекты) Учеб. Пособие для вузов М.: Радио и Связь 2004

1. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие М.: 2002.
2. Зегжда Д.П. Основы безопасности информационных систем: Учеб. пособие для студ. вузов. – М.: Горячая линия – Телеком, 2000. - 452с.
7. С.К. Ғаниев, М.М. Каримов, К.А. Ташев “Ахборот хавфсизлиги” –Ўқув қўлланма – Т., “Алоқачи”, 2008, 382 бет.
8. Д.Е Акбаров «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» -Тошкент, “Ўзбекистон маркаси” нашриёти, 2009 – 432 бет.
9. Шакина Л.Г. «Охрана труда на предприятиях связи» М: Радио и связь, 1983г
10. Охрана труда на предприятиях связи. Под. редакции Н.И. Баклашова. М.-1985 г.

ИЛОВА