ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ

“Ҳимояга рухсат этилди”

ТИ кафедраси мудири в.б _____ Б.О.Туйчиев

«_____»_____2015й

*«*КОРПОРАТИВ ТИЗИМЛАРНИ ТАШКИЛ ЭТИШДА VPN ТЕХНОЛОГИЯСИДАН ФОЙДАЛАНИШНИНГ АҲАМИЯТИ*»*

мавзусида

БИТИРУВ МАЛАКАВИЙ ИШИ

Битирувчи _____ З.А.Муртозаев
Имзо

Раҳбар _____ М.Ф.Тўраев
Имзо

Тақризчи _____ С.М.Исаев
Имзо

ҲФХ маслаҳатчиси _____ З.З.Нигматов
Имзо

Қарши– 2015

МУНДАРИЖА

Кириш

Интернет исталган компьютер эгасига чекланмаган ахборот ресурсларидан фойдаланишга имконият очиб бериш орқали жадаллик билан ривожланмоқда. Юқоридагилар билан бир қаторда, бугунги ишбилармонлар оламида шундай ҳолатлар кузатилиши мумкинки, бунда корпоратив тармоқдан фойдалана олиш, исталган вақтда жуда муҳим ҳолатга айланиши мумкин. Корхона ва ташкилотлар турли географик ҳудудларда жойлашган ишчи кучларидан фойдаланиш имконини берувчи технологияларни қўллашга ҳаракат қилмоқда. Бу технологиялар ходимлар ёрдамида хизмат сафари давомида ҳам ўзи турган меҳмонхона рақамидан тўғридан-тўғри корпоратив тармоққа кира олиш имкониятига эга бўлиши, уйда туриб ишлайдиганлар бўлса, реал вақт давомида компаниянинг бош офиси билан алоқа боғлаши мумкин. Шериклар ва хомашё етказиб берувчилар билан ҳамкорликни мустаҳкамлаш мақсадида, компаниялар улар учун ўзларининг тармоғида алоҳида бўлимларини ташкил этиш орқали янги маҳсулотларни татбиқ этишга сарфланадиган вақтни тежаш билан мижозларга хизмат кўрсатишни яхшилайдилар.

VPN хизмати ҳудудий жиҳатдан тарқалган локал тармоқларни ва мижозлар узелларини ягона корпоратив тармоққа бирлаштирилишини таъминлайди. VPN дан фойдаланиш мижозларга корпоратив инфратузилмани яратиш ва таъминлаш сарф-ҳаражатларини бир неча марта қисқартириш имконини беради. Бу эсамижознинг бир-биридан узоқлашиб кетган объектларининг ўзароалоқа қилишини сезиларли даражада енгиллаштиради. Ана шу тармоқ асосида ташкил этилган VPN, функционал жиҳатдан корхоналарда ишлатиладиган ихтиёрий ахборот тизимлари ва дастурлар билан уйғунлаша олади (маълумотлар базалари, SPM тизимлари, ERP, электрон почта, телефония, видеоконференция, телевидение каналлари, электрон савдо тизимлари, қўриқлаш ва хавфсизлик тизимлари ва ҳоказо).

Ушбу битирув малакавий ишида ҳимояланган виртуал хусусий тармоқларни қуриш технологияси, унинг афзалликлари, VPN тармоғини

ташкил этишнинг назарий ва амалий асослари, тармоқни ташкил этишнинг дастурий ва техник воситалари, VPN турлари, қўлланилиши, хизматларининг тавсифлари ва шу каби масалаларни ёритишга қаратилган.

Мавзунинг долзарблиги

Интернетнинг ривожланиши натижасида дунёда ахборотни тарқатиш ва фойдаланишда сифатий ўзгариш содир бўлди. Интернет фойдаланувчилари арзон ва қулай коммуникацияга эга бўлдилар. Корхоналар Интернет каналларидан жиддий тижорат ва бошқарув ахборотларини узатиш имкониятларига қизиқиб қолдилар. Аммо интернетнинг қурилиши принципи айрим фойдаланувчиларга ахборотни ўғирлаш ёки атайин бузиш имкониятини яратди. Одатда TCP/IP протоколлар ва стандарт Интернет-иловалар (e-mail, Web, FTP) асосида қурилган корпоратив ва идора тармоқлари суқилиб киришдан кафолатланмаганлар. Интернет тармоғида маълумотларни ҳиоялаш бугунги кунда ахборот коммуникация технологиялари соҳасининг долзарб масалаларидан бири ҳисобланади.

Шундай қилиб, VPN туннели очиқ тармоқ орқали ўтказилган уланиш бўлиб, у орқали виртуал тармоқнинг криптографик ҳимояланган ахборот пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги ҳимоялаш қуйидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг ҳақиқийлигини ва яхлитлигини текшириш.

Битирув малакавий ишининг мақсади ва вазифалари

Битирув малакавий ишини бажариш давомида қуйида келтирилган вазифаларни бажариш мақсад қилиб олинган.

1. VPNтармоғини ташкил этишнинг назарий ваамалий асослари ўрганиш.

2.VPN технологиясининг ютуқлари ва камчиликларини уммий таҳлил қилиш.

3. VPN тармоғини ташкил этишнинг дастурий ва техник воситаларини кўриб чиқиш.

4. Ҳимояланган виртуал хусусий тармоқларни қуриш технологиясини тадқиқ қилиш.

5. IPSec протоколлар стекини ҳимояланган виртуал хусусий тармоқлар қуришда ишлатилишини кўриб чиқиш.

6. VPN тармоғига дастурий ватехник хизмат кўрсатиш бўйичаамалий билим ва кўникмаларга эга бўлиш.

Битирув малакавий ишининг тузилиши.

Битирув малакавий иши қуйидаги қисмлардан ташкил топган. Кириш, асосий қисм, Ҳаёт фаолияти хавфсизлиги қисми, хулоса ва таклифлар, фойдаланилган адабиётлар ва интернет ресурслари рўйхати ва иловалар қисмларидан иборат.

БМИнинг кириш қисмида мавзунинг долзарблиги, ишнинг мақсади ва вазифалари хамда битирув малакавий ишининг тузилиши баён қилинган.

Асосий қисм БМИнинг мазмунини тўлиқ ёритиб бериш учун 2 таасосий бобдан ташкил топган.

I – боб.VPN тармоғини ташкил этишнинг назарий ва амалий асослари

II – боб. Ҳимояланган виртуал хусусий тармоқларни қуриш технологияси бўйича асосий тушунчаларни ўрганишга бағишланади. Бу боблар хам ўз навбатда бир қанча мавзуларни қамраб олган.

Ҳаёт фаолияти хавфсизлиги қисмида компьютер ва бошқаофис техникаси жихозларидан фойдаланувчилар учун хавфсизлик техникаси ва санитария, гигиена қоидалари келтириб ўтилган.

Хулоса қисмида БМИни бажариш ва тайёрлашда эгалланган амалий билим ва кўникмалар ва шулар асосида келиб чиққан умумий хулосалар баён этилган.

БМИни шакллантиришда фойдаланилган илмий адабиётлар, журналлар, Президентимиз И.А Каримов асарлари, хусусан АКТ сохасини ривожлантириш бўйича чикарилган бир қанча карор ва фармойишлари, газета ва илмий журнал нашрлари ва интернет ресурслари рўйхати фойдаланилган адабиётлар рўйхати кисмида келтириб ўтилган.

Илова қисмида БМИнинг хисоблаш тушунтириш ёзувининг электрон варианти, ишнинг тақдимот слайди, БМИгаоид бир қанча чизма ва графиклар компакт дискка ёзилиб, иш сўнгида илова қилинган.

I-БОБ. VPN ТАРМОҒИНИ ТАШКИЛ ЭТИШНИНГ НАЗАРИЙ ВА АМАЛИЙ АСОСЛАРИ

I.1. Корпоратив тизимларда қўлланиладиган алоқа тармоқларининг яратилиш тарихи

Маълумот узатиш тармоқлари қуйидаги белгиларга кўра классификацияланади:

- абонент тармоғидан фойдаланувчилар тоифаси;
- ташкилот усули;
- коммутация усули;
- маъумот узатиш канал тури;
- тармоқ хажми;
- тармоқда маълумот узатиш тезлиги;
- тармоқ структураси;
- бошқарув усули.

Маълумки, компьютер тармоқлари кўп соҳаларда бўлгани каби бизнес мақсадида эмас, балки ҳарбий соҳада, мудофаа ишларини ташкил этиш мақсадларида яратилган. Локал ҳисоблаш тармоқлари — LHT (LAN — Local Area Network) ни яратишишлари 1964-йил август ойида бошланган.Ўшанда RAND корпорацияси ходими PaulBaran « OnDistributed Communications: IXSecurity, Secrecy, andTamper-Free Considerations» номли меморандумини чоп етган эди. Ушбу меморандумда биринчи бўлиб, бошқарув маркази бўлмаган алоҳида ажратилган маълумот узатиш тармоқларини қуриш ғояси илгари сурилган ва ишлар билан АҚШ қуролли кучлари қўмондонлиги буюртмаси билан бажарилган эди. Лекин ушбу ғояларнинг амалиётга татбиқ этилиши орадан уч йил ўтгач, Буюк Британияда Доналд Девис томонидан амалга оширилди.

VPN тармоғи 1967-йилда, дунёда биринчи бўлиб, Британия Миллий физика лабораторияси (British National Physics Laboratory)да ЛҲТ ташкил этди. 1970-йиллар бошига келиб, бу тармоқ 200 нафар фойдаланувчига энг юқори тезлиги 0.25 Мбит/с бўлган маълумот алмашиш имкониятини берувчи

тармоқ вазифасини бажарди.Орадан 10 йил ўтиб, 1980-йилларда, ҳозирги кунда ҳамма жойда қўлланилаётган Ethernet локал тармоғининг биринчи стандарти (DEC, Intel ва Xerox компанияларининг биргаликдаги меҳнати) чоп этилди.

Биринчи ҳудудий тармоқ (WAN — Wide Area Network) ARPANET (Advanced Research Projects Agensy NETwork — Истиқболли тадқиқот лойиҳалари бўйича агентлик тармоғи) ARPA (Advanced Research Projects Agency) — АҚШ Мудофаа вазирлиги (DOD) қошидаги мудофаа ишлари истиқболли тадқиқот лойиҳалари бўйича агентлик раҳбарлиги ва молиявий кўмаги остида ташкил этилган. Бу агентлик кейинчалик DARPA (Defense Advanced Research Projects Agency — Мудофаа Истиқболли Тадқиқот Лойиҳалари Агентлиги) номини олган.

ARPANET — Пакетларни узиб улайдиган маълумотлар узатишга оид дастлабки глобал тармоқ. У ARPA ташаббуси билан 1968-йилда ҳозирги Интернет тармоғининг тажрибавий нусхаси яратилган.

1969-йил декабр ойида: UCLA — тармоқни тадқиқ қилиш Маркази, Станфорд тадқиқочилик институти, Санта-Барбара университети ва Юта университетлари боғланмалари бир тармоққа бирлаштирилди. Бир йилдан сўнг уларнинг сони ўн бештага етди ва маълумотлар алмашишда NCP (Network Control Protocol) протоколидан фойдаланила бошланди.

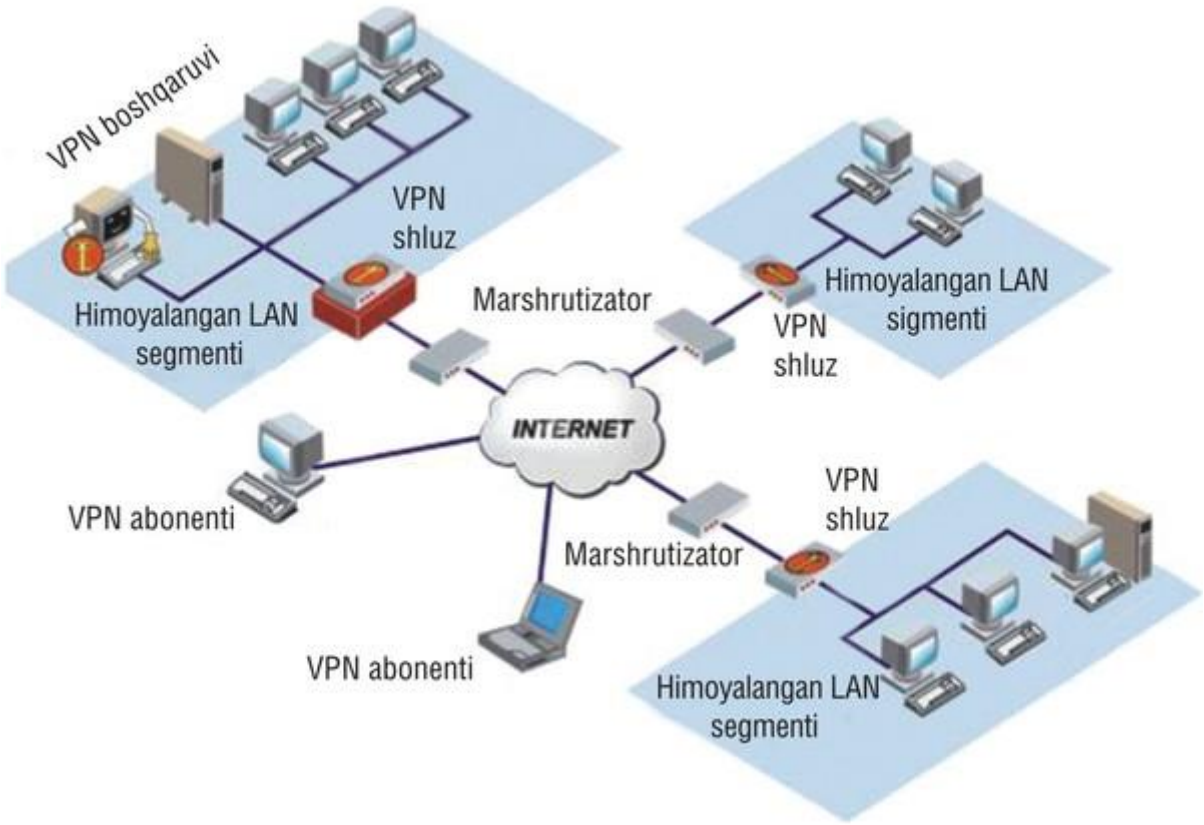
ARPANET нинг мақсади шундан иборат эдики, ундан фойдаланувчилар турли географик нуқталарда жойлашган пудратчилар, университетлар ва Мудофаа вазирлиги компьютер тармоқларининг бир-бирига боғланишини амалга ошириш ва ўша даврдаги ўта қувватли бўлган ҳисоблаш ресурсларидан биргаликда фойдаланишни таъминлашдан иборат эди.

1975-йилда тажриба тармоғи ишчи тармоқ деб еълон қилинди ва унга жавобгар етиб, ДСА Агентлиги (АҚШ Мудофаа алоқа Агентлиги) тайинланди. Шу вақтнинг ўзида мутахассислар бугунги кунда кенг қўлланилаётган TCP/IP (Transmission Control Protocol / Internet Protocol —

Узатиш жараёнлари бошқаруви протоколи/ Интернет-протокол) протоколлари асосини ишлаб чиқиш устида иш олиб бораётган эди.

TCP/IP протоколлари оиласи. Интернетда маълумотлар узатиш учун ишлатиладиган протоколлар тўплами. Дастлаб Unix операцион тизимлари учун яратилган. Ҳозирги пайтда барча асосий тизимларга ўрнатилади.
Бу ва кейинги ишлар бир неча минглаб тармоқларни бирлаштирадиган оммавий глобал тармоқ — Интернетнинг яратилишига олиб келди.

VPN (Virtual Private Network — виртуал хусусий тармоқ) — мантиқий тармоқ бўлиб, ўзидан юқоридаги бошқа тармоқ, масалан, Интернет асосида қурилади. Бу тармоқда коммуникацияларда умумий хавфсиз бўлмаган тармоқ протоколларидан фойдаланилишига қарамай, шифрлашдан фойдаланган ҳолда, ахборот алмашинишда бегоналарга берк бўлган каналлар ташкил қилинади. VPN ташкилотнинг бир неча офисларини улар ўртасида назорат қилинмайдиган каналлардан фойдаланган ҳолда, ягона тармоққа бирлаштириш имконини беради. Ўз навбатида, VPN алоҳида тармоқ хусусиятларини қамраб олган, лекин бу тармоқ умумий фойдаланиш тармоғи, масалан, Интернет орқали амалга оширилади. Туннеллаштириш методи ёрдамида маълумотлар пакети умумий фойдаланиш тармоғи орқали худди оддий икки нуқтали боғланишдаги каби трансляция қилинади. Ҳар қайси «маълумот жўнатувчи-қабул қилувчи» жуфтлиги ўртасида маълумотларни бир протоколдан иккинчи протоколга инкапсуляция қилиш имконини берувчи ўзига хос туннел — хавфсиз мантиқий боғланиш ўрнатилади.



1.1 расм- VPN каналининг ишлаш тамойили

Қуйидагилар туннелнинг асосий компонентлари ҳисобланади:

• ташаббускор;

• маршрутланувчи тармоқ;

• туннел коммутатори;

• бир ёки бир неча туннел терминаторлари.

VPNнинг ишлаш тамойили асосий тармоқ технологиялари ва протоколларидан фарқ қилмайди. Мисол учун, мижоз масофадан туриб, фойдаланиш учун серверга боғланишда стандарт PPP (Personal Post Protocol) протоколини юборади. Виртуал ажратилган линияларда локал тармоқлар ўртасида ҳам уларнинг маршрутизаторлари орқали PPP пакети алмашинади.

Туннеллаштириш мантиқий муҳитда пакетларни бир протоколдан ишлатилувчи иккинчи протоколга жўнатишни ташкиллаш имконини беради. Натижада, бир неча турли тармоқларни биргаликда ишлашида рўй берадиган, жўнатилаётган маълумотларни конфиденциаллиги ва

бутунлигини таъминлашни муҳимлигидан бошлаб, ташқи протоколлар ёки адресация схемалари номутаносиблигини бартараф этиш билан тугайдиган муаммоларни ҳал этиш имконияти пайдо бўлади. Корпорациянинг мавжуд тармоқ инфратузилмаси VPNдан фойдаланишга дастурий таъминот ёрдамида ёки қурилма таъминоти ёрдамида тайёрланган бўлиши мумкин. Виртуал хусусий тармоқни ташкиллашни айнан глобал тармоқ орқали кабел ўтказишга қиёслаш мумкин. Ушбу тармоқда масофадаги фойдаланувчи ва туннелнинг чекка қурилмаси ўртасидаги алоқа бевосита PPP протоколи бўйича ўрнатилади.

Фойдаланувчи нуқтаи назаридан, VPNнинг моҳияти — «виртуал ҳимояланган туннел», ёки у орқали масофадан туриб, Интернетнинг очиқ каналлари орқали маълумотлар омбори сервери, FTP ва почта серверларидан фойдалана олишни ташкиллаш йўлидир.

VPN технологиясининг физик моҳияти ҳар қандай интернет ва экстранет-тизимлар, аудио видеоконференциялар, электрон тижорат тизимларида ва бошқа ахборот тизимларида ахборот трафигини ҳимоя қила олиш имкониятини ўз ичига олади. Шундай қилиб, VPN — бу:

• криптографияга асосланган трафик ҳимояси;

• дунёнинг исталган нуқтасидан ички ресурслардан фойдаланиш имконини берувчи кафолатланган ҳимояловчи коммуникация воситаси;

• корпорациянинг коммуникация тизимини алоҳида ажратилган линия қуришга сарф этиладиган воситаларни ишлатмасдан ривожланишидир.

I.2. VPN технологиясидан фойдаланишнинг бугунги кундаги аҳамияти

VPN тармоқлари хизматлари бозорини ривожланишининг кўплаб омиллари мавжуд. Бозорда компанияларнинг макроиқтисодий кўрсаткичлари пасайиши уларнинг харажатини камайтирган ҳолда ўзларининг алоқа тармоқларининг самарали ишлашини ташкил этишга мажбур қилади. Корпорациялар (корхоналар ва фирмалар) ўз фаолиятини глобаллашиш жараёнида рақобатбардошлигини сақлаб қолиш учун юқори тезликдаги, ишончли ва самарали бўлган алоқа тармоқларига муҳтожлик сезадилар. Бизнеснинг мавжуд бошқарув тамойиллари ўзгармоқда: анъанавий бўлган «сотув — буюртма — харид» моделидан пакетли коммутация тармоқлари (масалан, Интернет) асосига қурилган виртуал хусусий тармоқни қўллашга олиб келувчи «телесавдо» ва «online — харид» методларини мисол келтириш мумкин.

VPN ўзининг оддий тузилишида Интернет орқали кўплаб масофавий фойдаланувчиларни ёки ташкилот тармоғи масофавий офисларини боғлайди. Айни пайтда компания ҳудудида ҳозир бўлмаган ёки бошқа шаҳарлардаги компания раҳбарияти билан алоқа ўрнатиш схемаси жуда содда. Масофадаги фойдаланувчи ўзи турган нуқтадан маҳаллий сервис-провайдерига Интернет (ISP — Internet Service Provider) хизмати учун чақирув жўнатади. Ундан сўнг чақирув шифрланади ва абонент ташкилот серверига Интернет орқали боғланади. Офис филиаллари ISP орқали ҳам ажратилган боғланишлардаги каби юқори тезликка эга бўлиши мумкин, лекин бунда шаҳарлараро алоқага қўшимча тўловлар тўланмайди.

ISP (Internet Service Provider)—Интернет хизматларини етказиб берувчи. Бошқа ташкилотларга ва хусусий шахсларга Интернетдан эркин фойдаланиш хизматларини ва қўшимча хизматларни (e-mail, news, xosting) тақдим қилувчи ташкилот.

Корхона ойлик алоқа ва Интернет сервис-провайдеридан фойдаланиш учун ҳақ тўлайди. Уларга Интернетдан фойдаланиш учун катта бўлмаган

тўлов мавжуд бўлган тежамкорликни таъминлайди. Кўпчилик ISPлар қулай бўлган тўлов схемасини тақдим этадиларки, бунда фойланиш учун тўлов қиймати сезиларли камаяди. Ҳатто баъзи технологиялар мавжудки, булар ёрдамида ISP нинг кафолатланган роуминг имкониятидан фойдаланиб, исталган жойда «ёпиқ» VPNдан фойдаланиш мумкин.

Шундай қилиб, VPNнинг ишлаши Интернетнинг иккита нуқтаси орасидаги «туннел» тузилишига асосланган. Мижоз компьютер провайдер билан стандарт «нуқта-нуқта»(PPP) боғланишни амалга оширади, ундан сўнг Интернет орқали марказий тугунга уланади. Шунинг билан чекка тугунларда маълумот алмашиш мумкин бўлган, ўзида «туннел»ни ифода этувчи VPN канали ташкил қилинади. Бу туннел провайдерни ўз ичига олган ҳолда бошқа фойдаланувчиларга «ноаниқ»ликни намоён этади.

I.3. VPN турлари, қўлланилиши ва хизматларининг тавсифи

VPN нинг учта асосий кўриниши қабул қилинган: масофадан туриб фойдаланиш имконияти мавжуд бўлган VPN (Remote Access VPN), ташкилот ичидаги VPN (Intranet VPN) ва ташкилотлараroVPN (Extranet VPN).

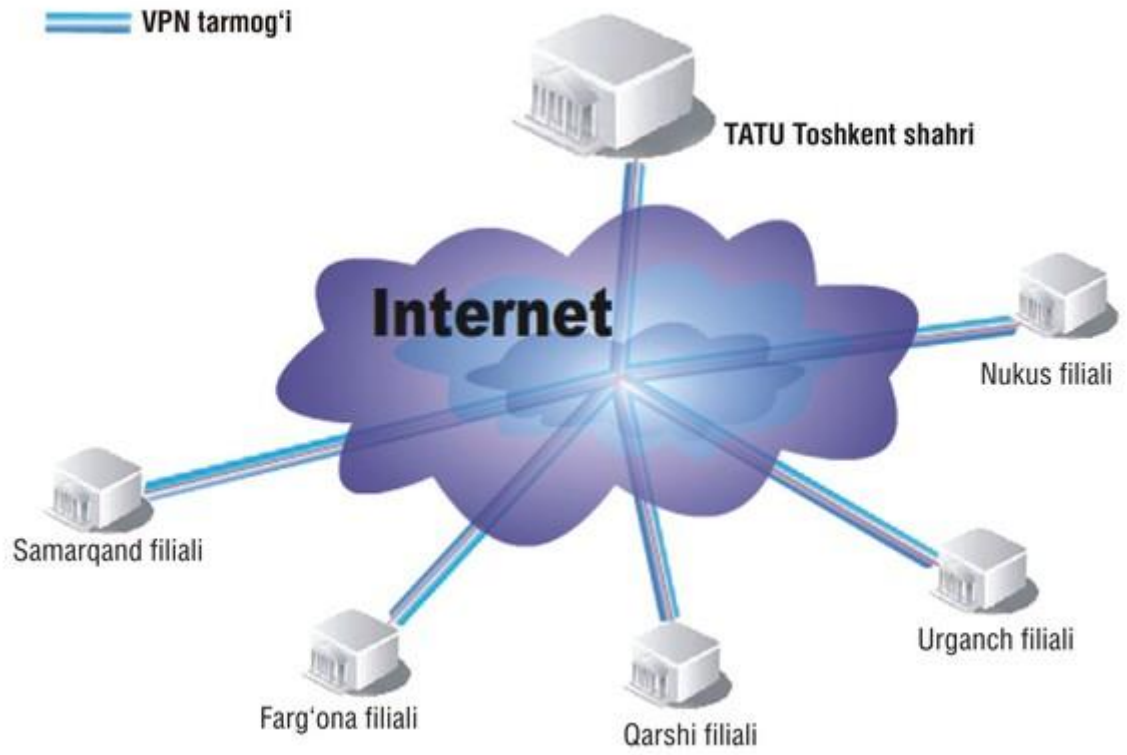
• масофадан туриб фойдаланиш имконияти мавжуд бўлган VPN баъзан DialVPN деб ҳам номланади. Улар мустақил dial-up –фойдаланувчиларга хавфсиз тарзда Интернет ёки бошқа умумий фойдаланиш тармоғи орқали марказий офис билан боғланиш имконини беради.

• Интранет VPN «нуқта-нуқта» ёки LAN-LAN VPN деб ҳам аталади. Бу тур VPN бутун Интернет ёки бошқа умумий фойдаланиш тармоғи орқали хавфсиз хусусий тармоқлар яратади.

• Extranet VPN бўлса, электрон тижорат учун идеал муҳит вазифасини бажаради. Бу VPN боғланиш ёрдамида бизнес ҳамкорлар, хом ашё етказиб берувчилар ва мижозлар билан хавфсиз боғланиш имконияти мавжуд. Extranet VPN — бу Интранет VPNнинг кенгайтирилган кўриниши бўлиб, унда ички тармоқни ҳимоя этиш мақсадида firewall дан фойдаланилади.

Юқорида биз VPN тармоғи, унинг бугунги ҳаётимиздаги аҳамияти, ишлаш тамойиллари ҳақида назарий маълумотлар келтириб ўтдик. Бугунги кунда Тошкент ахборот технологиялари университети ва унинг ҳудудий филиаллари орасида VPN тармоғи ташкил этилган бўлиб, ушбу соҳада амалга оширилаётган ишлар тўғрисида ҳам тўхталиб ўтсак.

ТАТУ билан филиаллар ўртасида VPN технологиясига асосланган, замонавий оптик толали алоқа кабелидан фойдаланилган корпоратив тармоқ ташкил этилган.



1.2-расм ТАТУ ва унинг филиаллари ўртасида ташкил этилган VPN тармоғи структураси

Ҳозирги кунда тезкор ахборот алмашинувини йўлга қўйиш мақсадида VPN тармоғи ишлаб турибди. Бугунги кунда филиалимиз профессор-ўқитувчилари ва талабалари VPN технологиясига асосланган корпоратив тармоқ орқали ТАТУ ички локал тармоғида, фойдаланишга рухсат этилган ахборот ресурсларидан, электрон кутубхонасидан, файл серверидан, электрон почта хизматидан, KARMAT-TUIT Elib дастури асосида ТАТУ ҳамда Алишер Навоий номли Ўзбекистон Миллий кутубхонаси ахборот ресурсларидан унумли фойдаланиш имкониятига эгадирлар.

Бундан ташқари, филиалимиз профессор-ўқитувчилари VPN тармоғига уланган ҳолда худди ички локал тармоқдаги сингари маълумот алмашиш имкониятига эга бўлдилар. Яъни, VPN тармоғига тармоқнинг логини ҳамда пароли терилади ва қайси IP-манзилда фойдаланишга рухсат этилган маълумот жойлашганлигини билган ҳолда шу IP-манзилдан маълумот олишлари ёки маълумот узатишлари мумкин.

Келажакда VPN тармоғи орқали Қарши филиали билан ТАТУ ўртасида ҳамда ривожланган мамлакатларнинг олий таълим муассасалари билан масофавий таълимни йўлга қўйиш ва улар билан илмий-амалий видеоконференциялар ўтказиш режалаштирилган.

VPN хизматларнинг тавсифи. VPN хизмати ҳудудий жиҳатдан тарқалган локал тармоқларни ва мижозлар узелларини ягона корпоратив тармоққа бирлаштирилишини таъминлайди. VPN дан фойдаланиш мижозларга корпоратив инфратузилмани яратиш ва таъминлаш сарф-ҳаражатларини бир неча марта қисқартириш имконини беради. Бу эса мижознинг бир-биридан узоқлашиб кетган объектларининг ўзаро алоқа қилишини сезиларли даражада енгиллаштиради. Ана шу тармоқ асосида ташкил этилган VPN, функционал жиҳатдан корхоналарда ишлатиладиган ихтиёрий ахборот тизимлари ва дастурлар билан уйғунлаша олади (маълумотлар базалари, SPM тизимлари, ERP, электрон почта, телефония, видеоконференция, телевидение каналлари, электрон савдо тизимлари, қўриқлаш ва хавфсизлик тизимлари ва ҳоказо).

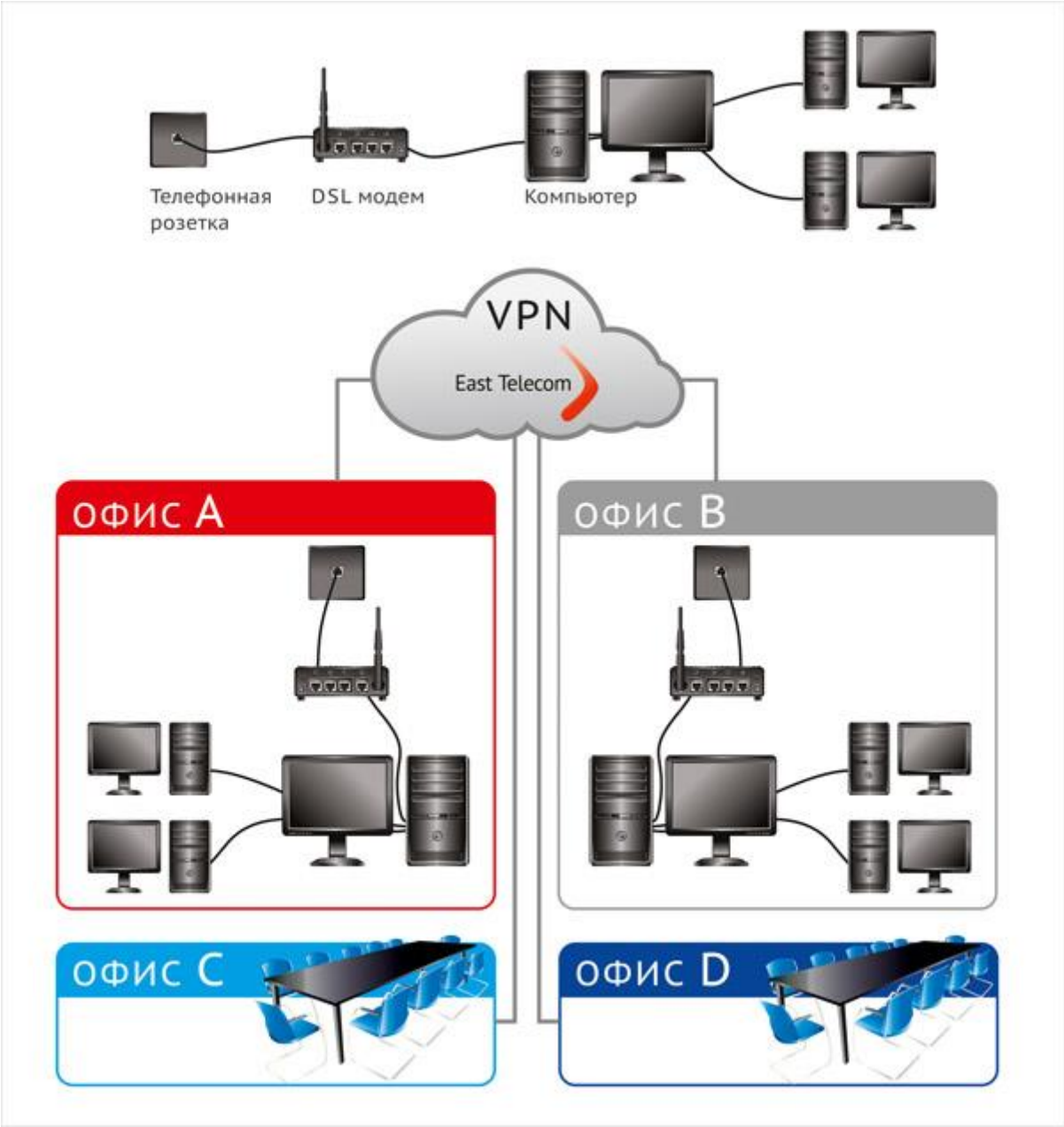
Турли маълумотлар трафигини узатишга (Интернет, овоз, видео) эҳтиёжи бўлган, Республика бўйича кенг тарқалган филиалларга эга йирик компаниялар ҳам, бир шаҳар чегарасидагина бир нечта офисларга эга унча катта бўлмаган компаниялар ҳам VPN фойдаланувчилари бўлиши мумкин. VPN нинг ахборот хавфсизлиги маълумотларни узатиш халқаро тармоқларига (Интернет) тўғридан-тўғри ҳимояланмаган уланишга эга бўлмаган, операторнинг ажратиб олинган транспорт тармоғида MPLS VPN технологияларини қўллаш ҳисобига таъминланади. Ҳимояланган IP – шлюзнинг яхлит функцияси ва маршрутизатор функцияларига эга бўлган абонент қурилмаларини қўллаш мижоз томонидан қўшимча канал яратувчи асбоб-ускуналар ва шахсий хавфсизлик шлюзларини ишлатиш заруриятидан халос этади. Иккинчи томондан, зарурат туғилганида мижоз ўзининг имкониятларидан келиб чиқиб, муҳим маълумотларни шифрлаш, электрон

калит ва сертификатлардан фойдаланиш каби қўшимча ҳимоя билан таъминлаши мумкин бўлади.

Иккинчи даражали виртуал хусусий тармоқ. L2 VPN (VPLS Virtual Private LAN Service) Иккинчи даражали виртуал хусусий тармоғи – географик жиҳатдан олисда жойлашган бир нечта офисларни юқори тезликдаги ягона хавфсиз тармоққа бирлаштириш усулидир. Иккинчи даражали виртуал хусусий тармоқларни яратиш бўйича ечимларнинг ноёблиги шундаки, L2 VPN муайян IP тармоқларига боғланмаган, ҳамда Ethernet даражасида ишлайди Бу шуни англатадики, виртуал хусусий тармоқ корпоратив тармоқларда турли тармоқ протоколларини қўллашга ҳеч қандай чеклов қўймайди. **VPLS технологияларини қўллашнинг афзалликлари:** • Маълумотларни узатиш протоколларининг бутун мажмуасидан фойдаланиш имконияти; • мижоз тармоғининг ички тузилмаси (ҳаттоки IP –тармоқ остилари поғонасида) фақатгина буюртмачи томонидан бошқарилиши ҳисобига хавфсизлик даражасининг юқори бўлиши;

• тармоқ бўйича исталган турдаги маълумотларни , шу жумладан канал даражасида шифрланган маълумотларни ҳам ўтказиш имкониятининг мавжудлиги.

Учинчи даражали виртуал хусусий тармоқ L3 VPN (Laer 3 Virtual Private Network, IPVPN) учинчи даражали виртуал хусусий тармоғи — бу кўп сонли бир-биридан узоқ масофада жойлашган офисларни энг оддий ва тежамли усул билан бирлаштириш имконини берадиган замонавий ечимдир. Учинчи даражали виртуал хусусий тармоқда (VPN/L3) VPN узеллари ўртасидаги ўзаро алоқа IP-тармоқ остилари даражасида амалга оширилади: Хусусан учинчи даражали виртуал хусусий тармоқ нафақат бош офисни филиаллар билан бирлаштириш учун, балки, масалан, бош компьютернинг POC-терминаллар ёки банкоматлар билан алоқасини ташкил этиш учун қўлланилиши мумкин. Уланиш чизмаси:



1.3-расм VPN тармоғини уланиш схемаси

II-БОБ. ҲИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАРНИ ҚУРИШ ТЕХНОЛОГИЯСИ

II.1. Ҳимояланган виртуал хусусий тармоқларни ташкил этиш

Интернетнинг ривожланиши натижасида дунёда ахборотни тарқатиш ва фойдаланишда сифатий ўзгариш содир бўлди. Интернет фойдаланувчилари арзон ва қулай коммуникацияга эга бўлдилар. Корхоналар Интернет каналларидан жиддий тижорат ва бошқарув ахборотларини узатиш имкониятларига қизиқиб қолдилар. Аммо интернетнинг қурилиши принципи нияти бузуқ одамларга ахборотни ўғирлаш ёки атайин бузиш имкониятини яратди. Одатда TCP/IP протоколлар ва стандарт Интернет-иловалар (e-mail, Web, FTP) асосида қурилган корпоратив ва идора тармоқлари суқилиб киришдан кафолатланмаганлар.

Интернетнинг ҳамма ерда тарқалишидан манфаат кўриш мақсадида тармоқ хужумларига самарали қаршилик кўрсатувчи ва бизнесда очиқ тармоқлардан фаол ва ҳавфсиз фойдаланишга имкон берувчи виртуал хусусий тармоқ VPN яратиш устида ишлар олиб борилди. Натижада 1990 йилнинг бошида виртуал хусусий тармоқ VPN консепсияси яратилди. "Виртуал" ибораси VPN атамасига иккита узел ўртасидаги уланишни вақтинча деб кўрилишини таъкидлаш мақсадида киритилган. Ҳақиқатан, бу уланиш доимий, қатъий бўлмай, фақат очиқ тармоқ бўйича трафик ўтганида мавжуд бўлади.

Виртуал тармоқ VPN ларни қуриш консепсияси асосида етарлича оддий ғоя ётади: агар глобал тармоқда ахборот алмашинувчи иккита узел бўлса, бу узеллар орасида очиқ тармоқ орқали узатилаётган ахборотнинг конфиденциаллигини ва яхлитлигини таъминловчи виртуал ҳимояланган туннел қуриш зарур ва бу виртуал туннелдан барча мумкин бўлган ташқи фаол ва пассив кузатувчиларнинг фойдаланиши хаддан ташқари қийин бўлиши лозим [1].

[1] А.В. Соколов, В.Ф. Шангин. Зашита информации в распределенных корпоративных сетях и системах. — М.: ДМК Пресс, 2002.

Шундай қилиб, VPN туннели очиқ тармоқ орқали ўтказилган уланиш бўлиб, у орқали виртуал тармоқнинг криптографик ҳимояланган ахборот пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги ҳимоялаш қуйидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг ҳақиқийлигини ва яхлитлигини текшириш.

Бу вазифалар бир бирига боғлиқ бўлиб, уларни амалга оширишда ахборотни криптографик ҳимоялаш усулларидан фойдаланилади. Бундай ҳимоялашнинг самарадорлиги симметрик ва асимметрик криптографик тизимларнинг биргаликда ишлатилиши евазига таъминланади. VPN қурилмалари томонидан шакллантирилувчи VPN туннели ҳимояланган ажратилган линия хусусиятларига эга бўлиб, бу ҳимояланган ажратилган линиялар умумфойдаланувчи тармоқ, масалан Интернет доирасида, сафланади.

VPN қурилмалари виртуал хусусий тармоқларда VPN-мижоз, VPN-сервер ёки VPN ҳавфсизлиги шлюзи вазифасини ўташи мумкин.VPN-мижоз одатда шахсий компьютер асосидаги дастурий ёки дастурий-аппарат комплекси бўлиб, унинг тармоқ дастурий таъминоти у бошқа VPN-мижоз, VPN-сервер ёки VPN ҳавфсизлиги шлюзлари билан алмашинадиган трафикни шифрлаш ва аутентификациялаш учун модификацияла-нади. Одатда VPN-мижознинг амалга оширилиши стандарт операцион тизим-Windows HT/2000 ёки Унихни тўлдирувчи дастурий ечимдан иборат бўлади.

VPN-сервер сервер вазифасини ўтовчи, компьютерга ўрнатилувчи дастурий ёки дастурий-аппарат комплексидан иборат. VPN-сервер ташқи тармоқларнинг рухсациз фойдаланишидан серверларни ҳимоялашни ҳамда алоҳида компьютерлар ва мос VPN-маҳсулотлари орқали ҳимояланган локал тармоқ сегментларидаги компьютерлар билан ҳимояланган уланишлар-ни ташкил этишни таъминлайди. VPN-сервер VPN-мижознинг сервер платформалари учун функсионал аналог ҳисобланади. У аввало VPN-

мижозлар билан кўпгина уланишларни қўллаб-қувватловчи кенгайтирилган ресурслари билан ажралиб туради. VPN-сервер мобил фойдаланувчилар билан уланишларни ҳам қўллаб-қувватлаши мумкин.

VPN ҳавфсизлик шлюзи. (Security Gateway) иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўзидан кейин жойлашган кўп сонли хостлар учун шифрлаш ва аутентификациялаш вазифаларини бажаради. VPN ҳавфсизли-ги шлюзи шундай жойлаштириладики, ички корпоратив тармоққа аталган барча трафик у орқали ўтади. VPN ҳавфсизлиги шлюзининг адреси кирувчи туннелланувчи пакетнинг ташқи адреси сифатида кўрсатилади, пакетнинг ички адреси эса шлюз орқасидаги муайян хост адреси ҳисобланади. VPN ҳавфсизлиги шлюзи алоҳида дастурий ечим, алоҳида аппарат қурилмаси, ҳамда VPN вазифалари билан тўлдирилган маршрутизаторлар ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Ахборот узатишнинг очиқ ташқи муҳити маълумот узатишнинг тезкор каналларини (Интернет муҳити) ва алоқанинг секин ишлайдиган умумфойдаланувчи каналларини (масалан, телефон тармоғи каналларини) ўз ичига олади. Виртуал хусусий тармоқ VPNнинг самарадорлиги алоқанинг очиқ каналлари бўйича айланувчи ахборотнинг ҳимояланиш даражасига боғлиқ.

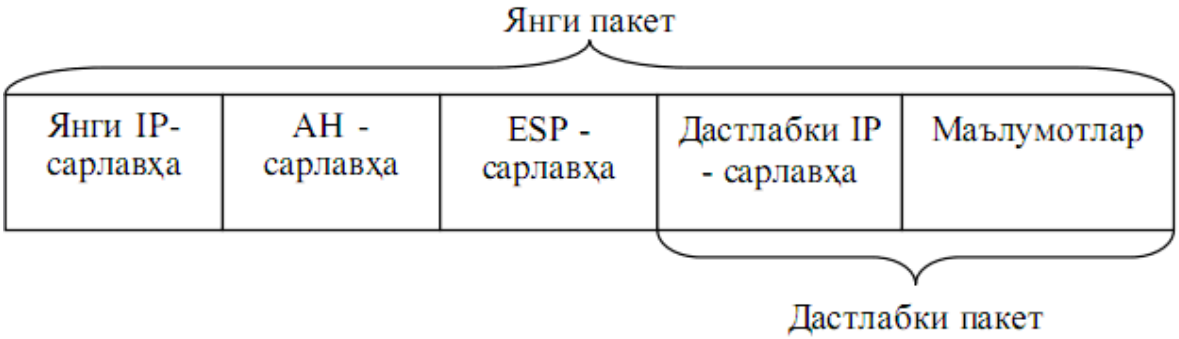
Очиқ тармоқ орқали маълумотларни ҳавфсиз узатиш учун инкапсуляциялаш ва туннеллаш кенг ишлатилади. Туннеллаш усули бўйича маълумотлар пакети умумфойдаланувчи тармоқ орқали худди оддий икки нуқтали уланиш бўйича узатилганидек узатилади. Ҳар бир "жўнатувчи-қабул қилувчи" жуфтлиги орасига бир протокол маълумотларини бошқасининг пакетига инкапсуляциялашга имкон берувчи ўзига хос туннел-мантиқий уланиш ўрнатилади.

Туннеллашга биноан, узатилувчи маълумотлар порцияси хизматчи ҳошиялар билан бирга янги "конверт"га "жойлаш" амалга оширилади.

Бунда пастроқ сатҳ протоколи пакети юқорироқ ёки худи шундай сатҳ протоколи пакети маълумотлари майдонига жойлаштирилади. Таъкидлаш

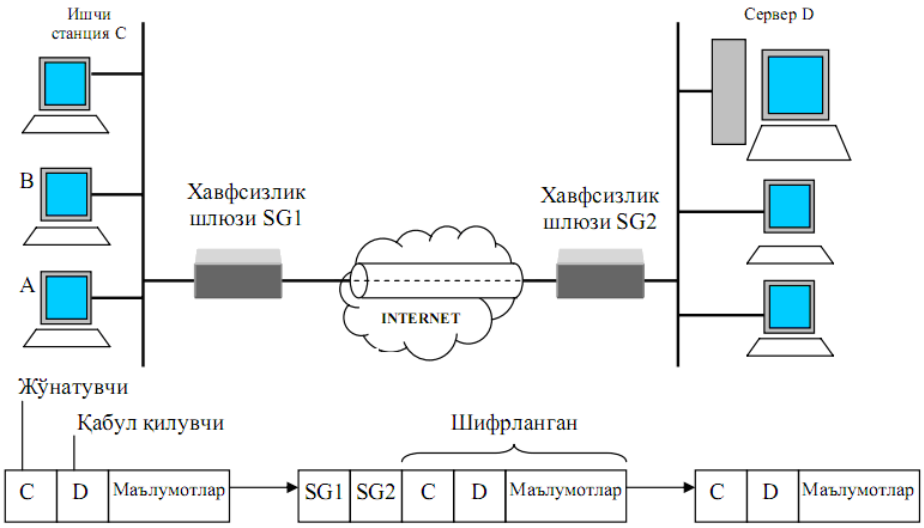
лозимки, туннелашнинг ўзи маълумотларни рухсациз фойдаланишдан ёки бузишдан ҳимояламайди, аммо туннеллаш туфайли инкапсуляцияланувчи дастлабки пакетларни тўла криптографик ҳимоялаш имконияти пайдо бўлади. Узатилувчи маълумотлар конфиденциаллигини таъминлаш мақсадида жўнатувчи дастлабки пакетларни шифрлайди, уларни, янги IP-сарлавҳа билан ташқи пакетга жойлайди ва транзит тармоқ бўйича жўнатади (2.1-расм).

Очиқ тармоқ бўйича маълумотларни ташишда ташқи пакет сарлавҳасининг очиқ каналларидан фойдаланилади.



2.1.-расм. Тунеллашга тайёрланган пакет мисоли

Ташқи пакет ҳимояланган каналнинг охирги нуқтасига келиши билан ундан ички дастлабки пакет чиқариб олиниб, расшифровка қилинади ва унинг тикланган сарлавҳаси ички тармоқ бўйича кейинги узатиш учун ишлатилади (2.2-расм)



2.2.-расм. Виртуал ҳимояланган туннел схемаси

Туннеллашдан пакет таркибини нафақат конфиденциаллигини, балки унинг яхлитлигини ва аутентилигини таъминлашда фойдаланилади. Бунда электрон рақамли имзони пакетнинг барча ҳошияларига тарқатиш мумкин.

Интернет билан боғланмаган локал тармоқ яратилганда компания ўзининг тармоқ қурилмалари ва компьютерлари учун ҳоҳлаган IP-адресдан фойдаланиши мумкин. Олдин яккаланган тармоқларни бирлаштиришда бу адреслар бир-бирлари ва Интернетда ишлатилаётган адреслар билан тўқнашишлари мумкин. Пакетларни инкапсуляциялаш бу муаммони ечади, чунки у дастлабки адресларни беркитишга ва Интернет IP адреслари маконидаги ноёб адресларни қўшишга имкон беради. Бу адреслар кейин маълумотларни ажратилувчи тармоқлар бўйича узатишда ишлатилади. Бунга локал тармоққа уланувчи мобил фойдаланувчиларнинг IP-адресларини ва бошқа параметрларини созлаш масаласи ҳам киради.

Тунеллаш механизми ҳимояланувчи канални шакллантирувчи турли протоколларда кенг қўлланилади. Одатда туннел фақат маълумотларнинг конфиденциаллиги ва яхлитлигининг бузилиши хавфи мавжуд бўлган очиқ тармоқ қисмида, масалан, очиқ Интернет ва корпоратив тармоқ кириш нуқталари орасида, яратилади. Бунда ташқи пакетлар учун ушбу икки нуқтада ўрнатилган чегара маршрутизаторларининг адресларидан фойдаланилса, охирги узелларнинг ички адреслари ички дастлабки пакетларда ҳимояланган ҳолда сақланади. Таъкидлаш лозимки, тунеллаш механизмининг ўзи қандай мақсадларда туннеллаш қўлланилаётганига боғлиқ эмас. Туннеллаш нафақат узатилаётган барча маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашда, балки турли протоколли (масалан IPV4 ва IPV6) тармоқлар орасида ўтишни ташкил этишда ҳам қўлланилади. Туннеллаш бир протокол пакетини бошқа протоколдан фойдаланувчи мантиқий муҳитда узатишни ташкил этишга имкон беради. Натижада бир неча турли хил тармоқларнинг ўзаро алоқалари муаммосини ҳал этиш имконияти пайдо бўлади.

Туннеллаш механизмини амалга оширилишига уч хил протоколлар:

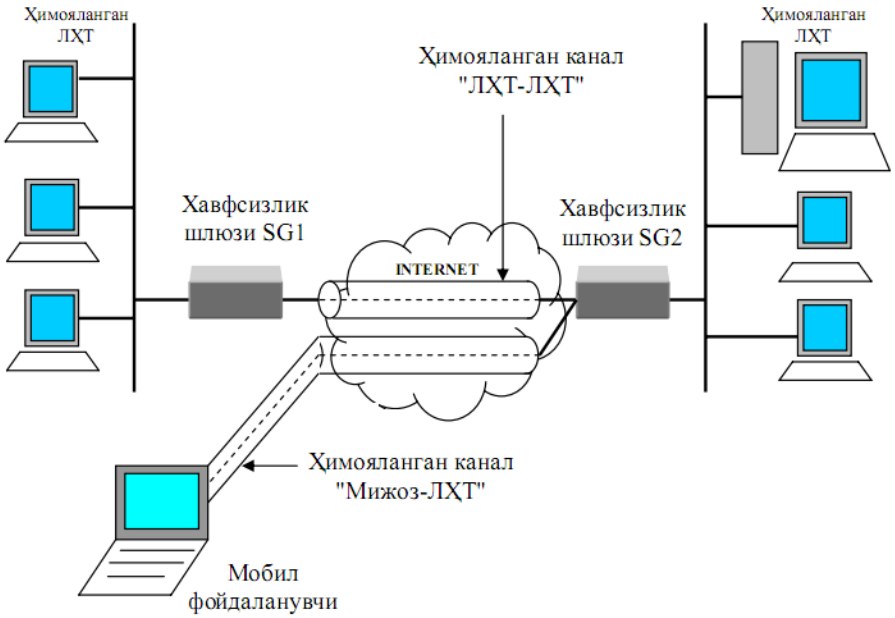
- протокол-"йўловчи", протокол элтувчи ва туннеллаш протоколи ишлаши натижаси деб қараш мумкин. Масалан, протокол-"йўловчи" сифатида битта корхона филиалларининг локал тармоқларида маълумотларни ташувчи транспорт протоколи IPX ишлатилиши мумкин. Элтувчи протоколнинг энг кўп тарқалган варианти Интернет тармоғининг IP протоколи ҳисобланади. Туннеллаш протоколи сифатида канал сатҳи протоколари

PPTP ва L2TP, ҳамда тармоқ сатҳи протоколи IPSec ишлатилиши мумкин.

Туннеллаш туфайли Интернет инфратузилмасини VPN-иловалардан беркитиш мумкин бўлади.

VPN туннеллари турли фойдаланувчилар учун яратилиши мумкин. булар ҳавфсизлик шлюзи бўлган локал тармоқ LAN ёки масофадаги ва мобил фойдаланувчиларнинг алоҳида компьютерлари бўлиши мумкин. Йирик корхонанинг виртуал хусусий тармоғини яратиш учун VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар керак бўлади. VPN-шлюзларни корхона локал тармоқларини ҳимоялаш учун ишлатиш мақсадга мувофиқ бўлса, VPN-серверлар ва VPN-мижозлардан масофадаги ва мобил фойдаланувчиларни Интернет орқали корпоратив тармоқ билан ҳимояланган уланишини ташкил этишда фойдаланилади.

Виртуал ҳимояланган каналларни қуриш усуллари. VPN ни лойиҳалашда одатда иккита асосий схема кўрилади (2.3-расм):



2.3-расм. "ЛҲТ-ЛҲТ" ва "Мижоз-ЛҲТ" хилидаги виртуал ҳимояланган каналлар

- локал тармоқлар орасидаги виртуал ҳимояланган канал ("ЛХТ-ЛҲТ" канал);

- узел ва локал тармоқ орасидаги виртуал ҳимояланган канал ("мижоз-ЛҲТ" канали).

Уланишнинг биринчи схемаси алоҳида офислар орасидаги қимматли ажратилган линиялар ўрнига ўтади ва улар орасида доимо фойдаланувчан, ҳимояланган каналларни яратади. Бу ҳолда ҳавфсизлик шлюзи туннел ва локал тармоқ орасида интерфейс вазифасини ўтайди ва локал тармоқ фойдаланувчилари бир-бирлари билан мулоқот қилишда туннелдан фойдаланадилар. Аксарият компаниялар VPN нинг бу ҳилидан глобал тармоқнинг мавжуд Фраме Релай каби уланишларни алмаштириш учун ёки уларга қўшимча сифатида фойдаланадилар.

VPN ҳимояланган каналнинг иккинчи схемаси масофадаги ёки мобил фойдаланувчилар билан уланишни ўрнатишга аталган. Туннелни яратишни мижоз (масофадан фойдаланувчи) бошлаб беради. Масофадаги тармоқни ҳимояловчи шлюз билан боғланиш учун у ўзининг компьютерида махсус мижоз дастурий таъминотини ишга туширади. VPNнинг бу тури коммутацияланувчи уланишларни ўрнига ўтади ва масофадан

фойдаланишнинг анъанавий усуллари билан бир қаторда ишлатилиши мумкин.

Виртуал ҳимояланган каналларнинг қатор вариантлари мавжуд. Умуман, орасида виртуал ҳимояланган канал шакллантирилувчи корпоратив тармоқнинг ҳар қандай иккита узели ҳимояланувчи ахборот оқимининг охирги ва оралиқ нуқтасига тааллуқли бўлиши мумкин. Ахборот ҳавфсизлиги нуқтаи назаридан ҳимояланган туннел охирги нуқталарининг ҳимояланувчи ахборот оқимининг охирги нуқталарига мос келиши варианти маъқул ҳисобланади. Бу ҳолда каналнинг ахборот пакетлари ўтишининг барча йўллари бўйлаб ҳимояланиши таъминланади. Аммо бу вариант бошқаришнинг децентрализацияланишига ва ресурс сарфининг ошишига олиб келади. Агар виртуал тармоқдаги локал тармоқ ичида трафикни ҳимоялаш талаб этилмаса, ҳимояланган туннелнинг охирги нуқтаси сифатида ушбу локал тармоқнинг тармоқлараро экрани ёки чегара маршрутизатори танланиши мумкин. Агар локал тармоқ ичидаги ахборот оқими ҳимояланиши шарт бўлса, бу тармоқ охирги нуқтаси вазифасини ҳимояланган алоқада иштирок етувчи компьютер бажаради.

Локал тармоқдан масофадан фойдаланилганида фойдаланувчи компьютери виртуал ҳимояланган каналнинг охирги нуқтаси бўлиши шарт. Фақат пакетларни коммутациялашли очиқ тармоқ, масалан Интернет ичида ўтказилувчи ҳимояланган туннел варианти етарлича кенг тарқалган. Ушбу вариант ишлатилиши қулайлиги билан ажралиб турсада, нисбатан паст ҳавфсизликка эга. Бундай туннелнинг охирги нуқталари вазифасини одатда Интернет провайдерлари ёки локал тармоқ чегара маршрутизаторлари (тармоқлараро экранлар) бажаради.

Локал тармоқлар бирлаштирилганида туннел фақат Интернетнинг чегара провайдерлари ёки локал тармоқнинг маршрутизаторлари (тармоқлараро экранлари) орасида шакллантирилади. Локал тармоқдан масофадан фойдаланилганида туннел Интернет провайдерининг масофадан фойдаланиш сервери, ҳамда Интернетнинг чегара провайдери ёки локал

тармоқ маршрутизатори (тармоқлараро экран) орасида яратилади. Ушбу вариант бўйича қурилган корпоратив тармоқлар яхши масштабланувчанлик ва бошқарилувчанликка эга бўлади. Шакллантирилган ҳимояланган туннеллар ушбу виртуал тармоқдаги мижоз компьютерлари ва серверлари учун тўла шаффоф ҳисобланади. Ушбу узелларнинг дастурий таъминоти ўзгармайди. Аммо бу вариант ахборот алоқасининг нисбатан паст ҳавфсизлиги билан характерланади, чунки трафик қисман очиқ алоқа канали бўйича ҳимояланмаган ҳолда ўтади. Агар шундай VPNни яратиш ва експлуатация қилишни провайдер ИСП ўз зиммасига олса, барча виртуал хусусий тармоқ унинг шлюзларида, локал тармоқлар ва корхоналарнинг масофадаги фойдаланувчилари учун шаффоф ҳолда қурилиши мумкин. Аммо бу ҳолда провайдерга ишонч ва унинг хизматига доимо тўлаш муаммоси пайдо бўлди.

Ҳимояланган туннел, орасида туннел шакллантирилувчи узеллардаги виртуал тармоқ компонентлари ёрдамида яратилади. Бу компонентларни *туннел инициаторлари* ва *туннел терминаторл*ари деб юритиш қабул қилинган.

Туннел инициатори дастлабки пакетни янги пакетга жўнатувчи ва қабул қилувчи хусусидаги ахбороти бўлган янги сарлавҳали пакетга инкап-суляциялайди. Инкапсуляцияланган пакетлар ҳар қандай протокол турига, жумладан маршрутланмайдиган протоколларга (масалан Нет БЕУЛ) мансуб бўлишлари мумкин. Туннел бўйича узатиладиган барча пакетлар IP пакетлари ҳисобланади. Туннелнинг инициатори ва терминатори орасидаги мар-шрутни одатда, Интернетдан фарқланиши мумкин бўлган, оддий маршрутланувчи тармоқ IP аниқлайди.

Туннелни инициаллаш ва узиш турли тармоқ қурилмалари ва дастурий таъминот ёрдамида амалга оширилиши мумкин. Масалан, туннел масофадан фойдаланиш учун улашни таъминловчи модем ва мос дастурий таъминот билан жиҳозланган мобил фойдаланувчининг ноутбуки томонидан инициалланиши мумкин. Инициатор вазифасини мос функсионал имкони-

ятларга эга бўлган локал тармоқ маршрутизатори ҳам бажариши мумкин. Туннел одатда, тармоқ коммутатори ёки хизматлар провайдери шлюзи билан тугалланади.

Туннел терминатори инкасуляциялаш жараёнига тескари жараённи бажаради. Терминатор янги янги сарлавҳаларни олиб ташлаб, ҳар бир дастлабки пакетни локал тармоқдаги адресатга йўллайди.

Инкапсулацияланувчи пакетларнинг конфиденциаллиги уларни шифрлаш, яхлитлиги ва ҳақиқийлиги эса электрон рақамли имзони шаклланти-риш йўли билан таъминланади. Маълумотларни криптографик ҳимоялашнинг жўда кўп усуллари ва алгоритмлари мавжуд бўлганлиги са-бабли, туннел инициатори ва терминатори ҳимоянинг бир хил усулларидан фойдаланишга ўз вақтида келишиб олишлари мақсадга мувофиқ ҳисобланади. Маълумотларни расшифровка қилиш ва рақамли имзони текшириш имкониятини таъминлаш учун туннел инициатор ива терминато-ри калитларни ҳавфсиз алмашиш вазифасини ҳам қўллаб-қувватлашлари зарур. Ундан ташқари, VPN туннеларини ваколатли фойдаланувчилар томонидан яратилишини кафолатлаш мақсадида ахборот алоқасининг асосий тарафлари аутентификациялашдан ўтишлари лозим. Корпорациянинг мавжуд тармоқ инфратузилмалари VPN дан фойдаланишга ҳам дастурий ҳам техник таъминот ёрдамида тайёрланишлари мумкин.

II.2. Ҳимояланган виртуал хусусий тармоқларнинг туркумланиши

Ҳимояланган виртуал хусусий тармоқлар VPN ни туркумлашни турли вариантлари мавжуд. Кўпинча туркумлашнинг қуйидаги учта аломати ишлатилади:

-OSI моделининг иш сатҳи;

- VPN техник ечимининг архитектураси;

- VPN ни техник амалга ошириш усули.

OSI моделининг иш сатҳи бўйича VPN нинг туркумланиши.

Ушбу туркумлаш анчагина қизиқиш тўғдиради, чунки амалга оширилувчи VPNнинг функсионаллиги ва унинг корпоратив ахборот тизимлари илова-лари ҳамда ҳимоянинг бошқа воситалари билан биргаликда ишлатилиши кўп ҳолларда танланган OSI сатҳига боғлиқ бўлади.

OSI моделининг иш сатҳ аломати бўйича канал сатҳидаги VPN, тармоқ сатҳидаги VPN ва сеанс сатҳидаги VPN фарқланади. Демак, VPNлар одатда OSI моделининг пастки сатҳларида қурилади. Бунинг сабаби шуки, ҳимояланган канал воситалари қанчалик пастки сатҳда амалга оширилса, уларни иловаларга ва татбиқий протоколларга шунчалик шаффоф қилиш соддалашади. Тармоқ ва канал сатҳларида иловаларнинг ҳимоя протоколларига боғлиқлиги умуман йўқолади. Шу сабабли, фойдаланувчилар учун универсал ва шаффоф ҳимояни фақат OSI моделининг пастки сатҳларида қуриш мумкин. Аммо, бунда биз бошқа муаммога-ҳимоя протоколининг муайян тармоқ технологиясига боғлиқлиги муаммосига дуч келамиз.

Канал сатҳидаги VPN. OSI моделининг канал сатҳида ишлатилувчи VPN воситалари учинчи (ва юқорироқ) сатҳнинг турли хил трафигини инкапсулациялашни таъминлашга ва "нуқта-нуқта" тилидаги виртуал туннелларни (маршрутизатордан маршрутизаторга ёки шахсий комптердан локал ҳисоблаш тармоғининг шлюзигача) қуришга имкон беради. Бу гуруҳга L2F (Layer 2 Forwarding) ва PPTP (Point-to-Point Tuneling Protocol) протоколлари ҳамда Cisco Systems и Microsoft фирмаларининг бирга ишлаб

чиққан L2TP (Layer 2 Tuneling Protocol) стандартидан фойдаланувчи VPN-маҳсулотлар тааллуқли.

Ҳимояланган каналнинг протоколи PPTP "нуқта-нуқта" уланишларида, масалан, ажратилган линияларда ишлаганда кенг қўлланилувчи PPP протоколига асосланган. PPTP протоколи иловалари ва татбиқий сатҳ хизматлари учун ҳимоя воситаларининг шаффофлигини таъминлайди ва тармоқ сатҳида ишлатилувчи протоколга боғлиқ эмас.

Хусусан, PPTP протоколи ҳам IP тармоқларида, ҳам IPX, DECNet ёки NetBeul протоколлари асосида ишловчи тармоқларда пакетларни ташиши мумкин. Аммо, PPP протоколи ҳамма тармоқларда ҳам ишлатилмаслиги сабабли (аксарият локал тармоқларида канал сатҳида Етҳернет протоколи ишласа, глобал тармоқларда ATM, Frame Relay тармоқлари ишлайди), уни универсал восита деб беллмайди. Йирик бирикма тармоқнинг турли қисмларида, умуман айтганда, турли канал протоколлари ишлатилади. Шу сабабли бу гетероген муҳит орқали канал сатҳининг ягона протоколи ёрдамида ҳимояланган канални ўтказиш мумкин эмас.

L2TP протоколи, еҳтимол, локал ҳисоблаш тармоқларидан фойдаланишни ташкил этишда устунлик қилувчи ечим бўлиб қолиши мумкин (чунки у, асосан, Windows операцион тизимига таянади.)

Тармоқ сатҳидаги VPN. Тармоқ сатҳидаги VPN-маҳсулотлар IP ни IPга инкапсуляциялашни бажаради. Бу сатҳдаги кенг тарқалган протокол-лардан бири Skip протоколидир. Аммо бу протоколни аутентификациялаш, туннеллаш ва IP-пакетларни шифрлаш учун аталган IPSec (IPSecуритй) протоколи аста-секин суриб чиқармоқда.

Тармоқ сатҳида ишловчи IPSec протоколи муросага асосланган вариант ҳисобланади. Бир томондан у иловадар учун шаффоф, иккинчи томондан кенг тарқалган IP протоколига асосланганлиги сабабли барча тармоқларда ишлаши мумкин. Шу орада есдан чиқармаслик лозимки, IPSecнинг спецификацияси IPга мўлжалланганлиги сабабли у тармоқ сатҳининг бошқа протоколлари трафиги учун тўғри келмайди. IPSec протоколи Л2ТП

протоколи билан биргаликда ишлаши мумкин. Натижада бу икки протокол ишончли идентификациялашни, стандартланган шифрлашни ва маълумотлар яхлитлигини таъминлайди. Иккита локал тармоқ орасидаги IPSec туннели маълумотлар узатувчи якка тармоқлар тўпламини қўллаб-қувватлаши мумкин. Натижада бу хилдаги иловалар масштабланиш нуқтаи назаридан иккинчи сатҳ технологияларига нисбатан устунликка эга бўлади [2].

IPSec протоколи билан масофадаги қурилмалар орасида криптографик калитларни ҳавфсиз бошқариш ва алмашиш масалаларини ечувчи IKE (Internet Key Exchange) протоколи боғланган. IKE протоколи калитларни алмашишни автоматлаштиради ва химояланган уланишни ўранатади, IPSec эса пакетларни кодлайди ва "имзо чекади". Ундан ташқари, IKE ўрнатилган уланиш учун калитни ўзгартириш имкониятига эга. Бу узатилувчи ахборотнинг конфиденциаллигини оширади.

Сеанс сатҳидаги VPN. Баъзи VPN лар "канал воситачилари" (sirsuit proxy) деб аталувчи усулдан фойдаланади. Бу усул транспорт сатҳи устида ишлайди ва ҳар бир сокет учун алоҳида трафикни ҳимояланган тармоқдан умумфойданувчи Интернет тармоғига ретрансляциялайди. (IP сокети TCP-уланишнинг ва муайян порт ёки берилган порт UDP комбинацияси орқали идентификацияланади. TCP/IP стекида бешинчи-сеанс сатҳи бўлмайди, аммо сокетларга мўлжалланган амалларни кўпинча сеанс сатҳи амаллари деб юритишади.)

Туннелнинг инициатори ва терминатори орасида узатилувчи ахборотни шифрлаш транспорт сатҳи TLS (Transport Layer Security) ёрдамида амалга оширилади. Тармоқлараро экран орқали аутентификацияланган ўтишни стандартлаш учун SOSCS деб аталувчи протокол аниқланган ва ҳозирда SOSCS протоколининг 5-версияси канал воситачиларини стандарт амалга оширилишида ишлатилади.

---

[2]Н.А.Олифер. Протоколи IPSec.//LAN.-2001.-№03; http://www.osp.ru/lan/ 2001/03/024.htm.

SOCKS протоколининг 5-версиясида мижоз компьютери воситачи (proxy) вазифаларини бажарувчи сервер билан аутентифкацияланган сокет (ёки сеанс) ўрнатади. Бу воситачи-тармоқлараро экран орқали боғланишнинг ягона усули. Воситачи, ўз навбатида, мижоз томонидан сўралган ҳар қандай амални бажаради. Воситачига сокет сатҳидаги трафик маълумлиги сабабли, у синчиклаб назорат қилиши, масалан, муайян илова-ларни, агар улар зарурий ваколатларга эга бўлмаса, блокировка қилиши мумкин.

Агар IPSec протоколи моҳияти бўйича, IP тармоқни ҳимояланган туннелга тарқаца, SOS CS протоколи асосидаги маҳсулотлар уни алоҳида ҳар бир илова ва ҳар бир сокетга кенгайтиради. Иккинчи ва учинчи сатҳнинг яратилган туннеллари иккала йўналишда бирдай ишласа, 5 сатҳнинг VPN тармоғи ҳар бир йўналишда узатишни мустақил бошқаришга рухсат беради. IPCec протоколга ва иккинчи сатҳ протоколларига ўхшаб 5 сатҳнинг VPN тармоғини виртуал хусусий тармоқларнинг бошқа турлари билан бирга ишлатилиши мумкин, чунки бу технологиялар бир-бирини инкор қилмайди.

Техник ечимининг архитектураси бўйича VPN нинг туркумланиши.

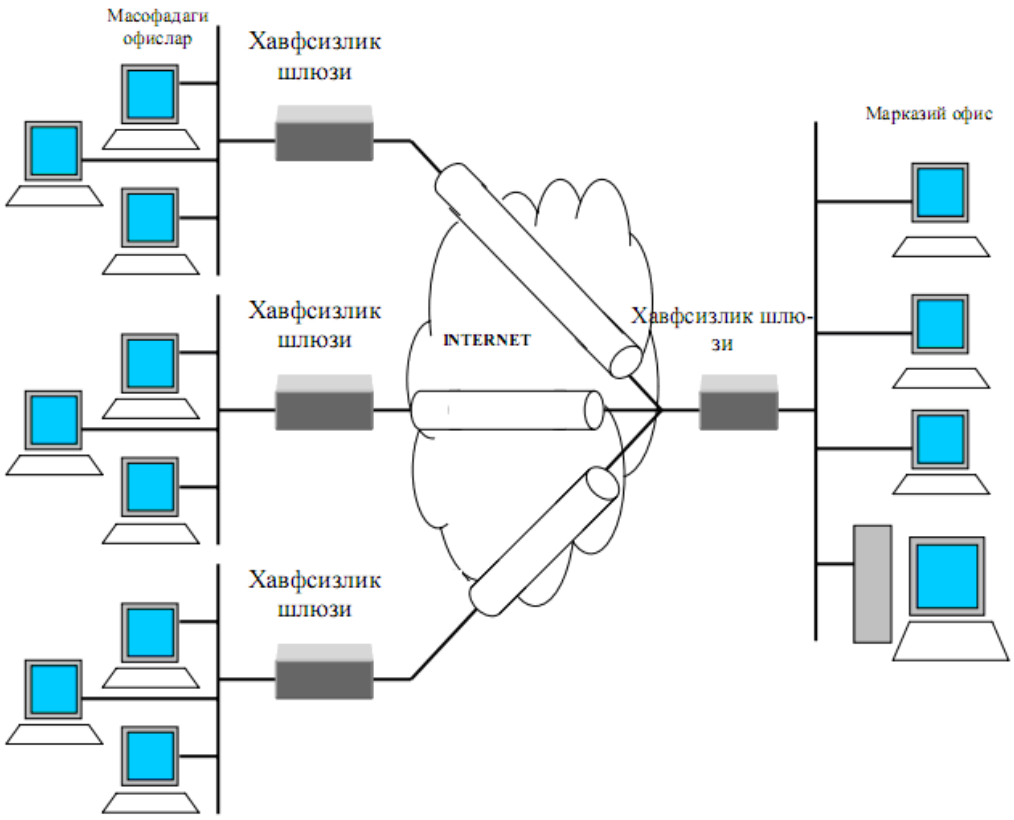
Ушбу туркумлаш бўйича виртуал хусусий тармоқлар қуйидаги уч турга бўлинади:

- корпорация ичидаги VPN тармоқ;
- масофадан фойдаланилувчи VPN тармоқ;
- корпорацияларо VPN тармоқ.

Корпорация ичидаги VPN тармоқ. Корпорация ичидаги VPN тармоқлар (Интранет VPN) корхона ичидаги бўлинмалар ёки алоқанинг корпорация тармоқлари (шу жумладан, ажратилган линиялар) ёрдамида бирлаштирилган корхоналар гуруҳи орасида ҳимояланган алоқани ташкил этиш учун ишлатилади. ўзининг филиаллари ва бўлимлари учун ахборотнинг марказлаштирилган омборидан фойдаланишга эҳтиёж сезган компа-ниялар масофадаги узелларни ажратилган линиялар ёки frame relay технологияси ёрдамида улайдилар. Аммо ажратилган линияларнинг ишлатилиши

эгалланадиган ўтказиш полосасининг ва объектлар орасидаги масофанинг катталашгани сари жорий сарф-ҳаражатларнинг ошишига сабаб бўлади.

Буларни камайтириш учун компания узелларини виртуал хусусий тармоқ ёрдамида улаши мумкин (2.4.-расм).



2.4.-расм. Компания узелларини виртуал хусусий тармоқ ёрдамида улаш.

Интранет VPN тармоқлар Интернетдан ёки сервис-провайдерлар томони-дан тақдим этилувчи бўлинувчи тармоқ инфратузилмаларидан фойдаланган ҳолда қурилади. Компания нархи қиммат ажратилган линиялардан воз кечиб, уларни арзонроқ Интернет орқали алоқа билан алмаштиради. Бу ўтказиш полосасидан фойдаланишдаги сарф-ҳаражатни жиддий камайтиради, чунки Интернетда масофа уланиш нархига ҳеч таъсир этмайди.

Интранет VPN учун қуйидаги афзалликлар характерли:

- конфиденциал ахборотни ҳимоялаш учун шифрлашнинг кучли криптографик протоколларидан фойдаланиш;

- автоматлаштирилган савдо тизими ва маълумотлар базасини бошқариш тизими каби жиддий иловаларни бажаришда ишлашининг ишончлилиги;

- сони тез ўсаётган фойдаланувчилар, янги офислар ва янги дастурий иловаларни самаралироқ жойлаштириш учун бошқаришнинг мослашувчанлиги.

Интернетдан фойдаланиб Интранет VPN ни қуриш VPN-технологияни амалга оширувчи энг рентабел усули ҳисобланади. Аммо Интернетда сервис даражаси умуман кафолатланмайди. Кафолатланган сервис даражасини ҳоҳловчи компаниялар ўзларининг VPNларини сервер-провайдерлари томонидан тақдим этилувчи бўлинувчи тармоқ инфтузилмаларидан фойдаланиб сафлаш имкониятларини кўришлари шарт.

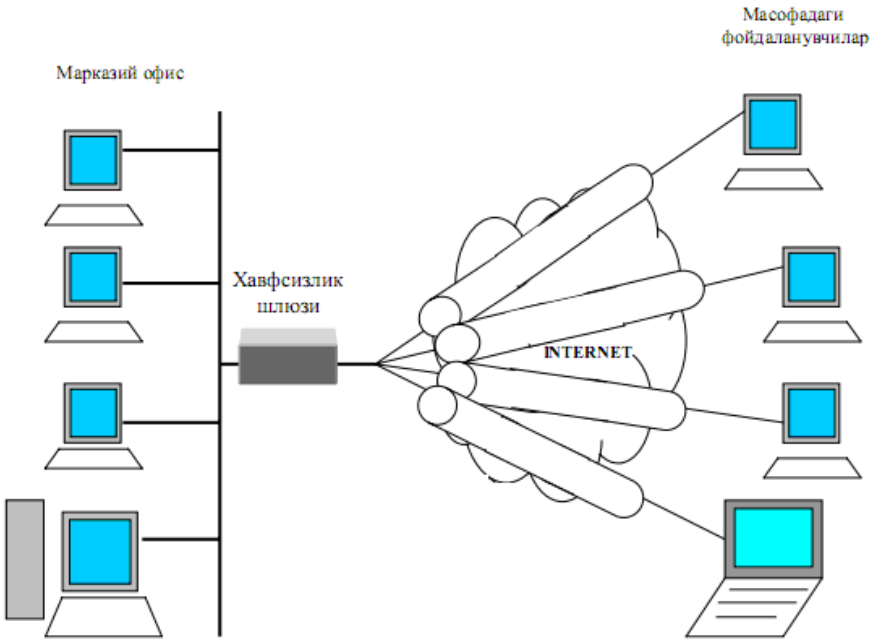
Масофадан фойдаланилувчи VPN тармоқ. Масофадан фойдаланилувчи виртуал хусусий тармоқлар VPN (Remote Access VPN) корпорациянинг мобил ёки масофадаги ходимларига (компания раҳбарияти, меҳнат сафаридаги ходимлар, касаначилар ва ҳ.) корхона ахборот ресурсларидан ҳимояланган масофадан фойдаланишни таъминлайди.

Масофадан фойдаланувчи виртуал хусусий тармоқларнинг (2.5-расм) коммутацияланувчи ва ажратилган линиялардан фойдаланишнинг ҳар ойдаги сарф-ҳаражатларини анчагина камайтиришга имкон бериши, уларнинг умумий еътироф этилишига сабаб бўлди. Уларнинг ишлаш принципи оддий: фойдаланувчилар глобал тармоқдан фойдаланишнинг маҳаллий нуқтаси билан уланишларни ўрнатади. Сўнгра уларнинг сўровлари Интернет орқали туннелланади. Бу шаҳарлараро ва халқаро алоқа учун тўловдан қутилишга имкон беради. Ундан кейин барча сўровлар мос узелларда тўпланади ва корпорация тармоқларига узатилади.

Хусусий бошқарилувчи тармоқлардан (Dial Networks) масофадан фойдаланилувчи VPN тармоқларга (Remote Access VPN) ўтиш қуйидаги афзалликларни беради:

- шаҳарлараро номерлар ўрнига маҳаллий номерлардан фойдаланиш имконияти шаҳарлараро телекоммуникацияга сарф-ҳаражатларни анчагина камайтиради;

- аутентификациялаш жараёнини ишончли ўтказишни таъминловчи масофадаги ва мобил фойдаланувчилар ҳақиқийлигини аниқлаш тизимининг самарадорлиги;



2.5.-расм. Масофадан фойдаланишли виртуал хусусий тармоқ.

- масштабланишнинг янада юқорилиги ва тармоққа қўшилувчи янги фойдаланувчилар сафланишининг оддийлиги;

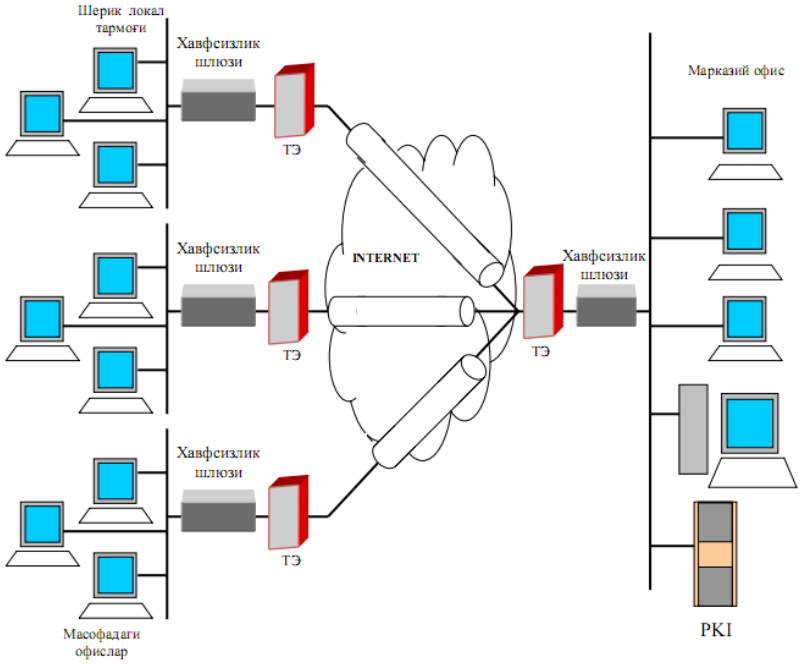
- компания эътиборини тармоқ ишлаши муаммолари ўрнига асосий корпорация бизнес-мақсадларига қаратиш.

Таъкидлаш лозимки, сезувчан корпорация трафигини ташишда очиқ тармоқ Интернетнинг бирлаштирувчи магистрал сифатида ишлатилишининг масштаби ошиб бормоқда. Бу ахборот ҳимояси механизмини ушбу технологиянинг энг муҳим елементига айлантиради.

Корпорацияларараро VPN тармоқ. Корпорацияларараро VPN тармоқлардан (Extranet VPN) бизнес бўйича стратегик шериклар, хусусан чет ел асосий таъминотчилар, йирик буюртмачилар, мижозлар ва ҳ. билан

самарали алоқани ва ахборотни ҳимояланган алмашинувини ташкил этишда фойдаланилади (2.6-расм).

Extranet-бир компания тармоғидан иккинчи компания тармоғининг тўғридан-тўғри фойдаланишини таъминлаш орқали иш юзасидан ҳамкорлик жараёнида алоқа ишончлилигини оширишга имкон берувчи технологиядир.



2.6-расм. Корпорацияларо extranet VPN тармоғи.

Extranet VPN тармоқлари умуман корпорация ичидаги виртуал хусусий тармоқларга ўхшаш, фарқи шундаки, корпорацияларо виртуал хусусий тармоқлар учун ахборот ҳимояси муаммоси кескинроқдир. Extranet VPN учун ишбилармон шериклар ўзларининг тармоқларида қўллашлари мумкин бўлган турли VPN-ечимлар билан алоқа қилиш имкониятларини кафолатловчи стандартлаштирилган VPN-маҳсулотлардан фойдаланиш характерлидир.

Бир неча компаниялар бирга ишлашга келишиб, бир-бирларига тармоқларини очишганида, улар янги шерикларининг фақат маълум ахборотдан фойдаланишларига йўл қўйишлари лозим. Бунда конфиденциал ахборот рухсатсиз фойдаланишдан ишончли ҳимояланиши зарур. Айнан, шу сабабли корпорацияларо тармоқларда очиқ тармоқ томонидан

тармоқлараро экран (брандмауер) ёрдамида назоратга катта аҳамият берилади. Ахборотдан ҳақиқий фойдаланувчининг фойдаланишини кафолатловчи аутентификациялаш ҳам муҳим ҳисобланади. Шу билан бир қаторда рухсациз фойдаланишдан ҳимоялашнинг сафланган тизими ўзига эътиборни жалб қилмаслиги шарт.

Ехтранет VPN уланишлари интранет VPN ва ремоте ассесс VPN лар амалга оширилишидаги ишлатилган архитектура ва протоколлардан фойдаланиб сафланади. Асосий фарқ шундан иборатки, ехтранет VPN фойдаланувчиларига бериладиган фойдаланишга рухсат улар шеригининг тармоғи билан боғлиқ.

Баъзида VPN тармоғининг локал варианти (Lokalnet VPN) алоҳида гуруҳга ажратилади. Лосалнет VPN локал тармоғи компания локал тармоғи ичида (одатда, марказий офис) айланувчи ахборотлар оқимидан компаниядан ишловчи "ортиқча қизиқувчи" ходимларнинг рухсациз фойдаланишидан ҳимоялашни таъминлайди. Таъкидлаш лозимки, ҳозирда VPNни амалга оширувчи турли усулларнинг конвергенсияси ғояси кўзга ташланмоқда.

Техник амалга ошириш бўйича VPN нинг туркумланиши. Виртуал хусусий тармоқнинг конфигурацияси ва характеристикалари кўп жиҳатдан ишлатиладиган VPN-қурилмаларининг турига боғлиқ.

Техник амалга ошириш бўйича VPN нинг қуйидаги гуруҳлари фарқланади:

- маршрутизаторлар асосидаги VPN;
- тармоқлараро экранлар асосидаги VPN;
- дастурий таъминот асосидаги VPN;
- ихтисослаштирилган аппарат воситалари асосидаги VPN.

Маршрутизаторлар асосидаги VPN. VPN қуришнинг ушбу усулига биноан ҳимояланган каналларни яратишда маршрутизаторлардан фойдаланилади. Локал тармоқдан чиқувчи барча ахборот маршрутизатор орқали ўтганлиги сабабли, унга шифрлаш вазифасини юклаш табиий.

Маршрутизатор асосидаги VPN асбоб-ускуналарига мисол тариқасида Cisco-Systems компаниясининг қурилмаларини кўрсатиш мумкин.

Тармоқлараро экранлар асосидаги VPN. Аксарият ишлаб чиқарувчиларнинг тармоқлараро экрани туннеллаш ва маълумотларни шифрлаш вазифаларини қўллаб-қувватлайди. Тармоқлараро экранлар асосидаги ечимга мисол тариқасида Chek Point Software Technoliges компаниясининг Fire Wall-1 маҳсулотини кўрсатиш мумкин. Шахсий компьютер асосидаги тармоқлараро экранлар фақат узатилувчи ахборот ҳажми нисбатан кичик бўлган тармоқларда қўлланилади. Ушбу усулнинг камчилиги бита ишчи ўрнига ҳисобланганда ечим нарҳининг юқорилиги ва унумдорликнинг тармоқлараро экран ишлайдиган аппарат таъминотига боғлиқлиги.

Дастурий таъминот асосидаги VPN. Дастурий усул бўйича амалга оширилган VPN маҳсулотлар унумдорлик нуқтаи назаридан ихтисослаштирилган қурилмадан қолишсада, VPN-тармоқларни амалга оширилишида етарли қувватга эга. Таъкидлаш лозимки, масофадан фойдаланишда зарурий ўтказиш полосасига талаблар катта эмас. Шу сабабли, дастурий маҳсулотларнинг ўзи масофадан фойдаланиш учун етарли унумдорликни таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзаллиги-қўлланилишининг мосланувчанлиги ва қулайлиги, ҳамда нархининг нисбатан юқори эмаслиги.

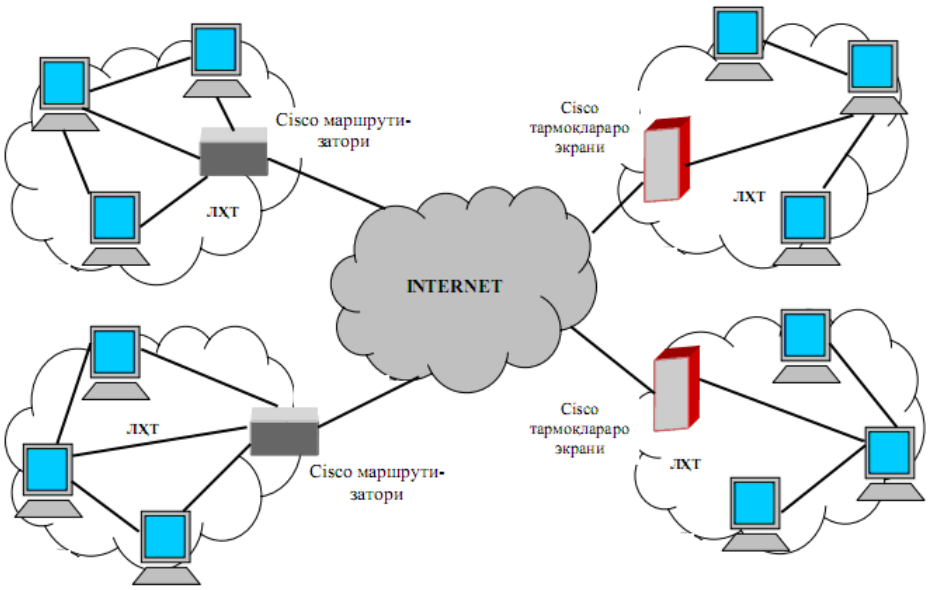
Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат воситалари асосидаги VPNларнинг энг муҳим афзаллиги унумдорлигининг юқорилигидир. Ихтисослаштирилган VPN тизимларда шифрлашнинг микросхемаларда амалга оширилиши тезкорликнинг таъминланишига сабаб бўлади. Ихтисослаштирилган VPN-қурилмалар ҳавфсизликнинг юқори даражасини таъминлайди, аммо уларнинг нарҳи анчагина юқори.

II.3. VPNтармоқларини қуриш учун ечимлар

Маршрутизаторлар асосидаги VPN. Ташқи дунё билан локал тармоқ алмашадиган барча ахборот машрутизатор орқали ўтади. Бу маршрутизаторларни чиқувчи пакетларни шифрловчи ва кирувчи пакетларни расшифровка қилувчи табиий платформага айлантиради. Бошқача айтганда, маршрутизатор, умуман, маршрутлаш вазифасини VPN вазифасини қўллаб-қувват-лаш билан бирга олиб бориши мумкин. Бундай ечим ўзининг афзалликлари ва камчиликларига эга. Афзаллиги-маршрутлаш ва VPN вазифаларини биргаликда маъмурлаш қулайлигидир. Корхона тармоқлараро экранни ишлатмасдан корпоратив тармоқ ҳимоясини фақат ҳам тармоқдан фойдаланиш бўйича, ҳам узатиладиган трафикни шифрлаш бўйича ҳимоялаш вазифала-рини биргаликда ҳал етувчи маршрутизатор ёрдамида ташкил етган ҳолларда машрутизаторларни VPNни қўллаб-қувватлашда ишлатилиши айниқса фойдалидур. Ушбу ечимнинг камчилиги маршрутлаш бўйича асосий амалларнинг трафикни кўп меҳнат сарфини талаб етувчи шифрлаш ва аутентификациялаш амаллари билан бирга олиб борилиши натижасида маршрути-затор унумдорлигига қуйиладиган талабларнинг ошиши билан боғлиқ.

Маршрутизаторларнинг унумдорлигини оширишга шифрлаш вазифаларини аппарат қўллаб-қувватлаш орқали эришилади. Ҳозирда барча маршрутизатор ва бошқа тармоқ қурилмаларини етакчи ишлаб чиқарувчилар ўзларининг маҳсулотларида турли VPN-протоколларини қўллаб-қувватлайдилар. Бу соҳада Cisco Systems ва 3Com компаниялари лидер ҳисобланадилар. Cisco Systems компанияси ўзлари ишлаб чиққан маршрутизаторларга энг кенг тарқалган стандартлар асосида VPNларни қуришга имкон берувчи канал сатҳи протоколини қўллаб-қувватловчи IOS 11.3 (Internetwork operation system 11.3) ва тармоқ сатҳи протоколи IPCесни киритди. L2Ф протоколи аввалроқ IOS операцион тизимнинг компонентига айланди ва Cisco ишлаб чиқарадиган барча тармоқлараро алоқа ва масофадан фойдаланиш қурилмаларида қўллаб-қувватланади.

Cisco маршрутизиторларида VPN вазифалари бутунлай дастурий йўл билан ёки шифрлаш сопроцессори бўлган махсус кенгайтириш платасидан фойдаланилган ҳолда амалга оширилиши мумкин. Охирги вариант VPN амалларида маршрутизатор унумдорлигини анчагина оширади. Cisco Systems компанияси томонидан ишлаб чиқилган VPN қуриш технологияси юқори унумдорлиги ва мосланувчанлиги билан ажралиб туради. Унда "тоза" ёки инкапсуляция қилинган кўринишда узатилувчи ҳар қандай IP-оқим учун шифрлаш билан туннеллаш таъминланади. Cisco компаниясининг маршрутизаторлари асосида VPN-каналларини қуриш операционтизимининг воситалари ёрдамида CiscoIOS 12.x. версиясидан бошлаб амалга оширилади. Агар мазкур операцион тизим компаниянинг бошқа бўлимларидаги Cisco чегара маршрутизаторларида ўрнатилган бўлса, бир маршрутизатордан иккинчисига "нуқта-нуқта" туридаги виртуал ҳимояланган туннеллар мажмуасидан иборат бўлган корпоратив VPN тармоқни шакллантириш имконияти бўлади (2.7-расм).



2.7-расм. Cisko маршрутизаторлари асосида корпоротив VPN тармоғини қуришнинг намунавий схемаси.

Маршрутизаторлар асосида VPNларни қуришда есда тутиш лозимки, бундай ёндашишнинг ўзи компаниянинг умумий ахборот ҳавфсизлигини таъминлаш муаммосини ҳал етмайди, чунки барча ички ахборот ресурслар

барибир ташқаридан хужум қилиш учун очиқ қолади. Бу ресурсларни ҳимоялаш учун, одатда, чегара маршрутизаторларидан кейин жойлашган тармоқлараро экранлардан фойдаланилади.

Cisco 1720 VPN Accecc Роутер маршрутизатори катта бўлмаган ва ўртача корхоналарда ҳимояланган фойдаланишини ташкил этишга аталган.

Бу маршрутизатор Интернет ва интратармоқлардан фойдаланишни ташкил этишга зарур бўлган имкониятларни таъминлайди ва CiscoIOS дастурий таъминот асосидаги виртуал хусусий тармоқларни ташкил этиш вазифаларини қўллаб-қувватлайди. CiscoIOS операцион тизими маълумотларни ҳимоялаш, хизмат сифатини бошқариш ва юқори ишончилиликни таъминлаш бўйича VPN вазифаларининг жуда кенг тўпламини таъминлайди.

Cisco 1720 маршрутизатори маълумотлар ҳимоясининг қуйидаги вазифаларини бажаради:

- тармоқлараро экранлаш. CiscoIOS FireWall компонента локал тармоқларни хужумлардан ҳимоялайди. Фойдаланишнинг контекстли назорати CBAC (Context-based access control) функцияси маълумотларни динамик ёки холатларга асосланган, иловалар бўйича дифференциалланган филтрлашни бажаради. Бу функция самарали тармоқлараро экранлаш учун жуда муҳим ҳисобланади. CiscoIOS FireWall компонента қатор бошқа фойдали вазифаларни ҳам, хусусан, "хизмат қилишдан воз кечиш" каби хужумларни аниқлаш ва олдини олиш, Жавани блокировка этиш, аудит ва вақтнинг реал масштабида огоҳлантиришларни тарқатиш вазифаларини бажаради.

- вақтнинг реал масштабида огоҳлантиришларни тарқатиш вазифаларини бажаради.

- шифрлаш. IPCec протоколидаги DES ва Triple DES шифрлаш алгоритмларини қўллаб қувватлаш маълумотларни конфиденциаллиги ва яхлитлигини ва маълумотлар манбаини аутентификациялашни (маълумотлар

глобал тармоқдан ўтганидан сўнг) таъминлаш мақсадида ишончли ва стандарт шифрлайди.

- туннеллаш. Туннеллашнинг IPCec, ГРЕ (Generic Routing Encapsulation), L2F ва L2TP стандартлари ишлатилади. L2F ва L2TP стандартлари масофадаги фойдаланувчиларнинг корхона локал тармоғида ўрнатилган Cisco 1720 маршрутизаторгача виртуал туннел ўтказганларида ишлатилади.

Бундай қўлланишда корхонада масофадан фойдаланиш серверига еҳтиёж қолмайди ва шаҳарлараро ёки халқаро қўнғироқлар учун тўлови тежалади.

- қурилмаларни аутентификациялаш ва калитларни бошқариш. IPCec катта тармоқларда маълумотлар ва қурилмаларни масштабланувчи аутентификациялашни таъминловчи калитларни бошқариш протоколи IKE, рақамли сертификатлар X.509 версия 3, сертификатларни бошқарувчи протокол CEP, ҳамда Verisign ва Entrust компания сертификат серверлари ма-дадланади.

- VPNнинг мижоз дастурий таъминоти. IPCec ва L2TP протоколларининг стандарт версиялари билан ишловчи ҳарқандай мижоз CiscoIOSбилан ўзаро алоқа қилиши мумкин.

- фойдаланувчиларни аутентификациялаш. Бунинг учун PAP, CHAP протоколлари, TACACSQ ва RADIUS тизимлари, фойдаланиш токенлари каби воситалардан фойдаланилида.

Виртуал ҳимояланган тармоқлар нафақат маълумотларни ҳимоялаш, балки ҳимоялашнинг юқори савияси QoS ни (Quality of Service) таъминлаши лозим. Cisco 1720 маршрутизатори QoS ни қуйидаги бошқариш механизмларини қўллаб-қувватлайди:

- фойдаланишнинг келишилган тезлиги CAR (Committed Access Rate) иловалар ёки фойдаланувчилар базасида қуйидаги учта муҳим вазифани бажаради:

• трафик турини туркумлайди;

• берилган иловага рухсат этилган ўтказиш қобилиятининг максимал даражасини ўрнатади;

• трафикнинг ҳар бир тури устиворлигини белгилайди;

- сиёсат асосида маршрутлаш (Policy Routing) ҳам трафикни туркумлайди ва устиворлайди ҳамда трафикнинг қайси турини маршрутизаторнинг мос чиқиш йўли портига жўнатиш лозимлигини ҳал этади;

- мулоҳазали одилона навбат WFQ (Weighted Fair Queneing) трафикни ҳисобга олган ҳолда мақбул жавоб вақтини таъминлайди;

- протокол RSVP иловаларга йўлнинг бошидан охиригача кафолатланган ўтказиш қобилиятини резервлашга имкон беради.

Маршрутизаторнинг мослашувчанлиги модулли конструксия ва иккита слотда ўрнатилувчи интерфейс WAH-карталари тўплами орқали таъминланади. Cisco 1720 моделида Cisco 1600, 2800, ва 3600 моделларда ишлатиладиган WAH-карталардан фойдаланилади.

Компания 3Com VPN технологияни амалга оширишда бошидан стандартларни кўзга тутган эди. VPN ни қўллаб қувватлаш унинг NetBuilder II, Super Stack II NetBuilder маршрутизаторларига Office Connect Net Builder Platform ларида ўрнатилган.

3Com компанияси PPTP ва Л2ТП протоколларни қўллаб қувватловчи масофадан фойдаланилувчи консентраторларни йирик ишлаб чиқарувчиларидан биридир. 3Com компаниясининг VPN тармоқлари IPCec билан бирга ишлатилади ва ташқи каталоглар, жумладан Novell NDS ва Windows NT Directo-ry Services лар билан ўзаро алоқа қилиш учун ишлаб чиқилган.

Компания Web-технологияга асосланган ва VPN юкланганлигини назоратлашга, ҳамда юз берувчи ходисалар асосида статистика ва ахборотни йиғишга аталган дастурий илова Transcend Ware Secure VPNManager ни ҳам ишлаб чиқди. Ундан ташқари 3Com крипто ҳимояланган туннелларни

осонгина яратишга имкон берувчи Web асосидаги инструментар воситаларини ишлаб чиқаради [3].

Интернет Девисес компаниясининг Fort Knox маршрутизаторларида тезлик ва қувват уйғунлашган. Ундаги тармоқни ҳимоялашни таъминлашга йўналтирилган IP-трафикни ишлаш вазифалари руйхатининг кенглиги унинг афзаллигидир. Fort Knox маршрутизатори тармоқлараро экран режимида ишлаши, НАТ стандарти бўйича адресларни трансляциялаши, ҳавфсизлик сиёсатини бошқариши, Web-саҳифалар ва DNS жадвал ёзувларини кешлаши, аудитни бажариши мумкин. Одатда Fort Knox корпоратив тармоқ чегарасида, корпоратив тармоқни глобал тармоқ билан уловчи маршрутизатордан кейин ўрнатилади. Демак, у бошқа локал тармоқлар билан VPN-алоқани ўрнатиш ва тармоқлараро экранлар каби фойдаланишни назоратлашнинг турли қоидаларини шакллантириши мумкин. Форт Кнохда НАТ адресларини трансляциялаш функциясининг мавжудлиги, унга ички IP-адресларни беркитиш ва маршрутизаторлар трафигини қайта йўналтириш имконини беради. Бу корпоратив тармоқ маъмурларини VPN ни қуришда маршрутизаторларни янгидан конфигурациялашдан озод этади. Fort Knox функциялари тўпламининг кенглигига қарамай унинг нархи оддий маршрутизатор нархига тенг.

Тармоқлараро экранлар асосидаги VPN. Локал тармоқнинг тармоқлараро экрани орқали, худди маршрутизатордагидек, бутун трафик ўтади. Шу сабабли, тармоқлараро экран ҳам чиқувчи трафикни шифрлаш, кирувчи трафикни расшифровка қилиш вазифасини бажариши мумкин.

Ҳозирди қатор VPN-ечимлар тармоқлараро экранларни VPNнинг қўшимча мадад функциялари билан тўлдирилишига таянади. Бу Интернет орқали бошқа тармоқлараро экранлар билан шифрланган уланишни ўрнатишга им-кон беради. Ахборот ҳавфсизлиги бўйича қатор

[3]S.K.G’aniyev, M.M. Karimov.Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi. Oliy o‘quv yurti talabalari uchun o‘quv qo‘llanma.-Toshkent Davlat texnika universiteti, 2003.

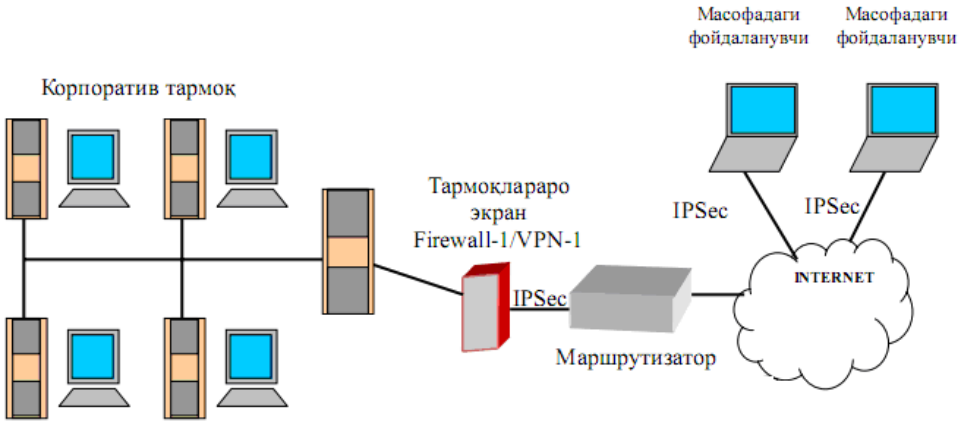
мутахассисларнинг фикрича VPNни тармоқлараро экранлар асосида қуриш, корпоратив тармоқларни очиқ тармоқлар хужумларидан комплекс ҳимоялаш нуқтаи назаридан, тўла асосланган ечимдир. Ҳақиқатан, тармоқлараро экран ва VPN-шлюз функциялари бир нуқтада, ягона бошқариш ва аудит тизими назоратида бирлаштирилса, корпоратив тармоқни ҳимоялаш функциялари битта қурилмада тўпланади. Натижада ҳимоя воситаларини маъмурлаш сифати ошади.

Аммо, ҳимоялаш воситаларининг бундай универсаллаштирилиши, ҳисоблаш воситаларининг мавжуд имкониятлари даражасида нафақат ижобий, балки салбий томонига ҳам эга. Шифрлаш ва аутентификациялаш амалларини ҳисоблаш мураккаблиги тармоқлараро экран учун анъанавий бўлган пакетларни филтрлаш амалларига нисбатан анча юқори. Шу сабабли, VPNнинг қўшимча вазифаларини амалга оширишда мураккаблиги катта бўлмаган амалларни бажаришга мўлжалланган тармоқлараро экран кўпинча керакли унумдорликни таъминламайди. Корпоратив тармоқ тезкор канал орқали очиқ тармоққа уланганида сифатли ҳимояни таъминлаш учун алоҳида аппарат, дастурий ёки комбинацияланган қурилма кўринишидаги VPN-шлюздан фойдаланиш лозим.

Аксарият тармоқлараро экранлар сервер дастурий таъминотидан иборат, шу сабабли унумдорликни ошириш муаммоси юқори унумдорликка эга бўлган компьютер платформасидан фойдаланиш эвазига ечилиши мумкин.

Chek Point Software Tekhnologies компанияси Интернет билан ишлаганда ахборот ҳавфсизлигини комплекс таъминлаш махсулотларини ишлаб чиқариш соҳасидаги етакчилардан бири ҳисобланади. Chek Point Fire Wall -1 тармоқлараро экран корпоратив ахборот ресурслари учун ягона комплекс доирасида ҳимоянинг чуқур эшелонланган чегарасини қуришга имкон беради. Бундай комплекс таркибига Check Point FW -1 нинг ўзи ва корпоратив VPN тармоқ (ҳимояланган туннеларни шакллантирувчи қисм тизим) қуриш учун маҳсулотлар тўплами Check PointVPN-1, ҳамда суқилиб киришни пайқаш воситалари FloodGate ва ҳ. киради.

Дастурий таъминотлар Check Point Fire Wall-1/VPN-1 асосида корпоратив тармоқ қуриш мисоли 2.8-расмда келтирилган.



2.8-расм. Check Point FireWall-1/VPN-1асосида корпоратив VPN тармоғини қуриш схемаси.

Chek Point VPN-1 қисм тизим таркибидаги барча маҳсулотлар ҳам ўзаро, ҳам оммавий брандмауер Fire Wall-1 билан узвий интеграцияланган. Chek Point компанияси "тармоқ-тармоқ" (VPN-1 Gateway) ва "тармоқ-масофадаги фойдаланувчи" (VPN-1 Gateway+VPN-1 Casy Remote) типидаги ҳимояланган тармоқларни ташкил этиш учун воситаларни тақдим этади. Chek Point VPN-1 маҳсулотлари очиқ стандартлар (IPCec) асосида амалга оширилган, фойдаланувчиларни аутентификациялашнинг ривожланган тизимига эга, очиқ калитларни (ПКИ) тақсимлашнинг ташқи тизимлари билан ўзаро алоқани қўллаб қувватлайди, бошқариш ва аудитнинг марказлаштирилган тизимини қуришга имкон беради ва ҳ.

Chek Point Fire Wall-1/VPN-1 нафақат очиқ, балки криптоҳимояланган трафикни ҳам назоратлайди. Тармоқлараро экран FW-1га келган маълумотлар WP-1 воситалари ёрдамида расшифровка қилинади, сўнгра ахборотлар пакети яна шифрланади ва ўтказиб юборилади.

VPN-1 қисм тизими трафикни нафақат криптографик беркитади, балки ахборотлар пакетини аутентификациялайди ҳам. Chek Point Fire Wall-1/VPN-1 каналларида трафикни шифрлашда машхур алгоритмлар DEC, 3-Dec, CAST, IDEA, FW31 ва ҳ. алгоритмлардан фойдаланилади. FW31 криптотизими Chek Point компаниясининг ишланмасидир. Ахборот

пакетларини аутентификациялашда MD5, SHA-1, CBS DEC ва MAC алгоритмлари ишлатилади.

VPN Gateway шлюзи-шифрлашнинг дастурий модули тармоқлараро экран FireWall-1 билан узвий интеграцияланган. Бу маҳсулот корхонага узатилувчи маълумотларнинг тўла конфиденциаллигини, аутентификацияланганлиги ва яхлитлигини кафолатлаган ҳолда Интернет орқали алоқа каналларини қуришга имкон беради. VPN функциялари корхонанинг умумий ҳавфсизлик сиёсатига тўла интеграцияланганлиги сабабли, брандмауер ва VPN-маҳсулотларни алоҳида бошқаришга эҳтиёж қолмайди.

VPNGateway шлюзи ҳимояланган VPN-туннелни ўрнатган ҳолда тармоқлар орасида Интренет орқали узатилаётган конфиденциал маълумотларни шифрлайди. Бу шлюз уни жавобгарлик доирасига, яъни унинг доменига кирувчи компьютерлардан келадиган маълумотлар оқимини шифрлайди. Бу локал тармоқ ёки ушбу шлюз орқасидаги оддий хостлар гуруҳи бўлиши мумкин. Бу маълумотлар тармоқнинг оммавий қисми бўйича шифрланган кўринишда узатилади, ички тармоқ бўйича узатилганда шифрланмайди. VPN-амалларининг барчаси охирги фойдаланувчи ва барча иловалар учун шаффофдир.

VPN-1 Gateway шлюзи шифрлашнинг бир неча алгоритмини ва бир неча калитларни бошқариш протоколини қўллаб-қувватлайди. Бу шлюз IKE (InternetKeyExchange) каби индустриал стандарт VPN-протоколларни қўллаб қувватлаши сабабли, экстратармоқларни ташкил этишда қўллаш қулай ҳисобланади.

Экстра тармоқларда VPN бизнес-шериклар орасида ҳавфсиз алоқани таъминлайди. Check Point компаниясининг VPN-маҳсулотлари IKE стандартига амал қилади.Шу сабабли улар қарши томон билан музокаралар жараёнида автоматик тарзда шифрлашнинг энг криптобардош алгоритмини (DESваTripleDES) ва аутентификациялашнинг энг қатъий алгоритмини (ShA-

1 ва MD5) танлайди. Ундан ташқари, шифрлашнинг махфий калитлари, максимал ҳимояланишни кафолатлаган ҳолда, тез-тез янгиланади.

VPN-1 Gateway шлюзи виртуал хусусий тармоқдаги иккита охирги узелларга ҳам шифрланган, ҳам шифрланмаган маълумотларни алмашишга имкон берувчи шифрлашнинг танлов режимини қўллаб-қувватлайди. Бунинг учун тармоқ маъмури трафиги учун ҳимоялашнинг алоҳида шартлари таъминланадиган иловаларни беради. Сўнгра VPN-1 Gateway ушбу иловалар маълумотларини шифрланган, қолган конфиденциал бўлмаган маълумотларни очиқ кўринишда узатишни бошлайди. Бундай мосланувчанлик VPN-1 Gateway шлюзининг унумдорлигини оширади.

VPN-1 Gateway шлюзи калитларни бошқаришнинг қуйидаги механизмларини қўллаб-қувватлайди: IPCec учун стандарт бўлган ИКЕ, калитларни бошқаришнинг саноат стандарти FW3, оммавий протокол SKIP ва калитларни қўл билан тарқатиладиган усули. У X.509 сертификатлари ва EntrusTechnologies компаниясининг сертификатлар серверлари технологияси асосида очиқ PKI калитларни бошқариш инфратузилмасини қўллаб-қувватлайди.

VPN-1 SecuRemote мижоз дастурий таъминоти VPN-1 GatewayShlyuziёрдамида "тармоқ-масофадаги фойдаланувчи" ҳилидаги ҳимояланган уланишларни ташкил этишда ишлатилади. Windows 9X/XP/NT/2000 бошқарувида ишловчи масофадаги компьютерларга VPN-1Secu Remotening ўрнатилиши Мобил ходимларнинг ёки телекомпьютерларнинг корхона бош тармоғи билан Интернет орқали ҳимояланган боғланишини таъминлайди.

VPN-1 Cesy Remote нинг маҳсулотларни OSI моделининг тармоқ сатҳида шифрлаши ва расшифровка қилиши ушбу амалларнинг барча иловалар учун шаффофлигини, мавжуд иловаларга ўзгартириш киритишни талаб қилмаган ҳолда, таъминлайди. SecuRemote фойдаланувчиларга VPN-воситалар ўрнатилган бир неча турли тармоқлар билан боғланишига имкон беради.

VPN-1 Accelator Card қурилмаси Chrysalis-ITS компанияси томонидан ишлаб чиқилган аппарат криптографик тезлатгичдир. VPNнинг ҳимояланган каналларида трафикни шифрлаш ва калитларни генерацияловчи амаллар анчагина ҳисоблаш мураккаблигига эга ва VPN орқали узатилувчи трафикнинг хажми ошган сари компьютернинг процессори ва хотирасининг хаддан ортиқ юкланиши рўй бериши мумкин. VPN-1 Accelator маҳсулоти бу муаммони ҳал этиши мумкин.

VPN-1 Асселатор Сард тезлатгичи VPN-1 Gateway шлюзи билан биргаликда ишлашга аталган ва ИКЕ ва IPCеслар талаб этадиган барча криптографик амалларни бажаради. VPN-1 AccelatorCard бевосита шлюз орқали маъмурланади.

VPNфункциялари ўрнатилган SecureZone тармоқлараро экрани SecureComputing компанияси томонидан ишлаб чиқилган ва асосий характеристикалари қуйидагича:

- VPNни қўллаб-қувватлаш функциялари — IPCec стандарти, DEC ва TripleDES, PKI бошқариш ва Netscape, EntrustvaVerisignкомпаниялардан X.509 сертификатлари;

- ихтисослаштирилган операцион тизими Secure OS (Unixнинг ҳимояланган варианти) бошқарувида ишлайди;

- қуйидагиларни қаноатлантирувчи аппарат платформалар: процессор IntelPentium, PentiumPro, ёки PentiumII; RAM-камида 64Мбайт; ташқи қурилмалар қаттиқ диск 4 Гбайт SCSI-2, қайишқоқ дисклар 3,5", COKOM, strimmerDAT; SVGAvideo, PS/2- билан бирга ишлай олувчи сичқон.

- стандарттармоқинтерфейслари: 2-4 Ethernet, FAST Ethernet, Token Ring ёки FDDI;

- бузилишга бардошлик хоссасига эга.

Secure Computing компанияси MicroSoft Windows муҳитида ишловчи, алоҳида фойдалунувчиларга TCP/IP протоколлари бўйича телефон тармоғи ёки пакетларни коммутацияловчи, оммавий тармоқдан ҳимояланган

масофавий фойдаланишни таъминловчи, IPCec билан бирга ишлай олувчи мижоз дастурий таъминотини (SecureClient) ҳам тавсия этади[4].

VPN функциялари ўрнатилган RaptorFirewall 5.0 тармоқлараро экрани Axent Technologies компанияси томонидан ишлаб чиқилган ва Eagle Firewallнинг модификацияланган маҳсулоти ҳисобланади. Бу тармоқлараро экраннинг характеристикалари қуйидагича:

- VPN мадади тармоқлараро экранга ўрнатилган;

- IPCec стандарти қўллаб-қувватланади, дастурий шифрлаш IP (текин тарқатилувчи шифрлаш усули swIPe);

- ҳавфсизликнинг умумий сиёсати тармоқлараро экранфункцияларига ва VPNфункцияси ёрдамида туннелланувчи трафикка тааллуқли;

- WindowsNT/2000 va Solaris операцион тизимлар бошқарувида ишлайди.

Ахент компанияси масофадаги фойдаланувчилар учун VPNнинг мижоз дастурий таъминотини ҳам тақдим этади. Raptor FireWall 5.0 версияси IPCec протоколи бўйича ҳимояланган виртуал тармоқ қурилишини таъминлайди.

Gauntlet Glabal VPN маҳсулоти Network Associates компанияси таркибига кирувчи Trusted Information Systems компаниясининг Gauntlet FireWall тармоқлараро экрани учун, ушбу тармоқлараро экран муҳитида узвий интеграцияланувчи, қўшимча дастурий маҳсулот ҳисобланади.

IPSec протоколига асосланган Gauntlet Global VPN қисм тизими трафикни криптографик ҳимоялашнинг қуйидаги иккита режимини қўллаб-қувватлайди:

- Smart Gate шлюзлари ёрдамида амалга оширилувчи тармоқлараро экрандан тармоқлараро экрангача;

- масофадаги мижоз дастурий таъминоти Gauntlet PC Extender ёрдамида амалга оширилувчи тармоқлараро экрандан масофадаги фойдаланувчи компьютеригача.

---

[4]Н.А.Олифер. Протоколи IPSec.//LAN.-2001.-№03; http://www.osp.ru/lan/ 2001/03/024.htm.

Gauntlet Global VPNда шифрлашнинг DEC алгоритми ишлатилади. Gauntlet Глобал VPN сертификация марказининг дастурий таъминоти билан ҳам тақдим этилади. Ушбу дастурий таъминот ёрдамида ташкилотлар X.509 стандартига мос келувчи рақамли сертификатларни генерациялаши ва текшириши мумкин.

VPN қуриш функциясини қўллаб-қувватловчи Border manager тармоқлараро экрани Nowell компаниясининг маҳсулоти бўлиб, нафақат VPN қуриш имкониятини, балки фойдаланишни чегаралашни, пакетларни филтрлаш ва тармоқ адресларини трансляциялашни таъминлайди, воситачи HTTPнинг хизматларини тавсия этади, Web саҳифаларини кешлайди, канал сатҳида шлюзларга эга, кўп протоколли маршрутлашни бажаради ва масофадан фойдаланишни қўллаб-қувватлайди.

Border Manager тармоқлараро экраннинг NDS (Novell Directory Service) каталоглари хизмати билан узвий интеграцияси ҳимояланган виртуал тармоқларни самарали бошқаришга имкон беради. Шифрлаш калитининг тақсимоти PCA криптотизими ва Диффи-Хеллман алгоритми бўйича амалга оширилади. Ахборот пакетларини криптографик беркитиш ва аутентификациялашда PC2 ва PCA криптотизимлардан фойдаланилади. Border Managerнинг бир версиясида IPCSec протоколи қўллаб-қувватланади. Border Manager тармоқлараро экран асосида қурилган ҳимояланган виртуал тармоқларда брандмауерлардан биринг асосий бўлиши, бошқариш маркази ролини бажариши лозим.

Ихтисослаштирилган дастурий таъминот асосидаги VPN. VPN қуришда ихтисослаштирилган дастурий воситалар кенг қўлланилади. VPN қуришнинг дастурий воситалари ҳимояланган туннелларни фақат дастурий шакллантиришга имкон беради ва улар ишлайдиган компьютерни TCP/IP маршрутизаторига айлантиради. Бу маршрутизатор шифрланган пакетларни қабул қилади, қайта шифрлайди ва локал тармоқ орқали тайинланган нуқтага узатади. Охирги вақтда бундай маҳсулотларнинг етарлича сони пайдо бўлди.

Ихтисослаштирилган дастурий таъминот кўринишида VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар бажарилиши мумкин.

Дастурий усул бўйича амалга оширилган VPN-маҳсулотлар унумдорлик нуқтаи-назаридан ихтисослаштирилган аппарат қурилмалардан қолишсада, дастурий маҳсулотлар масофадаги фойдаланувчиларга етарли унумдорликни осонгина таъминлайди. Дастурий маъсулотларнинг шубҳасиз афзаллиги ишлатилишида мосланувчанлиги ва қулайлиги, ҳамда нисбатан юқори бўлмаган нархидир. Аппарат шлюзларни ишлаб чиқарувчи кўпгина компаниялар (масалан, Time Step, VPNet, Shiva) ўзларининг маҳсулотларига стандарт операцион тизимда ишлашга мўлжалланган VPN-мижознинг дастурий амалга оширилишини қўшадилар.

Microsoft компаниясининг PAC ва PPAC дастурий маҳсулотлари. Microsoft компаниясининг масофадан фойдаланувчи дастурий сервери RAS (Remote Access Service) машҳур PPP (Point to Point Protocol) протоколнинг кенгайтирилган варианти-ҳимояланган канал протоколи PPTPni (Point-to-Point Tunneling Protocol)ўрнатилиши эвазига VPN технологияни қўллаб-қувватлайди. Трафикни туннеллаш очиқ IP-тармоқ бўйича узатиладиган стандарт PPP- фреймларни IP-датаграммаларга инкапсуляциялаш ва кейин шифрлаш орқали амалга оширилади.

RASнинг асосий афзаллиги-тежамлилиги, камчилиги-унумдорлигининг пастлиги. Ҳозирда бу маҳсулотнинг такомиллаштирилган версияси- RRAS (Routing and Remote Acces Service) пайдо бўлди. RRAS таркибидаги такомиллаштирилган дастурий кўп протоколли маршрутизатор маршрутлашнинг RIP (Routing Information Protocol)ваOSFP (Open Shortest Path First) протоколларини қўллаб-қувватлайди. PPACнинг бу хусусиятлари ундан VPN шлюзи каби "тармоқ-тармоқ" ўзаро алоқасида фойдаланишга имкон яратади.PACхизмати масофадан фойдаланувчиларнинг кўпчилигига (256 тагача) битта Windows HT серверига уланиш ва локал тармоқ ресурсларидан IPXваTCP/IP протоколлари бўйича фойдаланиш имкониятини беради.

AltaVista Tunnel 98 маҳсулотлари оиласи учта маҳсулотни ўзичига олади: Telecommuter Server, Extranet Server, AltaVista Tunnel Client. Telecommuter Server сервери Интернет корпоратив фойдаланувчилар орасида ҳимояланган туннеларни Интернет орқали ташкил этишга аталган. Ехтранет Сервер сервери ёрдамида тармоқлар орасида ҳимояланган канални ҳосил қилинади. Бу иккала сервер умумий Alta Vista Tunnel номига эга.

Alta Vista Tunnel Client VPN клиентнинг дастурий таъминотидир Alta Vista Tunnel 98 оиласининг барча маҳсулотлари фойдаланувчиларни аутентификациялашда ва PCA криптографик тизимнинг сессия калитларини алмашишда ишлатилади. Фойдаланувчиларни аутентификациялашда Security Dynamics компаниясининг аппарат калити SecurID ҳам ишлатилиши мумкин. Мижоз ва сервер янги сессия калитлари билан ҳар 30 минутда алмашишади. Маълумотларни шифрлашда PC4 алгоритмидан фойдаланилади. Маҳсулотларнинг ҳалқаро версияси PC4 алгоритми бўйича шифрлашда 56 ёки 4 битли калитлардан фойдаланади. Маълумотларни аутентификациялаш ва яхлитлигини таъминлаш учун МД5 хэш-функцияси ишлатилади. Alta Vista Tunnel 98 оиласининг маҳсулотлари LZO алгоритми бўйича маълумотларни зичлаштириши мумкин.

Ушбу оила маҳсулотлари аксарият замонавий операцион тизимлар-WindowsNT/2000, UnixBSD/OS, Unix BSD ва Digital Unix бошқарувида ишлаши мумкин. Windows NT/2000 операцион муҳитда Alta Vista Tunnel Server маҳсулоти бир вақтнинг ўзида 200 туннел уланишларини, Unix операцион муҳитда эса 2000 гача туннел уланишларни қўллаб-қувватлайди.

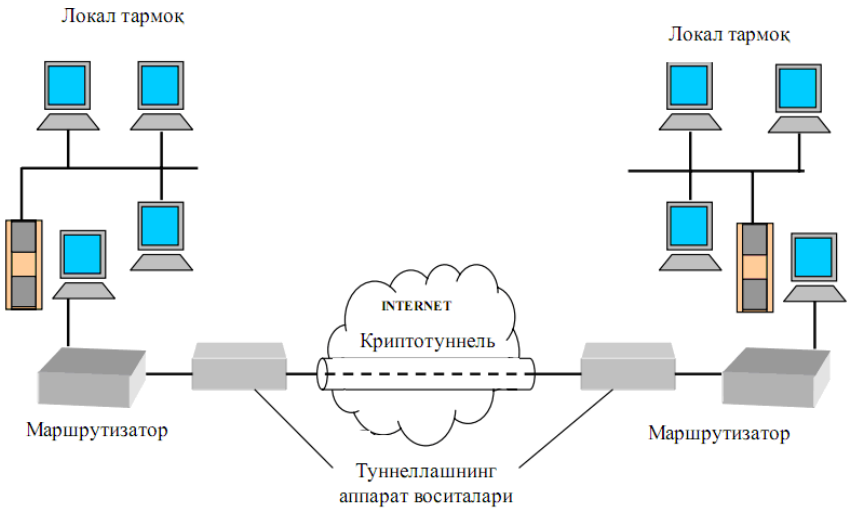
Ихтисослаштирилган аппарат воситалари асосидаги VPN.

Ихтисослаштирилган аппарат қурилмалари асосидаги VPN-воситаларнинг асосий афзаллиги-юқори унумдорлиги. VPN-пакетларни ишлашда керакли ҳисоблашлар хажми оддий пакетларни ишлашдагига нисбатан 50-100 марта ошади. Аппарат воситалари асосидаги VPN ларда юқори тезликка уларда шифрлашнинг ихтисослаштирилган микросхемаларда амалга оширилиши евазига эришилади. Бундай VPN-воситалар кўпинча

IPSec протоколи билан бирга ишлай олади ва локал тармоқлар орасида криптоҳимояланган туннелларни шакллантиришда ишлатилади. Баъзи ишлаб чиқарувчиларнинг VPNни шакллантирувчи асбоб-ускуналари бир вақтнинг ўзида "масофадаги компьютер-локал тармоқ" режимида ҳимояланган боғланишни ҳам қўллаб-қувватлайди.

Аппарат VPN-шлюзлар алоҳида аппарат қурилмаси кўринишида бўлади. Уларнинг асосий вазифаси-трафикни юқори унумдорлик билан шифрлаш. Бу VPN-шлюзлар X.509 рақамли сертификатлари PKI очиқ калитларни бошқариш инфратузилмалари билан ишлайди, LDAP бўйича маълумот берадиган хизматлар билан ишлашни қўллаб-қувватлайди. Аппарат ҳимояланган туннел ишлашининг энг оддий варианти - аппарат шифрлашдан фойдаланиб уланишларни яратиш. Туннеллашнинг аппарат воситалари одатда локал ва глобал тармоқларнинг туташган жойида, маршрутизатордан кейин ўрнатилади (2.9-расм) ва автоматик тарзда берилган трафикни шифрлайди. Бундай ёндашишнинг асосий афзаллиги шундаки, ишчи стансиялар ва маршрутизаторларнинг шакллантирилувчи крипто-туннеллар билан ҳеч қандай боғлиқлиги йўқ, VPN ўрнатилганида уларни конфигурациясини ўзгартириш талаб этилмайди.

Аппарат шлюзларни инсталляциялаш дастурий шлюзлар ва маршрутизаторлар ва брандмауерлар асосидаги шлюзларга нисбатан жуда осон амалга оширилади. Бундай қурилмаларни бошқариш иккита асосий масалани ечишни талаб этади: сертификация маркази орқали калитларни бошқариш ва ҳимояланган туннеллашни бошқариш. Аксарият аппарат туннеллаш воситаларида сертификация марказлари Windowsга мослашган дастурий иловалардир. Аппарат туннелларини марказлашган ҳолда бита иш жойида туриб бошқариш мумкин. Бошқарувчи дастурлар туннелнинг асосий ҳимоялаш функцияларининг бажарилишини ва хатоликларни ишлашни таъминлайди.



2.9-расм. Ихтисослаштирилган аппарат воситалар асосида тунеллаш схемаси.

Ихтисослаштирилган аппарат VPN-воситалар нархидан ташқари барча бўлиши мумкин бўлган кўрсаткичлари бўйича лидер ҳисобланади.

II.4. IPSec протоколлар стекини ҳимояланган виртуал хусусий тармоқлар қуришда ишлатилиши

IPSec протоколи (Internet Protocol Security) асосан IP тармоқларда маълумотларни ҳавфсиз узатишни таъминлашга аталган. IPSecнинг ишлатилиши қуйидагиларни кафолатлайди:

- узатилаётган маълумотларнинг яхлитлигини, яъни маълумотлар узатилишида бузилмайди, йўқолмайди ва такрорланмайди;

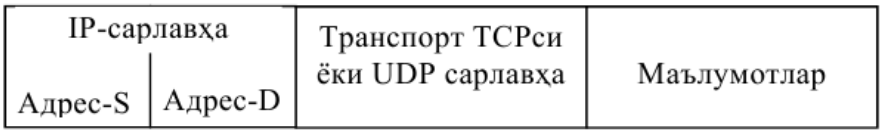
- жўнатувчининг аутентлигини, яъни маълумотлар ҳақиқий жўнатувчи томонидан узатилган;

-узатиладиган маълумотларнинг конфиденциаллигини, яъни маълумотлар шундай шаклда узатиладики, уларни рухсатсиз кўздан кечиришнинг олди олинади.

Таъкидлаш лозимки, маълумотлар ҳавфсизлиги тушунчасига одатда, яна бир талаб-маълумотларнинг фойдаланувчанлиги киритилади.

Маълумотларнинг фойдаланувчанлиги деганда маълумотлар етказилишининг кафолати тушунилади. IPSec протоколлари бу масалани ҳал етмайди ва уни транспорт сатҳи ISPга қолдиради. IPSec протоколлар стеки тармоқ сатҳида ахборот ҳимоясини таъминлайди. Бу ҳимоянинг ишловчи иловаларга кўринмаслигига олиб келади.

IP-пакет IP тармоқларда коммуникациянинг фундаментал бирлиги ҳисобланади. Унинг тузилмаси 2.10-расмда келтирилган. IP-пакет таркибида манба адреси C ва ахборот қабул қилувчининги адреси D, транспорт сарлавҳаси, бу пакетда ташилувчи маълумотлар хили хусусидаги ахборот ва маълумотларнинг ўзи бўлади.



2.10-расм. IP-пакет тузилмаси

Аутентификациялашни, узатилувчи маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлаш мақсадида, IPSec

протоколларининг стеки қатор стандартлаштирилган криптографик технологиялар асосида қурилган:

- калитларни алмаштириш очиқ тармоқдан фойдаланувчилар орасида махфий калитларни тақсимлашнинг Диффи-Хеллман алгоритми бўйича амалга оширилади;

- иккала томоннинг ҳақиқийлигини кафолатлаш ва main in-the middle хилидаги хужумларни олдини олиш мақсадида Диффи-Хеллман алгоритми бўйича алмашишларни имзолашда очиқ калитлар криптографиясидан фойдаланилади;

- очиқ калитларнинг ҳақиқийлигини тасдиқлашда рақамли сертификатлар ишлатилади;

- маълумотларни шифрлашда блокли симметрик алгоритмлардан фойдаланилади;

- хешлаш функциялари асосида ахборотларни аутентификациялаш алгоритмлари ишлатилади.

Ҳимояланган каналнни ўрнатиш ва қўллаб-қувватлашдаги асосий масалалар қуйидагилар:

- фойдаланувчилар ёки компьютерларни аутентификациялаш;

-ҳимояланган каналнинг охирги нуқталари орасида узатилувчи маълумотларни шифрлаш ва аутентификациялаш;

- каналнинг охирги нуқталарини маълумотларни аутентификациялашда ва шифрлашда керак бўладиган махфий калитлар билан таъминлаш.

Юқорида санаб ўтилган масалаларни ҳал этишда IPSec тизими ахборот алмашиш ҳавфсизлиги воситаларининг комплексидан фойдаланади. IPSec протоколининг аксарият амалга оширилишида қуйидаги компонентлардан фойдаланилади:

-IPSecнинг асосий протоколи. Ушбу компонент ҳимояни инкапсуляцияловчи протокол ESP (Encapsulation Security Payload)ни ва сарлавҳани аутентификацияловчи протоколи AH (Authentication Header)ни амалга оширади. У сарлавҳаларни ишлайди; пакетга қўлланиладиган

ҳавфсизлик сиёсатини аниқлаш учун SPD ва SAD маълумотлар базаси билан ўзаро алоқа қилади;

- калит ахборотларини алмашишни бошқариш протоколи IKE. IKE одатда фойдаланиш сатҳида қўлланилади (операцион тизимга ўрнатилгани бундан истисно);

- ҳавфсизлик сиёсатларининг маълумотлар базаси SPD (Security Policy Database). Бу энг муҳим компонентлардан бири бўлиб, пакетга қўлланиладиган ҳавфсизлик сиёсатини белгилайди. SPD дан асосий протокол IPSec томонидан кирувчи ва чиқувчи пакетларни ишлашда фойдаланилади;

- ҳавфсиз ассоциацияларнинг маълумотлар базаси SAD (Security Assocition Database). Бу маълумотлар базаси кирувчи ва чиқувчи ахборотни ишлаш учун ҳавфсиз ассоциациялар SA(SecerityAccatation) рўйхатини сақлайди. Чиқувчи SAлардан чиқувчи пакетларни ҳимоялашда, кирувчи SAлардан эса IPSec сарлавҳали пакетларни ишлашда фойдаланилади. SAD маълумотлар базаси СА билан қўлда ёки калитларин бошқариш протоколлари ИКЕ ёрдамида тўлдирилади;

- ҳавфсизлик сиёсатини ва ҳавфсиз ассоцияцияларни бошқариш. Бу-ҳавфсизлик сиёсатини ва САни бошқарувчи иловалар.

Асосий протокол IPSec (АН ва ESPни амалга оширувчи) TCP/IP протоколларининг транспорт ва тармоқ стеклари билан ўзаро узвий алоқада бўлади. IPSecни тармоқ сатҳининг қисми дейиш мумкин. IPSecнинг асосий модули иккита интерфейсни — кириш йўли ва чиқиш йўли интерфейсларни таъминлайди. Кириш йўли интерфейси кирувчи пакетлар томонидан, чиқиш йўли интерфейси эса чиқувчи пакетлар томонидан фойдаланилади.

IPSecнинг амалга оширилиши TCP/IP протоколлар стекининг транспорт ва тармоқ сатҳлари орасидаги интерфейсга боғлиқ бўлмаслиги лозим.

SPD ва CAD маълумотлар базаси IPSec ишлашига жиддий таъсир кўрсатади. Улардаги маълумотлар тузилмасини танлаш IPSec ишлашининг унумдорлигига таъсир этади.

IPSecдаги барча протоколларни иккита гуруҳга ажратиш мумкин:

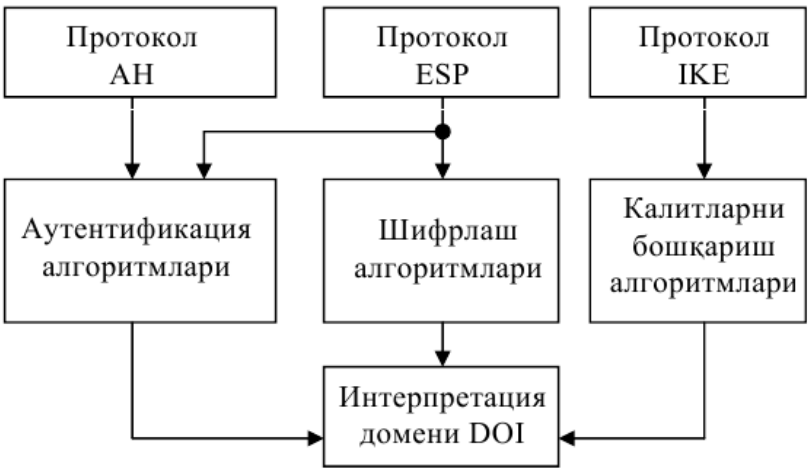
- узатилувчи маълумотларни бевосита ишловчи (уларнинг ҳавфсизлигини таъминлаш учун) протоколлар;

- биринчи гуруҳ протоколларига керакли ҳимояланган уланишлар параметрларини автоматик тарзда мувофиқлаштиришга имкон берувчи протоколлар.

IPSec ядросини учта АН, ESP ва виртуал канал ва калитларни бошқариш ИКЕ параметрларини мувофиқлаштирувчи протоколлар ташкил этади. IPSecнинг ҳавфсизлик воситаларининг архитектураси 2.11-расмда келтирилган.

Архитектуранинг юқори сатҳида қуйидаги протоколлар жойлашган:

- виртуал канал параметрларини мувофиқлаштирувчи ва калитларни бошқариш протоколи IKE. Бу протокол ҳимояланган канални инициализациялаш усулини, жумладан ишлатилувчи криптоҳимоялаш алгоритмларини мувофиқлаштиришни ҳамда ҳимояланган уланиш доирасида махфий калитларни алмашиш ва бошқариш муолажаларини белгилайди;



2.11-расм. IPSecнинг ҳавфсизлик воситаларининг архитектураси

- сарлавҳани аутентификацияловчи протокол АН. Бу протокол маълумотлар манбаини аутентификациялашни, уларнинг, қабул қилинганидан сўнг, яхлитлигини ва ҳақиқийлигини текшириш ва такрорий ахборотларнинг тиқиштирилишидан ҳимояни таъминлайди;

- ҳимояни инкапсуляцияловчи протокол ESP. Бу протокол узатилувчи маълумотларни криптографик беркитишни, аутентификациялашни ва

яхлитлигини таъминлайди ҳамда такрорий ахборотларнинг тиқиштирилишидан ҳимоялайди.

АН ва ESP протоколлари ҳар бири алоҳида ва биргаликда ишлатилиши мумкин. Бу протоколлар вазифаларининг қисқача баёнидан кўриниб турибдиики, уларнинг имкониятлари қисман бир хил. АН протоколи фақат маълумотларни яхлитлигини ва аутентификациялашни таъминлашга жавоб беради. ESP протоколи қувватлироқ ҳисобланади, чунки у маълумотларни шифрлаши мумкин, ундан ташқари АН протоколи вазифасини ҳам бажариши мумкин.

IKE, АН ва ESP протоколларининг ўзаро алоқалари қуйидагича кечади. Аввал ИКЕ протоколи бўйича иккита нуқта орасида мантиқий уланиш ўрнатилади. Бу уланиш IPSec стандартларида "ҳавфсиз ассоциация"- Сесуритй Ассосиатион, СА номини олган. Ушбу мантиқий канал ўрнатилишида каналнинг охирги нуқталарини аутентификациялаш бажарилади ҳамда маълумотларни ҳимоялаш параметрлари, масалан, шифрлаш алгоритми, сессия махфий калити ва ҳ. танланади. Сўнгра ҳавфсиз ассоциация СА томонидан ўрнатилган доирада АН ва ESP протоколи ишлай бошлайди. Бу протоколлар ёрдамида узатилувчи маълумотларнинг исталган ҳимояси, танланган параметрлардан фойдаланилган ҳолда, бажарилади.

IPSec архитектурасининг ўрта сатҳини IKE протоколида қўлланилувчи параметрларни мувофиқлаштириш ва калитларни бошқариш алгоритмлари ҳамда АН ва ESP протоколларида ишлатилувчи аутентификациялаш ва шифрлаш алгоритмлари ташкил этади.

Таъкидлаш лозимки, IPSec архитектурасининг юқори сатҳидаги виртуал канални ҳимоялаш протоколлари (АН ва ESP) муайян криптографик алгоритмларга боғлиқ эмас. Аутентификациялаш ва шифрлашнинг кўп сонли турли-туман алгоритмларидан фойдаланиш имконияти туфайли IPSec тармоқни ҳимоялашни ташкил этишнинг юқори даражада мосланувчанлиги таъминлайди. IPSecнинг мосланувчанлиги деганда ҳар бир масала учун унинг ечилишининг турли усуллари тавсия этилиши тушунилади. Бир масала

учун танланган усул, одатда, бошқа масалаларни амалга ошириш усулларига боғлиқ эмас. Масалан, шифрлаш учун DEC алгоритмининг танланиши маълумотларни аутентификациялашда ишлатилувчи дайджестни ҳисоблаш функциясини танлашга таъсир қилмайди.

IPSec архитектурасининг пастки сатҳи интерпретациялаш домени DOI (DomainofIntarpretation) дан иборат. Интерпретациялаш доменининг қўлланиш зарурияти қуйидагилар сабаб бўлди. AH ва ESP протоколлари модулли тузилмага эга, яъни фойдаланувчилар ўзаро келишилган ҳолда шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларидан фойдаланишлари мумкин. Шу сабабли, барча ишлатилувчи ва янги киритилувчи протокол ва алгоритмларнинг биргаликда ишлашини таъминловчи модул зарур. Айнан шу вазифалар интерпретациялаш доменига юклатилган.

Интерпретациялаш домени маълумотлар базаси сифатида IPSecда ишлатиладиган протоколлар ва алгоритмлар, уларнинг параметрлари, протокол идентификаторлари ва ҳ. хусусидаги ахборотларни сақлайди. Моҳияти бўйича интерпретациялаш домени IPSec архитектурасида фундамент ролини бажаради. AH ва ESP протоколларида аутентификациялаш ва шифрлаш алгоритмлари сифатида миллий стандартларга мос келувчи алгоритмлардан фойдаланиш учун бу алгоритмларни интерпретациялаш доменида руйхатдан ўтказиш лозим.

АНёки ESP протоколлари узатилувчи маълумотларни қуйидаги иккита режимда ҳимоялаши мумкин:

- туннел режимда; IP пакетлар бутунлай, уларнинг сарлавҳаси билан бирга ҳимояланади.

- траспорт режимида; IP пакетларнинг фақат ичидагилари ҳимояланади.

Туннел режими асосий режим ҳисобланади. Бу режимда дастлабки пакет янги IP пакетга жойланади ва маълумотлар тармоқ бўйича узатиш янги IP - пакет сарлавҳаси асосида амалга оширилади. Туннел режимида ишлашда ҳар бир оддий IP-пакет криптоҳимояланган кўринишда бутунлайча IPSec

конвертига жойланади. IPSec конверти, ўз навбатида бошқа ҳимояланган IP-пакетга инкапсуляцияланади. Туннел режими одатда махсус ажратилган ҳавфсизлик шлюзларида - маршрутизаторлар ёки тармоқлараро экранларда амалга оширилади. Бундай шлюзлар орасида ҳимояланган туннеллар шакллантирилади.

Туннелнинг бошқа томонида қабул қилинган ҳимояланган IP -пакетлар "очилади" ва олинган дастлабки IP -пакетлар қабул қилувчи локал тармоқ компьютерларига стандарт қоидалар бўйича узатилади. IP-пакетларни туннеллаш туннелларни эгаси бўлмиш локал тармоқдаги оддий компьютерлар учун шаффоф ҳисобланади. Охирги тизимларда туннел режими масофадаги ва мобил фойдаланувчиларни қўллаб-қувватлаш учун ишлатилиши мумкин. Бу ҳолда фойдаланувчилар компьютерида IPSecнинг туннел режимини амалга оширувчи дастурий таъминот ўрнатилиши лозим.

Транспорт режимида тармоқ орқали IP -пакетни узатиш бу пакетнинг дастлабки сарлавҳаси ёрдамида амалга оширилади. IPSec конвертига криптоҳимояланган кўринишда фақат IP-пакет ичидаги жойланади ва олинган конвертга дастлабки IP-сарлавҳа қўшилади. Транспорт режими туннел режимига нисбатан тезкор ва охирги тизимларда қўлланиш учун ишлаб чиқилган. Ушбу режим масофадаги ва мобил фойдаланувчиларни ҳамда локал тармоқ ичидаги ахборот оқимини ҳимоялашни қўллаб-қувватлашда ишлатилиши мумкин. Таъкидлаш лозимки, транспорт режимида ишлаш ҳимояланган ўзаро алоқа гуруҳига кирувчи барча тизимларда ўз аксини топади ва аксарият ҳолларда тармоқ иловаларини қайта дастурлаш талаб этилади.

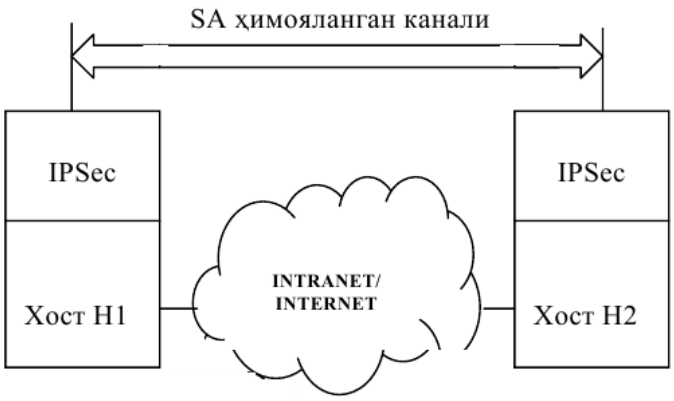
Туннел ёки транспорт режимидан фойдаланиш маълумотларни ҳимоялашга қуйиладиган талабларга ҳамда IPSec ишловчи узел ролига боғлиқ. Ҳимояланувчи канални тугалловчи узел-хост (охирги узел) ёки шлюз (ораликдаги узел) бўлиши мумкин. Мос ҳолда, IPSecни қўллашнинг қуйидаги учта асосий схемаси фарқланади:

- "хост - хост";

- "шлюз — шлюз";

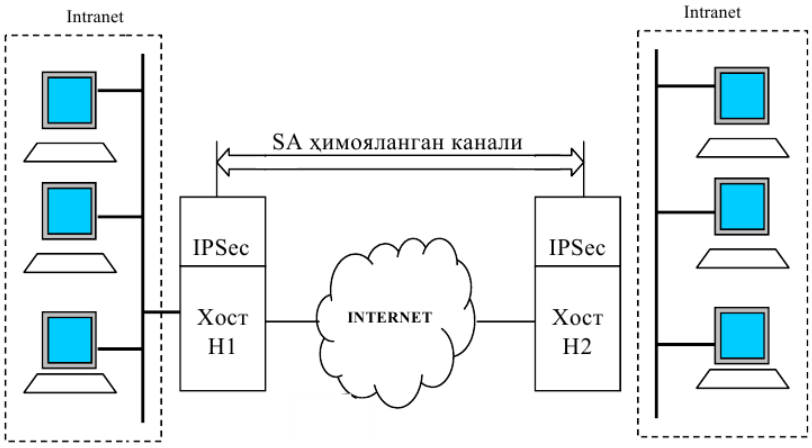
- "хост - шлюз";

Биринчи схемада ҳимояланган канал тармоқнинг охирги иккита узели, яъни Ҳ1 ва Н2 хостлар орасида ўрнатилади (2.12-расм), IPSecни қўллаб-қувватловчи хостлар учун транспорт, ҳам туннел режимларидан фойдаланишга рухсат берилади.



2.12-расм. "Хост - хост" схемаси

Иккинчи схемага биноан, ҳимояланган канал ҳар бирида IPSec протоколи ишловчи, ҳавфсизлик шлюзлари SG1 ва SG2 (Security Gateway) деб аталувчи ораликдаги иккита узеллар орасида ўрнатилади (2.13-расм).



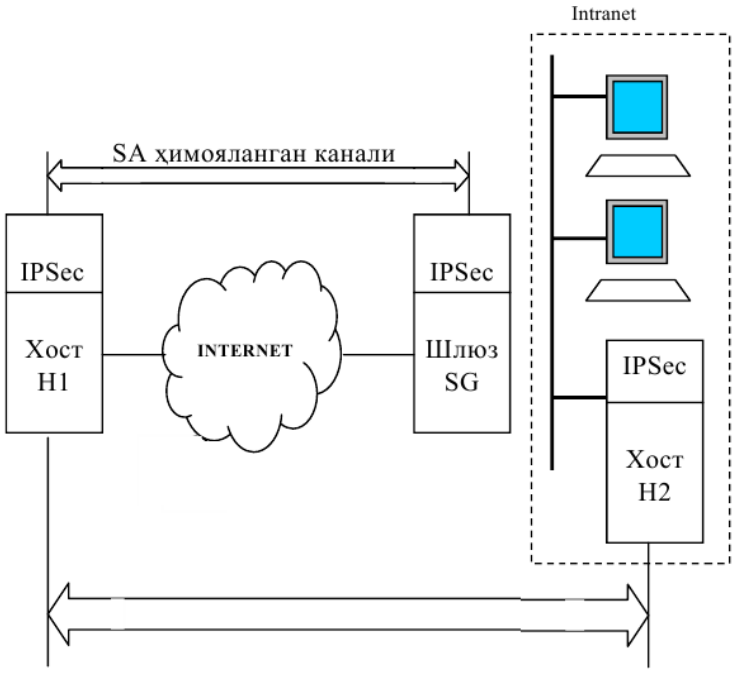
2.13-расм. "Шлюз-шлюз" схемаси.

Ҳавфсизлик шлюзи иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўзидан кейин жойлашган хостлар учун шифрлаш ва аутентификациялаш функцияларини бажаради. VPNнинг ҳавфсизлик шлюзи алоҳида дастурий

маҳсулот, алоҳида аппарат қурилма ҳамда VPN функциялари билан тўлдирилган маршрутизатор ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Маълумотларни ҳимояланган алмашиш тармоқларга уланган, ҳавфсизлик шлюзларидан кейин жойлашган ҳар қандай иккита охирги узеллар орасида руй бериши мумкин. Охирги узеллардан IPSec протоколни қўллаб-қувватлаш талаб қилинмайди, улар ўзларининг трафигини ҳимояланмаган ҳолда корхонанинг ишончли тармоғи Интранет орқали узатади. Умумфойдаланувчи тармоққа юборилувчи трафик ҳавфсизлик шлюзи орқали ўтади ва бу шлюз ўзининг номидан IPSec ёрдамида трафикни ҳимоялашни таъминлайди.

Шлюзларга фақат туннел режимида ишлашга рухсат берилади, гарчи улар транспорт режимини ҳам қўллаб-қувватлашлари мумкин (бу ҳолда самара кам бўлади). "Хост - шлюз" схемаси кўпинча ҳимояланган масофадан фойдаланишда ишлатилади (2.14-расм).



2.14-расм. "Хост - шлюз" схемаси.

Бу ерда ҳимояланган канал IPSec ишловчи масофадаги H1 хост ва корхона Интранет тармоғига кирувчи барча хостлар учун трафикни ҳимояловчи SG шлюз орасида ташкил этилади. Масофадаги хост шлюзга

пакетларни жўнатишда ҳам транспорт ва ҳам туннел режимларидан фойдаланиши мумкин, шлюз эса хостга пакетларни фақат туннел режимида жўнатади.

Бу схемани масофадаги H1 хост ва шлюз томонидан ҳимояланувчи ички тармоққа тегишли бирор H2 хост орасида параллел яна бир ҳимояланган канални яратиб модификациялаш мумкин. Иккита САдан бундай комбинациялаб фойдаланиш ички тармоқдаги трафикни ҳам ишончли ҳимоялашга имкон беради.

Ҳаёт фаолияти хавфсизлиги

Инсон учун мўлжалланган мукаммал ва хавфсиз техникани яратиш, иш ўрнини ташкил этиш ва мехнатни профилактика қилиш, иш фаолиятини комплекс ўрганиш, мехнат мухофазаси меъёрларида санитария қоидаларида ва техника хавфсизлиги чораларидан қонун йўли билан химояланади.

Мехнатни мухофаза қилиш қонунига кўра: кўпгина завод, корхона ва фирмаларда шахсни мехнат фаолиятининг тинч ва хавфсиз узатиш шарти бўлиши керак. Бу шартларни маъмурият ташкил этади.

У ерда янги замонавий олдингисига қараганда, хавфсизроқ техника билан таъминлаш ва ишлаб чиқариш жарохатини олдини олиш керак.

Мехнат гигиенаси одамларнинг ишлаб чиқариш мухитига одамларнинг соғлигига қандай таъсир килишни ўрганади. Ишлаб чикаришда эргономика ва эстетика-ишлаб чиқариш маданиятини бир қисми хисобланади яъни иш жойининг тўғри ташкил қилишдир. Масалан иш жойининг ёки иш столининг тўғри режалаштириш, шунда мониторни ўзини қулай туриши, клавиатура турадиган полкаси столнинг ичига кириб чиқувчи роликли, процессор столининг тагида унинг томонида бўлиши керак.

Ишхонанинг ёритилганлиги. Хозирги пайтда ишхоналарнинг ёритилганлиги стандарт равишда ўрнатилади: SNIP 11-4-79

Компьютер ва бошқа ташкилий техникаларда ишловчилар учун меъёрлар ва санитария қоидалари.

1. КТ ва ТТ ишларининг таркиби

1.1. КТси билан ишлайдиганлар ишлаб чиқариш муҳитини зарарли ва хавфли омиллари ҳамда меҳнат жараёни таъсирига учраши мумкин:

— электромагнит майдони — ЭММ (радиочастота, паст қувватли рентген нурланиши, ультрабинафша ва инфрақизил нурланиш);

— электростатик майдонларининг кучланганлиги;

— ҳавонинг ионизацияланиши;

— кимёвий омил, арзон, лазерли принтерлар ишлатилганда тонер бўёқ моддасининг чанги;

— метеорологик омил: жой иқлимининг ўзига хослиги, йил фасли, вентиляция ҳамда иситиш тизими ва бошқалар;

— механик ва электр қурилмаларида ишлаганда ҳосил бўладиган шовқин;

— электр токидан жароҳатланиш хавфи;

— руҳий ҳиссиётлар зўриқишининг ортиб кетиши;

— кўриш анализаторининг зўриқиши;

— бармоқлар ва панжанинг мускули ҳамкорлигида тез суръатда бажариладиган бир хил чегараланган ҳаракат;

— тананинг мажбурий, бир хил ишчи ҳолатда туриши, гипокенезия.

ТТлар билан ишлашда ҳавонинг ионлашуви, электромагнит майдонларининг кучланганлиги, азон, бўёқ моддаларининг чанги, мажбурий ишчи ҳолат зарарли ва хавфли омиллар ҳисобланади.

1.2. Техниканинг вазифаси ва касбга қараб, меҳнат тартиби ишнинг алоҳидалигини инобатга олган ҳолда ҳар хил бўлиши мумкин (бир ёки икки сменали ва сутка мобайнида). Бир смена давомийлиги 6 соат, 36 соатлик ҳафталик смена мобайнида овқатланиш учун танаффус 40 дақиқадан кам бўлмаслиги керак. Смена мобайнида микротанаффуслар киритиш лозим, улар иш вақтига киритилади.

1.3. Меҳнат шароити ва меҳнат тартиби, ақлий меҳнатнинг зўриқиши ва бошқа юкланишлар КТ ва ТТда ишлайдиганларнинг марказий асаб тизими функционал ҳолатининг ўзгаришига, таянч-ҳаракат аппарати ва қўл панжаларининг ўта зўрқишига олиб келиши мумкин. Гипокинезия ва ишнинг бир хиллиги ишчининг умумий толиқишини (иш қобилиятининг пасайиши) вужудга келтиради. Бундан ташқари, дисплей экрани олдида узоқ вақт бўлиш кўриш анализаторининг зўриқишига ҳамда толиқиш ва кўриш қобилиятининг сусайишига олиб келади. Ишчиларда тез-тез асабийлашиш, уйқунинг бузилиши, чарчоқ, кўз, бел, бўйин атрофи, қўл ва бошқа аъзоларда оғриқлар пайдо бўлиши мумкин.

1.4. Компьютер техникасида ишловчилар меҳнати оғирлиги ва зўриқиши бўйича асосан 2-даражали зарарли ва зўриқиш меҳнатига киради (Меҳнат

шароитларининг кўрсаткичлари бўйича гигиеник таснифи Ўзбекистон Республикаси Соғлиқни сақлаш вазирлиги томонидан 1996-йил 19-мартда тасдиқланган)

2. Хоналарда ишчи ўринларини ташкил этиш

2.1 Ишчи мебелининг конструкцияси ишчининг бўйи ва гавдасига мос бўлиши лозим. Тез-тез ишлатиб туриладиган меҳнат предметлари ва бошқариш органлари ишчи учун қулай бўлиши керак.

2.2. Иш столининг баландлиги 580—760 мм оралиғида сақланиши лозим, агар бунга имкон бўлмаса, столнинг баландлиги 720 мм бўлиши керак; стол устининг энг қулай ишчи ўлчами 1600х900мм ҳисобланади. Иш столининг тагида баландлиги бўйича 600 мм, эни бўйича 500 мм ва чуқурлиги бўйича 650 мм дан кам бўлмаган оёқ ҳаракати учун эркин бўшлиқ бўлиши керак. Иш столининг устида ҳужжатларни жойлаштиришга махсус жой мўлжалланмоғи керак, кўз билан унинг оралиғи, кўздан клавиатурагача бўлган масофадек бўлиши лозим, бу кўришдаги толиқишни анча камайтиради.

2.3. Иш стули (кресло) кўтариладиган - буриладиган, ўтириладиган ва суяниладиган қисми баландлиги бўйича созланиши, шунингдек, унинг контруксияси суянчиқ бурилиш бурчагининг ўзгаришини таъминловчи мослама билан жиҳозланган бўлиши керак. Кресло тирсак қўйгичга эга бўлиши, ҳар бир параметрлари енгил созланиши ва мустақил бўлмоғи лозим.

Ўтириладиган қисм юзасининг баландлиги 400—500 мм оралиғида сақланиши, эни 400 мм, чуқурлиги 380 мм дан кам бўлмаслиги лозим, унинг горизонтал текисликдаги эгилиши 400 мм. Суянчиқнинг қиялик бурчаги ўтириладиган қисм текислигига нисбатан 90—110° оралиғида ўзгариши даркор.

Иш стулининг устки қисмидаги қоплама материали кирланишдан осон тозаланиши, ярим юмшоқ, сирпанмайдиган, электролизат-сияланмайдиган ва қопламаси ҳаво ўтказувчан бўлиши мақсадга мувофиқ.

Ишчи ўринда оёқ учун таглик инобатга олиниши лозим. Унинг узунлиги 400 мм, эни 350 мм ни ташкил этиши керак. Тагликнинг

баландлиги 0—150 мм ва қиялик бурчаги 0—20° оралиғида бўлиши, юзаси тарам-тарам қопламали бўлиши керак.

3.Компьютер техникаси билан ишловчиларнинг меҳнат қилиш ва дам олиш тартиби

3.1. Ишловчиларнинг энг қулай меҳнат қилиш ва дам олиш шароитлари улар меҳнатининг асабий-руҳий зўриқиш даражаси, организм ҳар хил тизими функционал ҳолатининг динамикаси, иш қобилияти ҳамда қатъий белгиланган иш вақти ва танаффусларнинг тартиби инобатга олинган ҳолда белгиланади:

— асосий танаффус тушлик овқатланиш вақти ҳисобланади, КТ ва ТТда ишловчилар иш фаолиятининг алоҳидалигини инобатга олиб, дам олиш тартибига, қўшимча икки — тўрт тартибли микротанаффуслар киритилиши, ҳар бирининг давомийлиги 10—15 дақиқадан бўлмоғи керак. 6 соатли иш кунида икки танаффус уа 12 соатли иш кунида 3-4 танаффус зарур. 6 соатли иш сменасида тушлик овқатланиш иш вақтидан 3 соат кейин бўлганда, қўшимча тартибли танаффуслар иш бошлагандан 1,5-2 соатдан сўнг ва тугашидан 1,5-2 соат олдин берилиши шарт. 12 соатли иш кунида тушлик овқатланиш 5 соат ишлагандан сўнг, биринчи танаффус иш бошлангандан 2 соат кейин, иккинчиси 6 соатдан сўнг, учинчисини 8 соат ва тўртинчиси иш тугашидан 1,5-2 соат олдин берилиши шарт;

- КТ билан ишлаганда меҳнат ва дам олиш тартиби, бажарилаётган ишнинг узлуксизлиги ва хусусиятига боғлиқ бўлиши лозим: маълумотлар узлуксиз киритилганда, дастурни тахрир қилишда, маълумотни экрандан ўқишда, видеомонитор билан ишлаш давомийлиги 4 соатдан ошмаслиги керак. Қолган вақтни бошқа ишларга сарфламоқ лозим.

- ишчи ҳаракатларнинг бир хиллик миқдори, смена давомида 40000 дан ошмаслиги керак.

3.2. КТ ва ТТ билан ишлаганда ҳаддан ташқари зўриқиш ва толиқишнинг олдини олиш мақсадида, ўз вақтида тартибли микротанаффуслар ва жисмоний машқлар комплексини бажариш зарур.

3.3. Асабий-руҳий, кўриш ва мускул зўриқишини камайтириш, толиқишнинг олдини олиш мақсадида психофизиологик кучланишни камайтириш ва чарчоқни йўқотиш сеансларини танаффус вақтларида ва иш кунидан кейин ўтказиш мақсадга мувофиқ. Бу сеанслар махсус жиҳозланган хоналарда олиб борилиши лозим, руҳий чарчоқни камайтириш хонаси иш жойидан 75 м дан узоқда бўлмаслиги керак.

3.4. Ишчиларнинг зўриқишини камайтириш учун уларнинг иш билан юкланишини бир меъёрда тақсимлаш ва иш фаолиятининг хусусиятига қараб оқилона рағбатлаш лозим;

3.5. КТ уа ТТ да доимий ишлашга бажараётган иши бўйича малакаси тўғри келган, меҳнат хавфсизлиги бўйича ўқитилган, ишни олиб бориш усуллари ва меҳнат мухофазаси бўйича йўл-йўриқдан ўтган 18 ёшга тўлган ўсмирларга рухсат этилади;

3.6. Ишга рухсатномаси бор шахслар, доимий равишда КТ ҳамда ТТда ишлайдиганлар, ишга киришдан олдин ва кейинчалик йилда икки марта Ўзбекистон Республикаси Соғлиқни сақлаш Вазирлигининг 27.07.92-йилдаги ПҚ 400 буйруғига асосан даврий тиббий кўрикдан ўтишлари шарт.

Хулоса

IPSec асосида ҳимояланган канални қуриш схемалари турли-туман виртуал ҳимояланган тармоқларни (VPN) яратишда кенг қўлланилади. IPSec асосида турли архитектурага эга бўлган виртуал ҳимояланган тармоқлар, жумладан масофадан фойдаланувчи VPN (Remote Access VPN), корпорация ичидаги VPN(Интранет VPN) ва корпорацияларо VPN(ExtranetVPN) қурилади.

IPSec асосидаги VPN-технологияларининг афзаллигини қуйидаги сабаблар орқали изоҳлаш мумкин:

- тармоқ сатҳининг ҳимояси тармоқда ишловчи барча татбиқий тизимлар учун шаффоф, яъни барча иловалар ҳимояланган тармоқда ҳеч қандай тузатишсиз ва ўзгаришсиз худди очиқ тармоқда ишлаганидек ишлайверади;

- ҳимоялаш тизимининг масштабланувчанлиги таъминланади, яъни мураккаблиги ва унумдорлиги турли бўлган объектларни ҳимоялаш учун мураккаблиги, унумдорлиги, нархи даражаси бўйича адекват бўлган ҳимоялашнинг дастурий ёки дастурий-аппарат воситаларидан фойдаланиш мумкин;

- масштабланувчи қатордаги ахборотни ҳимоялаш маҳсулотлари бирга ишлай оладилар, шу сабабли уларни турли сатҳдаги объектларда (масофадаги ягона терминаллардан то ихтиёрий масштабли локал тармоқларгача) ресурсларидан ва трафигидан барча бегоналар фойдалана олмайдиган ягона корпоратив тармоққа бирлаштириш мумкин.

Шундай қилиб, VPN туннели очиқ тармоқ орқали ўтказилган уланиш бўлиб, у орқали виртуал тармоқнинг криптографик ҳимояланган ахборот пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги ҳимоялаш қуйидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;

- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);

- етказиладиган ахборотнинг ҳақиқийлигини ва яхлитлигини текшириш.

Битирув малакавий ишида қуйида келтирилган вазифалар бажарилди.

2. VPNтармоғини ташкил этишнинг назарий ваамалий асослари ўрганилди.

2.VPN технологиясининг ютуқлари ва камчиликларини уммий таҳлил қилинди.

3. VPN тармоғини ташкил этишнинг дастурий ва техник воситаларини кўриб чиқилди.

4. Ҳимояланган виртуал хусусий тармоқларни қуриш технологияси тадқиқ қилинди.

5. IPSec протоколлар стекини ҳимояланган виртуал хусусий тармоқлар қуришда ишлатилиши кўриб чиқилди.

6. VPN тармоғига дастурий ва техник хизмат кўрсатиш бўйича амалий билим ва кўникмаларга эга бўлинди.

Ушбу битирув малакавий ишини бажариш ва тайёрлашда ўз мутахассислигимга оид бир қанча амалий билим ва кўникмаларга эга бўлдим ва бу билим ва кўникмаларни келажакда ишлаб чиқаришда ва таълим сохасида қўллашга харакат қиламан.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Каримов И.А. “Мамлакатимизда демократик ислоҳотларни янада чуқурлаштириш ва фуқаролик жамиятини ривожлантириш Консепсияси”. – Т., 2010.
2. Ўзбекистон Республикасининг «Ахборотлаштириш тўғрисида»ги қонуни// Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси.-2004.-№1–2. -10-м.
3. Ўзбекистон Республикасининг «Ахборот эркинлиги принсиплари ва кафолатлари тўғрисида»ги қонуни// Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2003. – №1. – 2-м.
4. С.С.Қосимов. Ахборот технологиялари. Ўқув қўлланма. — Тошкент. "Алоқачи", 2006.
5. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармоқларида информация ҳимояси. Олий ўқув юрти талабалари учун ўқув қўлланма.-Тошкент Давлат техника университети, 2003.
6. В.И. Завгородный. Комплексная защита информации в компьютерных системах: Учебное пособие.-М: Логос; ПБОЮЛ Н.А.Егоров, 2001.
7. Г.Н. Устинов. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия "Безопасност".-М.:СИНТЕГ, 2000.
8. Мерит Максим, Девид Поллино. Безопасност беспроводных сетей. Информационные технологии для инженеров.-Москва. 2004.
9. А. Соколов, О. Степанюк. Зашита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.
10. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент.-2003.-№1,2.
11. А.В. Беляев. Методы и средства зашиты информации //ҳттп://www.ситфорум.ру/ интернет/инфсесйре/иц2000_01.ҳтмл.
12. Век Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент-2000-№4-5.
13. А. Галатенко. Активный audit//Get Info.-1999.-№8.

14. А.В. Лукатский. Адаптивная безопасность сети// Компьютер-Пресс. - 1999.-8.

15. Н.А.Олифер. Протоколи IPSec.//LAN.-2001.-№03; http://www.osp.ru/lan/ 2001/03/024.htm.

16. А.А. Петров. Компьютерная безопасность. Криптографические методи зашиты.-М.: ДМК Пресс, 2000.

17. Программно-аппаратные средства обеспечения информационной безопасности. Зашита программ и данных: Уч.пособие для ВУЗов/ Авт.: П.Й. Белкин и др. —М.:Радио и связ, 1999.

18. Й.В. Романетс, П.А. Тимофеев, В.Ф. Шангин. Зашита информации в компьютерных системах и сетьях: 2-е изд., перераб. и доп. — М.: Радио и связ, 2001.

19. А.В. Соколов, В.Ф. Шангин. Зашита информации в распределенных корпоративных сетях и системах. —М.: ДМК Пресс, 2002.

20. Типовые решения по применению технологии межсетевих экранов для зашиты информационных ресурсов / ООО "Конфидент". —СПб., 2001.

21. “Ахборот технологияси. Ахборотларни криптографик мухофазаси. Маълумотларни шифрлаш алгоритми” Ўзбекистон Давлат стандарти. ЎзДСт 1105:2006.

22. www.nasa.gov/statistics/

23. www.security.uz

24. www.cert.uz

25. www.uzinfocom.uz