ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Ғаниев С. К.,
Каримов М. М.,
Ташев К. А.

АХБОРОТ ХАВФСИЗЛИГИ

Ахборот-коммуникацион тизимлар хавфсизлиги

Олий укув юрт талабалари учун мўлжалланган

МУНДАРИЖА

МУК.АДДИМА

Илдам кдцамлар билан ривожланаётган компьютер ахборот технологиялари хаётимизда сезиларли узгаришларга сабаб булмокда. "Ахборот" тушунчаси сотиб олиш, сотиш, бирор нарсага алмашиш ва х,. мумкин булган махсус товарни белгилашда тез-тез ишлатила бошланди. Бунда ахборотнинг нархи купинча у жойлашган компьютер тизими нархидан юз ва минг марта юкори булади. Демак, ахборотни рухсатсиз фойдаланишдан, атайин узгартиришдан, йук, килишдан ва бошка жиноий харакатлардан химоялаш заруриятининг пайдо булиши табиийдир.

Ахборотни химоялаш муаммоси компьютер тизимлари ва тармоклари сохасида фаолият курсатувчи мутахассислар хамда замонавий компьютер воситаларидан фойдаланувчилар эътиборини жалб этмокда. Айни пайтда компьютер фани ва амалиётининг ушбу долзарб муаммоси Давлат тилида ёзилган илмий-техник ва укув адабиётларда етарлича уз аксини топмаган.

Укувчи эътиборига хавола этилаётган китоб ахборот-коммуникацион тизимлар хавфсизлигига багишланган ва 13 та бобдан иборат.

Китобнинг *биринчи бобида* ахборот хавфсизлигининг хрзирги хрлатига бахр берилади. Компьютер жиноятчилиги тахдил этилиб, тармок, ахборотига буладиган намунавий хужум усуллари келтирилади х,амда ахборот хавфсизлигини бузувчининг модели тавсифланади.

Китобнинг *иккинчи бобида* Internet тармокнинг асосий ахборот хизматалари тавсифланади. Internet да электрон бизнес ва электрон тижоратнинг асосий моделлари тахлилланади. Электрон савдо ва Internet - хизматларнинг асосий турлари тавсифланади. Электрон бизнес тизими хавфсизлигининг муаммолари курилади.

Китобнинг *учинчи бобида* ахборот хавфсизлигининг асосий тушунчалари курилади, хавфсизликни таъминлашнинг амалда текширилган принциплари хамда хавфсизлик сиёсатини яратиш жараёни тавсифланади. Ахборот-коммуникацион тизимлар ва тармоклар хавфсизлигига куйиладиган та-лаблар келтирилади. Ахборот хавфсизлигини таъминловчи чоралар хусуси-да суз юритилади.

Китобнинг *туртинчи боби* ахборот хавфсизлигининг хукукий ва ташкилий таъминотига багишланган. Хавфсизликнинг халкаро ва миллий хукукий меъёрлари хусусида суз юритилади.

Китобнинг *бешинчи боби* ахборотни химоялашнинг криптографик усулларига багишланган булиб, маълумотларни шифрлашнинг блокли симметрик алгоритмлари, жумладан, АКШнинг янги стандарти AES тахлил этилади. Замонавий асимметрик криптотизимлар мухркама этилади. Хэшлаш функцияларининг асосий хусусиятлари ва ишлатилиш сох,алари аникданади. Ракамли имзони генерациялаш ва текшириш муолажалари курилади. Калитларни бошкариш - калитларни таксимлаш жараёнига алохида эътибор килинади.

Китобнинг *олтинчи бобида* тизимнинг фойдаланувчилар билан узаро алокасидаги асосий жараёнлар - фойдаланувчи харакатини аутентификациялаш, авторизациялаш ва маъмурлаш тушунтирилади. Куп мартали ва бир мартали пароллар, хамда ракамли сертификатлар асосидаги аутентификациялаш хусусиятлари тахлил этилади. Фойдаланувчини идентификациялаш ва аутентификациялашнинг намунавий схемалари курилади. Симметрик ва асимметрик криптоалгоритмларга асосланган катъий аутентификациялашга алох,ида эътибор берилади. Аутентифкациялашнинг Kerberos протоколи мухркама этилади. Биометрик идентификациялаш ва аутентификациялаш воситалари тавсифланади.

Китобнинг *еттинчи бобида* тармоклараро экранларнинг функциялари тахдил этилиб, уларнинг OSI моделининг турли сатхларида ишлаши хусусиятлари мухркама килинади. Тармокларо экранлар асосида тармокни х,имоялаш схемалари тавсифланади. Шахсий ва таксимланган тармок, экранларининг ишлатилиши курилади.

Китобнинг *саккизинчи бобида* химояланган виртуал хусусий тармокдарни куриш концепцияси курилади ва уларнинг асосий хусусияти - туннеллаш шархланади. Виртуал химояланган каналларни к,уриш вариантлари тахдилланади. Химояланган виртула хусусий тармокдарнинг катор аломатлари буйича туркумланиши курилади. VPN технологиянинг корпоратив ахборот тизимлари ва тармокдарида к,улланилишининг техник ва иктисодий афзалликлари курсатилади. OSI очик, тизимлар узаро алока эталон моделининг канал ва сеанс сатхдарида химояланган виртуал каналлар

курилишининг муаммолари мухркама этилади. IPSec протоколлар стекининг архитектураси курилиб, уларнинг химояланган хусусий тармоклар куришда ишлаштилиши курилади.

Китобнинг *тущизини бобида* очик, калитларни бошкариш инфратузилмаси PKI курилади. Очик, калитларнинг ракамли сертификатларини ишлатиш зарурияти асосланади. PKI нинг ишлаш принциплари мухркама этилади. Сертификациялашнинг базавий моделлари, PKI нинг мантикий тузилмаси ва компонентлари келтирилади.

Китобнинг *унинчи боби* ахборот хавфсизлигини адаптив бошкаришнинг долзарб муаммоларига багишланган. Корпоратив тармок, хавфсизлигини адаптив бошкариш концепцияси тавсифланади. Химояланишни тахлиллашнинг технологиялари ва воситалари батафсил мухркама этилади. Тармок, ахборотини тахлиллаш усуллари, хужумларни аникдаш тизимларининг компонентлари ва архитектураси курилади. Компьютер вирусларидан химояланишнинг долзарб муаммолари хам ушбу бобдан урин олган. Компьютер вирусларининг туркумланиши келтирилади, вирус хаёт цикли боскичлари тахлилланади ва вирусларнинг ва бошка зарар келтирувчи дастурларнинг асосий тарк,алиш каналлари курилади. Вирусга карши дастурларнинг асосийлари мух,окама этилади. Вирусга карши х,имоя тизимини куриш масаласи курилади.

Китобнинг *ун биринчи боби* маълумотларни узатиш тармогида ахборотни х,имоялаш муаммосига багишланган. Маълумотларни узатиш тармоги компонентларига ва архитектурасига реал таъсир этувчи функционал, архитектуравий ва бошкариш (маъмурий) талаблар курилади. Алока каналларида маълумотларни химоялаш усуллари мух,окама этилади.

Китобнинг *ун иккинчи боби* симсиз алока тизимларида ахборот х,имоясининг долзарб масалаларига багишланган. Симсиз тармок, концепцияси ва тузилмаси курилади. Симсиз тармок, хавфсизлигига тахдидлар батафсил тахлил этилиб, симсиз тармок, хавфсизлиги протоколлари мухркама

этилади. Симеиз курилмалар хавфеизлиги муаммолари хам ушбу бобдан урин олган.

Китобнинг *ун учинчи боби* тармок, хавфеизлиги воситаларини бошкариш усулларига багишланган. Ахборот тизимларини бошкаришнинг кенг тарк,алган методологияси ITIL тавсифланади. Корхона микёсида ахборотни химоялаш тизимини бошкариш масаласи таърифланади. Хавфсизликни марказлаштирилган бошкаришнинг глобал ва локал хавфсизлик сиёсатига асосланган истик,болли архитектурасига алох,ида эътибор берилади. Ахборот тизимлари хавфеизлигининг аудити ва мониторинги курилади. Хавфхатарларни тахлиллаш ва бошк,ариш муаммоси, хамда тармок, хавфсизлик тизимини куриш методологияси тавсифланади.

К,улланмани тайёрлашда якиндан ёрдам берган (VII ва XI боблар) техника фанлари номзоди А.А. Ганиевга, так,ризчиларга х,амда ук,ув кулланма х,ак,идаги барча фикр мулох,азалари учун хурматли китобхонларга муаллифлар уз миннатдорчиликларини изх,ор этадилар.

Муаллифлар

I боб. АХБОРОТ ХАВФСИЗЛИГИГА ТАХДИДЛАР

1.1. Ахборот урушлар ва киберхужумлар

Хавфсизлик - хар куни биз тукнашадиган хаётимизнинг жихати: эшикни кулфлаймиз, кимматбахр нарсаларни бегона кузлардан беркитамиз ва хамённи дуч келган жойда крлдирмаймиз. Бу "ракамли дунёга" хам раем булиши шарт, чунки хар бир фойдаланувчининг компьютери карокчи хужуми объекти булиши мумкин.

Коммерция ташкилотлари хавфеизликни таъминлаш узининг биринчи галдаги вазифаси эмас, балки уни таъминлашга сарф этиладиган харажатларни мукаррар бало деб хдеоблаб келганлар. Кандайдир даражада бу "окилона иш": нихрят, усиз хам иш бажаришда тусиклар тулиб-тошиб ётибдику?! Аммо фирманинг барча корпоратив биноларига кеча-кундуз киришга рухсат беришга журъат этувчи акли жойида "саноат капитанлари"ни курганмисиз? Албатта, йук,! Хдтто кичкина компания биносининг кириш йулида сизни к,оровул, ёки киришни чегараловчи ва назоратловчи тизими к,арши олади. Ахборотни химоялаш эса х,али кунгилдагидек эмас. Ахборотни к,андай йукртиш мумкинлигини ва бу к,андай окибатларга олиб келишини барча хам тушунавермайди.

Йирик уйинчилар яхшигина сабок, олдилар: хакерлар Yahoo.com, Amazon.com каби компанияларга ва х,атто космик тадкикрт агентилиги NASAra катта зарар етказдилар. Хавфсизлик хизмати бозорининг энг йирик номоёндаларидан бири RSA Security, харкандай тахдидга к,арши чора борлиги хусусидаги уйламасдан к,илган баёнотидан бир неча кундан кейин, хужумга дучор булди[29].

Одатда одамлардан ёки предметлардан чикадиган ва зарар етказадиган тахдидлар к,уйидаги синфларга булинади: *ички* ёки *ташци* ва *тузилмаланган* (маълум объектга карши) ёки *тузилмаланмаган* ("кимга Худо беради" к,абилида адресланувчи). Масалан, компьютер вируслари "ташк,и тузилмаланмаган тахдидлар" сифатида туркумланади ва тамомила оддий х,исобланади. К,изиги шундаки, фойдаланувчилар узининг компьютерини муайян нишон деб хисобламайдилар, улар узларини яхшигина

химоялангандек сезадилар. Керакли химоя даражаси аксарият хрлларда ишингизнинг хрлатига боглик,. Агар ташкилотингиз ёки компаниянгиз кандайдир тазйик, нишони булса, агар сиз миллий энергетик ресурсларни таксимловчи ёки миллий алока тармокдарига хизмат килувчи давлат инфратузилмаси таркибида булсангиз, оддий террористлар бомбаларини ва пистолетларини четга куйиб, турли-туман дастурий воситалар ёрдамида ташкилотингизга электрон хужумни амалга ошириш масаласини курадилар. Иккинчи томондан, савдо-сотик, ва маркетинг буйича оддий ташкилот хусусида суз борса, факат мижозлар руйхатини угриловчи хизматчиларингиз тугрисида, калбаки кредит карточкалари буйича товар олувчи фирибгарлар, тармогингизга прейскурантлардан фойдаланиш максадида кирувчи ракиблар, Web-сайтингизни таъмагирлик максадида бузувчилар ва шунга ухшашлар тугрисида кайгуришингизга тугри келади.

Аммо, вах,имага урин йук,. Биринчи навбатда кундалик эх,тиёж чоралари курилиши лозим. Ахборотга эга булишнинг энг оммабоп усули оддий угрилик. Сиз иш столингизда кечага мумайгина пулни крлдириб кетмайсизу. Нима учун бокувчингиз-шахсий компьютер хавфсизлигини таъминлашга озгина вакт сарф килмайсиз? Бу нафак,ат аппарат воситалар ига, балки маълумотларга х,ам тааллукди. Маълумотларни угирлатиш ёки йук,отиш катта, баъзида, тузатиб булмайдиган зарар келтиради.

Маълумки, тизим маъмурлари барча махфий материаллардан фойдаланиш имконига эга ва, одатда, компания фойдасидан уз улушларига эга эмаслар. Шу сабабли худди улар ташкилот хавфсизлигига тахдид сола олувчилар ичида энг каттаси х,исобланадилар. Таъкидлаш лозимки, компания ишга кирувчиларни синчиклаб текширади. Худди шундай, хавфсизлик хизматини таъминловчиларга, айник,са маслахат бериш, режалаштириш ва муъмурлашни тавсия этувчиларга дик,к,ат билан к,араш лозим.

Цивилизация ривожининг замонавий боскичида ахборот нафакат жамоат ва давлат институтлари фаолиятида, балки х,ар бир инсон хаётида х,ал к,илувчи ролни уйнайди. Куз олдимизда жамиятнинг ахборотлашиши шиддат билан ва купинча олдиндан билиб булмайдиган тарзда ривожланмокда.

Биз эса унинг ижтимоий, сиёсий, ик,тисодий ва бошкд ок,ибатларини тушуниб етишга бошлаймиз, холос. Жамиятимизнинг ахборотлашиши ягона дунё ахборот маконининг яратилишига олиб келадики, бу макон доирасида ахборотни йигаш, ишлаш, сакдаш ва субъектлар - инсонлар, ташкилотлар, давлатлар уртасида алмашиш амалга оширилади.

Равшанки, сиёсий, ик,тисодий, илмий-техникавий ва бошкд ахборотларни тезликда алмашиш имконияти жамият хдётининг барча сох,аларида ва айник,са ишлаб чикдришда ва бошкдришда янги технологияларнинг кулланилиши сузсиз фойдалидир. Аммо, саноатнинг тезликда рифожланиши Ер экологиясига тахдид сола бошлади, ядро физикаси сохасидаги ютукдар ядро уруши хавфини тугдирди. Ахборотлаштириш хам жиддий муаммолар манбаига айланиши мумкин.

Урушлар доимо булган. Вак,т утиши билан урушни олиб бориш бутун бир фанга айланди. Хдркдндай фандагидек урушда узининг тарихи, узининг к,оидаси, машхур намоёндалари, узининг методологияси пайдо булди.

Замонавий уруш гояси жуда илдамлаб кетди. Энди унинг макони - бутун ер шари. Уруш локал кдрок,чи хужумидан бир неча давлатларни вайрон к,илувчи глобал муаммога айланди.

Турли мамлакатларнинг харбий доктриналарида электрон к,урол ривожи режалари ва махсус вазифаларга мулжалланган дастурий таъминот тугрисида эслатишлар кузга ташланмокда. Турли разведка манбаларидан келаётган ахборотнинг тахдили натижасида хулоса к,илиш мумкинки, баъзи бир давлатларнинг рахбарлари хужумкор кибер-дастурларни яратишни молияламокдал ар.

Ахборот урушига оддий воситалар ёрдамида х,арбий х,аракатлар самара бермайдиган х,олларга нисбатан стратегик альтернатива сифатида к,аралмокда.

Харбийлар томонидан киритилган *ахборот уруши* атамаси реал, к,иргинли ва емирувчи харбий харакатлар билан боглик, шафк,атсиз ва хавфли фаолиятни англатади. Бу урушнинг алох,ида к,ирралари-штаб уруши, электрон уруши, психологик амаллар ва х,.

Хдр кандай уруш, ахборот уруши шу жумладан, замонавий курол ёрдамида олиб борилади. Ахборот куроли ёрдамида, уруш олиб борилувчи барча куроллардан фаркди уларок,, эълон килинмаган ва купинча дунёга куринмайдиган урушларни олиб бориш мумкин (олиб борилмокда хам). Бу куролнинг таъсир объектлари - иктисодий, сиёсий, ижтимоий ва х,. каби жамият ва давлат институтлари. Маълумотларни узатиш тармокдарининг келажак жанглар майдонига айланиши аллакачон эътироф этилган.

Ахборот куроли хужумда ва мудофаада "электрон тезлик" билан ишлатилиши мумкин. У энг илгор технологияларга асосланган булиб, харбий низоларни дастлабки боскичида х,ал этилишини таъминлайди хамда умуммаксад кучларнинг кулланилишини истисно килади. Ахборот куроли кулланишининг стратегияси хужумкор характерга эга. Аммо хусусий заифлик нуктаи назари мавжуд, айник,са фукрролик секторида. Шу сабабли бундай куролдан ва ахборот терроризмидан х,имояланиш муаммоси хрзирда биринчи уринга чик,к,ан. Фойдаланувчиларига дунё тармокдарида ишлашни таъминловчи мамлакатларнинг миллий ахборот ресурсларининг заифлиги - хар икки томонга хавфли нарса.

Ахборот куроли деганда ахборот массивларини йукртиш, бузиш ёки угирлаш воситалари, х,имоялаш тизимини йук,отиш, к,онуний фойдаланувчилар фаолиятини чегаралаш асбоб-ускуналар ва бутун компьютер тизими ишлаши тартибини бузиш воситалари тушунилади.

Хрзирда хужумкор ахборот куроли сифатида к,уйидагиларни курсатиш мумкин:

- *компьютер вируслари* - купайиш, дастурларда урнашиш, алок,а линиялари, маълумотларни узатиш тармокдари буйича узатилиш, бошк,ариш тизимларни ишдан чикариш ва шунга ухшаш к,обилиятларга эга;

- *мантщий бомбалар* - сигнал буйича ёки урнатилган вактда харакатга келтириш мак,садида х,арбий ёки фукаро инфратузилмаларига урнатилувчи дастурланган к,урилмалар;

- *телекоммуникация тармокларида ахборот алмашинувини бостириш воситалари,* давлат ва харбий бошкарув каналларида ахборотни сохталаштириш;

- *тестли дастурларни бетарафлаштириш воситалари;*

- объект дастурий таъминотига айгокчилар томонидан атайин киритилувчи турли хил *хатоликлар.*

Универсаллик, махфийлик, дастурий-аппарат амалга оширилишининг хар хиллиги, таъсирининг кескинлиги, кулланилишининг вакти ва жойини танлаш имконияти, нихрят, фойдалилиги ахборот куролини хаддан ташкари хавфли килади. Бу куролни, масалан, интеллектуал мулкни химоялаш воситасига ухшатиб никрблаш мумкин. Ундан ташкари, у хатто уруш эълон килмасдан хужум харакатларини автоном тарзда олиб бориш имконини беради.

Замонавий жамиятда ахборот куролини ишлатиш харбий стратегияси фукаро сектори билан узвий богаанган. Ахборот куролининг, унинг таъсири шакли ва усулларининг пайдо булиши ва кулланиши хусусиятларининг турли-туманлилиги ундан химояланишнинг мураккаб масалаларини вужудга келтирди.

Ахборот куроли к,улланилишини олдини олиш ёки кулланиши ок,ибатларини бартараф к,илиш учун куйидаги чораларни куриш л озим:

- ахборот ресурсларининг физик асосини ташкил этувчи моддий-техник объектларни х,имоялаш;

- маълумотлар базалари ва банкларининг меёрий ва муттасил ишлашини таъминлаш;

- ахборотдан рухсатсиз фойдаланишдан, уни бузилишидан ёки йук, к,илинишидан химоялаш;

- ахборот сифатини саклаш (уз вактидалиги, аникдиги, тулалиги ва фойдаланувчанлиги).

Давлатнинг дунё очик, тармогига уланишининг иктисодий ва илмий-техник сиёсатини ахборот хавфсизлиги орк,али куриш лозим. Бу очик,, фукароларнинг ахборотга ва интеллектуал мулкга эга булиш крнуний х,ук,укини сакдашга мулжалланган сиёсат мамлакат худудида тармок, асбоб-ускуналарини унга ахборот куроли элементларининг киришидан саклашни кузда тутиш лозим. Бу муаммо хрзирда, чет эл ахборот технологияларини оммавий сотиб олинаётган пайтда ута мухимдир.

Маълумки, дунё ахборот маконига уланмасдан мамлакат иктисодини ривожлантириб булмайди. Internet тармоги томонидан таъминланган ахборот ва хисоблаш ресурсларидан оператив фойдаланишни давлатчиликни, фукаролик жамияти институтларини мустахкамлаш, ижтимоий инфратузилмаларининг ривожланиш шартлари сифатида талкин этиш мумкин.

Аммо мамлакатнинг х,алкаро телекоммуникация тизимида ва ахборот алмашинувида иштирокининг ахборот хавфсизлиги муаммосини комплекс х,ал килмасдан мумкин эмаслигини аник, тасаввур этиш лозим. Айникса хусусий ахборот ресурсларини химоялаш муаммоси ахборот ва телекоммуникация технологиялар сохасида ривожланган мамлакатлардан технологик оркада крлаётган мамлакатлар учун жиддий хисобланади.

Ахборот куролини ишлаб чикишни ва уни ишлатишни химиявий ва бактериологик курол каби такиклаш эхтимолдан узок,. Худди шу каби купгина мамлакатларнинг ягона глобал ахборот маконини шакллантириш буйича уринишларини чегаралаб булмайди.

Тизим маъмури учун химоянинг макбул даражасини таъминлашнинг ягона усули-ахборотга эга булиши, чунки хрзирча ахборот хужумига энг тез реакция берадиган инсон хисобланади. Демак, ахборотни химоялаш маъмурларининг укитишта ва профессионал усишига сарф-харажат ахборот хужумларига карши турувчи энг самарали восита х,исобланади.

1.2. Ахборот-коммуникацион тизимлар ва тармо^ларда таадидлар ва заифликлар

Тармок, технологиялари ривожининг бошлангич боск,ичида вируслар ва компьютер хужумларининг бошк,а турлари таъсиридаги зарар кам эди, чунки у даврда дунё иктисодининг ахборот технологияларига богликдиги катта эмас эди. Хрзирда, хужумлар сонининг доимо усиши х,амда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига богликдиги шароитида машина вактининг йук,олишига олиб келувчи х,атто озгина хужумдан келган зарар жуда катта ракамлар орк,али х,исобланади. Мисол тарикасида келтириш мумкинки, фак,ат 2003 йилнинг биринчи чора-

гида дунё микёсидаги йукртишлар 2002 йилдаги барча йукртишлар йигиндисининг 50%ини ташкил этган, ёки булмаса 2006 йилнинг узида Россия Федереациясида 14 мингдан ортик, компьютер жиноятчилиги хрлатлари кайд этилган[29, 30, 32].

Корпоратив тармокларда ишланадиган ахборот, айникса, заиф булади. Хрзирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлгон ахборотнинг муомалага кириши имконининг жиддий ошишига куйидагилар сабаб булади:

- компьютерда ишланадиган, узатиладиган ва сакланадиган ахборот хажмининг ошиши;
- маълумотлар базасида мухимлик ва махфийлик даражаси турли булган ахборотларнинг тупланиши;
- маълумотлар базасида сакланаётган ахборотдан ва хисоблаш тармок, ресурларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сониниг ошиши;
- фойдаланувчиларни боглаш учун Internet глобал тармогини ва алоканинг турли каналларини кенг ишлатиш;
- фойдалувчилар компьютерлари уртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига тахдид деганда ахборотнинг бузилиши ёки йук,отилиши хавфига олиб келувчи химояланувчи объектга к,арши к,илинган харакатлар тушунилади. Олдиндан шуни айтиш мумкинки, суз барча ахборот хусусида эмас, балки унинг фак,ат, мулк эгаси фикрича, коммерция кийматига эга булган кисми хусусида кетяпти.

Замонавий корпоратив тармоклар ва тизимлар дучор буладиган кенг тарк,алган тахдидларни тахдиллаймиз. Хисобга олиш лозимки, хавфсизликка тахдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташкарисида (ташк,и манба) булиши мумкин. Бундай ажратиш тугри, чунки битта тахдид учун (масалан, угирлаш) ташки ва ички манбаларга карши х,аракат усуллари турлича булади. Булиши мумкин булган тахдидларни хамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур хисобланади.

Тез-тез буладиган ва хавфли (зарар улчами нуктаи назаридан)

тахдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат курсатувчи бошка шахсларнинг атайин килмаган хатоликлари киради. Баъзида бундай хатоликлар (нотугри киритилган маълумотлар, дастурдаги хатоликлар сабаб булган тизимнинг тухташи ёки бузилиши) тугридан тугри зарарга олиб келади. Баъзида улар нияти бузук, одамлар фойдаланиши мумкин булган нозик жойларни пайдо булишига сабаб булади. Глобал ахборот тармогида ишлаш ушбу омилнинг етарлича долзарб килади. Бунда зарар манбаи ташкилотнинг фойдаланувчиси хам, тармок, фойдаланувчиси хам булиши мумкин, охиргиси айникса хавфли.

Зарар улчами буйича иккинчи уринни угирлашлар ва сохталаштиришлар эгаллайди. Текширилган хрлатларнинг аксариятида ишлаш режимлари ва химоялаш чоралари билан аъло даражада таниш булган ташкилот штатидаги ходимлар айбдор булиб чикдилар. Глобал тармокдар билан богланган к,увватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йукдиги бундай фаолиятга к,ушимча имкон яратади.

Хафа булган ходимлар (хатто собикдари) ташкилотдаги тартиб билан таниш ва жуда самара билан зиён етказишлари мумкин. Ходим ишдан бушаганида унинг ахборот ресурсларидан фойдаланиш хук,ук,и бекор килиниши назоратга олиниши шарт.

Хозирда ташки коммуникация оркали рухсатсиз фойдаланишга атайин килинган уринишлар булиши мумкин булган барча бузилишларнинг 10%ини ташкил этади. Бу катталик анчагина булиб туюлмаса хам, Internetfla ишлаш тажрибаси курсатадики, к,арийб х,ар бир Internet-сервер кунига бир неча марта сукилиб кириш уринишларига дучор булар экан. Хавф-хатарлар тахлил к,илинганида ташкилот корпоратив ёки л окал тармоги компьютерларининг хужумларга к,арши туриши ёки булмаганида ахборот хавфсизлиги бузилиши фактларини к,айд этиш учун етарлича химояланмаганлигини х,исобга олиш зарур. Масалан, ахборот тизимларини

хдмоялаш Агентлигининг (АКД1) тестлари курсатадики, 88% компьютерлар ахборот хавфсизлиги нуктаи назаридан нозик жойларга эгаки, улар рухсатсиз фойдаланиш учун фаол ишлатишлари мумкин. Ташкилот ахборот тузилмасидан сасофадан фойдаланиш холлари алохдда курилиши лозим.

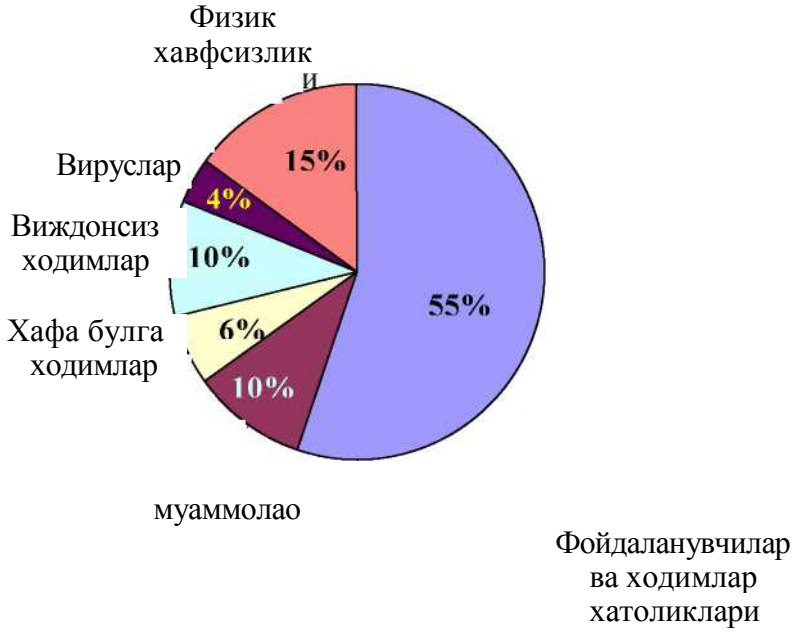
Химоя сиёсатини тузишдан аввал ташкилотда компьютер мухити дучор буладиган хавф-хатар бахрланиши ва зарур чоралар курилиши зарур. Равшанки, химояга тахдидни назоратлаш ва зарур чораларни куриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни химоялаш буйича хеч кандай чоралар курилмаганида кутиладиган йук,отишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер мух,ити икки хил хавф-хатарга дучор булади:

1. Маълумотларни йук,отилиши ёки узгартирилиши.
2. Сервиснинг тухтатилиши.

Тахдидларнинг манбаларини аникдаш осон эмас. Улар нияти бузук, одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий тахдид х,исобланади. 1.1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари буйича статистик маълумотларни тасвирловчи айланма диаграмма келтирилган.



1.1-раем. Хавфсизликнинг бузилиш манбалари.

l.l.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармок, ва тизими хавфсизлигига тахдиддарни самарали камайтириш учуй харакатларни каерга йуналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шугулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайтириш буйича чоралар курилиши зарур. Шу билан бир каторда корпоратив тармок, ва тизимга хам ташкаридан, хам ичкаридан буладиган хужумларни олдини олиш буйича тармок, хавфсизлиги масаласини ечишга жиддий эътиборни каратиш зарур.

1.3. Компьютер жиноятчилигининг та^лили

Компьютер жиноятчилиги статистикаси тахдил этилса кайгули манзарага эга буламиз. Компьютер жиноятчилиги етказган зарарни наркотик моддалар ва куролларнинг нокрнуний айланишидан олинган фойдага киёслаш мумкин. Факат АКШда "электрон жиноятчилар" етказган хар йилги зарар карийб 100 млд. долларни ташкил этар экан.

Якин келажакда жиноий фаолиятнинг бу тури даромадлилиги, пул маблагларининг айланиши ва унда иштирок этувчи одамлар сони буйича якин вактларгача нокрнуний фаолият орасида даромаддиги билан биринчи уринни эгаллаган нокрнуний бизнеснинг уч туридан узиб кетиш эхтимоллиги катта. Бу нок,онуний бизнеслар-наркотик моддалар, курол ва кам учрайдиган ёввойи х,айвонлар билан савдо килиш.

Давлат ва хусусий компаниялар фаолиятининг социологик тадк,ик,и маълумотларига к,араганда XXI асрнинг биринчи йилларида иктисодий сохадаги жиноятчилик банк ва бошк,а тизимларнинг ахборот-коммуникацион комплексларига булиши мумкин булган гаразли иктисодий харакатларга каратилган булади.

Кредит-молия сох,асидаги компьютер жиноятчилигининг сони муттасил усиб бормокда. Масалан онлайн магазинларида 25%гача каллоблик тулов амаллари к,айд этилган. Шунга карамасдан Fap6 давлатларида электрон тижоратнинг-юкрри даромадли замонавий бизнеснинг фаол ривожланиши кузга ташланмокда. Маълумки, бу сох,а ривожланиши билан параллел

равишда "виртуал" каллобларнинг хам даромади ошади. К,аллоблар энди якка хрлда харакат килмайдилар, улар пухталик билан тайёрланган, яхши техник ва дастурий куролланган жиноий гурухдар билан, банк хизматчиларининг узлари иштирокида ишлайдилар.

Хавфсизлик сохасидаги мутахассисларнинг курсатишича бундай жиноятчиларнинг улуши 70%ни ташкил этади. "Виртуал" угри узининг хамкасби-оддий боскинчига нисбатан куп топади. Ундан ташкари "виртуал" жиноятчилар уйидан чикмасдан харакат киладилар. Фойдаланишнинг электрон воситаларини ишлатиб килинган угрилик зарарининг уртача курсаткичи факат АКТ Идя банкни куролли боскинчиликдан келган зарарнинг уртача статистик зараридан 6-7 марта катта.

Банк хизмати ва молия амаллари сохасидаги турли хил к,аллоблик натижасида йукотишлар 1989 йили 800 млн. доллардан 1997 йили - 100 млрд. долларга етган. Бу курсаткичлар усаяпти, аслида юк,орида келтирилган маълумотлардан бир тартибга ошиши мумкин. Чунки куп йукртишлар аникланмайди ёки эълон к,илинмайди. Узига хос *"индамаслик сиёсати"яи* тизим маъмурларининг узининг тармогидан рухсатсиз фойдаланганлик тафсилотини, бу нохуш ходисанинг такрорланишидан куркиб ва узининг х,имоя усулини ошкор этмаслик важида мухркама этишни хохламасликлари билан тушуниш мумкин.

Компьютер ишлатиладиган инсон фаолиятининг бошка сох,аларида хам вазият яхши эмас. Йилдан-йилга хукукни мух,офаза к,илувчи органларига компьютер жиноятчилиги хусусидаги мурожаатлар ошиб бормокда.

Б арча мутахассислар вирусларнинг тарк,алиши билан бир каторда ташк,и хужумларнинг кескин ошганлигини эътироф этмокдалар. Куриниб турибдики, компьютер жиноятчилиги натижасида зарар катъий ортмокда. Аммо компьютер жиноятчилиги купинча "виртуал" к,аллоблар томонидан амалга оширилади дейиш х,ак,ик,атга тугри келмайди. Хрзирча компьютер тармокдарига сук,илиб кириш хавфи хар бири узининг усулига эга булган хакерлар, кракерлар ва компьютер карокчилари томонидан келмокда.

Хакерлар, бошка компьютер карокчиларидан фаркди х,олда, баъзида, олдиндан, мактаниш мак,садида компьютер эгаларига уларнинг тизимига ки-

риш ниятлари борлигини билдириб куядилар. Муваффакиятлари хусусида Internet сайтларида хабар берадилар. Бунда хакер мусобак,алашув ниятида кирган компьютерларига зарар етказмайди.

Кракерлар (cracker) - электрон "угрилар" манфаат максадида дастурларни бузишга ихтисослашганлар. Бунинг учун улар Internet тармоги буйича таркатилувчи бузишнинг тайёр дастурларидан фойдаланадилар.

Компьютер карокчилари - ракрбат килувчи фирмалар ва хатто ажнабий махсус хизматлари буюртмаси буйича ахборотни угирловчи фирма ва компанияларнинг юкрри малакали мутахассислари. Ундан ташкари улар бегона банк счетидан пул маблагларини угирлаш билан хам шугулланадилар.

Баъзи "мутахассислар" жиддий гурух, ташкил киладилар, чунки бундай криминал бизнес ута даромадлидир. Бу эса тез орада, "виртуал" жиноятнинг зарари жиноят бизнесининг анъанавий хилидаги зарардан бир тартибга (агар куп булмаса) ошишига сабаб булади. Хрзирча бундай тахдидни бетарафлаштиришнинг самарали усуллари мавжуд эмас.

1.4. Тармовдаги ахборотга буладиган намунавий хужумлар

Б арча хужумлар Internet ишлаши принципларининг кандайдир чегараланган сонига асосланганлиги сабабли масофадан буладиган намунавий хужумларни ажратиш ва уларга к,арши кандайдир комплекс чораларни тавсия этиш мумкин. Бу чоралар, х,ак,ик,атан, тармок, хавфсизлигини таъминлайди.

Internet протоколларининг мукаммал эмаслиги сабабали тармокдаги ахборотга масофадан буладиган асосий намунавий хужумлар куйидагилар:

- тармок, трафигини тахлиллаш;
- тармокнинг ёлгон обьектини киритиш;
- ёлгон маршрутни киритиш;
- хизмат килишдан воз кечишга ундайдиган хужумлар.

Тармок трафигини тахлиллаш. Сервердан Internet тармоги базавий протоколлари FTP (File Transfer Protocol) ва TELNET (Виртуал терминал протоколи) буйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини утиши лозим. Фойдаланувчини идентификациялашда ахборот сифатида унинг идентификатори (исми)

ишлатилса, ау-тентификациялаш учун *порол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдалувчиларнинг пароли ва идентификатори тармок, оркали очик,, шифрланмаган куринишда узатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

Ахборот алмашинувида InternetHHHr масофадаги иккита узели алмашинув ахборотини *пакетларга* булишади. Пакетлар алока каналлари оркали узатилади ва шу пайтда ушлаб крлиниши мумкин.

FTP ва TELNET протоколларининг тахлили курсатадики, TELNET паролни символларга ажратади ва паролнинг хар бир символини мое пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бутунлайича битта пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг махсус сканер-дастурлари ёрдамида фойдаланувчининг исми ва пароли булган пакетни ажратиб олиш мумкин. Худди шу сабабли, хрзирда оммавий туе олган ICQ дастури хам ишончли эмас. ICQHHHr протоколлари ва ахборотларни саклаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб крлиниши ва очилиши мумкин.

Асосий муаммо алмашинув протоколида. Базавий татбикий проколларнинг TCP/IP оиласи анча олдин (60 йилларнинг охири ва 80-йилларнинг боши) ишлаб чик,илган ва ундан бери умуман узгартирилмаган. Утган давр мобайнида таксимланган тармок, хавфеизлигини таъминлашга ёндашиш жиддий узгарди. Тармок, уланишларини химоялашта ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чикилди. Аммо бу протоколлар эскиларининг урнини олмади (SSL бундан истисно) ва стандарт макрмига эга булмади. Бу протоколларининг стандарт булиши учун эса тармокдан фойдаланувчиларнинг барчаси уларга утишлари лозим. Аммо, Internetfla тармокни марказлашган бошкариш булмаганлиги сабабли бу жараён яна куп йиллар давом этиши мумкин.

Тармоцнинг ёлгон объектини киритиш. Хар кандай таксимланган тармокда к,идириш ва адреслаш каби "нозик жойлари" мавжуд. Ушбу жараёнлар кечишида тармок,нинг ёлгон объектини (одатда бу ёлгон хост) киритиш имконияти тугилади. Ёлгон обьектнинг киритилиши натижасида адре-сатга узатмокчи булган барча ахборот аслида нияти бузук, одамга

тегади. Тахминан буни тизимингизга, одатда электрон почтани жунатишда фойда-ланадиган провайдерингиз сервери адреси ёрдамида киришга кимдир удда-сидан чикдани каби тасаввур этиш мумкин. Бу хрлда нияти бузук, одам ун-чалик кийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса хатто ундан шубхаланмасдан узингиз барча электрон почтангизни жунатган б улар эдингиз.

Кдндайдир хостга мурожаат этилганида адресларни махсус узгартиришлар амалга оширилади (IP-адресдан тармок, адаптери ёки мар-шрутизаторининг физик адреси аникланади). Internets бу муаммони ечиш-да ARP(Adress Resolution Protocol) протоколидан фойдаланилади. Бу куйидагича амалга оширилади: тармок, ресурсларига биринчи мурожаат этилганида хост кенг куламли ARP-суровни жунатади. Бу суровни тармокнинг берилган сегментидаги барча станциялар кабул килади. Суровни кабул килиб, хост суров юборган хост хусусидаги ахборотни узининг ARP-жадвалига киритади, сунгра унга у^{зининг} Ethernet-адреси булган ARP-жавобни жунатади. Агар бу сегментда бундай хост булмаса, тармокнинг бошк,а сегментларига мурожаатга имкон берувчи маршрутиза-торга мурожаат к,илинади. Агар фойдаланувчи ва нияти бузук, одам бир сегментда булса, ARP-суровни ушлаб крлиш ва ёлгон ARP-жавобни йуллаш мумкин булади. Бу усулнинг таъсири факат битта сегмент билан чегараланганлиги тасалли сифатида хизмат килиши мумкин.

ARP билан булган холга ухшаб DNS-суровни ушлаб к,олиш йули билан Internet тармогига ёлгон DNS-серверни киритиш мумкин.

Бу куйидаги алгоритм буйича амалга оширилади:

1. DNS-суровни кутиш.
2. Олинган суровдан керакли маълумотни чик,ариб олиш ва тармок, буйича суров юборган хостга ёлгон DNS-жавобни хакикий DNS-сервер номидан узатиш. Бу жавобда ёлгон DNS-сервернинг IP-адреси курсатилган булади.

3. Хостдан пакет олинганида пакетнинг IP-сарлавхасидаги 1P-адресни ёлгон DNS сервернинг IP-адресига узгартириш ва пакетни серверга узатиш (яъни ёлгон DNS-сервер узининг номидан сервер билан иш олиб боради).
4. Сервердан пакетни олишда пакетнинг IP-сарлавхасидаги IP-адресни ёлгон DNS-сервернинг IP-адресига узгартириш ва пакетни хостга узатиш (ёлгон DNS серверни хост хакикий хисоблайди).

Ёлгон маршрутни киритиш. Маълумки, замонавий глобал тармокдари бир-бири билан *тармоц узеллари* ёрдамида уланган тармок, сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан кабул килувчига узатишга хизмат килувчи тармок, узелларининг кет-макетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошкарувчи махсус протоколлар мавжуд. Internetflara бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи - ICMP (Internet Control Message Protocol) ва маршрутизаторларни масофадан бошкариш протоколи SNMP (Simple Network Manegment Protocol) мисол булаолади. Маршрутни узгартириш хужум килувчи ёлгон хостни киритишдан булак нарса эмас. Хатто охирги объект хакикий булса, хам маршрутни ахборот барибир ёлгон хостдан утадиган килиб к,уриш мумкин.

Маршрутни узгартириш учун хужум килувчи тармоккд тармок,ни бошк,арувчи к,урилмалар (масалан, маршрутизаторлар) номидан берилган тармок,ни бошкарувчи протоколлар орк,али аникданган махсус хизматчи хабарларни жунатиши лозим. Маршрутни муваффакиятли узгартириш натижасида хужум килувчи таксимланган тармокдаги иккита объект алмашадиган ахборот ок,имидан тула назоратга эга булади, сунгра ахборотни ушлаб крлиши, тахлиллаши, модификациялаши ёки оддийгина йук,отиши мумкин. Бошк,ача айтганда тахдидларнинг барча турларини амалга ошириш имконияти тугилади.

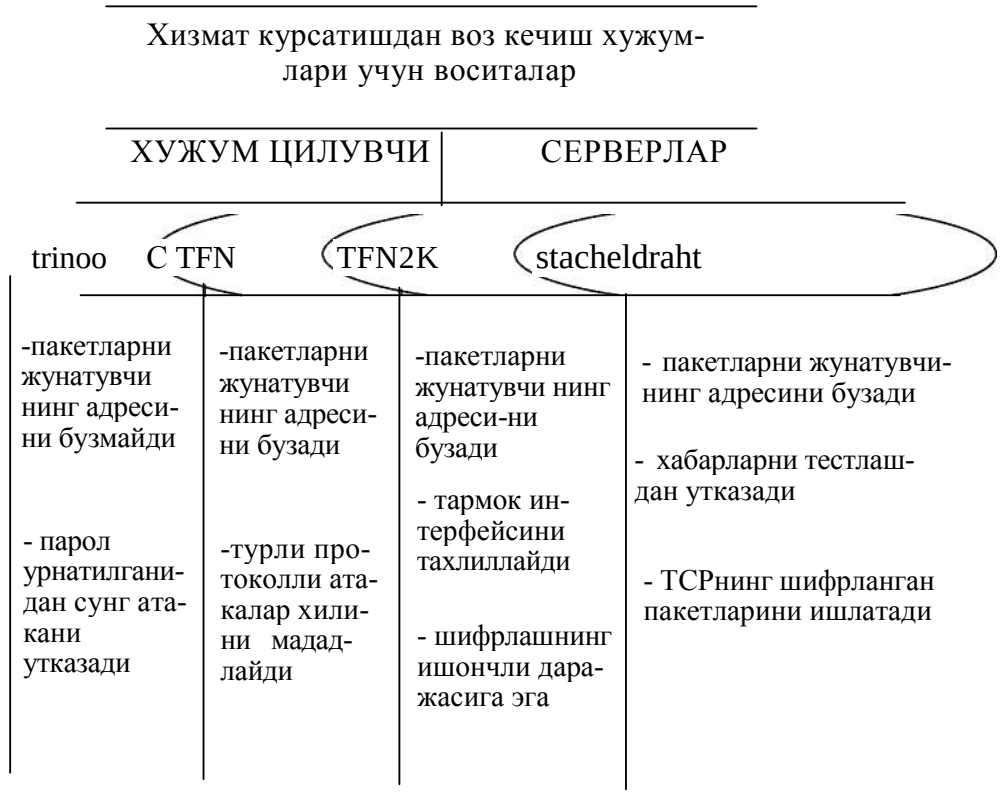
Хизмат килишдан воз кечишга ундайдиган таксимланган хужумлар - DdoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили булсада, к,урк,инчли тезлик билан таркалмокда. Бу хужумларнинг узи анчагина ёкимсиз булгани етмаганидек, улар бир вактнинг узида масофадан бошкарилувчи юзлаб хужум килувчи серверлар

томонидан бошланиши мумкин.

Хакерлар томонидан ташкил этилган узелларда DDoS хужумлар учун учта инструментал воситани топиш мумкин: trinoo, Tribe FloodNet (TFN) ва TFN2K. Якинда TFN ва trinooHHHr энг ёкимсиз сифатларини уйгунлаштирган яна биттаси stacheldraht ("тикон симлар") пайдо булди.

1.2-расмда хизмат килишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари келтирилган.

Хизмат килишдан воз кечишга ундайдиган оддий тармок, хужумида хакер танлаган тизимига пакетларни жунатувчи инструментидан фойдаланади. Бу пакетлар нишон тизимининг тулиб тошиши ва бузилишига сабаб булиши керак. Купинча бундай пакетларни жунатувчилар адреси бузиб курсатилади. Шу сабабли хужумнинг хакикий манбасини аникдаш жуда кийин.



1.2-расм. Хизмат килишдан воз кечишга ундапдиган хужум воситаларининг характер истикалар и

DDoS хужумларини ташкил этиш битта хакернинг кулидан келади, аммо бундай хужумнинг эффекти *агентлар* деб аталувчи хужум килувчи

серверларнинг ишлатшшши хдсобига анчагина кучаяди. TFNfla *серверлар* (server), а йпоода *демонлар* (daemon) деб аталувчи бу агентлар хакер томонидан масофадан бошкарилади.

1.5. Ахборот хавфсизлигини бузувчининг модели

Булиши мумкин булган тахдидларни олдини олиш учун нафакат операцион тизимларни, дастурий таъминотни химоялаш ва фойдаланишни назорат килиш, балки бузувчилар туркумини ва улар фойдаланадиган усулларни аникдаш лозим.

Сабаблар, максаддар ва усулларга боглик, хрлда ахборот хавфсизлигини бузувчиларни туртта категорияга ажратиш мумкин:

- саргузашт кддирувчилар;
- гоявий хакерлар;
- хакерлар-профессионаллар;
- ишончсиз ходимлар.

Саргузашт кидирувчи, одатда, ёш, купинча талаба ёки юкрри синф укувчиси ва унда уйлаб килинган хужум режаси камдан-кам булади. У нишонини тасодифан танлайди, к,ийинчиликларга дуч келса чекинади. Хавфсизлик тизимида нуксонли жойни топиб, у махфий ахборотни йигишга тиришади, аммо х,еч качон уни яширинча узгартиришга уринмайди. Бундай саргузашт к,идирувчи муваффак,иятларини факат якин дустлари-касбдошлари билан уртокдашади.

¥ояли хакер - бу хам саргузашт кидурувчи, аммо мохиррок,. У узининг эътик,оди асосида муайян нишонларни (хостлар ва ресурсларни) танлайди. Унинг яхши курган хужум тури Web-сервернинг ахборотини узгартириши ёки, жуда кам хрлларда, хужум килинувчи ресурслар ишини блокировка килиш. Саргузашт кидирувчиларга нисбатан гояли хакерлар муваффак,иятларини кенгрок аудиторияда, одатда ахборотни хакер Web-узелда ёки Usenet анжуманида жойлаштирилган х,олда эълон киладилар.

Хакер-проффесионал х,аракатларнинг аник, режасига эга ва маълум ресурсларни мулжаллайди. Унинг хужумлари яхши уйланган ва одатда бир

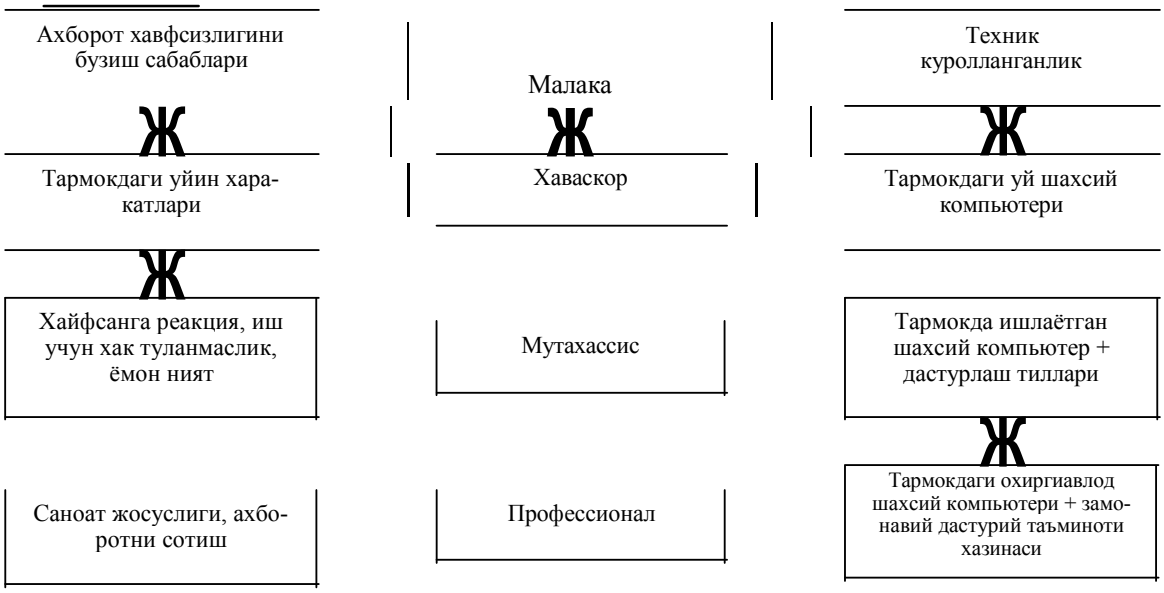
неча боскичда амалга оширилади. Аввал у дастлабки ахборотни йигади (операцион тизим тури, такдим этиладиган сервислар ва кулланиладиган химоя чоралари). Су игра у йигилган маълумотларни хисобга олган хрлда хужум режасини тузади ва мое инструментларни танлайди (ёки хатто ишлаб чикади). Кейин, хужумни амалга ошириб, махфий ахборотни олади ва нихрят харакатларининг барча изларини йук, килади. Бундай хужум килувчи профессионал, одатда яхши молияланади ва якка ёки профессионаллар командасида ишлаши мумкин.

Ишончсиз ходим узининг харакатлари билан саноат жосуси етказадиган муаммога тенг (ундан хам куп булиши мумкин) муаммони тугдиради. Бунинг устига унинг борлигини аниклаш мураккаброк,. Ундан ташкари унга тармокнинг ташки химоясини эмас, балки факат, одатда унчалик катьий булмаган тармокнинг ички химоясини бартараф килишига тугри келади. Аммо, бу хрлда унинг корпоратив маълумотлардан рухсатсиз фойдаланиши хавфи бошка х,ар к,андай нияти бузук, одамникидан юк,ори булади.

Юк,орида келтирилган ахборот хавфеизлигини бузувчилар категорияларини улар ни малакалари буйича гурухдаш мумкин: хаваскор (саргузашт к,идирувчи), мутахассис (гояли хакер, ишончсиз ходим), профессионал (хакер-профессионал). Агар бу гурухдар билан хавфеизликнинг бузилиши са-баблари ва хар бир гурух,нинг техник к,уролланганлиги такдосланса, ахборот хавфеизлигини бузувчининг умумлаштирилган моделини олиш мумкин (1.3-раем).

Ахборот хавфеизлигини бузувчи, одатда маълум малакали мутахассис булган х,олда компьютер тизимлари ва тармоклари хусусан, уларни химоялаш воситалари хусусида барча нарсаларни билишга уринади. Шу сабабли бузувчи модели куйидагиларни аниклайди:

- бузувчи булиши мумкин булган шахслар категорияси;
- бузувчининг булиши мумкин булган нишонлари ва уларнинг мухимлик ва хавфеизлик даражаси буйича рутбаланиши;
- унинг малакаси хусусидаги тахминлар; унинг техник куролланганлигининг бахоси;
- унинг харакат х,арактери буйича чеклашлар ва тахминлар.



1.3-расм. Ахборот хавфсизлигини бузувчининг модели

Тизимдан рухсатсиз фойдаланишга мажбур этиш сабабларининг диапазони етарлича кенг: компьютер билан уйнаганидаги хаяжон кутаринкилигидан то жирканч менеджер устидан хокимлик хиссиётигача. Бу билан нафакат кунгил очишни хохловчи хаваскорлар, балки профессионал дастурчилар хам шугулланади. Улар паролни танлаш, фараз килиш натижасида ёки бошка хакерлар билан алмашиш йули оркали кулга киритадилар. Уларнинг бир кисми нафакат файлларни куриб чик,ади, балки файлларнинг мазмуни билан к,изик,а бошлайди. Бу жиддий тахдид х,исобланади, чунки бу хрлда беозор шухликни ёмон ният билан килинган х,аракатдан ажратиш кийин булади.

Як,ин вактгача рахбарлардан норози хизматчиларнинг уз мавк,еларини суиистеъмол килган х,олда тизимни бузишлари, ундан бегоналарнинг фойдаланишларига йул куйишлари ёки тизимни иш х,олатида каровсиз к,олдиришлари ташвишлантирар эди. Бундай харакатларга мажбур этиш сабаблари куйидагилар:

- хайфсанга ёки рах,бар томонидан танбех,га реакция;
- иш вактидан ташк,ари бажарилган ишга фирма хак, туламаганидан норозилик;

- фирмани кандайдир янги тузилаётган фирмага ракиб сифатида заифлаштириш максадида касос олиш каби ёмон ният.

Рахбардан норози ходим жамоа фойдаланувчи хисоблаш тизимларига энг катта тахдидлардан бирини тугдиради. Шунинг учун хам хакерлар билан курашиш агентлиги индивидуал компьютер сохибларига жон деб хизмат курсатадилар.

Профессионал хакерлар-хисоблаш техникасини ва алока тизимини жуда яхши биладиган компьютер фанатлари (мутаассиблари) хисобланади. Тизимга кириш учун профессионаллар омадга ва фаразга таянмайдилар ва кандайдир тартибни ва тажрибани ишлатадилар. Уларнинг максади-химояни аникдаш ва йукртиш, хисоблаш курилмасининг имкониятларини ургапиш ва максадига эришиш мумкинлиги тугрисида карорга келиш.

Бундай профессионал хакерлар категориясига куйидаги шахслар киради:

- сиёсий максадни кузловчи жиноий гурухдарга кирувчилар;
- саноат жосуслик максадларида ахборотни олишга уринувчилар;
- текин даромадга интилувчи хакерлар гурухи.

Умуман профессионал хакерлар хавф-хатарни минималлаштиришга уринадилар. Бунинг учун улар бирга ишлашга фирмада ишлайдиган ёки фирмадан якинда ишдан бушатилган ходимларни жал б этадилар, чунки бегона учун банк тизимига киришда ошкор булиш хавфи жуда катта. Хакикатан, банк хисоблаш тизимларининг мураккаблиги ва юкрри тезкорлиги, хужжатларни юргизиш ва текшириш усулларининг мунтазам такомиллаштирилиши бегона шахе учун хабарларни ушлаб колиш ёки маълумотларни угирлаш мак,садида тизимга урнашишига имкон бермайди. Профессионал хакерлар учун яна бир кушимча хавотир-тизимдаги бир компонентнинг узгариши бошк,а бир компонентнинг бузилишига олиб келиши ва хатардан дарак берувчи сигналга сабаб булиши мумкин.

Хакерлар хавф-хатарни камайтириш максадида одатда молиявий ва оилавий муаммоларга эга булган ходимлар билан контактга кирадилар. Купгина одамлар х,аётида хакерлар билан тукнашмасликлари мумкин, аммо алкаголга ёки к,иморга ружу к,уйган ходимлар билмасдан жиноий гурух, би-

лан богаанган кдндайдир бир букмекердан кдрздор булиб к,олишлари мумкин. Бундай ходим кдндайдир уйин-кулги кечасида сухбатдошининг профессионал агент эканлигига шубха к,илмаган х,олда ортик,ча гапириб юбориши мумкин.

II боб. ЭЛЕКТРОН БИЗНЕС ВА УНИНГ ХАВФСИЗЛИГИ МУАММОЛАРИ

2.1 Internet нинг асосий ахборот хизматлари

Internet тармога коммуникациянинг ва ахборотдан фойдаланишнинг турли-туман усулларини таклиф этади. Шу сабабли у тезликда купгина компаниялар ахборот тизимларининг ажралмас кисми булиб крлди- Internet тармоги хар кандай абонентлар учун маълумотларни транзит узатиш буйича транспорт хизматларидан ташкари юкрри савияли тармок, сервисларининг (хизматларининг) етарли даражада кенг тупламини хам таъминлайди. Бу хизматларни такдим этувчи компьютерлар серверлар деб аталса бу хизматлардан фойдаланувчи компьютерлар мижозлар деб аталади. Бу атамалар компьютер - сервер ва компьютер-мижозларда ишлатиладиган дастурий таъминотга хам тааллукли.

Куйида оммавий Internet сервисларини кискача куриб чикамиз.

World Wide Web (WWW) Internet даги энг кенг таркалган, оммавий сервис хисобланади. Internet ухшаб WWW сервисининг хам эгаси йук,, аммо хар бир WWW серверга ахборотни жойлаштиришга жавобгар одамлар ёки ташкилотлар хамда дастурлар ва асбоб-ускуналарнинг ишлашини таъминловчи сервер маъмурлари мавжуд.

WWW сервиси Internet даги гиперматнли хужжатларни таркатиш учун фойдаланади. *Гипематн* — белги сузлари (командалари) урнатилган матн булиб, бу белги сузлари оркали бу матннинг бошка жойига, бошк,а хужжатларга, расмларга х,авола килинади. Гиперматнли х,авола хужжати фойдаланувчига бошк,а хужжатлардаги ахборотга осонгина утиш имконини беради.

Фойдаланувчи гиперматнни укиётганида матндаги ёритилган (ажратилган) сузни куради. Бу сузга курсорни тугрилаб сичк,онча тугмачаси босилса, экранда бу суз х,авола к,илган, масалан, бу матннинг

бошка параграфи пайдо булади. WWW да таянч сузлар буйича бошка хужжатнинг бутунлай бошка матнига тушиб крлиш, кандайдир дастурга кириш, маълум харакатларни бажариш мумкин.

Шундай килиб, фойдаланувчилар хужжат матнидаги ажратилган сузлар, тасвирлар ва график элементларини танлаб, исталган йуналишда кучишлари ва очик-ойдин узларини кизиктирган хужжатларга сакраб утишлари мумкин (хужжатнинг каерда жойлашишидан катьий назар).

World Wide Web даги ахборотдан фойдаланишда мижоз компьютерларида *браузер* (browser) деб аталувчи махсус дастурий таъминот ишлатилади. Бу илова фойдаланувчига асосан World Wide Web серверлари тавсия этган Internet нинг турли-туман маълумотлари буйича кучишига имкон беради. Хозирда Microsoft Internet Explorer ва Netscape Navigator браузерлари оммавий туе олган.

Гиперматнли файллар махсус *гиперматнни белгиловчи тил* HTML (Hyper Text Mark-up Language) ёрдамида ёзилади. Таъкидлаш лозимки, тасвирлар ва бошка номатн ташкил этувчилари хужжат матнига жойлаштирилмайди, балки алохида сакланади. Бунинг урнига хужжат матнига зарур ташкил этувчи файл номини курсатувчи хавола жойлаштирилади. 1998 йили хужжатнинг маъноли мазмунини хам таъсифловчи *белгилашнинг кенгайтирилган тили* стандарти XML (Extended Mark-up Language) кабул килинди. Замонавий браузерлар хужжатларни XML ва HTML форматларида укийди.

Гиперматнлар мухарририга эга булиб, ишчи мухитнинг исталган тузилмасини, шу жумладан хужжатларни, файлларни, маълумотларни, тасвирларни, дастурий таъминотни ва х,. яратиш мумкин ва бу янги дастурий таъминот эмас, балки оддий гиперматн булади. WWW сервиси ахборотни йигиш, таркатиш ва урганиш жихатидан чегараланмаган имкониятга эга. Улар таъминлайдиган график воситалар фойдаланувчилар ва компаниялар орасида борган сари шухрат крзоняпти.

Хар к,андай компания Internetra бир ёки бир нечта серверни улаб узининг Web-узелини яратиши мумкин. Бундай компаниялар хужжатларини World Wide Web га жойлаштириш имкониятига эга буладилар ва бу хужжатлардан браузери булган хар к,андай Internet фойдаланувчиси фойдаланиши мумкин. World Wide Web тавсия этадиган маркетинг

имкониятларидан фойдаланишга бошлаган компаниялар бу хизматнинг реклама ва махсулотни сотишда гоят катта афзалликларга эга эканлигини тушуна бошлайдилар.

WWW сервиси фойдаланувчига нафакат статик мазмунли хужжатларни курсатишга крдир. HTML-хужжатларда фойдаланувчи тулдирадиган ва серверга кайтариладиган шакллар булиши мумкин. Шакл тулдирилишида фойдаланувчи такдим этилган муълумотларга боглик, хрлда сервер динамик тарзда "дархрл" жавоб хужжатини шакллантиради ва кандайдир кушимча харакатларни бажаради масалан, кредит варакасидан пулни олади, авиачиптани брон килади, ёки хабарни фойдаланувчи курсатган пейджерга юборади. Тавсиф этилган технология асосида купгина Internet-магазинлар маълумот берадиган хизматлар, талабнома берадиган тизимлар ва х,. яратилади.

WWW, браузерлар ва бу хизматда ишлатилувчи "мижоз-сервер" моделининг пайдо булиши билан татбикий дастур яратувчилари универсал интерфейс ва тармок, технологияларига эга булдилар.

Энди ахборот тизимини яратиш учун керакли шаклларни ёзиш ва бу шаклларни фойдаланувчилар томонидан тулдирилишига сервер реакциясини дастурлаштириш талаб этилади. Мижоз компьютерида фак,ат WWW - браузер ишлатилади, яъни тизим билан ишлашда хеч к,андай к,ушимча дастурий таъминот урнатилиши талаб этилмайди. Бундай тизим *Web-интерфейсли* тизим деб аталади. Шаклларни ишлашга кушимча х,олда WWW браузерга сервердан дастурни юклаш ва уни фойдаланувчи компьютерида бажариш имконини беради. Бундай дастурлар Java ва Java Script тилларида ёзилади ва Web-интерфейсни бойитади. Аммо бундай дастурларнинг бажарилиши сезиларли х,исоблаш ресурсларини талаб этиши мумкин ва доимо хавфсизлик нуктаи назаридан бенук,сон булавермайди.

Доменли исмлар сервиси DNS. Internet даги хар бир компьютер, у билан тармокдаги бошк,а компьютернинг уланишига имкон берувчи узининг шахсий ягона адресига эга булиши шарт. Internet даги компьютер адреслар (улар IP-адреслар деб юритишади) икки хил ёзув шаклига эга: ракамли адрес ва доменли исм. Доменли исмлар сервиси DNS бошка сервислар томо-

нидан компьютернинг доменли исмини ракамли IP адресга трансляцияси учун ишлатилади.

Рщамли IP-адрес компьютернинг 32 битли идентификатори булиб, хар бири 8 битдан иборат 4 октетга булинади. Хар бир октет унли санок, системасида ёзилиб, октетлар киймати нукталар оркали ажратилади. Ракамли IP-адресга мисол 184.94.125.53 адреснинг ракамли шакли компьютерларда ва тармок, хизматининг махсус асбоб-ускуналарида ишлатилади. Одамлар учун ракамли адрес нокулай, эсда крлиши кийин ва кам маъноли ахборотни элтади.

Одамлар одатда *доменли адреслардан* фойдаланишади, бунинг устига хар бир доменли исм, ракамли IP-адрес каби Internet даги факат битта компьютерни аниклайди. Доменли исм нукталар билан ажратилган бир неча суз ёки кискартиришлардан иборат, масалан dot.msk.ru. Доменли исм компьютер макони хусусидаги фойдали ахборотни элтади. Исмнинг четки унг кисми юкрри сатх, доменини, яъни ушбу компьютер жойлашган компьютерларнинг катта гурухини билдиради. Бизнинг мисолда бу ru-Russia, Россия сузининг к,иск,артирилгани. Бу юкрри сатх домени Россияда Internet га уланган компьютерларни бирлаштиради. ш доменининг ичида к,исм доменлар кичикрок, у[лчамли] минтак,а бор, масалан msk.ru(Москва). Доменли исмнинг четки чап кисми кием доменининг ичидаги компьютер исмини билдиради (dot).

Доменли исм хар доим хам уч киемдан иборат булмайди. Аммо, хар кандай хрлда четки унг кием юкрри сатх, доменини, четки чап кисми, компьютернинг уз исмини, крлганлари, унгдан чапга-бири иккинчисига солинган ва х,ар бир кейингиси олдингисининг к,исми булган к,исм доменларни билдиради.

Юк,ори сатх, доменлари икки хил булади. Биринси мамлакат номининг икки х,арфли к,иск,артирилишидан иборат, масалан ru-Россия (Russia), fr-Франция (France), uz-Узбекистон (Uzbekistan) ва х,. Барча кискартиришлар стандарт х,исобланади ва Халкаро стандартлаштириш ташкилоти (ISO) томонидан аникданган. Иккинчи хил юк,ори сатх, доменлари-умумий доменлар - "машгулот тури" буйича уч х,арфли белгига эга.

2.1-жадвалда юкрри сатх умумий доменларининг таркалган белгиланиш руйхати келтирилган.

2.1-жадвал

Доменнинг белгиси	Ташкилот тури
com	Тижорат ташкилотлари (масалан. www.ibm.com)
edu	Олий VKVB юртлари тармоги (масалан. strawb.mit.edu)
gov	Х,укумат ташкилотлари (масалан. whitehouse.sov)
org	Бошка организациялар (масалан. isoc.org)
net	Тармок, ишлашга тааллукди Internet провайдерлари ва бошка ташкилотлар. (масалан, Uznet.net)
int	Х,алкаро ташкилотлар. масалан www.nato.int

Домен исмини ракамли IP-адресга узгартириш Internet нинг махсус сервери ёрдамида амалга оширилади. Бу сервер доменли нем тизими (Domain Name System) деб аталади. Бундай узгартирувчиларни бажарувчи компьютерлар DNS-серверлар деб аталади. Хдр бир доменда унга хизмат килувчи DNS-сервер мавжуд.

Файл архивларидан фойдаланиш. Internet да купгина серверлар файл архивларидан ошкора фойдаланишга таклиф этади. Архив тематик каталогларнинг оддий дарахти булиб, каталогларда асосан дастурий таъминотнинг, хужжатларнинг, китоблар матнининг ва х,. зичлаштирилган файллари сакданади. Файлли архифлардан турли платформа ва операцион тизимлар учун дастурий таъминотни топиш мумкин. Сервердан файлларни фойдаланувчи Компьютерра жунатиш FTP протоколи (File Transfer Protocol) ёрдамида амалга оширилади.

Аксарият мижоз дастурий воситаларига компьютерлар учун FTP билан ишлаш учун махсус дастурлар киритилган, масалан Windows операцион тизими томонидан таъминланадиган ftp.exe дастури. Бу дастур протоколнинг барча имкониятларини, жумладан парол буйича фойдаланишни ва масофадаги компьютер файллари билан ишлаш буйича амалларнинг тулик, тупламини амалга оширади. Одатда ошкора архивлардан оддий фойдаланувчиси учун архивдан аноним фойдаланиш ва у ёки бу файлни уз компьютерига узатиш имкониятига эга булиши етарли.

Хдр кандай WWW-браузер ошкора FTP архивлардан аноним фойдаланиш учун кулай ва тушунарли интерфейсга эга.

FTP-сервер билан богланиш урнатилганидан сунг браузер дарчасида файл тизимининг каталоглар ва файллар куринишидаги оддий тасвири пайдо булади. Каталогга сичкрнча тугмачасининг босилиши ушбу каталогга утишга, файлга сичкрнча тугмачасининг босилиши эса файлнинг фойдаланувчи компьютерига юкланишига олиб келади.

Электрон почта - компьютер тармокларида амалга оширилган хизматнинг дастлабки сервисларидан бири булиб, фойдаланувчиларга электрон хабарларни юбориш ва кабул килиш имкониятини беради.

Фойдаланувчи электрон почта оркали хабарларни юбориши, уларни узининг электрон почта кутисида олиши, мухбирлари хатига уларнинг адреслари буйича автоматик тарзда жавоб бериши, хатининг нусхаларини бирданига бир неча кабул килувчиларга таркатиши, олинган хатни бошка адресга жунатиши, турли хат-хабарлар учун почта кутисининг бир неча булимларини тузиши, хатга матнли файлларни киритиши ва х. мумкин.

Электрон почта корпоратив интра-тармокда жуда маъсулиятли вазифани бажаради. У ходимлар уртасидаги алок,анинг уз вактидалигини таъминлайди ва хизмат муолажаларини тезлаштиради. Электрон почтанинг хабарларга файлларнинг киритиши имконияти, ходимларга хар кандай ахборотни - оддий хисоботдан то янгиланган дастурий таъминот ва тулак,онли мультимедиа такдимотини тарк,атишига имкон беради.

Купгина компаниялар узларнинг электрон почта тизимларини Internetra тарк,атиш орк,али кенгайтирадилар. Глобал электрон к,ути компаниянинг географик таркрк, булимлари ва филиалларини бир-бири билан боглаб, уларнинг ходимларига марказий офис хизматлари билан осонгига ахборот алмашиш имконини беради.

Электрон почтани компанияни унинг мобил фойдаланувчилари билан алокасини ташкил этишда к,уллаш кулай хисобланади. Компания бутун мамлакат буйича тармокга кириш нукталарини таъминловчи Internet хизмати провайдерларининг такдим килганларидан х,ам фойдаланиши мумкин.

Электрон почта буюртмачилар ва таъминловчилар алокаси самарадорлигини оширади. Хабарлар ва хужжатларнинг электрон форматда узатилиши кушимча афзаллик тугдиради, яъни кабул килувчи бундай маълумотларни осонгина узгартириши ва исталган максадда ишлатиши мумкин.

Internetfla электрон почта билан ишлаш учун TCP/IPra асосланган SMTP, POP ёки IMAP тадбикий протоколлар ишлатилади.

Почтани узатувчи оддий протокол SMTP (Simple Mail Transfer Protocol) Internet почта серверлари уртасида хабарлар узатишни бажаради. SMTP хабар нусхаларини турли адреслар буйича узатиш учун купайтиришга ва шу тарика таркатиш руйхатини шакллантиришга имкон беради. Почта сервери маълум доменли исмга юборилаётган барча хабарларнинг кабул килинишига жавобгардир. Хар бир фойдаланувчи (почта кугиси) учун серверда махсус файл ажратилади ва бу файлга келадиган хабарларни, качон фойдаланувчи уларни олиш учун сервер билан богланишини кутган хрлда, жойлаштирилади.

Сервер адресатларига унинг фойдаланувчиларидан келган хабарларни хам таркатади. Олдиндан у DNS' хизматидан кайси сервер адресатнинг доменли исмига жавобгар эканлигини аниклайди, сунгра бу сервер билан SMTP протоколи буйича алока урнатади.

POP почта протоколи (Post Office Protocol) фойдаланувчига унга келган электрон хабарлардан фойдаланишга, яъни фойдаланувчи компьютери ва фойдаланувчи почта кутиси руйхатга олинган почта сервери билан алока урнатилишига имкон беради. Техника нуктаи назаридан фойдаланувчи почтани олиш учун кайси компьютердан узининг сервери билан богланиши ва бу компьютер сервердан кандай узок, масофада жойлашганлиги ах,амиятли эмас. Фак,ат, фойдаланувчи компьютери Internetra уланган ва унда POP протоколини таъминловчи почта дастури урнатилган булиши лозим.

Фойдаланувчининг почта серверидан фойдаланишида *ШАР протоколи* хам ишлатилади. Бу протокол мураккаброк, булиб, фойдаланувчига почтани бевосита серверда каталоглашга ва саклашта имкон беради.

Замонавий электрон почта нафакат хабарларни, балки хабарга кушилган ихтиёрий мазмунли ва форматли бир неча файлларни (attachments) узатиш крбилиятига эга. Бундай хатлар SMTP ва POP-3 протоколлари ёрдамида одатдагидек кабул килинади, почта серверларида ишланади ва Internet оркали узатилади.

Шуни эсдан чикармаслик лозимки, электрон почта катта хажмли хабарларни узатишга мулжалланмаган ва купгина серверлар кабул килинувчи ва жунатилувчи хабарлар хажмини мажбуран бир неча мегабайтларга чегаралайди.

Телеанжуманлар ва тарцатиш хизматлари. Телеанжуман хизмати ёки тармок янгиликлари (Usenet news) ошкора (бутун дунё ёки регионал) эълонлар тахтаси булиб, унда хар бир киши хабар жунатиши ва хар бир киши бошкалар жунатган хабарларни укиши мумкин. Бу хабарлар тамомила турли характерга эга ва муайян одамга эмас, балки кенг оммага адресланган. Мохияти буйича, Usenet-жамоа (очик) мунозара клубларидир.

Фойдаланишнинг кулайлигини таъминлаш максадида мавзулар «кизикишлар» буйича алох,ида гурухларга ажратиш кабул килинган ва бу алох,ида гурухлар анжуманлар деб юритилади.

Гурухларга ажратиш иерархик (шажаравий), масалан :

- сотр.languages- умуман дастурлаш тилларига багишланган гурух;
- сотр.languages, c. - С дастурлаш тилига багишланган гурух;
- сотр.languages, c. libraries - С тили библиотекасига багишланган гурух.

Бутун дунё янгиликлар гурухининг жами бир неча мингга тенг ва улар булиши мумкин булган барча натижаларни к,амраб олганлар. Регионал тарк,атилувчи янгиликлар гурухи х,ам мавжуд.

Телеанжуманлар махсус серверлар тармоги буйича тарк,атилиб хар бир сервер тармок, янгиликларини узатувчи протокол NNTP (Network News Transfer Protocol) ёрдамида мижозларнинг маълум бир сонига хизмат курсатади.

Телеанжуман хизматидан фойдаланиш учун фойдаланувчи компьютерига хизмат курсатувчи янгиликлар сервери булиши лозим. Бундай сервер

адресный провайдердан ёки тармок, маъмуридан булиш мумкин. Мижоздастурлар телеанжуманлардан фойдаланиш учун WWW- броузерларига (Netcape) ёки почта дастурларига (MS Outlook Express) интеграциаланган, мустак,ил иловалар хам мавжуд. Махсус почта серверлари томонидан бажариладиган электрон почта буйича таркатиладиган хабарларнинг тематик руйхатлари телеанжуманларга ухшаш. Махсус почта серверларининг энг йириги Россияда-Subseribe.ru. Кдндайдир таркатишта ёзилиш учун ушбу адрес буйича уз браузерини юбориш лозим.

Шундай таркатишлар хам мавжудки, уларга хабарларни факат бошкарувчи жунатиши мумкин ва, мое хрлда, ёзилувчилар факат бошкарувчига жавоб беришлари мумкин. Яна бошка таркатиш тури- «купчиликдан купчиликка» мавжуд, яъни хар кандай ёзилувчи барча руйхатга хабарни жунатиши мумкин.

Internet^a мулещот хизматлари. ICQ хизмати. ICQ (Intelligent Call Query) хизмати номини купинча "I seek you" (Мен сени кидираяпман) сузи билан богаашади. Бу хусусий хизмат хозирда AOL Time Warner (АК.Ш) компаниясига тегишли булиб, 1997 йилнинг бошида пайдо булган ва ун миллионлаб фойдаланувчиларига эга. Бундай хизмат Microsoft (Microsoft Instant Messenger) фирмаси томонидан хам курсатилади. Internet дан фойдаланувчи узининг компьютерига, руйхатдан утишига ва сунгра ушбу хизмат билан ишлашига имкон берувчи, ICQ - мижозни урнатиши мумкин. Руйхатдан утишда фойдаланувчига идентификацион номери берилади ва сунгра у куйидаги хизматлардан фойдалана олади.

- ICQ номерига эга булган InternetflaH фойдаланувчиларга вактнинг реал режимида хабарларни жунатиш (пейджерга ухшаш);

- сухбат куриш мумкин булган ICQ фойдаланувчилари билан чат (chat-ингилизча "сузлаш "маъносини беради);

- бошк,а фойдаланувчига файлларни жунатиш ва бошкалар.

***IRC** хизмати.* IRC (Internet Relay Chat) хизмати купгина одамларнинг вактнинг реал режимида (клавиатурада хабарларни териш йули билан) сухбат куришларига имкон беради.

Умумий чалкашликларни олдини олиш максадида сухбатдошлар мухокаманинг турли мавзуларини таъминловчи каналларга бирлаштирилади. IRC каналларига уланиш учуй *mire* ёки *pirck* каби махсус мижоз-дастур талаб килинади. Каналларнинг барча номлари фунт белгиси «#» билан бошланади. Масалан, #hottub кидириш ва сухбат учуй оммавий канал хисобланади. Баъзи мижоз-дастур л ар бир неча каналга бир вактнинг узида богаанишга имкон беради.

IRC дастури дарчасига киритган кандайдир хабарингиз бирор вактдан сунг каналингизнинг бошка катнашчилари экранида пайдо булади ва худди шундай, сизнинг IRC серверингизга уланган бошка IRC фойдаланувчилари киритган хабар сизнинг экранингизда акслантирилади.

Web-интерфейсли чат серверлар («сузлашув» серверлари) тарк,алди. Чат-серверлар дастурий таъминот урнатилган WWW - серверлар булиб, бу дастурий таъминот бу серверга уланган фойдаланувчиларга оддий браузер ёрдамида бир-бирларига вактнинг реал режимида хабарлар жунатишга имкон беради. Мох,ияти билан бу сервис IRCra ухшайди, аммо ундан фойдаланиш учун оддий браузер булиши кифоя.

Telnet сервиси масофадаги компьютерда дастурни бажаришга мулжалланган. Telnet дастури ёрдами фойдаланувчи бошка компьютерда «дарча» очади: у худди масофадаги компьютер клавиатураси олдида утирганидек командаларни киритиши, цаетурни ишга тушириши ва унинг бажарилиши натижаларини кузатиши мумкин. Бу хизматцан ОС UNIX билан ишлайдиганлар купцан бери фойдаланадилар. Терминал фойдаланиш имконияти энци Windows 2000 операцион тизимининг версиясида хам пайцо булци.

Interne^a ахборотни кидириш. Internet ца, хусусан, WWW ца ахборотни кидирув серверлари ёцрамида амалга оширилаци. Бу серверлар вактивакти билан Internetoarn WWW-хужжатлар мазмунини сканерлаб, у ёки бу ахборотли хужжатларга хаволаларни топишга имкон берувчи маълумотлар базасини тузаци. Россияца энг машхур кидирув серверлари - Яндекс (www.yandex.ru) ва Рамблер (www.rambler.ru), «катта» Interne^a-www.google.com, www.altavista.com ва www.yahoo.com.

Кддирув серверлари билан узаро харакат оддий www- браузер оркали амалга оширилади. Одатда, кидирув сервери икки хил усулни мададлайди: *таянч сузлар буйича ва иерархик (игажара) классификаторы буйича.*

Таянч сузлар буйича кидирувни амалга ошириш учуй фойдаланувчи кидирув сохасини иложи борича аникрок, белгиловчи бир неча сузни ифодалаши лозим. Сунгра, у бу сузларни кидирув сервери такдим этган шаклга киритиб, кидирув тугмачасини босади. Сервер суровни кабул килиб, курсатилган сузлар булган хужжатларни кидириш максадида узининг маълумотлар базасини сканерлайди ва топилган хужжатларга хаволалар руйхатини кайтаради. Одатда, хужжатлар таянч сузлар мухимлигининг пасайиши тартибида сараланган. Хдвола билан бирга хужжат мазмунининг аннотацияси ёки унинг биринчи катори чикарилади. Бу эса фойдаланувчига хужжатнинг керак ёки керак эмаслигини бахрлашга имкон беради. Фойдаланувчи исталган хавола буйича сичкрнча тугмачасини босиб, узини кизиктирган хужжатни бутунлай куриб чик,иши мумкин.

Купгина к,идирув серверлари табиий тилга кушимча ВА, ЁКИ, ЭМАС операторлари булган ва кизиктираётган сузлар орасидаги жоиз масофани курсатадиган суровларнинг расмий мантикий тилини мададлайди.

Иерархик(шажара) классификатори буйича кидирувга асосан исталган натижага етишмагунча, олдин руйхатдаги ахборотнинг катта булишини, сунгра унинг булинмасини ва х,. танлаш амалга оширилади. Хар бир кадамда фойдаланувчи тематикаси берилган булимга мое келувчи хужжатларга илова руйхатини ёки унинг булинмалари руйхатини куриб туради. Масалан:Фан-^Криптография-^Асимметрик криптотизмлар^Рак,амли имзо. У ёки бу кидирув усулини куллаш муайян масала орк,али аникланади.

К,идирувнинг яна бошк,а усулларидан FTP - серверларда архивларни куриб чикиш, телеанжуманлар ва тарк,атишлардан фойдаланилади. Одатда файлли архивлар иерархик (шажара) классификаторларига ухшаб тузилмаланган булади. Энг катта архивлардан бири ftp://ftp.funet.fi/ адреси буйича жойлашган. Тематик телеанжуманлар ва таркатишларга кандайдир тривиал булмаган масалани тушунтирувчи фойдали ахборотни ёки тажрибали мутахассислар тавсиларини топиш мумкин.

2.2. Электрон бизнес ва тижорат моделлари

Электрон бизнесни купинча учинчи минг йилнинг технологияси деб аташади. Internet да электрон бизнеснинг ривожи 1995 йилдан, тармокни хусусий фойдаланувчилар томонидан узлаштира бошлашларидан бошланган. Худди шу йили биринчилардан булган Amazon-Internet магазини очилган.

Баъзида электрон бизнес ва электрон тижорат тушунчаларини аралаштиришади, аммо улар орасида анчагина фарк, бор:

- электрон бизнес (e-business) - фаолият самарадорлигини кутариш максадида компания асосий бизнес жараёнларини Internet-технологиялардан фойдаланиб амалга оширишдир. Бошкача айтганда электрон бизнес - компаниянинг ички ва ташки алокаларини амалга ошириш учун глобал ахборот тармокдаридан фойдаланувчи хизмат фаолиятидир.
- электрон тижорат (e-commerce) электрон бизнеснинг мухим таркибий кисмидир. Электрон тижорат бизнес-фаолиятининг турли шаклларини - чакана ва улгуржи савдо, маркетинг, корхоналар орасидаги битим, иловаларни арендага бери, хизматларни такдим эти шва х,. камраб олади. Бу барча хизмат амаллари электрон шаклда компьютер тармокдари (корпоратив ёки Internet) ёрдамида амалга оширилади. Internet-тижорат электрон тижоратнинг кисми булиб, барча транзакциялар ва битимлар электрон усулда глобал тармок, оркали амалга оширилади.

Янги бозор замонавий ахборот технологияларининг кулланишига асосланган ва истеъмолчи билан оператив (онлайн режимида) алока килинишига мулжалланган. Як,ин орада электрон савдо амаллари хар к,андай бизнеснинг асосий кисми булиб к,олади.

Internet-технологиялардан фойдаланувчи компаниялар рак,ибларига нисбатан афзаллика аввало масалаларини оператив х,ал к,илишлари эвазига эришадилар. B2C, B2B ва P2P схемалари х,озирда электрон бизнесни олиб боришнинг асосий моделлари хисобланади.

B2C (Business - to - Consumer) *"бизнес истеъмолчи" схемаси* Internet оркали хусусий кишига молларни ва хизматларни чакана сотишни ифода-

лайди.

B2B (Business - to - Business) *"бизнес-бизнес" схемаси* компанияларнинг бир бири билан махсус ахборот технологияларидан ва маълумотларни электрон алмашиш стандартларидан фойдаланган хрлда узаро алокасини ифодалайди.

P2P (Peer - to - Peer ёки Partner - to - Partner) *бизнес муносабатнинг "тенг-тенг" схемаси* Internetfla бир хил хрлатда булган шериклар уртасидаги бизнес муносабатни ифодалайди.

B2B "бизнес-истеъмолчи" модели. Тижорат нуктаи назаридан B2C "бизнес-истеъмолчи" модели электрон тижоратнинг энг истикболли йуналиши хисобланади, чунки унинг асосини электрон чакана савдо ташкил этади. Internet оркали чакана савдо иктисодиётнинг тез ривожланаётган сохаси булиб электрон тижорат бозорининг анча-мунча улушини ташкил этади. B2C тизимларига куйидагилар тааллукди:

- савдо компанияларининг Web-дизайн воситалари ёрдамида расмийлаштирилган *Web-витриналар;*

- *Internet- магазинлар,* уларда, одатда, витринадан ташкари Internet оркали электрон савдо жараёнини бошкариш учун керакли бизнес - инфратузилма - back office мавжуд;

- back office лари компаниянинг савдо бизнес - жараёнлари билан тула интеграцияланган Internet-магазинлардан иборат савдо *Internet-тизимлар.*

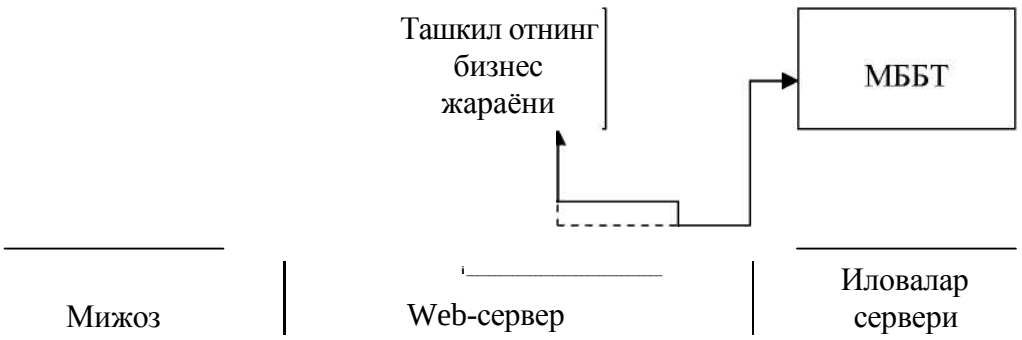
Уччало х,олда х,ам Internet орк,али савдо к,илинсада, х,ар бир вариант савдо жараёнининг турли автоматлаштирилган даражасига эга. Харидорларга хизмат килиш мураккаблиги нук,таи назаридан турли савияга эга, савдо килишга харажат хам турлича.

Web-витриналар амалга оширилишида нисбатан арзон ва етарлича оддий сайтлар х,исобланади. Техника нуктаи назаридан Web-витрина- каталог, навигация тизими ва буюртмани расмийлаштириш (менеджерга кейинги ишланиш учун узатилади) мажмуидир. Бошкача айтганда Web-витрина ёрдамида буюртмага савдо ташкил этилади. Бундай сайтларда маълум компаниянинг товарлар руйхати (прайс-лист) онлайн каталоги куринишида куйилади. Таъкидлаш лозимки, Web-витринанинг рентабеллиги оддий савдо

юритиш рентабеллигидан унчалик фарк, килмайди.

Internet-магазинлар. Электрон интернет-магазинларнинг ахборот технологиялари Internet дан фойдалана олувчи харидорга уйидан чикмасдан туриб турли фирмаларнинг товар ва хизмат навлари билан танишишга, уларнинг сифати ва нархи буйича ахборот олишга, Internet оркали туловни амалга оширишга ва уйга етказиб бериш билан харид килишта имкон беради. Умумий хрлда Internet-магазиннинг асосий вазифалари-харидорга ахборот хизматини курсатиш, буюртмаларни ишлаш, туловларни амалга ошириш хамда турли статистик ахборотларни йигиш ва тахлиллаш.

Internet-магазинни бошкариш схемаси 2.1-расмда келтирилган.



2.1-раем. Internet-магазинни бошқариш схемаси

Бу схемада:

- Web-сервер - тушган суровларни таксимлайди, фойдаланишни чегаралайди;

- иловалар сервери - барча тизим ишлашини, хусусан Internet-магазин бизнес мантикини бошкаради;

- МББТ(маълумотлар базасини бошкариш тизими) иловалар, мижозлар, счетлар ва х,. хусусидаги ахборотни саклашни ва ишлашни амалга оширади.

Талабга жавоб берадиган Internet-магазиннинг таъминоти Web-витринаникига Караганда кимматга тушсада, унинг имкониятлари жуда кенг ва рентабеллиги юкрри. Ундан ташкари, ахборотнинг динамик ишланиши ва маълумотлар базасининг мавжудлиги эвазига Internet-магазин хар бир руйхатдан утган харидор билан индивидуал ишлаш имкониятига эга.

Савдо Internet тизимлари чакана Internet савдо ривожининг юкрри погонаси хисобланади. Савдо Internet тизимининг Internet-магазиндан фарки унинг сотувчининг автоматлаштирилган корпоратив тизими билан интеграцияланганидир. Бу эса компаниянинг молия-хужалик фаолиятини оптималлаштиришга имкон беради.

Савдо Internet-тизими сотувни бевосита Internet оркали ташкил этишни мулжаллаган ишлаб чикарувчи компаниялар учун энг яхши танлов хисобланади. Бу хрлда савдо Internet тизими сотув ахборот тизимини иш-лаб-чикариш ва етказиб бериш тизими билан богловчи бугин вазифасини утайди. Савдо Internet тизимининг ишлатилиши харажатларнинг купгина кисмларини, хусусан тайёр махсулотнинг катта захирасини омборга жойлаштириш харажатининг кискаришига олиб келади.

B2B "бизнес-бизнес" модели. Бу модел компанияларнинг бир-бири билан, мое ахборот технологиялари ва маълумотларни электрон алмашиш

стандартларидан фойдаланиб узаро электрон алок,асини ифодалайди. Корхона ва компаниялар B2Bнинг махсус виртуал майдончаси (электрон биржа) оркали ахборот алмашиш, янги партнерлар ва таъминловчиларни топиш хамда савдо амалларини утказиш имкониятига эга булади.

B2B-майдончанинг (электрон биржанинг) тахминий схемаси 2.2-расмда келтирилган.

Расмдан куриниб турибдики, B2B-савдо майдончаси марказлаштирувчи Web-портал асосида истеъмолчилар ва танъминловчилар учун ечимларни бир бутунга бирлаштиради. Таъминловчилар ва истеъмолчилар сифатида йирик, урта ва кичик компаниялар иштирок этишлари мумкин.

Истеъмолчилар

2.2-расм. B2B-мапдонча (электрон биржа) схемаси.

Савдо майдончасининг муайян хилига боглик, хрлда майдончани яратувчилар истеъмолчиларга ёки таъминловчиларга зарур булган компонентларни амалга оширилишига ургу берадилар.

Internet биржалар каталоглар буйича сотиб олиш ва сотишни, таъминлаш занжирини режалаштириш, махсулотни биргаликда ишлаб чик,иш, аукцион оркдпи савдони ва х,. мададлайди. Окдбат натижада Internet биржалар бизнес буйича партнерлар алокдсини оптималлаштиришга имкон яратади ва умуман бизнес самарасини оширади.

Бизнес муносабатнинг P2P "тенг-тенг" схемаси. P2P схеманинг асосини Internet-аукционлар ташкил этади ва уларда турли товар ва хизматларни сотиб олиш/сотиш амалга оширилади. Аукционлар тармокда савдони ташкил этувчининг сайтига урнатилган махсус дастурий таъминот ёрдамида утказилади. Internet-аукционд а катнашиш учуй фойдаланувчи аукцион WWW-серверларнинг бирига аъзо булиши ва товар олиш (ёки узининг товарини сотиш учун такдим этиш) истагини маълум килиши лозим. Руйхатдан утишга банкда электрон хисоб раками булиши кифоя. Руйхатдан утганидан сунг фойдаланувчи узининг паролини айтади.

2.3. Internet оркали электрон туловларни амалга ошириш

Internetra мулжалланган электрон тулов тизими Internet оркали товар ва хизматларни сотиб олиш, сотиш жараёнида молия ташкилотлари, бизнес ташкилотлари, ва Internet-фойдаланувчилари уртасида хисоблашларни амалга оширувчи тизимдир. Электрон тижоратнинг хар кандай тизимининг иши Internetra мулжалланган электрон тулов тизими асосида узаро х,исоблашларни амалга ошириш билан тугайди. Одатда, бу тизимлар мавжуд анъанавий тулов тизимининг аналоглари булиб, асосий фарки - бутун тулов жараёни электрон ракам шаклда Internet имкониятларидан фойдаланган х,олда амалга оширилади.

Айнан тулов тизими буюртмаларни ишлаш хизматини ёки электрон

витринани барча стандарт атрибутли, талабга тула жавоб берадиган магазинга айлантиришга имкон беради. Бунда харидор сотувчининг сайтида товар ёки хизматни танлаб компьютердан узокдашмасдан туловни амалга ошириши мумкин.

Электрон тижорат тизимида туловлар куйидаги к,атор шартларнинг бажарилишида амалга оширилади:

- *конфиденциалликнинг сацланиши* — Internet оркали туловлар амалга оширилишида харидор маълумотларининг (масалан, кредит карта номери) факат конун билан белгиланган ташкилот-ларгина билиши кафолатланиши шарт;
- *ахборот яхлитлигининг сакланиши-харид* хусусидаги ахборот хеч ким томонидан узгартирилиши мумкин эмас;
- *аутентификация-харидоряар* ва сотувчилар иккала томон хам хакикий эканлигига ишонч хрсил килишлари шарт;
- *тулов воситаларининг кулайлиги* - харидорларга кулай булган хар кандай воситалар билан тулов имконияти;
- *авторизация* - жараён, бу жараён кечувида транзакция утказилиши хусусидаги талаб тулов тизими томонидан маъкулланади ёки рад этилади. Бу муолажа харидорнинг маблаги борлигини аникдашга имкон беради;
- *сотувчига буладиган хавф-хатарнинг кафолатлари* - Internetfla савдо килаётганида сотувчи товарни кайтариш ва харидорнинг инсофсизлиги билан боглик, купгина хавф-хатарга дуч келади. Хавф-хатар микдори тулов тизими провайдери ва савдо занжирига киритилган бошк,а ташкилотлар билан махсус битим оркали келишиб олиниши шарт;
- транзакция учун туловни минималлаштириш-буюртма ва товарга тулов транзакцияларининг ишланиши учун тулов, табиийки, товарнинг умумий нархига киради, демак, транзакция нархининг пасайиши фирманинг ракрбатбардошлигини оширади. Таъкидлаш мух,имки транзакция учун хар кандай х,олатда, хатто харидор товарни к,айтарганда хам, туланиши шарт.

Хозирда Internet-мулжалланган тулов тизимининг куйидаги хиллари

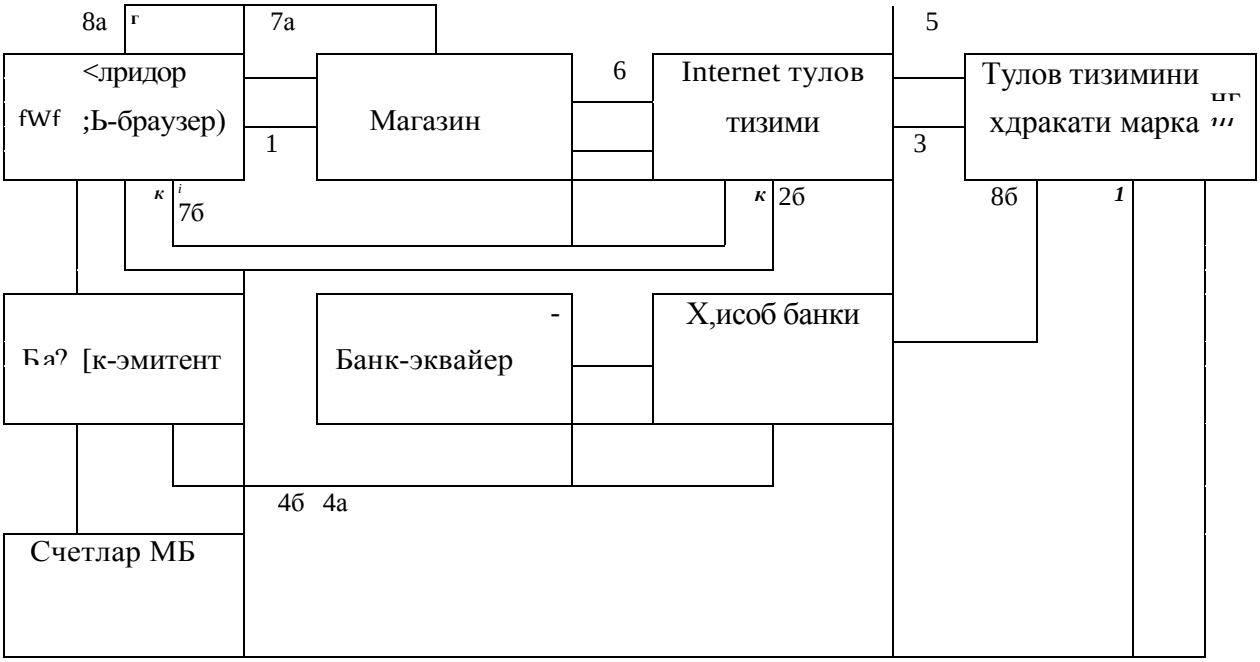
ишлатилмокда:

- кредитли (кредит карточкалари билан ишловчи);
- дебетли (электрон чеклар ва ракамли накди билан ишловчи).

Кредит тизимлар. Internetra мулжалланган тулов тизими кредит карточкалари билан ишловчи анъанавий тулов тизимининг аналоги хисобланади. Фарки, барча транзакцияларнинг Internet орк,али утказилиши ва натижада, х,имоялашнинг ва аутентификациянинг к,ушимча воситаларининг зарурлигидадур. Кредит карточкалари мижозга банк томонидан берил-ган кредит хдсобидан товарлар ва хизматларни тулашда ишлатилади. Кредит карточкалари буйича харид килинганида тизим карточкани автори3а-циялайди ва мижознинг тулашга крдирлигини текширади.

Хрзирда мавжуд Internetra мулжалланган тулов тизимлари бир-биридан транзакцияларининг хавфсизлик даражаси ва сотувчи ва харидорга зарур булган дастурий таъминоти билан фаркданади.

Internetra мулжалланган кредитли тулов тизимининг ишлаши принципини курайлик (2.3-раем.)



2.3-расм. Internetza мулжалланган кредит тулов тизимининг умумий схемаси.

Кредит карталари ёрдамида Internet орк,али туловларни амалга оширишда к,уйидагилар к,атнашади:

харидор - Web-браузерли компьютерга эга ва Internet дан фойдалана олувчи мижоз;

банк-эмитент - бунда харидорнинг х,исоб счети жойлашган. Банк-эмитент карточкалар чик,аради ва мижознинг молиявий мажбуриятларини бажарилишига кафил х,исобланади;

сотувчилар - товарлар ва хизматлар каталогларини олиб борувчи ва мижозлардан харидга буюртма олувчи серверлар;

банк-эквайерлар - сотувчиларга хизмат курсатувчи банклар. Хар бир сотувчи хисоб счетини сакловчи ягона банкка эга;

InternetHum тулов тизими-бошкд катнашчилар уртасида воситачи вазифасини утовчи электрон компонентлар; *анъанавий тулов тизими* - карталарга хизмат килувчи молия-вий ва технологик воситалар;

тулов тизимининг харакат маркази - анъанавий тулов тизими катнашчилари уртасида ахборот ва технологик алокаларни таъминловчи ташкилот;

тулов тизимининг хисоб банки — харакат марказининг топшириги буйича тулов тизими катнашчилари уртасида узаро хисобни бажарувчи кредит ташкилот.

Туловларни схемаси куйидагича амалга оширилади (2.3-расмга к,аралсин).

1. Харидор электрон магазинда товарлар саватини шаклланти-ради ва "кредит картаси" тулов усулини танлайди.
2. Сунгра кредит картасининг параметрлари (номерли, эгаси нинг исми, уз кучини йукртиш санаси) кейинги авторизациялаш учун InternetHHHr тулов тизимига узатилиши лозим. Бу амал иккита усул ёрдамида бажарилиши мумкин:
   - магазин орк,али, яъни карта параметрлари бевосита магазин сайтига киритилади, сунгра улар InternetHHHr тулов тизимига узатилади (2а);
   - тулов тизимининг серверида (26).

   Иккинчи йулнинг афзаллиги равшан. Бу хрлда карталар хусусидаги маълумот магазинда крлмайди ва, демак, унга учинчи шахснинг эга булиши ёки сотувчининг алдаши хавф-

хатари пасаяди. Иккала усулда х,ам кредит карта реквизитларини узатишда нияти бузук, одамлар томонидан уларнинг тармокда ушлаб к,олиш имконияти мавжуд. Буни олдини олиш учун карта тугрисидаги маълумот шифрланиб узатилади. Демак, харидор-сотувчи, сотувчи-Internet тулов тизими, харидор-Internet тулов тизими алокалари химояланган протоколлар ёрдамида амалга оширилиши максадга мувофик, хисобланади.

3. InternetHHHr тулов тизими суровни авторизациялаш учун анъанавий тулов тизимига узатади.

4. Кейинги кадам банк-эмитентнинг счетларининг онлайнли маълумотлар базасини олиб боришига боглик,. Маълумотлар базаси булса харакат маркази картани авторизациялаш учун банк-эмитентга узатади(4а) ва сунгра унинг натижасини олади(4б). Агар бундай база булмаса, харакат маркази карта

эгалари счетининг хрлати тугрисидаги маълумотни, стоп-варакаларни узи сакдайди ва авторизация суровини бажаради. Бу маълумотлар банк эмитентлар томонидан мунтазам янгиланиб турилади.

5. Авторизация натижаси Internet тулов тизимига узатилади.

6. Магазин авторизация натижасини олади.

7. Харидор авторизация натижасини магазин оркали (7а) ёки бевосита Internet тулов тизими оркали (76) олади.

8. Авторизациянинг ижобий натижасида:

- магазин хизмат курсатади ёки товар жунатади (8а);
- харакат маркази хисоб банкига бажарилган транзакция хусусида х,исоб банкига маълумот беради (86). Харидорнинг банк-эмитентдаги счетидан магазиннинг банк-эквайеридаги счетига пул утказилади.

Кредит карточкали тулов тизимининг камчиликлари сифатида куйидагиларни курсатиш мумкин:

- харидор учун кредит счетини очиш зарурияти;
- карточкаларни авторизациялаш ва мижознинг тулашга

к,одирлигини текшириш зарурияти транзакция утказишдаги чик,имларнинг усишига олиб келади ва бундай тизимларнинг Internet тулов тизимнинг максадли бозори булган микротуловларга мосланишини ёмонлаштиради;

- кредит карточкаларни туловга кабул килувчи магазинлар сонининг чегаралганлиги;
- анонимликнинг йуклиги ва бунинг натижасида савдо тузилмалари томонидан сервис курсатилиши.

Бу хил тизимлар ичида оммавий туе олганлари - First Virtual, Open Market, Cyber Cash ва SET протоколидан фойдаланувчи тулов тизимлари**[24].**

Дебет тизимлари. Дебет тулов тизимлари чеклар ва накд пулларнинг ракамли эквивалентларидан фойдаланишга асосланган. Туловларнинг дебет схемалари уларнинг чекли ва оддий пулли офлайн прототипларига ухшаш курилган. Схемада иккита мустакил томон: эмитентлар ва фойдаланувчилар иштирок этади. *Эмитент* деганда тулов тизимини бошкарувчи субъект тушунилади. У тулов воситаларини (масалан, банк счетларидаги пуллар) ифодаловчи кандайдир электрон бирликларни чикаради. Тизим *фойдаланувчилари* иккита бош вазифани бажаради. Улар чикарилган электрон бирликлардан фойдаланиб туловларни утказади ва Internetra кабул килади. Таъкидлаш мухимки, мижоз факат ушбу онда унинг банк счетидаги маблагга эгалик к,илиши мумкин. Тулов амаллари мижознинг молиявий активи улчамини камайтириш йули билан амалга оширилади.

Электрон чеклар оддий к,огоз чекларининг аналогидир. У туловчининг узининг банкидаги счетидан тулов к,абул к,илувчи счетига пул утказиш хусусидаги фармойишидан иборат. Бу амал олувчининг банкда чекни курсатиши билан амалга оширилади.

Электрон чекнинг кргоз чекдан асосий фарки к,уйидагилар:

- к,огоз чекни тулдирганда, туловчи узининг х,ак,ик,ий имзосини куйса, онлайн вариантида эса рак,амли электрон имзо ишлатилади;
- чекларнинг узи электрон куринишда берилади.

Электрон пуллар реал пулларни тула моделлайди. Бунда эмиссион ташкилот-эмитент реал пулларнинг турли тизимларда турлича номланувчи (масалан, купонлар) электрон аналогларини чик,арадилар. Уларни фойдала

нувчилар сотиб олиб улар ёрдамида харидлар учун тулайдилар, сунгра сотувчи эмитентда уларни бекор килади. Эмиссия вактида хар бир пул бирлиги бекор килинишидан аввал уни чикарувчи тузилма томонидан текширилади электрон мухр оркали тасдикданади.

Физик пулларнинг хусусиятларидан бири-уларниниг анонимлиги, яъни уларга качон ва ким ишлатгани курсатилмайди. Баъзи тулов тизимлари харидорга аналогия буйича электрон накд пулни шундай олишга имкон тугдирадики, улар билан пул орасидаги богликликни аникдаш мумкин булмайди. Бу кур имзолар деб аталувчи схемалар ёрдамида амалга оширилади.

2.4. Internet - хизматлар

Хрзирда Internet-хизматининг куйидаги тижорат шакллари кенг таркалган:

- Internet-банкинг;
- Internet-трейдинг;
- Internet-сугурта;
- ASP иловаларини ижарага бериш буйича хизмат курсатиш.

Internet-банкинг. Замонавий Internet-технологиялар банкларга хизматларининг бир кисмини янги савияга утказишга ва шу орк,али янги мижозларни жалб этишга ва уларга хизмат килиш харажатларини пасайтиришга имкон яратади. Анъанавий банкларнинг аксарияти уз мижозларига электрон хизмат килиш ва счет туловининг кушимча шаклларини тавсия этади. Фак,ат Internetfla иш юритувчи банклар нисбатан як,инда пайдо булди. Улар Web-банклар деб аталади. Энг йирик Web-банклар сирасига First Internet Bank, Net-Bank, CompuBank ва катор бошк,а банклар тааллукди.

Internet-банкинг деганда, одатда, мижозга оддий компьютер ёрдамида стандарт браузерни ишлатиб банк счетидан Internet оркали тугридан-тугри фойдаланиш имкониятининг берилиши тушунилади. Internet-банкинг тизимининг намунали варианти мижозларга банк офисларидаги физик шахе-

ларга (табиийки, накд пул билан бажариладиган амаллар бундан истисно) тақдим этилувчи банк хизматининг тулик, тупламини уз ичига олади.

Хрзирда Internet-банкинг хизмати хар бири Internet оркали амалга оширилувчи куйидаги имкониятларга эга:

- накд пулсиз хисоб-китобларни бажариш;
- коммун ал хизматлар учун тулови;
- InternetflaH фойдаланиш учун тулови;
- уяли ва пейджинг ал ока операторлари счетларини тулаш;
- ички ва банклараро хужжат асосидаги туловларни бажариш;
- уз счетлари буйича маблагларни утказиш;
- исталган вакт оралиги учун уз счетлари буйича барча банк амалларини кузатиш;

Internet-банкинг тизимидан фойдаланиш мижозларга катор имтиёзлар беради:

- фоизли ставкалари нисбатан юкрри;
- шахсан банкка бориш зарурияти йуклиги хисобидан мижознинг вакти жиддий тежалади;
- мижоз суткада 24 соат шахсий счетини назоратлаш ва молия бозоридаги вазиятнинг узгаришига тездан реакция курсатиш имкониятига эга.

Internet-банкинг тизимлари пластик карталар буйича амалга ошириладиган амалларни кузатишда жуда аскртади-карта х,исобидан маблагни чик,ариш тизимлар томонидан тайёрланган хисоблар буйича кучирмада дарх,ол акслантирилади. Бу мижозга уз амалларини назоратлашда кулайлик тугдиради.

Internet-трейдинг. Internet-технологиялар фонд бозори учун жуда истикболли. Internet-технологиялар туфайли, дунёда буш капитални к,уйишнинг энг яхши усули сифатида тан олинган кимматбахр к,огозларни сотиб олиш, хрзирда барча хрхдовчилар учун осон. Internet-трейдинг инвесторларни битимларни тузишнинг соддалиги ва онлайн-брокерларнинг хизматига таърифларнинг пастлиги билан узига жалб килади.

InternetHHHr замонавий имкониятлари кучмас мулк билан буладиган амалларни (сотиб олиш, сотиш, алмаштириш, мерос буйича бериш, ижара-

га бериш ва х,.) анъанавий шаклларига нисбатан айтарлича енгиллаштириш ва тезлаштиришга имкон беради. Мижоз уйидан чикмасдан кучмас мулкни сотиб олиши ва сотиши, мутахассис маслахатини олиши мумкин. Бу амалларни бажариш учун компьютери, InternetflaH фойдалана олиши ва банкда счети булиши кифоя.

Internet-су гурта. Сугурталаш деганда сугурталанувчи-мижоз (сугурта хизматларини сотиб олувчи) билан сугурталовчи (бундай хизматларни такдим этувчи) уртасида шартнома муносабатларини урнатиш ва мададлаш тушунилади. Сугурталовчи сугурта дастурини ишлаб чикади ва аниклайди, мижозга таклиф этади, агар сугурталанувчи рози булса иккала томон шартнома тузади. Мижоз бирданига ва мунтазам туловларни амалга оширади, сугурталовчи, уз навбатида, сугурта холат келиши билан сугурталанувчига сугурта шартномаси шартлари буйича компенсация пулини тулашга мажбурият олади.

Битимга келишиш жараёнида сугурта сугурта полней деб аталувчи хужжат шакллантирилади. Бу хужжат сугурталовчи ва сугурта компанияси учун юридик хужжат хисобланади. Унда сугурта объекти (мол-мулк, одам, маъсулият), сугурталанувчи холат, сугурта муддатининг бошланиши ва нихояси, сугурта суммаси, сугурта мукофоти каби мухим томонлари олдиндан айтиб утилади.

Ривожланган мамлакатлар сугурта компанияларида сугурта полисларини амалга оширувчи Internet-каналлар мавжуд.

ASP иловаларини ижарага бериш буйича хизмат курсатиш. Янги иктисодиёт ривожининг истикболли йуналишларидан бири ASP (Applications Service Providing) иловаларини ижарага бериш буйича хизмат курсатишдир. Internet ёки хусусий тармок, орк,али фойдаланувчидан узокдаги серверда жойлашган иловалардан фойдаланишни ASP иловалари амалга оширади.

ASP иловаларининг провайдери узининг серверларига иловаларнинг дастурий таъминотини урнатади ва улардан мижозларнинг фойдаланишини таъминлайди. Мижоз компьютерига бундай дастурий таъминотни урнатиши, уни янгилаши, захира нусхалаши ва х- шарт эмас. Барча ишларни ASP

провайдери бажаради. Мижоз провайдерга иловалардан фойдалангани учун ижара хакини тулайди.

Компанияларнинг ASP хизматларидан фойдаланишининг сабаби куйидагилар.

- компания эхтиёж сезган энг янги технологиялардан хавф-хатарсиз, катта харажатсиз ва маъмурий жавобгарсиз фойдаланиш;
- иловалардан тезда фойдаланиш зарурияти;
- агар компанияни илова кандайдир сабабларга тула крниктирмаса, осонгина воз кечиш имконияти.

Якин йилларда ASP бозорининг тез усиши кутилмокда. Бу эса, уз навбатида, барча компанияларга исталган бизнес-иловалардан бир хилда фойдаланишни такдим этиш оркали, бизнес ривожида баркарорликни таъминлайди. Аксарият аналитикларнинг фикрича, кейинчалик ASP модели бизнес иловалардан фойдаланиш усулларининг орасида устунлик килиши мумкин.

2.5 Электрон бизнес тизими хавфсизлигининг муаммолари

Электрон бизнес харидор ва сотувчи орасидаги алокани ташкил этиш, буюртмани ифодалаш, мухокама килиш, узгартириш, товарларни ва хизматларни сотиш усулларини хамда туловни амалга ошириш жараёнларини узгартириш учун янги технологиялардан фойдаланади. Х,озирда электрон тижорат ва бизнеснинг аксарият муаммолари ахборот хавфсизлиги билан боглик,, яъни хавфсизлик муаммолари электрон тижорат ва бизнес ривожидаги жиддий тусик, хисобланади.

Хдр к,андай тижорат компаниясининг бошк,а компаниялар билан ёки ушбу компаниянинг булимлари орасида алок,а урнатилиши зарур. Хрзирда глобал Internet тармоги узининг узеллари уртасида ишончли ва арзон ахборот алмашинувини таъминлайди. Очик, глобал Internet тармоги каналларидан фаол фойдаланувчи электрон бизнеснинг ишлаши жараёнида купгина хавф-хатарлар пайдо булади.

InternetflaH фойдаланиш каналлари компаниянинг ахборот ресурсларидан четдан фойдаланишга имкон бериши мумкин. Коммуникацион, хусусан HTTP - протокол асосидаги дастурлардан эхтиётсизлик билан фойдаланиш ахборот тизимининг ишга лаёкатлигини бузувчи ва/ёки ахборот тизимимаълумотларини бузувчи махсус дастур - "Троян отларининг" киришига олиб келиши мумкин. Бу хил дастурларнинг ичида вируслар энг таркалган. Узига хос малакали мутахассислар корпоратив ахборот тармокларига билинмасдан кириш учун купинча умуммаксад тармокдардан фойдал анадилар.

Электрон кутисининг тез-тез ишлатилиши нияти бузук, одамларга электрон бизнес билан шугулланувчи ташкилот фойдалананувчилари номларини обрусизлантиришга ёрдам бериши мумкин. Фойдаланувчилар маълумотларини (исмлар, пароллар, PIN - кодлар ва х,.) сакдовчи тизимининг заиф жойларини кидиришдан тармокда кенг ишлатилувчи махсус дастурлардан фойдаланиш мумкин.

Internet конфиденциал ахборотни дунёнинг исталган нуктасига юбориши мумкин, аммо агар у етарлича химояланмаган булса, ушлаб крлиниши, нусхалаштирилиши, узгартирилиши хамда хар кандай четдаги фойдаланувчилар - нияти бузук, одамлар, ракиблар ва оддий кизикувчилар томонидан укилиши мумкин. Масалан, етарлича химояланмаган тулов топшириги ёки кредит карточка номерини жунатаётганда эсда тутиш лозимки, жунатиш хусусий/шахсий тармок, орк,али амалга оширилмаяпти ва четдаги фойдаланувчилар хабарингизни манипуляция килиш имкониятига эга. Ундан ташк,ари хабарингиз алмаштирилиб к,уйилиши мумкин: хабарларни худди *B* фойдаланувчидан юборилганидек *A* фойдаланувчидан юбориш усуллари мавжуд. Internet тармоги махсус пакет, тамомила к,онуний пакетлар, сонининг хаддан ташк,ари купилги узатишдаги бузилишлар, тармок, компонентларининг носозлиги туфайли ишга лаёкат булмаслиги мумкин. Бундай холлар "хизмат к,илишдан воз кечиш" деб аталади ва электрон тижорат учун энг жиддий тахдид хисобланади. 2.2-жадвалда ахборот хавфсизлиги бузилишининг статистикаси келтирилган[24].

2.2-Жадвал

Ахборот хавсизлиги бузилишининг турлари	**К,айд этилганлиги %**	**Йукотишлар %**
Корпоротив тармокдан рухсатсиз четдан фойдаланиш	**44**	**25**
Хизмат килишдан воз кечиш	**32**	**28**
Узатишда маълумотларни алмаштириш	**17**	**18**
Фаол тинглаб куриш	**2**	**1**
Тармокдан рухсатсиз ички фойдаланиш	**97**	**62**
Ахборотдан рухсатсиз ички фойдаланиш	**55**	**32**

Ахборот хавфсизлиги электрон бизнес тизимининг энг мухим элементларидан бири хисобланади ва усуллар ва воситаларнинг бутун бир туплами ёрдамида таъминланиши шарт. Электрон тижорат сохасидаги савдо кулами Internet хавфсизлиги масалаларидан ташвишланган харидорлар, сотувчилар ва молия инситутларининг бошидан кечирувчи куркувлари билан чегараланади. Бу куркувлар, хусусан, куйидагиларга асосланади:

- конфиденциалликка кафолатнинг йуклиги- кимдир маълумотларингизни узатилаётганида ушлаб крлиши ва кийматли ахборотни (масалан, кредит карточкангизнинг номерини, товар етказиб бериш санаси ва адрес) топишга уриниши мумкин;

амалда иштирок этувчиларни текшириш даражасининг етарли эмаслиги - транзакция катнашчилари текширилмаганида томонларнинг бири "маскарад" уюштириши мумкинки, унинг окибати иккинчи томонга анча кимматга тушади. Масалан, харидор сайтга кириб ундаги компаниянинг х,ак,ик,ийлигига шубх,а к,илади, шундай х,ол х,ам руй бериши мумкинки, харидор кредит карточкасининг номерини етарлича ваколатга эга булмаган шахсга беради;

- сотувчида буюртма берган харидор кредит карточкасининг крнуний эгаси эканлигинининг текшириш имкони йук,;

- кредит карточкасининг банк-эмитенти туловни бажаришга талаб к,уйган сотувчини текширишни истаб крлиши мумкин;

- маълумотлар яхлитлигига кафолат йук, - хатто маълумотларни жунатувчи индентификацияланган булсада, учинчи томон маълумотларни, улар узатилиши вактида, узгартириш имкониятига эга.

Ахборот хавфсизлигини таъминлаш нуктаи назаридан электрон тижоратнинг намунавий кулланилишини - Internet оркали махсулотга ва хизматларга эга булишни курайлик. Ушбу жараён куйидаги боскичлар оркали ифодаланиши мумкин.

1. Буюртмачи Web-сервер оркали махсулот ёки хизматни танлайди ва мое буюртмани расмийлаштиради.
2. Буюртма магазиннинг буюртмалар маълумотлари банкига киритилади.
3. Буюртма берилган махсулот ёки хизматни олиш мумкинлигини маълумотларнинг марказий базаси оркали текширилади.
4. Агар махсулотнинг олиниши мумкин булмаса, буюрмачи у тугрида огохдантирилади ва махсулот ёки хизматга эга булиш жараёни тухтатилади. Махсулотга суров бошка складга (буюртмачи розилигида) йуналтирилиши мумкин.
5. Агар махсулот ёки хизмат мавжуд булса буюртмачи туловни тасдикдайди ва буюртма мое маълумотлар базасига киритилади. Элек трон магазин мижозга буюртма тасдигини юборади. Купгина холларда (айник,са эндигина иш бошлаган компанияларда) буюртмалар, товарларнинг борлигини текшириш ва х,. учун ягона маълумотлар базаси мавжуд.
6. Мижоз онлайн режимида буюртма хакини тулайди.
7. Товар буюртмачига етк,азилади.

Электрон тижорат билан шугулланадиган компаниялар юкррида келтирилган боск,ичларда дуч келадиган тахдидлар к,уйидагилар:

- электрон магазин Web-сайтининг сах,ифасини алмаштириб к,уйиш. Бу тахдидни амалга оширишнинг асосий усули - фойдаланувчи суровини бошк,а серверга йуллаш. Бу тахдид олтинча боскичда буюртмачи кредит карточкасининг номерини киритганда кучаяди;

- ёлгон буюртмалар бериш ва электрон магазин ходимлари томонидан фирибгарлик килиш. Хрзирда ички/ташки тахдидлар муносабати 60/40ни ташкил этади;
- электрон тижорат тизимида узатиладиган маълумотларни ушлаб крлиш. Буюртмачининг кредит картаси хусусидаги ахборотни ушлаб колиш узгача хавф-хатарни тугдиради;
- компаниянинг ички тармогига кириш ва электрон магазин компонентларини обрусизлантириш;
- "хизмат килишдан воз кечиш " (denial of service) хужумини амалга ошириш ва электрон тижорат ишлашини ёки унинг узелини бузиш.

Ушбу тахдидлар натижасида компания - электрон битим провайдери - мижозлар ишончини йукртади, моддий зарар куради. Баъзи холларда бу компанияларга кредит карточка номери фош килингани учун даъво кузгатилиши мумкин. "Хизмат килишдан воз кечиш" хужумси натижасида электрон магазиннинг ишлаши бузилиши мумкин, унинг ишга лаёкатлигини тиклашга инсон, вакт ва материал ресурслари талаб этилади.

Ill боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИИ ЙУЛЛАРИ

3.1. Ахборотни щшоялаш концепцияси

Нияти бузук, одамларни ёлгиз фойдаланувчилар эмас, балки корпоратив компьютер тармоклари кизиктиради. Айнан бундай тармокларда ахборотнинг йуолиши, рухсатсиз модификацияланиши жиддий окибатларга олиб келиши мумкин.

Компьютер тармокдарини химоялаш уйда фойдаланувчи компьютерларни химоялашдан фаркданади (гарчи индивидуал ишчи станцияларни химоялаш-тармок, химоясининг ажралмас кисми). Чунки, аввало, бундай масала билан саводли мутахассислар шугулланадилар. Шу билан бирга корпоратив тармок, хавфсизлиги тизимининг асосини четки фойдаланувчилар учун ишлаш кулайлиги ва техник мутахассиларга куйиладиган талаблар уртасида муросага етишиш ташкил этади.

Компьютер тизимига икки нуктаи назардан караш мумкин: унда фак,ат ишчи станциялардан фойдаланувчиларни куриш мумкин, ёки факат тармок, операцион тизимининг ишлашини хисобга олиш мумкин.

Симлар буйича утувчи ахборотли пакетлар мажмуини х,ам компьютер тармоги дейиш мумкин. Тармок,ни ифодалашнинг бир неча сатх,лари мавжуд. Худи шундай тармок, хавфсизлиги муаммосига турли сатхдарда ёндашиш мумкин. Мое хрлда х,ар бир сатх, учун х,имоялаш усули турлича булади. Тизимнинг ишончли х,имояланиши х,имояланган сатхдар сони билан белгиланади.

Биринчи, куриниб турган ва амалда энг кийин йул-ходимларни тармок, хужумларини к,ийинлаштирувчи хатти-харакатга ургатиш. Бу бир к,арашда осондай туюлсада, аммо мушкул иш. Internet дан фойдаланишни чегаралаш лозим.

Аксарият фойдаланувчилар чегараланишлар сабабини билмайдилар. Шунинг учун такик,илар аник, ифодаланиши лозим.

Компьютер тармокдари ахборотини химоялашга химоялаш тадбирларининг ягона сиёсатини хамда хукукий, ташкилий-маъмурий ва инженер-техник характерга эга чоралар тизимини утказиш оркали эришилади.

Тармокда ахборотни химоялашнинг зарурий даражасини ишлаб чикишда ходимлар ва рахбариятнинг узаро жавобгарлиги, шахе ва ташкилот манфаатларига риоя килиш, хукукни мухрфаза килувчи органлар билан узаро алока хисобга олинади. Ракрбатли шароитда хизматларнинг катта сонини такдим этиш ва хизмат килиш вактини кискартириш орк,али етакчи уринни саклаб крлиш ва янги мижозларни жалб этиш мумкин. Бунга факат барча амалларни автоматлаштиришнинг зарурий даражасини таъминлаш эвазига эришиш мумкин. Айни замонда хисоблаш техникасининг ишлатилиши билан нафакат пайдо булган муаммолар х,ал этилади, балки янги ахборотни бузилиши ва йук,отилиши, тасодифан ва атайин модификацияланиши хамда ахборотни бегоналар тарафидан рухсатсиз олиниши билан боглик, ноъананавий тахдидлар пайдо булади.

Мавжуд х,олатнинг тахдили курсатадики, ахборотни х,имоялаш учун к,илинадиган тадбирлар даражаси, одатда, автоматлаштириш даражасидан паст. Бундай орк,ада к,олиш жиддий окибатларга олиб келиши мумкин.

Автоматлаштирилган комплексларда ахборотнинг заифлигига х,исоблаш ресурелариниг концентрацияланиши, уларнинг худудий так,симланганлиги, магнит элтувчиларида маълумотларнинг катта х,ажмини узок, вакт сакданиши, купгина фойдаланувчиларнинг ресурелардан бир вактда фойдаланиши сабаб булади.

Бундай шароитда химоялаш чораларини куриш заруриятига шубха к,илмаса булади. Аммо куйидаги к,ийинчиликлар мавжуд:

- х,озирги кунда х,имояланган тизимларнинг ягона назарияси йук,;
- х,имоя воситаларини ишлаб чикарувчилар хусусий масалаларни ечиш учун асосан алохида компонентларни тавсия этадилар, химоялаш тизимини шакллантириш ва бу воситаларнинг бирга ишлатилиши масалалари эса истеъмолчи ихтиёрига крлдирилади;

• ишончли химояни таъминлаш учун техник ва ташкилий муаммолари комплексини х,ал этиш ва мое хужжатларни ишлаб чикиш зарур.

Юкррида санаб утилган кийинчиликларни бартараф килиш учун нафакат алохида корхона, балки давлат даражасидаги ахборот жараёнларида иштирок этувчилари харакатининг координацияси зарур. Ахборот хавфсизлигини таъминлаш етарлича жиддий масала. Шунинг учун аввало ахборот хавфеизлиги концепциясини ишлаб чикиш зарур. Концепцияда миллий ва корпоратив манфаатлар, ахборот хавфсизлигини таъминлаш принциплари ва мададлаш йуллари аникланади ва уларни амалга ошириш буйича масалалар таърифланади.

Концепция - ахборот хавфеизлиги муаммосига расмий кабул килинган карашлар тизими ва уни замонавий тенденцияларни хисобга олган хрлда ечиш йуллари.

Концепцияда ифодаланган максадлар, масалалар ва уларни булиши мумкин булган ечиш йуллари асосида ахборот хавфсизлигини таъминлашнинг муайян режалари шакллантирилади.

Концепцияни ишлаб чик,ишни уч боск,ичда амалга ошириш тавсия этилади (3.1-раем).

I боск,ич	Х,имояланувчи объект к,ийматини аникдаш
II боск,ич	Бузгунчининг булиши мумкин булган хдракатларини тахлиллаш
III боск,ич	Объектга урнатилган ахборотни х,имоялаш воситаларининг ишончлилигини бах,олаш

3.1—раем. Ахборот химояси концепциясини ишлаб чикиш боскичлари

Биринчи боскдгчда х,имоянинг мак,садли курсатмаси, яъни кдндай реал бойликлар, ишлаб чикдриш жараёнлари, дастурлар, маълумотлар базаси х,имояланиши зарурлиги аникданиши шарт. Ушбу боскдгчда х,имояланувчи алохдда объектларни ахдмияти буйича табакдлаштириш мак,садга мувофик, х,исобланади.

Иккинчи боск,ичда хдмояланувчи объектга нисбатан булиши мумкин булган жиноий хдракатлар тахдилланиши л озим. Ик,тисодий жосуслик, терроризм, саботаж, бузиш оркдли угирлаш каби кенг таркдлган жиноятчиликларнинг реал хавф-хатарлик даражасини аниклаш мух,им хдсобланади. Сунгра, нияти бузук, одамларнинг х,имояга мух,тож асосий объектларга нисбатан хдракатларининг эх,тимоллигини тах,лиллаш лозим.

Учинчи боск,ичнинг бош масаласи-вазиятни, хусусан узига хос мах,аллий шароитни, ишлаб чикдриш жараёнларини, урнатиб к,уйилган х,имоянинг техник воситаларини тах,лиллашдан иборат.

3.2. Ахборот зщмоясининг стратегияси ва архитектураси

Ахборот хавфсизлиги стратегияси ва хдмоя тизими архитектураси (3.2-расм) ахборот хавфсизлиги концепцияси асосида ишлаб чик,илади.

Ахборот хавфсизлиги буйича тадбирлар комплексининг асосини ахборот х,имоясининг стратегияси ташкил этиши лозим. Унда ишончли х,имоя тизимини куриш учун зарурий мак,садлар, мезонлар, принциплар ва муолажалар аникданади. Яхши ишлаб чик,илган стратегияда нафакдт х,имоя даражаси, рах,наларни кддириш, брандмауэрлар ёки ргоху-серверлар урнатиладиган жой ва х,. уз аксини топиши лозим, балки ишончли хдмояни кафолатлаш учун уларни ишлатиш муолажалари ва усуллари х,ам аникданиши лозим.

Ахборот хдмояси умумий стратегиясининг мух,им хусусияти хавфсизлик тизимини тадк,икдашдир. Иккита асосий йуналипши ажратиш мумкин:

- хдмоя воситаларининг тах,лили;
- хужум булганини аникдаш.

Ахборот хавфсизлиги
концепцияси

Ахборот хавфсизлигини таъминлаш иерархиясидаги иккинчи масала сиёсатни аниклашдир. Унинг мазмуни энг рационал воситалар ва ресурслар, курилаётган масала максади ва унга ёндашиш ташкил этади. Х,имоя сиёса-ти-умумий хужжат булиб, унда фойдаланиш кридалари санаб утилади, сиёсатни амалга ошириш йуллари аникланади ва химоя мухитининг базавий архитектураси тавсифланади. Бу хужжат матннинг бир нечта сахифаларидан иборат булиб, тармок, физик архитектурасини шакллантира-ди, ундаги ахборот эса химоя махсулотини танлашни аникдайди.

3.3. Ахборот хавфсизлигининг сиёсати

Ахборот хавфсизлигининг сиёсатини ишлаб чикишда, аввало химоя килинувчи объект ва унинг вазифалари аникданади. Сунгра душманнинг бу объектга кизикиши даражаси, х,ужумнинг эх,тимолли турлари ва куриладиган зарар бах,оланади. Нихрят, мавжуд карши таъсир воситалари етарли химояни таъминламайдиган объектнинг заиф жойлари аникданади.

Самарали хдмоя учун хдр бир объект мумкин булган тахдидлар ва хужум турлари, махсус инструментлар, куроллар ва портловчи моддаларнинг ишлатилиши эхтимоллиги нуктаи назаридан бах,оланиши зарур. Таъкидлаш лозимки, нияти бузук, одам учун энг кимматли объект унинг эътиборини тортади ва эх,тимолли нишон булиб хизмат килади ва унга карши асосий кучлар ишлатилади. Бунда, хавфсизлик сиёсатининг ишлаб чикилишида ечими берилган объектнинг реал хдмоясини таъминловчи масалалар х,исобга олиниши лозим.

Карши таъсир воситалари хдмоянинг тулик, ва эшелонланган концепциясига мое келиши шарт. Бу дегани, карши таъсир воситаларини маркизида х,имояланувчи объект булган концентрик доираларда жойлаштириш лозим. Бу х,олда душманнинг исталган объектга йули х,имоянинг эшелонланган тизимини кесиб утади. Мудофаанинг хдр бир чегараси шундай ташкил килинадики, куриклаш ходимининг жавоб чораларини куришига етарлича вакт мобайнида хужумчини ушлаб туриш имкони булсин.

Сунгги боскичда к,арши таъсир воситалари к,абул к,илинган х,имоя концепциясига биноан бирлаштирилади. Бутун тизим хдёти циклининг бошлангич ва кутилувчи умумий нархини дастлабки бах,олаш амалга оширилади.

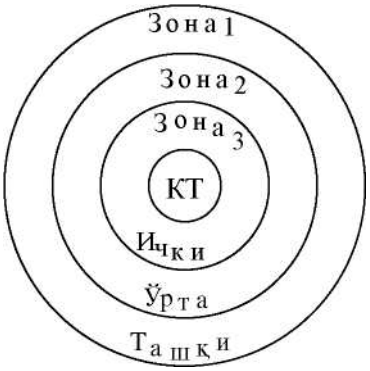
Агар бир бинонинг ичида турли х,имоялаш талабларига эга булган объектлар жойлашган булса, бино отсекларга булинади. Шу тарика умумий назоратланувчи макон ичида ички периметрлар ажратилади ва рухсатсиз фойдаланишдан ички х,имоя воситалари яратилади. Периметр, одатда, физик тусикдар оркали аникданиб, бу тусикдардан утиш электрон усул ёки куриклаш ходимлари томонидан бажарилувчи махсус муолажалар ёрдамида назоратланади.

Умумий чегарага ёки периметрга эга булган бинолар гурух,ини х,имоялашда нафакат алох,ида объект ёки бино, балки унинг жойланиш жойи х,ам хдеобга олиниши зарур. Куп сонли бинолари булган ер участкалари хавфеизликни таъминлаш буйича умумий ёки кисман мое келадиган талабларга эга булади, баъзи участкалар эса периметр буйича тусиккд ва ягона йулакка эга. Умумий периметр ташкил этиб, хдр бир бинодаги хдмоя

воситаларини камайтириш ва уларни факат хужум килиниши эхтимоли купрок, булган мухим объектларга урнатиш мумкин. Худди шу тарика участкадаги хар бир иморат ёки объект хужумчини ушлаб крлиш имконияти нуктаи назаридан бахрланади.

Юкрридаги келтирилган талаблар тахдили курсатадики, уларнинг барчаси ахборотни ишлаш ва узатиш курилмаларидан хукуксиз фойдаланиш, ахборот элтувчиларини угирлаш ва саботаж имкониятини йул куймасликка олиб келади.

Бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага утиш йулида жойлаштирган хрлда концентрик х,алка куринишида ташкил этиш максадига мувофик, хисобланади (3.2-расм).



1 -зона. Компьютер тармоғи (КТ) хавфсизлигининг таш^и зонаси
Таъминланиши: - физик тусиклар
- периметр бўйлаб ўтиш жойлари
- худудга кириш назоратининг ноавтоматик тизими

2- зона. КТ хавфсизлигининг ўртадаги зонаси
Таъминланиши: - эшиклари электрон химояланган назорат пунктлари
- видеокузатиш
- бум буш зоналарни чикдриб ташлаш

3-зона. КТ хавфсизлигининг ички зонаси
Таъминлаш: - шахсий компьютерга фойдаланиш фак^ат назорат тизими оркдли
- идентификациялашнинг биометрик тизими

3.3-расм. Бинодаги компьютер тизимининг хавфсизлик тизими

Ахборот хизмати бинолари ва хоналарига киришнинг назорати масаласига келсак, асосий чора-нафакат бино ва хоналарни, балки воситалар комплексини, уларнинг функционал вазифалари буйича ажратиш ва изоляциялаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тулдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш х,имояланувчи объектнинг мух,имлигини, воситаларга кетадиган харажатни ва назорат тизими ишончлилиги даражасини, ижтимоий жихатларни ва инсон нафси бузуклигини олдиндан урганишга асосланади. Бармок,, кафтлар, куз тур

пардаси, кон томирлари излари ёки нуткни аниклаш каби биометрик индентификациялаш ишлатилиши мумкин. Шартнома асосида техник воситаларга хизмат курсатувчи ходимларни объектга киритишнинг махсус режими кузда тутилган. Бу шахслар идентификацияланганларидан сунг объектга кузатувчи хамрохдигида киритилади. Ундан ташкари уларга аник, келиш режими, маконий чегараланиш, келиб-кетиш вакти, бажарадиган иш характери урнатилади.

Нихрят, бино периметри буйича бостириб киришни аникдовчи турли датчиклар ёрдамида комплекс кузатиш урнатилади. Бу датчиклар объектни куриклашнинг марказий пости билан богланган ва булиши мумкин булган бостириб кириш нукталарини, айникса ишланмайдиган вактларда, назорат килади.

Вакти-вакти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошка чик,иш йулларининг физик х,имояланиш ишончлилигини текшириб туриш лозим.

Хдр бир хонага ичидаги нарсанинг мухимлилигига боглик, фойдаланиш тизимига эга булган зона сифатида каралади. Кириш-чик,иш хук,ук,и тизими шахе ёки объект мухимлигига боглик, хрлда селекцияли ва даражалари буйича рутбаланган булиши шарт. Кириш-чик,иш хукуки тизими марказлашган булиши мумкин (рухсатларни бошкариш, жадвал ва календар режаларининг режалаштирилиши, кириш-чик,иш хук,ук,ининг ёзма намуналари ва х,.)-

Назорат тизимини вакти-вакти билан текшириб туриш ва уни доимо ишга лаёкатли хрлда саклаш лозим. Буни ихтисослашган булинмалар ва назорат органлари таъминлайди.

Шахсий компьютер ва физикавий химоя воситалари каби улчамлари кичик асбоб-ускуналарни кузда тутиш мумкин.

Юк,орида келтирилганларга хулоса к,илиб, компьютер тармокдарини химоялашда ахборот хавфеизлиги сиёсати к,андай аникланиши хусусида суз юритамиз. Одатда куп сонли фойдаланувчиларга эга булган корпоратив компьютер тармоклари учун махсус "Хавфсизлик сиёсати" деб аталувчи,

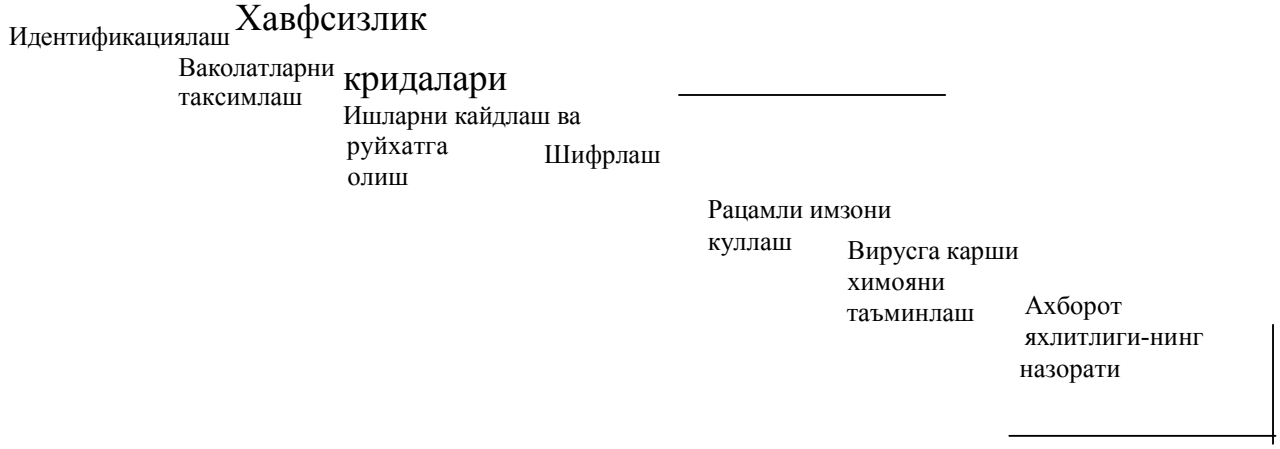
тармокда ишлашни маълум тартиб ва кридаларга буйсиндирувчи (регламентловчи) хужжат тузилади.

Сиёсат одатда икки кисмдан иборат булади: умумий принциплар ва ишлашнинг муайян кридалари. Умумий принциплар Internetfla хавфсизликка ёндашишни аникласа, кридалар нима рухсат этилишини ва нима рухсат этилмаслигини белгилайди. Кридалар муайян муолажалар ва турли кулланмалар билан тулдирилиши мумкин.

Одатда хавфсизлик сиёсати тармок, асосий сервисларидан (электрон почта, WWW ва х,.) фойдаланишни регламентлайди хамда тармокдан фойдаланувчиларни улар кандай фойдаланиш хукукига эга эканликлари билан таништиради. Бу эса уз навбатида фойдаланувчиларни аутентификациялаш муолажасини аникдайди.

Бу хужжатга жиддий ёндашиш лозим. Химоянинг бошка барча стратегияси хавфсизлик сиёсатининг катъий бажарилиши тахминига асосланган. Хавфсизлик сиёсати фойдаланувчилар томонидан купгина маломат орттирилишига сабаб булади, чунки унда фойдаланувчига маън этилган нарсалар очик-ойдин ёзилган. Аммо хавфсизлик сиёсати расмий хужжат, у бир томондан Internet такдим этувчи сервисларда ишлаш зарурияти, иккинчи томондан мое мутахассис-профессионаллар тарафидан ифодаланган хавфсизлик талаблари асосида тузилади.

Автоматлаштирилган комплекс х,имояланган х,исобланади, качонки барча амаллар объектлар, ресурелар ва муолажаларни бевосита х,имоясини таъминловчи катъий аникланган к,оидалар буйича бажарилса (3.4-расм).



3.4-расм. Ахборот хавфеизлиги сиёсатини таъминлашнинг асосий цоидалари.

Химояга куйиладиган талабларнинг асосини тахдидлар руйхати ташкил этади. Бундай талаблар уз навбатида хдмоянинг зарурий вазифалари ва х,имоя воситаларини аниклайди.

Демак, компьютер тармогада ахборотни самарали х,имоясини таъминлаш учун х,имоя тизимини лойих,алаш ва амалга ошириш уч боскичда амалга оширилиши керак.

- хавф-хатарни тахлиллаш;
- хавфсизлик сиёсатини амалга ошириш;
- хавфсизлик сиёсатини мададлаш.

Биринчи боскичда компьютер тармоганинг заиф элементлари тахлилланади, тахдидлар аникланади ва бах,оланади, хдмоянинг оптимал воситалари танланади. Хавф-хатарни тахлиллаш хавфсизлик сиёсатини кабул килиш билан тугалланади.

Иккинчи боскич - хавфсизлик сиёсатини амалга ошириш молиявий харажатларни хдсоблаш ва масалаларни ечиш учун мое воситаларни танлаш билан бошланади. Бунда танланган воситалар ишлашининг ихтилофли эмаслиги, воситаларни етказиб берувчиларнинг обруси, хдмоя механизмлари ва бериладиган кафолатлар хусусидаги тула ахборот олиш имконияти каби омиллар хдеобга олиниши зарур. Ундан ташкари, ахборот хавфеизлиги буйича асосий кридалар акс эттирилган принциплар хдеобга олиниши керак.

Учинчи боск,ич - хавфсизлик сиёсатини мададлаш боскичи энг мухдм х,исобланади. Бу боск,ичда утказиладиган тадбирлар нияти бузук, одамларнинг тармоккд бостириб киришини доимо назорат килиб туришни, ахборот объектини х,имоялаш тизимидаги "рах,на"ларни аникдашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш х,олларини х,исобга олишни талаб этади. Тармок, хавфеизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури буйнида булади. У хавфеизликнинг муайян тизими бузилишининг барча холларига оператив муносабат билдириши, уларни тахлиллаши ва молиявий воситаларнинг максимал тежалишини х,исобга олган х,олда х,имоянинг зарурий аппарат ва дастурий воситаларидан фойдаланиши шарт.

3.4. Ахборот-коммуникацион тизимлар ва тармсщлар хавфсизлигига куйиладиган талаблар

Куйида Россия Федарациясида ишлаб чик,илган компьютер тармокдарида ахборотни хдмоялаш сохасига тааллукди хужжатлар хусусида суз юритилади. Хужжатларда куйилган талаблар давлат секторида ёки таркибида давлат сири булган ахборотни ишловчи тижорат ташкилотларида бажарилиши шарт. Бошка тижорат тузилмалар учуй хужжатлар тавсия характерига эга.

Хужжатлардан бири ахборотдан рухсатсиз фойдаланишдан химоялаш буйича талабларни акс эттиради ва "Автоматлаштирилган тизимлар. Ахборотдан рухсатсиз фойдаланишдан химоялаш. Автоматлаштирилган тизимларнинг туркумланиши ва ахборотни химоялаш буйича талаблар" деб номланади.

Бу хужжатда хавфсизликнинг исталган даражасига эришиш буйича асосланган чораларни ишлаб чикиш ва куллаш максадида автоматлаштирилган тизимларнинг ахборотни химоялаш нуктаи назаридан ишлаши шароитлари буйича туркумланиши келтирилган. Хар бир химоялаш буйича маълум минимал талаблар мажмуи оркали характерланувчи химояланишнинг тук,к,изта синфи белгиланади (3.1-жадвал).

3.1-жадвал. Компьютер тармоцларининг щмояланиш синфлари.

Талаблар	Синфлар								
	ЗБ	ЗА	2Б	2А	1Д	1Г	1В	1Б	1А
Фойдаланишни бошцариш цисм ттимига									
Идентификациялаш, ущщийлигини текшириш ва субъектлар фондаланишининг									
- тизимга	х	х	х	х	х	х	х	х	х
- терминалларга, ЭХ,Мга, ЭХ,М тармоги узелларига, алок,а каналларига, ЭХ,Мни ташк,и курилмаларига				х		х	х	х	х
- дастурларга	-	-	-	х	-	х	х	х	х
- жилдларга, каталогларга, файлларга, к,айдларга	-	-	-	х	-	х	х	х	х
Ахборот окдмларини бошкдриш	-	-	-	х	-	-	х	х	х
Рупхатга ва уисобга олиш цисм тизимига									
Руйхатга ва ^исобга олиш									
- субъектларнинг тизимга(дан) киришини (чик,ишини)	х	х	х	х	х	х	х	х	х
- босма (график) ^ужжатларни беришни	-	х	-	х	-	х	х	х	х
- дастурни ва жараёнларни (топширикдар, масалалар)ишга туширишни (тугаллашни)		х		х		х	х	х	х

- субъект дастурларидан фойдаланишни (химояланувчи файллардан фойдаланиш, уларни яратиш ва йукртиш, алока линиялари ва каналлари оркали узатишни)				x		x	x	x	x
- субъект дастурлариданфойдаланишни (терминаллардан, ЭХМдан, ЭХМ тармоги узелларидан, алока каналларидан, ЭХМ ташки курилмаларидан, дастурли жилдлардан, катлоглардан, файллардан, кайдлар хршияларидан фойдаланишни)				x		x	x	x	x
- фойдаланувчи субъектлар ваколатларини узгартиришларни	-	-	-	-	-	-	x	x	x
- химояланувчи фойдаланиш объектнинг яратилишини	-	-	-	x	-	-	x	x	x
Ахборот элтувчиларини хисобга олиш	x	x	x	x	x	x	x	x	x
Оператив хотира ва ташки туплагичларни тозалаш	-	x	-	x	-	x	x	x	x
Химояни бузишга уринишни сигнализацияси	-	-	-	-	-	x	x	x	x
Криптографии цисм тизимига									
Конфиденциал ахборотни шифрлаш	-	-	-	-	-	-	x	x	x
Фойдаланишни турли субъектларига (субъектлар гурухига) тегишли ахборотни турли калитларда шифрлаш									x
Аттестациядан утган (сертификацияланган) криптографик воситалардан фойдаланиш								x	x
Яхликликни таъминловчи цисм тизимига									
Дастурий воситалар ва ишланувчи ахборотнинг яхлитлигини таъминлаш	x	x	x	x	x	x	x	x	x
Хисоблаш техникаси воситалари ва ахборот элтувчиларини куриклаш	x	x	x	x	x	x	x	x	x
Ахборот химояси маъмуриятининг (хизматининг) мавжудлиги	-	-	-	x	-	-	x	x	x
Ахборот химояси тизимини вакти-вакти билан тестлаш	x	x	X	x	x	x	x	x	x
Ахборот химояси тизимини тиклаш воситаларининг мавжудлиги	x	x	x	x	x	x	x	x	x
Сертификацияланган химоя воситаларидан фойдаланиш	-	x	-	x	-	-	x	x	x

Синфлар ахборот ишланиши хусусиятлари билан бир-биридан фаркланувчи учта гурухга булинади. Хдр бир гурух, ичида ахборотнинг кдйматлигига (конфиденциаллигига) богаик, хрлда химоя буйича талаблар иерархияси ва, демак, химояланиш синфлари сакланади. Хдр бир гурух, курсаткичларини, охиргисидан бошлаб куриб чикамиз.

Учинчи гурух, бир хил конфиденциаллик даражасига эга булган элтувчиларда жойлаштирилган барча ахборотдан фойдаланувчи бита фонда-

ланувчи ишлайдиган тизимлардан иборат. Гурухда иккита - ЗБ ва ЗА синфлари мавжуд.

Иккинчи гурух, х,ар хил конфиденциаллик даражасига эга булган ишланувчи ва/ёки элтувчиларда жойлаштирилган барча ахборотдан фойдаланишга бир хил хукукли фойдаланувчилари булган тизимлардан иборат. Гурухда иккита - 2Б ва 2А синфлари мавжуд.

Биринчи гурух, купчилик фойдаланувчи тизимлардан иборат булиб, уларда бир вактнинг узида конфиденциаллик даражаси турли ахборот ишланади ва/ёки сакданади. Гурухда бешта -1Д, 1Г, 1В, 1Б ва 1А синфлари мавжуд.

Умумий х,олда х,имоялаш тадбирлари 4 та кием тизимни уз ичига олади:

- фойдаланишни бошкариш;
- руйхатга ва хдеобга олиш;
- криптографик;
- яхлитликни таъминлаш.

Хисоблаш техникаси воситаларини рухсатсиз фойдаланишдан х,имояланиш курсаткичлари "Х,исоблаш техникаси воситалари. Ахборотни рухсатсиз фойдаланишдан хдмоялаш. Х,имоялаш курсаткичлари" деб аталувчи х,ужжатда келтирилган. Унда ахборотдан рухсатсиз фойдаланишдан х,имояланишнинг 7 синфи аникланган. Энг пастки синф - еттинчи, энг юкрри синф - биринчи. Хдр бир синф х,имояланиш талабларини олдингисидан мерос килиб олади. Химоянинг амалга оширилган моделлари ва уларни текшириш ишончлилигига боглик, х,олда синфлар туртта гурух,га ажратилади.

Биринчи гурухда фак,ат еттинчи синф булади (минимал х,имояланиш).

Иккинчи гурух, танланадиган х,имоя билан характерланиб олтинчи ва бешинчи синфларни уз ичига олади. Танланувчи х,имоя номма-ном айтилган объектларнинг тизимнинг номма-ном айтилган объектлардан фойдаланишни кузда тутади. Бунда х,ар бир "субъект-объект" жуфтлиги учун фойдаланишнинг рухсат этилган турлари аникданиши шарт. Фойдаланиш назорати х,ар бир объектга ва хдр бир субъектга кулланилади.

Учинчи гурух, мухтор хукукли х,имоя билан характерланиб, туртинчи, учинчи ва иккинчи синфларни уз ичига олади. Мухтор хукукли хдмоя тизимнинг хдр бир субъект ва объектига, унинг мое иерархиядаги урнини курсаатувчи туркумлаш белгисини бериш тизимдан фойдаланувчи ёки махсус ажратилган субъект томонидан амалга оширилади. Ушбу хукукга кирувчи синфлардан талаб килинадиган нарса-фойдаланишнинг диспетчерини (reference топког-хдволалар монитори) амалга оширилиши.

Фойдаланиш назорати барча объектларга нисбатан хдр кандай субъект томонидан очик, ва яширин фойдаланишда амалга оширилиши шарт. Фойдаланишга рухсат бериш факат танланадиган ва мухтор хукукли кридаларнинг биргаликда рухсати булгандагина амалга оширилиши мумкин.

Туртинчи гурух, тасдикланган хдмоя билан характерланиб факат биринчи синфни уз ичига олади.

Тизим хдмояланиш синфини олиши учун к,уйидагиларга эга булиши л озим:

- тизим буйича маъмур кулланмаси;
- фойдаланувчи к,улланмаси;
- тестлаш ва конструкторлик хужжатлар.

Юкррида куриб утилганидек, х,озирда компьютер жиноятчилиги жуда хдм турли-туман. Бу компьютердаги ахборотдан рухсатсиз фойдаланиш, дастурий таъминотга мантикий бомбаларни киритиш, компьютер вирусларини ишлаб чикиш ва тарк,атиш, компьютер ахборотини угирлаш, дастурий- хдсоб комплексларини ишлаб чик,ишда, к,уришда ва эксплуатациясида пала-партишлик.

Ахборот хавфеизлигининг бевосита таъминловчи, компьютер жиноятчилигининг олдини олувчи барча чораларни к,уйидагиларга ажратиш мумкин:

- хукукий;
- ташкилий-маъмурий;
- инженер-техник.

Хук,ук,ий чораларга компьютер жиноятчилиги учун жавобгарликни белгиловчи меъёрларни ишлаб чик,иш, дастурчиларнинг муаллифлик

хукукини хдмоялаш, жиноий ва фукаролик крнунчилигини хамда суд жараёнини такомиллаштириш киради. Уларга яна компьютер тизимларини яратувчи устидан жамоатчилик назорати масалалари хамда, агар компьютер тизимларининг битимга келган мамлакатларнинг харбий, иктисодий ва ижтимоий жихатларига таъсири булса, чеклашлар буйича мое х,алкаро шартномаларни кабул килиш киради. Факат охирги йилларда компьютер жиноятчиликларига хукукий кураш муаммолари буйича ишлар пайдо булди.

Ташкилий-маъмурий чораларга компьютер тизимларини куриклаш, ходимларни танлаш, махсус мухим ишларни бир киши томонидан бажарилиши х,олларига йул куймаслик, марказ ишдан чик,к,анида унинг ишга лаёкатлигини тиклаш режасининг мавжудлиги, барча фойдаланувчилардан (юк,ори рах,барлар х,ам бунга киради) химояланиш воситаларининг универсаллиги, марказ хавфеизлигини таъминлашга мутасадди шахсларга жавобгарликни юклаш, марказ жойланадиган жойни танлаш ва х,. киради.

Инженер-техник чораларга компьютер тизимидан рухсатсиз фойдаланишдан х,имоялашни, мух,им компьютер тизимларни резервлаш, угирлаш ва диверсиядан х,имояланишни таъминлаш резерв электр манбаи, хавфеизликнинг махсус дастурий ва аппарат воситаларини ишлаб чик,иш ва амалга ошириш ва х,. киради.

IV боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ХУК,УК,ИИ ВА ТАШКИЛИИ ТАЪМИНОТИ

4.1. Ахборот хавфсизлиги сохасида хукущш бошкариш

Ахборот хавфсизлигининг хукукий таъминоти - ахборотни химоялаш тизимида бажарилиши шарт булган крнун чикариш актлар, меъёрий-хукукий хужжатлар, кридалар йурикномалар, кулланмалар мажмуи. Хозирда ахборот хавфсизлигининг хукукий таъминоти масаласи хам амалий, хам крнунчилик жихатидан фаол урганиб чикилмокда.

Компьютер жиноятчиликларини к,илиш инструментлари сифатида телекоммуникация ва хисоблаш техникаси воситалари, дастурий таъминот ва интеллектуал билим ишлатилади. Компьютер жиноятчиликларини килиш сохаси сифатида нафакат компьютерлар, глобал ва корпоратив тармоклар (Interne tyintranet), балки ахборот технологиясининг замонавий, юкрри унумли воситалари хамда ахборотнинг ката хажми ишланадиган, масалан, статистик ва молия институтлари, танланади.

Шу сабабли, хар кандай ташкилот фаолиятини турли- туман ахборотни олиш учун кулда ёки хисоблаш техникаси воситалари ёрдамида ишлаш, ахборотни тахлиллаш натижасида кандайдир муйаян ечимларни олиш ва уларни алока каналлари оркали узатишсиз тасаввур этиб булмайди. Компьютерга хам тажовуз объекти, хам тажовуз килувчи инструмент сифатида караш мумкин. Агар компьютер фак,ат тажовуз обьекти булса, к,онун бузилишини мавжуд хукукий меъёрлар орк,али бахолаш мумкин. Агар компьютер факат инструмент булса «техник воситаларни к,уллаш» аломати етарли булади. Юк,оридаги тушунчаларни бирлаштириш мумкин - компьютер бир вактнинг узида х,ам инструмент ва хам объект. Хусусан бундай вазиятга машина ахборотининг угирланиши факти таалукди.

Агар ахборотнинг угирланиши моддий ва маънавий бойликларнинг йук,отилиши билан боглик, булса, бу факт жиноят сифатида бахрланади. Шунингдек агар ушбу факт билан миллий хавфсизлик, муаллифлик манфа-

атлари боглик, булса, жиноий жавобгарлик Узбекистан Республикаси конунларида бевосита кузда тутилган.

Хар кандай давлатда ахборот хавфсизлигининг хукукий таъминоти халкаро ва миллий хукукий меъёрларни уз ичига олади (4.1-раем)

4.1-расм. Ахборот хавфсизлигини таъминлашнинг хуцуций меъёрлар

Хукукий бошкариш предметлари куйидагилар.

- ахборот химоясининг хукукий режими;

- ахборотлаштириш жараёнларида крнуний муносабат катнашчиларининг хукукий макоми;

- субъектларнинг, уларнинг ахборот тузилмалари ва тизимлари ишлаши жараёнининг турли боск,ич ва сатхдаридан хук,ук,ий мак,омиини х,исобга олган хрлда, муносабатлари тартиби;

Ахборот хавфеизлиги буйича конунларни Узбекистон Республикаси бутун крнунлар тизимининг ажралмас к,исми сифатида тасаввур к,илиш мумкин, хусусан:

- таркибида ахборотлаштириш масалаларига дойр меъёрлар булган конституция к,онунлари;

- таркибида ахборотлаштириш масалаларига дойр меъёрлар булган умумий асосий крнунлар (мулк, ер ости бойликлари, ер, фукрролар хукуки, фукрролик, солик, хусусида);

- хужаликнинг алохида тузилмаларига, иктисодиётга, давлат органлари тизимига тегишли бошкариш ва уларнинг макрмини аниклаш буйича крнунлар. Бу крнунлар ахборот масалалари буйича алохида меъёрларни уз ичига олади;

- муносабатларнинг, хужалик сох,аларининг жараёнларнинг муайян мухитига бутунлай тегишли махсус крнунлар. Буларга ахборотлаштириш буйича крнунлар тааллукли;

- ахборотлаштириш сохасидаги к,онун талабларининг бажарилишини регламентловчи меъёрий хужжатлар;

- к,онунлар билан белгиланган ахборотлаштириш сох,асидаги меъёрий хужжатлар;

- таркибида ахборотлаштириш сохасида к,онун бузилишига жавобгарлик меъёрлари булган Узбекистон Республикасининг хук,ук,ни мух,офаза к,илиш крнунлари.

Компьютер тармокдари хавфсизлигини таъминловчи давлат хукукий механизмининг ривожланмаган шароитида корхонанинг давлат ва ходимлар жамоаси билан муносабатларни хукукий асосда ростловчи хужжатлари жиддий ахамиятга эга булади. Бундай мух,им хужжатлар таркибига куйидагиларни киритиш мумкин:

- корхона (фирма, банк) устави;

- жамоа шартномаси;

- жамоа ходимлари билан тузилган, тижорат сири булган маълумотлар химоясини таъминлаш буйича талабларга эга мехнат шартномалари;

- ишчи ва хизматчиларнинг ички мехнат тартиб к,оидалари;

- рахбарлар, мутахассислар ва хизмат курсатувчи ходимларнинг мансаб билан богланган мажбуриятлари.

4.2. Ахборот хавфсизлигининг ташкилий-маъмурий таъминоти

Ахборотни ишончли химоя механизмини яратишда ташкилий тадбирлар мухим рол уйнайди, чунки конфиденциал ахборотлардан рухсатсиз фойдаланиш асосан, техник жихатлар билан эмас, балки химоянинг элементар кридаларини эътиборга олмайдиган фойдаланувчилар ва ходимларнинг жиноятқорона харакатлари, бепарволиги, совукдонлиги ва маъсулиятсизлиги билан боглик,.

Ташкилий таъминот конфиденицал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий кийинчилик тугдирувчи ижрочиларнинг ишлаб-чикариш ва узаро муносабатларини меъёрий-хукукий асосида регламент - лашдир.

Ташкилий тадбирларга куйидагилар киради:

- хизматчи ва ишлаб чикариш бино ва хоналарни лойих,алашда, куришда ва жихрзлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий максади худудга ва хоналарга яширинча кириш имконини йукртиш; одамларнинг ва транспортнинг юриши назоратининг кулайлигини таъминлаш; фойдаланишнинг алох,ида тизимига эга булган ишлаб-чикариш зоналарини яратиш ва х,.;

- ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбир ларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш кридалари билан ишлашни ургатиш, ахборот химояси к,оидасини бузганлиги учун жавобгарлик даражаси ва х,. билан таништириш киради;

- ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил к,илиш;

- хона ва худудларни ишончли к,урикдаш;

- хужжатлар ва конфиденциал ахборот элтувчиларини сакдаш ва ишлатиш, шу жумладан к,айд этиш, бериш, бажариш ва кайтариш тартибларига риоя килиш;

- ахборот х,имоясини ташкил этиш, яъни муайян ишлаб чикариш жамоаларида ахборот хавфсизлигига жавобгар шахсни тайинлаш, конфиденциал ахборот билан ишловчи ходимлар ишини мунтазам текшириб туриш.

Бундай тадбирлар хар бир муайян ташкилот учун узига хос хусусиятга эга булади.

Ташкилий тадбирларнинг талайгина кисмини ходимлар билан ишлаш эгаллайди. Мулкчиликнинг турли шаклларига эга булган корхона ходимлари билан ишлашда ташкилий тадбирлар, умумий хрлда куйидагиларни уз ичига олади:

- ишга кабул килишда сухбат. Сухбат натижасида номзоднинг мое буш жойга кабул килиниши максадга мувофиклиги аникланади;
- муайян корхонада конфиденциал ахборот билан ишлаш кридалари ва муолажалари билан танишиш; ишга кабул килинувчи корхона тижорат сирларини саклаши буйича тилхат ва фирма сирларини ошкор килмасликка ваъда беради;
- ходимларни конфиденциал ахборот билан ишлаш кридалари ва муолажаларига укитиш. Ходимларни укитишда нафакат ишлаб-чикариш куникмаларига эга булиш ва уларни юкрри даражада саклаш, балки уларни саноат (ишлаб чикариш) махфийлиги ахборот хавфеизлиги, интеллектуал мулк ва тижорат сирлари химояси талабларини бажариш зарурлигига катъий ишонч рух,ида тарбиялаш кузда тутилади. Мунтазам ук,итиш рахбарият ва ходимларнинг корхона тижорат манфаатларини химоя к,илиш масалалари буйича билимдонлик даражасини ошишига имкон яратади;
- ишдан бушаётганлар билан сух,бат. Сухбат давомида ишдан бушаётган ходимнинг фирма сирларини фош килмасликка катъий ваъда бериши лозимлиги таъкидланади ва бу ваъда, одатда, тилхат орк,али расмийлаштирради.

Тадбирларнинг мух,им йуналишларидан бири иш юритиш ва хужжат юритиш тизимини пухта ташкил этиш хисобланади. Бу эса уз иш юритиш тартибини, хужжатларни кайдлаш, ишлаш, сакдаш, йукртиш ва мавжудлигини хамда тугри бажарилишини назорат килишни таъминлайди. Тизимни амалга оширишда хужжатлар хавфеизлигига ва ахборот конфиденциаллигига алох,ида эътибор бериш лозим.

Ахборотни хужжатлаштириш катъий белгиланган к,оидалар ёрдамида амалга оширилади. Бу к,оидаларнинг асосийлари ГОСТ 6.38-90 "Ташкилий-

бошкарувчи хужжатлар тизими. Хужжатларни расмийлаштиришга талаблар", ГОСТ 6.10.4-84 "Унификацияланган хужжатлар тизими. Хисоблаш техника воситалари оркали яратилувчи машина элтувчиларидаги ва машинограммалардаги хужжатларга хукукий куч бериш" кабилар баён этилган. Бу ГОСТларда ахборотга хужжат хукукини берувчи 31 та реквизитлар кузда тутилган, аммо бу реквизитларнинг барчасининг хужжатда мавжудлиги шарт эмас. Асосий реквизит - матн. Шу сабабли, хар кандай равон баён этилган матн хужжат хисобланади ва унга хукукий куч бериш учун сана ва имзо каби мухим реквизитларнинг мавжудлиги кифоя.

Автоматлаштирилган ахборот тизимларидан олинган хужжатлар учун алохида тартиб кулланилади. Бунда, маълум холларда, масофадан олинган ахборот электрон имзо билан тасдикланади. Ахборотни химоялаш учун барча ташкилий тадбирларни таъминловчи махсус маъмурий хизматни яратиш талаб килинади. Унинг штат тузилмаси, сони ва таркиби фирманинг реал эхтиёжлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий хрлати оркали аникданади.

Маъмурий тадбирларга куйидагилар киради:

- операцион тизимнинг тугри конфигурациясини мададлаш;
- иш журналларининг назорати;
- пароллар алмашишининг назорати;
- химоя тизимида "рахна"ларни аникдаш;
- ахборотни химояловчи воситаларни тестлаш.

Тармок, операцион тизимининг тугри конфигурациясини мададлаш масаласини, одатда, тизим маъмури х,ал этади. Маъмур операцион тизим (одамлар эмас) риоя килиши лозим булган маълум кридаларни яратади. Тизимни маъмурлаш - конфигурация файлларини тугри тузишдир. Бу файлларда (улар бир нечта булиши мумкин, масалан тизимнинг х,ар бир кисмига биттадан файл) тизим ишлаши кридаларининг тавсифи булади.

Хавфсизлик маъмури компьютер тармоги х,олатини оператив тарзда (тармок, компьютерлари химояланиши холатини кузатиш оркали) ва оператив булмаган тарзда (ахборот х,имояси тизимидаги вокеаларни к,айдловчи журналларни тахлиллаш орк,али) назоратлаш лозим. Ишчи станциялар со-

нининг ошиши ва турли-туман компонентлари булган дастурий воситаларнинг ишлатилиши ахборот химояси тизимидаги ходисаларни кайдлаш журналлар хажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар хажми шунчалик ошиб кетиши мумкинки, маъмур улар таркибини жоиз вакт мобайнида тахдиллай олмайди.

Тизим заифлигининг сабаби шундаки, биринчидан, фойдаланувчини аутентификациялаш тизими фойдаланувчи исмига ва унинг паролига (куз туридан фойдаланиш каби экзотик хрлллар бундан мустасно), иккинчидан, фойдаланувчи тизимида тизимни маъмурлаш хукуки берилган супервизорнинг (supervisor) мавжудлигига асосланади. Супервизор паролини саклаш режимининг бузилиши бутун тизимдан рухсатсиз фойдаланиш имконини яратади.

Ундан ташкари бундай кридаларга асосланган тизим-статик, кртиб крлган тизим. У факат катъий маълум хужумларга карши тура олиши мумкин. Олдиндан кузда тутилмаган кандайдир янги тахдиднинг пайдо булишида тармок, хужуми нафакат муваффакиятли, балки тизим учун куринмайдиган булиши мумкин. Шунинг учун, муассасада ишлатилувчи ахборотнинг кайсиси х,имояга мух,тож эканлигини аник, тасаввур к,илиш мух,им х,исобланади. Мавжуд ахборотни тахлиллашдан бошлаш лозим. Бу муолажалар ахборот х,имоясини таъминлаш буйича тадбирларни дифференциаллаш имконини беради ва натижада, сарф-харажатларнинг к,иск,аришига сабаб булади.

Ахборот х,имояси тизимини эксплуатация килиш боск,ичида хавфсизлик маъмурининг фаолияти фойдаланувчилар ваколатларини уз вактида узгартиришдан х,амда тармок, компьютерларидаги х,имоя механизмларини созлашдан иборат булади. Фойдаланувчилар ваколатларини ва компьютер тармокларида ахборотни химоялаш тизимини созлашни бошк,ариш муаммоси, масалан, тармокдан марказлаштирилган фойдаланиш тизимидан фойдаланиш асосида х,ал этилиши мумкин. Бундай тизимни амалга оширишда тармок, асосий серверида ишловчи махсус фойдаланишни бошк,арувчи сервердан фойдаланилади. Бу сервер марказий х,имоя маълумотлари базасини локал х,имоя маълумотлари базаси билан автоматик тарзда синхронлайди.

Фойдаланишни бошкаришнинг бу тизимида фойдаланувчи ваколати вакти-вакти билан узгартирилади ва марказий химоя маълумотлари базасига киритилади, уларнинг муайян компьютерларда узгариши навбатдаги синхронлаш сеансида вактида амалга оширилади.

Ундан ташкари фойдаланувчи паролини ишчи станцияларининг бирида узгартирса, унинг янги пароли марказий химоя маълумотлари базасида автоматик тарзда аксланади, хамда бу фойдаланувчи ишлашига рухсат берилган ишчи станцияларга узатилади.

4.3. Ахборот хавфсизлиги буйича стандартлар ва спецификациялар

Ахборот хавфсизлиги сохасида мутахассислар уз фаолиятларида мое стандартлар ва снецификацияларни четлаб уташолмайдилар. Бунга сабаб, биринчидан стандартлар ва спецификациялар - аввало ахборот хавфеизлигининг муолажавий ва дастурий-техник даражалари буйича билимларини туплаш шаклларидан бири. Уларда малакали мутахассислар томонидан ишлаб чикилган, тасдикданган юкрри сифатли ечимлар ва методологиялар кайд этилган. Иккинчидан, стандартлар ва спецификациялар аппарат-дастурий тизимлар ва уларнинг компонентларининг узаро кушила олишлигини таъминловчи асосий восита хисобланади. (Intemet-уюшмада бу восита хакикатдан самарали ишламокда).

Стандартлар ва спецификацияларнинг бир-биридан жиддий фаркланувчи иккита гурухини ажратиш мумкин:

- ахборот тизимларини ва хавфеизлик талаблари буйича химоя воситаларини бахрлаш ва туркумлаш учун аталган бахолаш стандартлари;
- химоя воситалари ва усулларини амалга ошириш ва улардан фойдаланишнинг турли жихатларини регламентловчи спецификациялар.

Бу гурухлар маълумки, ихтилофга бормайдилар, балки бир-бирини тулирадилар. Бахрлаш стандартлари ташкилий ва архитектуравий спецификациялар вазифасини утаган холда ахборот тизимларининг ахборот хавфсизлиги нуктаи назаридан мухим булган тушунчалари ва жихатларини тавсифлайди. Спецификациялар эса архитектура белгилаган ахборот тизи-

мини кандай курит лозимлигини ва ташкилий талабларни кандай крндирилишини аниклайди.

Халкаро эътирофни крзонган ва ахборот хавфсизлиги сохасида кейинги ишланмаларда жуда кучли таъсир курсатган биринчи бахолаш стандарта АКД1 мудофаа вазирлигининг *«Туксарик кшпоб»* (мукрванинг ранги буйича) деб аталувчи «Ишончли компьютер тизимларини бахолаш мезонлари» (Department of Defeuse Trusted Computer System Evaliation Criteria, TCSEC) стандарта булди. Муболагасиз тасдикдаш мумкинки, «Туксарик, китоб»и ахборот хавфсизлигининг тушунчалар негизини ифодалайди. Ундаги тушунчаларнинг санаб утишнинг узи етарли: *хавфсиз ва ишончли тизимлар, хавфсизлик сиёсати, кафолатлик даражаси, хисоб-китоблилиги, ишончли хисоблаш асоси, мурожаатлар монитори, хавфсизликнинг ядроси ва периметри.*

«Туксарик китоб»дан сунг чикарилган хужжатлардан бири *«Туксарик китоб»нинг тармок конфигурациялари учун изохи»* (Trusted Network Interpretation) энг мухим хужжат хисобланади. Бу хужжат икки кисмдан иборат. Биринчи кием изохнинг узига багишланган булса, иккинчи кисмида узига хос ёки тармок, конфигурациялари учун айникса мух,им булган *хавфсизлик сервислари* тавсифланади. Биринчи киемга киритилган энг мухим тушунчалардан бири - тармокдаги ишончли хисоблаш асоси. Мухим жихат-тармок, конфигурацияларининг динамиклиги. Химоялаш механизмлари орасида *конфиденциалликлик* ва *яхлитликни* таъминловчи *криптография* ажратилган. Фойдаланувчанлик масалалари, уни таъминлашдаги архитектуравий принципларнинг шакллантирилиши уз вакти учун тартибли ёндашиши булди.

Так,симланган ахборот тизимларини обьектга мулжалланган тарзда коммуникацияларни криптографик х,имоялаш билан биргаликда декомпозициялашнинг назарий асосини - мурожаатлар мониторини фрагментлашнинг корректлиги шартининг етарлилигини айтиб утиш лозим.

Бахрлаш стандартларидан яна бири *«Европа мамлакатларининг уйгунлаштирилган мезонлари»ш* ахборот тизими ишлаши лозим булган шароитларга априор шартлар йук,. Фараз килинадики, аввал бахрлаш максади ифодаланади, сунгра сертификациялаш органи бу максадга

кднчалик тулик, эришилишини, яъни, муайян вазиятда хавфсизликнинг архитектураси ва амалга оширилиши механизмларининг канчалик корректлигини ва самаралилигини аниклайди. Бахрлаш максадини ифодалашни енгиллаштириш ниятида стандартда хукумат ва тижорат тизимларига хос функционналликнинг унта тахминий синфлари тавсифланган.

Ушбу стандартда ахборот технологиялар тизимлари ва махсулотлари уртасидаги фарк, таъкидланади, аммо талабларини унификациялаш ниятида ягона - *бахолаш объекты* тушунчаси киритилади. Стандартда хавфсизлик функциялари (сервислари) ва уларни амалга оширувчи механизмлар орасида фаркнинг курсатилиши хамда кафолатланишнинг икки жихати - хавфсизлик воситаларининг *самарадорлиги* ва *корректлигининг* ажратилиши мухим хисобланади. Бахрлаш стандартлари гурухига ахборот хавфсизлигининг муайян, аммо мухим ва мураккаб жихатини регламентловчи АКД1нинг *«Криптографии модуллар учун хавфсизлик талаблари"* Федерал стандарта хамда *«Ахборот технологиялар хавфсизлигини бахоловчи мезонлар»* халкаро стандарти тааллукли.

Техник спецификациялар орасида биринчи урингa, сузсиз, Х800 «Очик тизимлар узаро х,аракати учун хавфсизлик архитектураси» хужжатини куйиш лозим. Бу хужжатда хавфсизликнинг энг мухим тармок, сервислари ажратилган: *аутентификация, фойдаланишни боигкарииг,* маълумотларни конфиденциаллиги ва ёки яхлитлигини таъминлаш, х,амда к,илинган х,аракатдан *тонишнинг мумкин эмаслиги.* Сервисларни амалга ошириш учун хавфсизликнинг куйидаги тармок, механизмлари ва уларнинг комбинациялари кузда тутилган: *шифрлаш, электрон ракамли имзо,* фойдаланишни бошкариш, маълумотлар яхлитлигининг назорати, аутентификация, *трафикни тулдириш, маршрутлашни боигкарииг, нотаризация.* Хавфсизликнинг сервислари ва механизмлари амалга оширилувчи етти сатхди эталон моделининг сатхдари танланган. Нихоят, таксимланган конфигурациялар учун хавфсизлик воситаларининг маъмурлаш масалалари батафсил куриб чикилган.

Internet - уюшманинг RFC 1510 «Аутентификациянинг тармок, сервери Kerberos (VS)» спецификацияси хусусий, аммо мухим ва долзарб му-

аммога турли таксимланган мухитда тармоккд ягона кириш концепциясини мададдаган хрлда аутентификациялашга тегишли.

Kerberos аутентификациялаш сервери ишончли учинчи тараф булиб, хизмат курсатилувчи субьектларнинг махфий калитларига эга ва уларга хакикийликнинг жуфтлашиб текширишда ёрдам беради. KerberosHmrr мижоз компонентларининг аксарият замонавий операцион тизимларда мавжудлиги унинг канчалик мухим эканлигидан далолат беради.

IPsec техник спецификацияси тармок, сатх,ида конфиденциаллик ва яхлитлик воситаларининг тулик, тупламини тавсифланган хрлда, муболагасиз фундаментал ахамиятга эга. IPsec асосида юкррирок, сатх, (татбикий сатхга кадар) протоколларини химоялаш механизми хамда хавфсизликнинг тугалланган воситалари, хусусан вертуал хусусий тармокдар курилади. Албатта IPsec криптографик механизмларига ва калит инфратузилмаларига таянади.

Транспорт сатхи хавфсизлиги ва сигналлари (Transport Layer Security, TLS) хам шундай характерланади. TLS спецификацияси турли вазифаларни бажарувчи купгина дастурий махсулотларда ишлатилувчи оммавий Secure Socket Layer (SSL) протоколини ривожлантиради ва ойдинлаштиради.

Юкррида эслатиб утилган инфратузилма нуктаи назаридан X.500 *«Директория хизмати:* концепциялар, моделлар ва серверлар обзори» (The Directory: Overview of consepts, models and services) ва X.509 *«Директория хизмати: сертификатлар, очик калитлар ва атрибутлар каркаслари»* (The Directory: Pubbic-key and attributc sertificate framworks) тавсиялари жуда мухим хисобланади. X.509 тавсияларида очик, калитлар ва атрибутлар яъни очик, калитлар инфратузилмаси ва имтиёзларни бошкаришнинг базавий элементлари сертификатларининг формати тавсифланган.

Маълумки, ахборот хавфеизлигини таъминлаш компелкс муаммо булиб, крнуний, маъмурий, муолажавий ва дастурий-техник сатхдарда чораларни келишилган хрлда куришни талаб этади.

Маъмурий сатхнинг базавий хужжати ташкилот *хавфсизлиги сиёсатини* ишлаб чикишда ва амалга оширишда Internet - уюшманинг «Ташкилот ахборот хавфсизлиги буйича кулланма»си (Site Security Handbook)

наъмунали кумакчи вазифасини уташи мумкин. Унда хавфсизлик сиёсати муолажаларини шакллантирилишининг амалий жихатлари ёритилади, маъмурий ва муолажавий сатхдарнинг асосий тушунчалари изохланади, тавсия этувчи харакатларнинг сабаблари курсатилганган, хавф-хатарлар тахлили, ахборот хавфсизлигининг бузилишига муносабат ва бузилиш бартараф этилганидан кейинги харакат мавзуларига тухтаб утилган.

«Ахборот химояси бузилишига кандай муносабат билдириш лозим» (Expections for Computer Security Incident Response) тавсиясида юкррида келтирилган масалалардан ташкари фойдали ахборот ресурсларига хаволаларни хамда муолажавий даражадаги амалий маслахатларни топиш мумкин.

Корпоратив ахборот тизимини ривожлантиришда ва кайта тузишда *«Internet-хизмат билан таъминловчини* кандай танлаш лозим» (Site Security Handbook Addendum for ISPs) тавсияси сузсиз фойдалидир. Биринчи галда унинг кридаларига ташкилий ва архитектуравий химоялашни шакллантириш жараёнида риоя килиш лозим.

Британия стандарти BS 7799 «Ахборот хавфсизлигини бошкариш. Амалий кридалар» (Code of practice for information security managment) ахборот хавфсизлигига жавобгар ташкилот рахбарлари учун фойдали хисобланади. Бу стандарт жиддий узгартиришсиз КОЛЕС 17799 халкаро стандартга кучирилган.

Бу борада мустакил диёримиз Узбекистан Республикасида ахамиятга молик булган улкан ишлар олиб борилмокда. Бунга мисол тарикасида Узбекистан алока ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадкикртлари маркази томонидан ишлаб чикилган O'z DSt 1092:2005 "Ахборот технологияси. Маълумотларни криптографик мух,офазаси. Электрон рак,амли имзони шакллантириш ва текшириш жараёнлари", O'z DSt 1105:2006 "Ахборот технологияси. Маълумотларни криптографик мухрфазаси. Маълумотларни шифрлаш алгоритми", O'z DSt 1106:2006 "Ахборот технологияси. Маълумотларни криптографик мухрфазаси. Хешлаш функцияси" ва O'z DSt 1108:2006 "Ахборот технологияси. Очик, тизимлар узаро богликдиги. Электрон ракамли имзо очик, калити сертификати ва атрибут сертификатининг тузилмаси" стандартларини

ва RH 45-187:2006 «Хавфсизлик талаблари» бошкарув хужжатини курсатиб утиш мумкин. Ушбу марказ томонидан ишлаб чикилган стандартлар №05-11 12.04.2006 йилда Узбекистан стандартлаштириш, метрология ва сертификациялаш агентлиги томонидан тасдикданган.

Бундан ташкари юртимизда ахборот хавфсизлиги сохасида фаолият юритаётган Узбекистан алока ва ахборотлаштириш агентлиги кршидаги "Илмий-техник ва маркетинг тадкикотлари маркази", «Uzlnfocom» ва бошка ташкилотларни айтиб утиш мак,садга мувофик,. Чунки бу ташкилотларнинг юртимиз равнаки учун кушаётган хиссаси катта ахамиятга эга.

V боб. АХБОРОТНИ ХДМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ

5.1. Криптографиянинг асосий коидапари ва таърифлари

Ахборотнинг хдмоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. *Ахборотни шифрлаш* деганда очик, ахборотни (дастлабки матнни) шифрланган ахборотга узгартириш (шифрлаш) ва аксинча (расшифровка килиш) жараёни тушунилади. Шифрлаш криптотизимининг умумлаштирилган схемаси 5.1-расмда келтирилган.

5.1-расм. Шифрлаш криптотизимининг умумлаштирилган схемаси.

Узатилувчи ахборот матни М криптографик узгартириш $E_{к1}$ ёрдамида шифрланади, натижада шифрматн *С* олинади:

$$C = E_{k1}(M)$$

бу ерда *к* — шифрлаш калити деб аталувчи *Е* функциянинг параметри.

Шифрлаш калити ёрдамида шифрлаш натижаларини узгартириш мумкин. Шифрлаш калити муайян фойдаланувчига ёки фойдаланувчилар гурух,ига тегишли ва улар учуй ягона булиши мумкин. Муайян калит ёрдамида шифрланган ахборот факат ушбу калит эгаси (ёки эгалари) томонидан расшифровка килиниши мумкин.

Ахборотни тескари узгартириш куйидаги куринишга эга:

$$M' = D_{k2}(C)$$

D функцияси *Е* функцияга нисбатан тескари функция булиб, шифр матнни расшифровка килади. Бу функция х,ам *kl* калит куринишидаги к,ушимча параметрга эга. *к* ва *к2* калитлар бир маъноли мосликка эга

булишлари шарт. Бу хрлда расшифровка килинган М' ахборот Мга эквивалент булади. *к2* калити ишончли булмаса *D* функция ёрдамида *М'=М* дастлабки матнни олиб булмайди.

Криптотизимларнинг иккита синфи фаркланади:

- симметрик криптотизим (бир калитли);
- асимметрик криптотизим (иккита калитли).

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка килиш учун битта калитнинг узи ишлатилади. Демак, шифрлаш калитидан фойдаланиш хукукига эга булган хар кандай одам ахборотни расшифровка килиши мумкин. Шу сабабли, симметрик криптотизимлар махфий калитли криптотизимлар деб юритилади. Яъни шифрлаш калитидан факат ахборот аталган одамгина фойдалана олиши мумкин. Шифрлашнинг симметрик криптотизими схемаси 5.2-расмда келтирилган.

5.2-расм. Симметрик шифрлаш криптотизимининг схемаси.

Электрон хужжатларни узатишнинг конфиденциаллигини симметрик криптотизим ёрдамида таъминлаш масаласи шифрлаш калити конфиденциаллигини таъминлашга келтирилади. Одатда, шифрлаш калити маълумотлар файли ва массивидан иборат булади ва шахсий калит элтувчисидан масалан, дискетда ёки смарт-картада сакланади. Шахсий калит элтувчиси эгасидан бошка одамларнинг фойдаланишига к,арши чоралар курилиши шарт.

Симметрик шифрлаш ахборотни "узи учун", масалан, эгаси йуклигида ундан рухсатсиз фойдаланишни олдини олиш мак,садида, шифрлашда жуда кулай хисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантик,ий ёки физик дискларни шаффоф(автоматик) шифрлаш булиши мумкин.

Симметрик шифрлашнинг нокулайлиги - ахборот алмашинуви бошланмасдан олдин барча адресатлар билан махфий калитлар билан айирбошлаш заруриятидир. Симметрик криптотизимда махфий калитни алоканинг умумфойдаланувчи каналлари оркали узатиш мумкин эмас. Махфий калит жунатувчига ва кабул килувчига калитлар таркатилувчи химояланган каналлар орк,али узатилиши керак.

Симметрик шифрлаш алгоритмининг маълумотларни абонентли шифрлашда, яъни шифрланган ахборотни абонентга, масалан Internet оркали, узатишда амалга оширилган вариантлари мавжуд. Бундай криптографик тармокнинг барча абонентлари учуй бита калитнинг ишлатилиши хавфсизлик нуктаи назаридан ножоиздир. Хакикатан, калит обрусизлантирилганда (йукртилганида, угирлатилганда) барча абонентларнинг хужжат алмашиши хавф остида крлади. Бу х,олда калитларнинг матрицаси (5.3-расм) ишлатилиши мумкин.

1	**кП**	**k12**	КО		**k1n**
2	**$k_2$1**	$К_2$Г	k_{23}		**$К_{2П}$**
3	**$k_{з}$1**	КЗГ	КЗЗ		**k_{3n}**

1-абонент учун калитлар туплами

2- абонент учун калитлар туплами

3- абонент учун калитлар туплами

п- абонент учун калитлар туплами

5.3-расм. Калитларматрицаси

Калитлар матрщаси абонентларнинг жуфт-жуфт богаанишли жадвалидан иборат. Жадвалнинг хар бир элементи / ва *j* абонентларни боглашга мулжалланган ва ундан фак,ат ушбу абонентлар фойдалана оладилар. Мое х,олда, калитлар матрицаси элементлари учун куйидаги тенглик уринли.

к,,1	**$К_{,,2}$**	$К_{,,3}$		**knn**

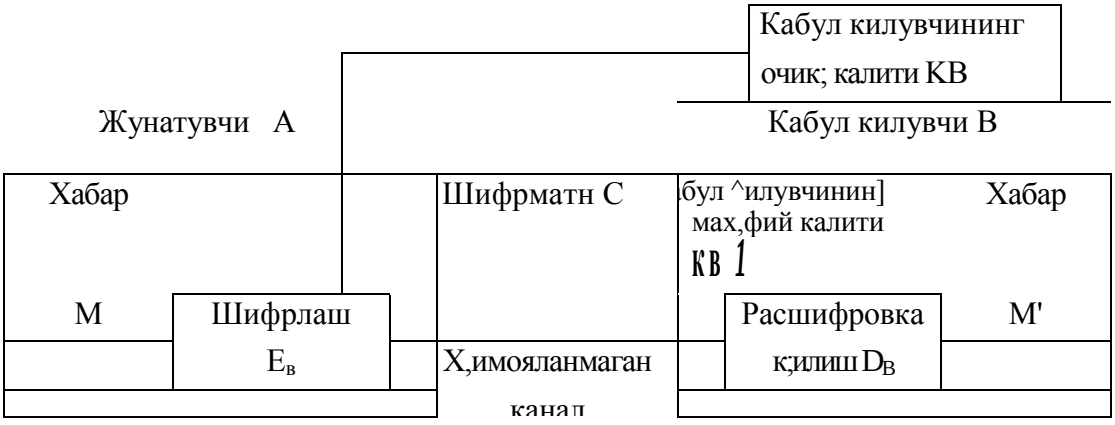
Матрицанинг хар бир /- катори муайян / абонентнинг крлган *N-1* абонентлар билан богланишини таъминловчи калитлар тупламидан иборат. Калитлар туплами (тармок, тупламлари) криптографик тармокнинг барча абонентлари уртасида таксимланади. Таксимлаш алоканинг *химояланган каналлари* орк,али ёки кулдан-кулга тарзда амалга оширилади.

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка килишда турли калитлардан фойдаланилади:

- *очик калит К* ахборотни шифрлашда ишлатилади, махфий калит *к* дан хисоблаб чикарилади;
- *махфий калит к,* унинг жуфти булган очик, калит ёрдамида шифрланган ахборотни расшифровка килишда ишлатилади.

Махфий ва очик, калитлар жуфт-жуфт генерацияланади. Махфий калит эгасида крлиши ва уни рухсатсиз фойдаланишдан ишончли химоялаш зарур (симметрик алгоритмдаги шифрлаш калитига ухшаб). Очик, калитнинг нусхалари махфий калит эгаси ахборот алмашинадиган криптографик тармок, абонентларининг хар бирида булиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 5.4-расмда келтирилган.



5.*4-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.*

Асимметрик криптотизимда шифрланган ахборотни узатиш куйидагича амалга оширилади: 1. Тайёргарлик боскичи:

- абонент *В* жуфт калитни генерациялайди: махфий калит $к_в$ ва очик, калит $К_в$;

- очик, калит $K_в$ абонент *A* га ва крлган абонентларга жунатилади.

2. А ва *B* абонентлар уртасида ахборот алмашиш:

- абонент *A* абонент 5нинг очик, калити $K_в$ ёрдамида ахборотни шифрлайди ва шифрматнни абонент 5га жунатади;
- абонент *B* узининг махфий калити k_B ёрдамида ахборотни расшифровка килади. Х,еч ким (шу жумладан абонент *A* хам) ушбу ахборотни расшиф ровка килаолмайди, чунки абонент 5нинг махфий калити унда йук,.

Асимметрик криптотизимда ахборотни химоялаш ахборот кабул килувчи калити k_B нинг махфийлигига асосланган.

Асимметрик криптотизимларнинг асосий хусусиятлари куйидагилар:

1. Очик, калитни ва шифр матнни химояланган канал оркали жунатиш мумкин, яъни нияти бузук, одамга улар маълум булиши мумкин.
2. Шифрлаш $E_в$*: M -> C* ва расшифровка килиш D_B*: C -> M* алгоритмлари очик,.

5.2. Симметрии шифрлаш тизими

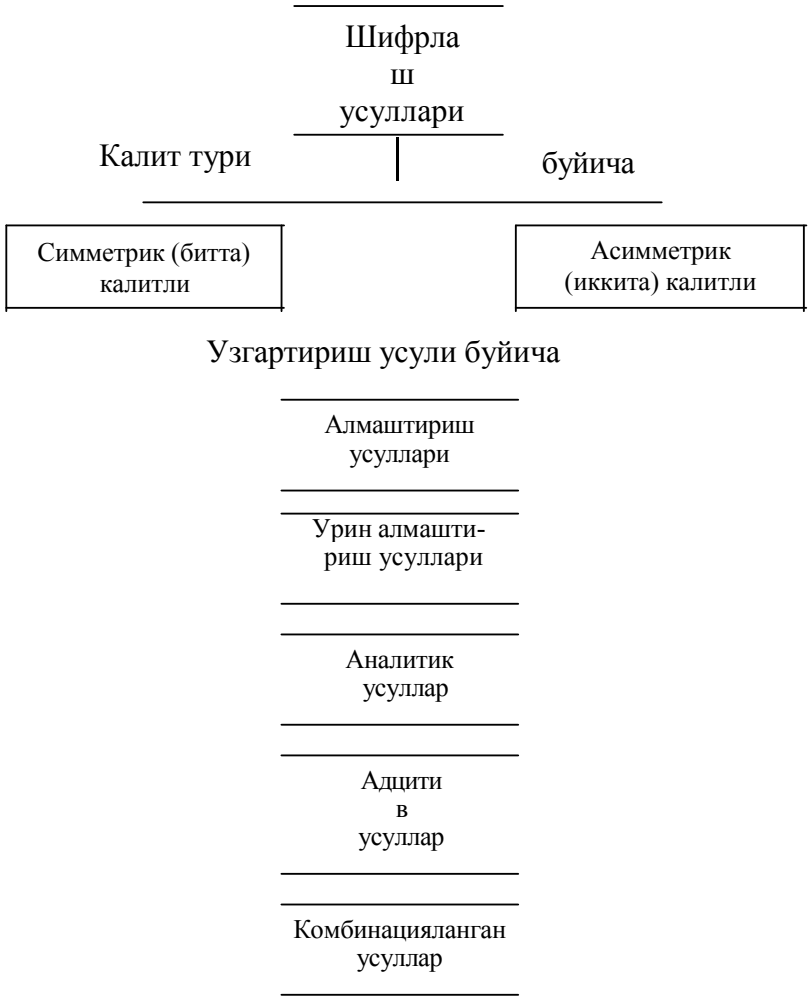
Шифрлаш усуллари турли аломатлари буйича туркумланиши мумкин. Туркумланиш вариантларидан бири 5.5-расмда келтирилган.

Алмаштириш усуллари. Алмаштириш (подстановка) усулларининг мох,ияти бир алфавитда ёзилган ахборот символларини бошка алфавит символлари билан маълум крида буйича алмаштиришдан иборатдир. Энг содда усул сифатида ***турридан туFри алмаштиришни*** курсатиш мумкин. Дастлабки ахборот ёзилувчи A_o алфавитнинг % символларига шифрловчи A_j алфавитнинг s_n символлари мое куйилади. Оддий хрлда иккала алфавит х,ам бир хил символлар тупламига эга булиши мумкин.

Иккала алфавитдаги символлар уртасидаги мослик маълум алгоритм буйича К символлар узунлигига эга булган дастлабки матн T_o символларининг рак,амли эквивалентларини узгартириш орк,али амалга оширилади.

Моноалфаеитли алмаштириш алгоритми к,уйидаги к,адамлар кетма-кетлиги куринишда ифодаланиши мумкин

l-кадам. [lxR] улчамли дастлабки A_o алфавитдаги хдр бир символ s_0 G $T(i=l,K)$ ни A_o алфавитдаги s_{Oi} символ тартиб ракамига мое келувчи $h_{Oi}(s_{Oi})$ сонга алмаштириш йули билан ракамлар кетма-кетлиги L_{Oh} ни шакллантириш.



5.5-расм. Шифрлаш усулларининг туркумланиши.

2-кддам. L_{Oh} кетма-кетлигининг хдр бир сонини $h_{li}=(k_1xh_{Oi}(s_{Oj})+k_2)(modR)$ формула оркали х,исобланувчи L_{lh} кетма-кетликнинг мое сони h_n га алмаштириш йули билан L_{lh} сон кетма-кетлигини шакллантириш, бу ер-да k_rунлик коэффицент; А:$_2$-силжитиш коэффициенти. Танланган κ_p κ_2 коэффицентлар h_{Oi}, h_n сонларнинг бир маъноли мослигини таъминлаши лозим, $h_n=0$ олинганида эса $h_n=R$ алмашинуви бажарилиши керак.

3-к,адам. L_{lh} кетма-кетликнинг х,ар бир сони $h_n(s_n)mi$ [lxR] улчамли шифрлаш алфавитнинг мое s_n G $T_1\{i=\,K)$ символи билан алмаштириш йули билан Tj шифрматнни х,осил к,илиш.

4-кадам. Олинган шифрматн узгармас *Ь* узунликдаги блокларга ажратилади. Агар охирги блок тулик, булмаса блок оркасига махсус символтулдирувчилар жойлаштирилади(масалан, *).

Мисол. Шифрлаш учун дастлабки маълумотлар куйидагилар:

$Г_0$=<ХИМОЯ_ХИЗМАТИ>

$А_0$=<АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУК;ГХ_>

А,=<ОРЁЬЯТЭ-ЖМЧХАВДЙФК;КСЕЗПИЦГХЛЪШБУЮ кгн>

R=36; k1=3; k_2=15; b=4

Алгоритмнинг кадамба-кадам бажарилиши куйидаги натижаларни олинишига олиб келади.

Ькадш^$_{o/}$=<35,10,14,16,31,36,23,10,9,14,1,20,10>

,21,17,36,14,12,9,6,21,18,3,9>

3-кадам. 7><ХЖЕФНВХЖТЕК;ЁЖ>

4-кадам. 7><ХЖЕФ НВХЖ ТЕКЁ Ж***>

Расшифровка килишда блоклар бирлаштирилиб *К* символли шифрматн T_1 х,осил к,илинади. Расшифровка килиш учун к,уйидаги бутун сонли тенгламани ечиш л озим:

$$k_1h_{01}+k_2=nR+h_{1i}$$

$к_р$ $к_2$, h_n ва *R* бутун сонлар маълум булганда h_{Oi} катталиги п ни сара-лаш оркали х,исобланади. Бу муолажани шифрматннинг барча символларига тадбик, К.ИЛИШ унинг расшифровка килинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристкаларининг бир хиллигидир. Дастлабки матн к,айси тилда ёзилганлигини билган криптоаналитик ушлаб к,олинган ахборотларни статистик ишлаб, иккала алфавитдаги символлар уртасидаги мувофикдикни аникдаши мумкин.

Полиалфавитли алмаштириш усуллари айтарлича юкрри криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришни куйидагича тасаввур этиш мумкин. ^V-алфавитли алмаштиришда дастлабки $А_о$ алфавитдаги s_{01} символи $А_1$ алфавитдаги s_n символи

билан алмаштирилади ва х,. S_{0N} ни S_{NN} символ билан алмаштирилганидан сунг $SQ_{(N+1)}$ СИМВОЛНИНГ урнини Aj алфавитдаги $S_{1(N+1)}$ символ олади ва х,.

Полиалфавитли алмаштириш алгоритмлари ичида ***Вижинер жадеали (матрицаси)*** $T_в$ ни ишлатувчи алгоритм энг кенг таркалган. Вижинер жадвали *[RxR]* улчамли квадрат матрицадан иборат булиб, (*Я*-ишлатилаётган алфавитдаги символлар сони) биринчи каторида символлар алфавит тартибида жойлаштирилади. Иккинчи катордан бошлаб символлар чапга битта уринга силжитилган х,олда ёзилади. Сикиб чик,арилган символлар унг тарафдаги бушаган уринни тулдиради (циклик силжитиш). Агар узбек алфавита ишлатилса, Вижинер матрицаси [36х36] улчамга эга булади (5.5-расм).

АБВГД..
БВГДЕ..
ВГДЕЖ.
АБВГ

5.6-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиган *М* символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тулик, матрицасидан *[(М+1),Щ* улчамли шифрлаш матрицаси $T_{(ш)}$ ажратилади. Бу матрица биринчи катордан ва биринчи элементлари калит символларига мое келувчи каторлардан иборат булади.

Агар калит сифатида <ГУЗА> сузи танланган булса, шифрлаш матрицаси бешта катордан иборат булади. (5.7-расм)

АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУЩОС
ЕХ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУК;
УК;ГХ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУК;ГХ_АБВДЕЁЖ
АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯУК;ГХ_

5.7-расм. «Руза» калити учун шифрлаш матрицаси

Вижинер жадвали ёрдамида шифрлаш алгоритми куйидаги кадамлар кетма-кетлигидан иборат.

1 -кддам. Узунлиги *М* символли калит *К* ни танлаш.

2-кадам. Танланган калит *К* учуй *[(М+1),Щ* улчамли шифрлаш матрицаси $T_ш$*=(Ьу)* ни куриш.

3- кадам. Дастлабки матннинг хар бир символи s_{Or} тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-кадам. Дастлабки матн символлари шифрлаш матрицаси $T_ш$ дан куйидаги крида буйича танланган символлар билан кетма-кет алмаштирилади.

1) *К* калитнинг алмаштирилувчи s_{Or} символга мое k_m символи аникданади;

2) шифрлаш матрицаси $T_ш$ даги $к_m$ = Ь^ шарт бажарилувчи / к,атор топил ади.

3) $s_{or} = b_u$ шарт бажарилувчи *j* устун аникданади.

4) s_{or} символи $Ь_ц$ символи билан алмаштирилади.

5-кадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг буш жойлари махсус символ-тулдирувчилар билан тулдирилади.

Расшифровка к,илиш к,уйидаги кетма-кетликда амалга оширилади.

1-к,адам. Шифрлаш алгоритмининг 3-к,адамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-к,адам. Шифрматндан s_{lr} символлари ва мое калит символлари $к_m$ кетма-кет танланади. $T_ш$ матрицада $k_m = Ь_ц$ шартни каноатлантирувчи *i* к,атор аникданади. /-к,аторда $b_ij=s_{lr}$ элемент аникданади. Расшифровка килинган матнда *г* - урнига $Ь_ц$ символи жойлаштирилади.

3-кадам. Расшифровка к,илинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Мисол. K=<FYЗA> калиги ёрдамида T=<ПАХТА FАРАМН> дастлабки матнни шифрлаш ва расшифровка килиш талаб этилсин. Шифрлаш ва расшифровка килиш механизми 5.7-расмда келтирилган

Полиалфавитли алмаштириш усулларининг криптобардошлиги оддий алмаштириш усулларига Караганда айтарлича юкрри, чунки уларда дастлабки кетма-кетликнинг бир хил символлари турли символлар билан алмаштирилиши мумкин. Аммо шифрнинг статистик усулларига бардошлилиги калит узунлигига боглик,.

Дастлабки матн	IIAXTA_FAPAMИ
Калит	F УЗАЕУЗАГУЗ А
Алмаштирилган сунгги матн	МУЯТГЯЕАНУФИ
Шифрматн	МУЯТ *¥ЯЕА* НУ ФИ
Калит	ГУЗА ГУЗА ГУЗА
Расшифровка килинган матн	ПАХТ А_FA РАМИ
Дастлабки матн	ПАХТА_ГАРАМИ

5.8-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли.

Урин алмаштириш усуллари. Урин алмаштириш усулларига биноан дастлабки матн белгиланган узунликдаги блокларга ажратилиб хар бир блок ичидаги символлар урни маълум алгоритм буйича алмаштирилади.

Энг осон урин алмаштиришга мисол тарикасида дастлабки ахборот блокини матрицага катор буйича ёзишни, укишни эса устун буйича амалга оширишни курсатиш мумкин. Матрица каторларини тулдириш ва шифрланган ахборотни устун буйича укиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица улчамига) боЕлик,. Масалан узунлиги 64 символга тенг булган блок (матрица улчами 8х8) учун калитнинг $1,6*10^9$ комбинацияси булиши мумкин. Узунлиги 256 символга тенг булган блок (матрица улчами 16х16) калитнинг мумкин булган комбинацияси $1,4*10^{26}$ га етиши мумкин. Бу хрлда калитни саралаш масаласи замонавий ЭХМлар учун хам мураккаб хисобланади.

Гамильтон маршрутларига асосланган усулда хам урин алмаштиришлардан фойдаланилади. Ушбу усул куйидаги кадамларни бажариш орк,али амалга оширилади.

1 -кадам. Дастлабки ахборот блокларга ажратилади. Агар шифрлануvчи ахборот узунлиги блок узунлигига каррали булмаса, охирги блокдаги

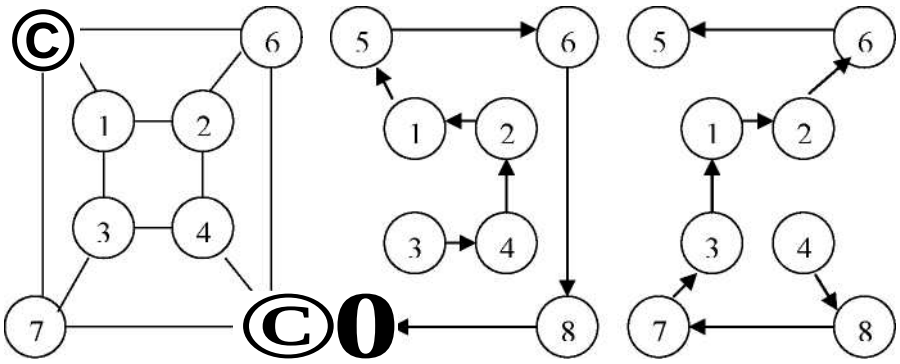
буш уринларга махсус хизматчи символлар-тулдирувчилар жойлаштирилади(масалан, *).

2-кадам. Блок символлари ёрдамида жадвал тулдирилади ва бу жадвалда символнинг тартиб раками учуй маълум жой ажратилади (5.9-расм).

3-кадам. Жадвалдаги символларни укиш маршрутларнинг бири буйича амалга оширилади. Маршрутлар сонининг ошиши шифр криптобардошлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида берилади.

4-кадам. Символларнинг шифрланган кетма-кетлиги белгиланган *L* узунликдаги блокларга ажратилади. *L* катталик 1-кадамда дастлабки ахборот булинадиган блоклар узунлигидан фаркланиши мумкин.

Расшифровка килиш тескари тартибда амалга оширилади. Калитга мое хрлда маршрут танланади ва бу маршрутга биноан жадвал тулдирилади.



5.9-расм. 8-элементли жадвал ва Гамильтон маршрутлари вариантлари.

Жадвалдан символлар элемент номерлари келиши тартибида укилади.

Мисол. Дастлабки матн T_o «УРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Калит ва шифрланган блоклар узунлиги мое хрлда куйидагиларга тенг: *К=<2,1Л>, L=4.* Шифрлаш учун 5.9-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матриц ал ар и тулдирилган маршрутлар 5.10-расмда келтирилган куринишга эга.

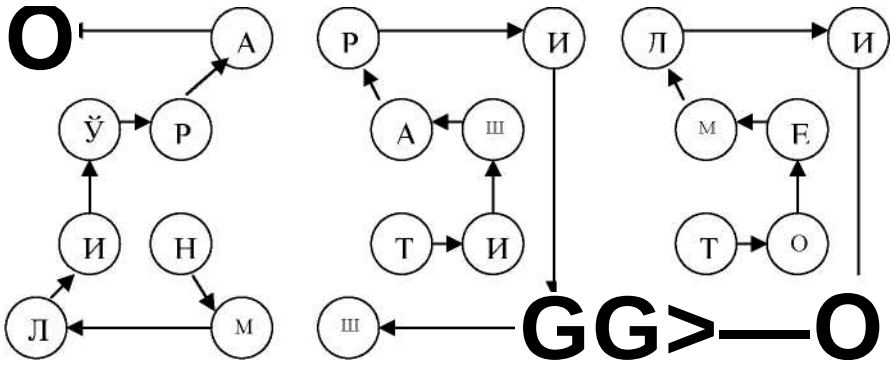
1 -кадам. Дастлабки матн учта блокка ажратилади. Ь7=<УРИН_АЛМ>,

2-к,адам. 2,1,1 маршрутли учта матрица тулдирилади;

3-кадам. Маршрутларга биноан символларни жой-жойига куйиш оркали шифрматнни хрсил килиш.

$Г_1$=<НМЛИУРА_ТИШАРИ_ШТОЕМДИ**> 4-кадам. Шифрматнни блокларга ажратиш.

УРА_ ТИША РИ_Ш ТОЕМ ДИ**>



5.10-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

Амалиётда урин алмаштириш усулини амалга оширувчи махсус аппарат воситалар катта ахамиятга эга (5.11-расм).

1 ----------		---------- 0
1		1
1		1
0		0
1		1
0		0
1		1
0		0
		1
0 ----------		---------- 1
1		1

Шифрлаш *Ўрин* Расшифровка килиш *алмаштириш схемаси.*

5.11-расм

Дастлабки ахборот блокининг параллел иккили коди (масалан, икки байт) схемага берилади. Ички коммутация хисобига схемада битларнинг

блоклардаги уринлари алмаштирилади. Расшифровка килиш учуй эса схеманинг кириш ва чикиш йуллари узаро алмаштирилади.

Урин алмаштириш усулларининг амалга оширилиши содда булсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш оркали фош килиш мумкин. Иккинчидан, агар дастлабки матн узунлиги *К* символлардан ташкил топган блокларга ажратилса, шифрни фош этиш учуй шифрлаш тизимсига биттасидан бошка барча символлари бир хил булган тест ахборотининг *К-1* блокини юбориш кифоя.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асослан-ган шифрлаш усуллари энг куп таркалган. Дастлабки ахборотнинг 5_K=IIZ?¸II вектор куринишида берилган *к*- блокини шифрлаш А=Иа(-/И матрица калит -ни B_K векторга купайтириш оркали амалга оширилади. Натижада Q=llc(ll вектор куринишидаги шифрматн блоки х,осил к,илинади. Бу векторнинг элементлари $c_г = \wedge_{i,j} a_{ij}.b_j$. ифодаси оркали аникданади.

Ахборотни расшифровка килиш $C_к$ векторларини *А* матрицага теска-ри булган А"[1] матрицага кетма-кет купайтириш оркали аникданади. Мисол. $Г_0$=<АЙЛАНА> сузини матрица-калит

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

ёрдамида шифрлаш ва расшифровка килиш талаб этилсин.

Дастлабки сузни шифрлаш учун куйидаги к,адамларни бажариш лозим.

1-кадам. Дастлабки сузнинг алфавитдаги харфлар тартиб раками кетма-кетлигига мое сон эквивалентини аникдаш.

$$T = <1,10,12,1,14,1>$$

2-к.адам. *А* матрицани B_J={ 1,10,12} ва B_2={ 1,14,1} векторларга купайтириш.

$$\begin{vmatrix} 1 & 4 & 8 \\ & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 1 \\ 1 \end{vmatrix} = \begin{vmatrix} 13 \\ 97 \\ 15 \end{vmatrix}$$

$$\begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 1 \\ 1 \end{vmatrix} = \begin{vmatrix} 65 \\ 10 \\ 13 \end{vmatrix}$$

3-кадам. Шифрланган сузни кетма-кет сонлар куринишида ёзиш.

1=<137,97,156,65,103,137> Шифрланган сузни расшифровка килиш куйидагича амалга оширила-

ди:

1-кадам. А матрицанинг аникловчиси хдсобланади:

A|=-115 .

2-кадам. Хдр бир элементи А матрицадаги a_{ij} элементнинг алгебраик тулдирувчиси булган бириктирилган матрица А* аникланади.

$$A^* = \begin{vmatrix} 1 & -3 & -15 \\ 52 & -43 & \\ 15 & -48 & 22 \\ -5 & & \end{vmatrix}$$

3-кадам. Транспонирланган матрица A^m аникланади.

$$A^T = \begin{vmatrix} 17 & & \\ 52 & 22 & -48 \\ -3 & -43 & \\ -15 & 15 & \end{vmatrix}$$

4-кадам. Куйидаги формула буйича тескари матрица А"[1] х,исобланади:

$$A^{-1}$$

Хисоблаш натижасида к,уйидагини оламиз.

$$A^{-1} = \begin{vmatrix} -17/17115 & -52/52115 & 48/48115 \\ V & 43/43115 & -22/5115 \\ 15/15115 & -15/15115 & 5/5115 \end{vmatrix}$$

5-кадам. B_t ва Во векторлар аникданади:

$$Bj=A^{-1}Cj; \qquad B_2 = A^{-1} C_2.$$

$$A = \begin{vmatrix} & " \% 5 & 48/5115 \\ 3 & 15 & -22/5115 \\ 15 & \sim \% 5 & 5/5115 \end{vmatrix} \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 1 \\ 1 \end{vmatrix}$$

$$\text{Я,} = \begin{vmatrix} -17/ & 52/\ 52115 & 48 \\ 17115 & & 48115 \\ 8/ & 43 & -\ \%\ 5 \\ 3115 & 5115 & \\ 15 & 15 & \\ 15115 & 5115 & \end{vmatrix} \begin{vmatrix} 65 \\ 10 \\ 13 \\ 7 \end{vmatrix} = \begin{vmatrix} 1 \\ 1 \\ 1 \end{vmatrix}$$

6-кддам. Расшифровка килинган сузнинг сон эквивалента $Г_5$=<1,10,12,1,14,1> символлар билан алмаштирилади. Натижада дастлабки суз $Г_0$=<АЙЛАНА> хрсил булади.

Шифрлашнинг аддитие усуллари. Шифрлашнинг *аддитие усулларига* биноан дастлабки ахборот символларига мое келувчи ракам кодларини кетма-кетлиги ***гамма*** деб аталувчи кандайдир символлар кетма-кетлигига мое келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашиннг аддитив усуллари ***гаммалаш*** деб хам аталади.

Ушбу усуллар учун калит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги калит узунлигига ва унинг статистик характеристикаларининг текислигига боглик,. Агар калит шифрланувчи символлар кетма-кетлигидан киска булса, шифрматн криптоаналитик томонидан статистик усуллар ёрдамида расшифровка килиниши мумкин. Калит ва дастлабки ахборот узунликлари канчалик фаркданса, шифр-матнга муваффак,иятли хужум эх,тимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта булган тасодифий сонларнинг даврий булмаган кетма-кетлигидан иборат булса, калитни билмасдан туриб шифрматнни расшифровка к,илиш амалий жих,атдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда калит сифатида рак,амларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг куп тарк,алган ва самарали х,исобланади. Генератор псевдотасодифий сонларнинг чексиз кетма-кетлигини шакллантиришда нисбатан к,иск,а узунликдаги дастлабки ахборотдан фойдаланади.

Псевдотасодифий сонлар кетма-кетлигини шакллантиришда конгруэнт генераторлардан хам фойдаланилади. Бу синф генераторлари сонларнинг шундай псевдотасодифий кетма-кетликларини шакллантирадики, улар учун генераторларнинг даврийлиги ва чикиш йули кетма-кетликларининг тасо-

дифийлиги каби асосий характеристкаларини катъий математик тарзда ифодалаш мумкин.

Конгруэнт генераторлар ичида узининг соддалиги ва самаралилиги билан чизикди генератор ажралиб туради. Бу генератор куйидаги муносабат буйича сонларнинг псевдотасодифий кетма-кетликларини шакллантиради.

$$T(i+1) = (a \blacksquare T(i) + c) \bmod m;$$

бу ерда *a* ва *c* - узгармаслар, Т(0) -тугдирувчи(сабаб булувчи) сон сифатида танланган дастлабки катталик.

Бундай датчикнинг такрорланиш даври *d* ва *С* катталикларига боглик,. m киймати одатда I^s га тенг килиб олинади, бу ерда s-ЭХМдаги сузнинг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг такрорланиш даври с-ток, сон ва *a* (mod4)=l булгандагина максималь булади. Бундай генераторларни аппарат ёки программ воситалари орк,али осонгина яратиш мумкин.

Шифрлашнинг комбинацияланган усуллари. Кудратли компьютерлар, тармок, технологиялари ва нейронли х,исоблашларнинг пайдо булиши хрзиргача умуман фош килинмайди деб хисобланган криптографик тизимларни обрусизлантирилишига сабаб булди. Бу эса уз навбатида юк,ори бардошликка эга криптографик тизимларни яратиш устида ишлашни такозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. К,уйида энг кам вакт сарфида криптобардошликни жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида суз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки боскичда амалга оширилади. Биринчи боскичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи боскичда шифрланган маълумотлар махсус усул буйича кайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фаркли булган сон матрицасига купайтиришдан фойдаланиш мумкин.

Гаммалашни к,уллашда агар шифр гаммаси сифатида ракамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош килиш жуда кийин. Одатда шифр гаммаси х,ар бир шифрланувчи суз учун

тасодифий узгариши лозим. Агар шифр гаммаси шифрланган суз узунлигидан катта булса ва дастлабки матннинг хеч кандай кисми маълум булмаса, шифрни факат тугридан-тугри саралаш оркали фош этиш мумкин. Бунда криптобардошлик калит улчами оркали аникданади. Шифрлашнинг бу усулидан купинча хдмоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз Кбайтини шифрлаш имконияти мавжуд. Расшифровка килиш жараёни-калит маълум булганида шифр гаммасини кайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага купайтиришни куллашда шифрланган матн бир байт узунликдаги f_i векторларга ажратилади ва хдр бир вектор квадрат матрица \^4_{1}} га купайтирилади ва шифрланган векторлар шакллантирилади:

Бу усулнинг асосий афзаллиги сифатида унинг маълумотлар ишланишининг турли жабхаларидаги мосланувчанлигини курсатиш мумкин. Хар бир вектор алохида шифрланганлиги сабабли маълумотлар блокини узатиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти тугилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

Расшифровка килиш жараёнида шифрланган /* векторларни тескари матрица |га купайтирилади.)■

Комбинацияланган усулларнинг юкрри самарадорлигига унинг иккала боскичини аппарат усулда амалга ошириш орк,али эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка килиш вакти ошиб кетади. Шу сабабли комбинацияланган усуларни аппарат-дастурий усулда, яъни усулнинг бир боскичи аппарат усулда, иккинчи

боскичи дастурий усулда амалга оширилиши максадга мувофик, хисобланади.

5.3. Асимметрик шифрлаш тизимлари

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очик, калит ёрдамида шифрланса, махфий калит ёрдамида расшифровка килинади. Асимметрик шифрлаш тизимларини очик, калитли шифрлаш тизимлар деб хам юритилади.

Очик, калитли тизимларини к,уллаш асосида кайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар куйидаги хусусиятларга эга. Маълумки *x* маълум булса *y=f(x)* функцияни аникдаш осой. Аммо унинг маълум киймати буйича *x* ни аникдаш амалий жихатдан мумкин эмас. Криптографияда яширин деб аталувчи йулга эга булган бир томонли функциялар ишлатилади. *z* параметрли бундай функциялар куйидаги хусусиятларга эга. Маълум *z* учун E_z ва D_z алгоритмларини аникдаш мумкин. E_z алгоритми ёрдамида аникдик сохасидаги барча *x* учун *fz(x)* функцияни осонгина олиш мумкин. Худди шу тарифа D_z алгоритми ёрдамида жоиз кийматлар сох,асидаги барча *y* учун тескари функция *x—f }(y)* х,ам осонгина аникданади. Айни вактда жоиз к,ийматлар сох,асидаги барча *z* ва деярли барча, *y* учун хатто E_z маълум булганида х,ам/[1](>')ни х,исоблашлар ёрдамида топиб булмайди. Очик, калит сифатида *y* ишлатилса, махфий калит сифатида *x* ишлатилади.

Очик, калитни ишлатиб шифрлаш амалга оширилганда узаро мулок,атда булган субъектлар уртасида махфий калитни алмашиш зарурияти йук,олади. Бу эса уз навбатида узатилувчи ахборотнинг криптох,имоясини соддалаштиради.

Очик, калитли криптотизимларни бир томонли функциялар куриниши буйича фаркдаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алохида тилга олиш уринли. Хозирда энг самарали ва кенг тарк,алган очик, калитли шифрлаш алгоритми сифатида RSA алгоритмини

курсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Rivest, Shamir ва Adleman).

Алгоритм модуль арифметикасининг даражага кутариш амалидан фойдаланишга асосланган. Алгоритмни куйидаги кадамлар кетма-кетлиги куринишида ифодалаш мумкин.

1-кадам. Иккита 200дан катта булган туб сон p ва q танланади.

2-кадам. Калитнинг очик, ташкил этувчиси п хрсил килинади

$$n=p*q.$$

3-кадам. Куйидаги формула буйича Эйлер функцияси хисобланади:

Эйлер функцияси п билан узаро туб, 1 дан п гача булган бутун мусбат сонлар сонини курсатади. Узаро туб сонлар деганда 1 дан бошка бирорта умумий булувчисига эга булмаган сонлар тушунилади.

4-к,адам. $f(p,q)$ киймати билан узаро туб булган катта туб сон d танлаб олинади.

5-кадам. К,уйидаги шартни к,аноатлантирувчи е сони аникланади e-

$$d\text{-}1\ (modf(p, q)).$$

Бу шартга биноан $e-d$ купайтманинг $f(p,q)$ функцияга булишдан крлган к,олдик, 1га тенг. е сони очик, калитнинг иккинчи ташкил этувчиси сифатида кабул килинади. Махфий калит сифатида d ва n сонлари ишлатилади.

6-к,адам. Дастлабки ахборот унинг физик табиатидан к,атъий назар ракамли иккили куринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блокларга ажратилади, бу ерда $L—L$ $>\log_2(«+l)$ шартини к,аноатлантирувчи энг кичик бутун сон. Хдр бир блок [0, $n-1$] оралик,ка тааллукди бутун мусбат сон каби курилади. Шундай килиб, дастлабки ахборот $X(i)$, $i=l,I$ сонларнинг кетма-кетлиги орк,али ифодаланади. / нинг к,иймати шифрланувчи кетма-кетликнинг узунлиги орк,али аникданади.

7-кадам. Шифрланган ахборот куйидаги формула буйича аникданувчи $Y(i)$ сонларнинг кетма-кетлиги куринишида олинади:

$$\boldsymbol{Y(i) = (X(i))e(modn).}$$

Ахборотни расшифровка килишда куйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d (mod n).$$

Мисол. <ГАЗ> сузини шифрлаш ва расшифровка килиш талаб этил-син. Дастлабки сузни шифрлаш учуй куйидаги кадамларни бажариш лозим. 1-кадам. *p=3* ва *q=ll* танлаб олинади. 2-кадам. n = 3 -11 = 33 хисобланади. 3-кадам. Эйлер функцияси аникданади. *f(p,q) = (З-\)-(U-\) = 20*

4-кадам. Узаро туб сон сифатида *d-Ъ* сони танлаб олинади.

5-кадам. (e-3)(mod20) = 1шартини каноатлантирувчи e сони танланади. Айтайлик, *e-1*.

6-кадам. Дастлабки сузнинг алфавитдаги харфлар тартиб раками кетма-кетлигига мое сон эквивалента аникданади. А харфига -1, Г харфига-4, 3 харфига -9. Узбек алфавитида Збта харф ишлатилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак булади. Дастлабки ахборот иккили кодда куйидаги куринишга эга булади:

000100 000001 001001.

Блок узунлиги *L* бутун сонлар ичидан $Z>\log_2(33 + 1)$ шартини каноатлантирувчи минималь сон сифатида аникданади. *n* =33 булганлиги сабабли *L=6*.

Демак, дастлабки матн *X(г)* << 4,1,9 > кетма-кетлик куринишида ифодаланади.

7-кладам. *X(i)* кетма-кетлиги очик, калит {7,33} ёрдамида шифрланади:

$$Y(1) = (4^7)(mod33) = 16384(mod33) = 16$$

$$Y(2) = (1^7)(mod33) = 1(mod33) = 1$$

$$Y(1) = (9^7)(mod33) = 4782969(mod33) = 15$$

Шифрланган суз Y(i)=<16,1,15>

Шифрланган сузни расшифровка килиш махфий калит {3,33} ёрдамида бажарилади.:

$$Y(1) = (16^3)(\text{mod}33) = 4096(\text{mod}33) = 4$$

$$Y(1) = (1^3)(\text{mod}33) = 1(\text{mod}33) = 1\ Y(1) =$$

$$(15^3)(\text{mod}33) = 3375(\text{mod}33) = 9$$

Дастлабки сон кетма-кетлиги расшифровка килинган X(/)=<4,1,9> куринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Келтирилган мисолда хисоблашларнинг соддалигини таъминлаш максадида мумкин булган кичик сонлардан фойдаланилди.

Элъ-Гамал тизими чекли майдонларда дискрет логарифмларнинг хисобланиш мураккаблигига асосланган. RSA ва Эль-Гамал тизимларининг асосий камчилиги сифатида модуль арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини курсатиш мумкин. Бу уз навбатида айтарлича хисоблаш ресурсларини талаб килади.

Мак-Элис криптотизимида хатоликларни тузатувчи кодлар ишлатилади. Бу тизим RSA тизимига нисбатан тезрок, амалга оширилсада, жиддий камчиликка эга. Мак-Элис криптотизимсида катта узунликдаги калит ишлатилади ва олинган шифрматн узунлиги дастлабки матн узунлигидан икки марта катта булади.

Б арча очик, калит ли шифрлаш усуллари учун *NP-ту лик,* масалани (тулик, саралаш масаласи) ечишга асосланган криптотахлил усулидан бошка усулларининг йуклиги к,атъий исботланмаган. Агар бундай масалаларни ечувчи самарали усуллар пайдо булса, бундай хилдаги криптотизим обрусизлантирилади.

Юк,орида курилган шифрлаш усулларининг криптобардошлиги калит узунлигига боглик, булиб, бу узунлик замонавий тизимлар учун, лоакал, 90 битдан катта булиши шарт.

Айрим мухим к,улланишларда нафак,ат калит, балки шифрлаш алгоритми хам махфий булади. Шифрларнинг криптобардошлигини ошириш учун бир неча калит (одатда учта) ишлатилиши мумкин. Биринчи калит ёрдамида шифрланган ахборот иккинчи калит ёрдамида шифрланади ва х,.

5.4. Шифрлаш стандартлари

Россиянинг ахборотни шифрлаш стандарти. Росссия Федерациясида хисоблаш машиналари, комплекслари ва тармокларида ахборотни криптографик узгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар махфийлик даражаси ихтиёрий булган ахборотни хеч кандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усулларида амалга оширилиши мумкин.

Стандартда ахборотни криптографик узгартиришнинг куйидаги алгоритмлари мавжуд:

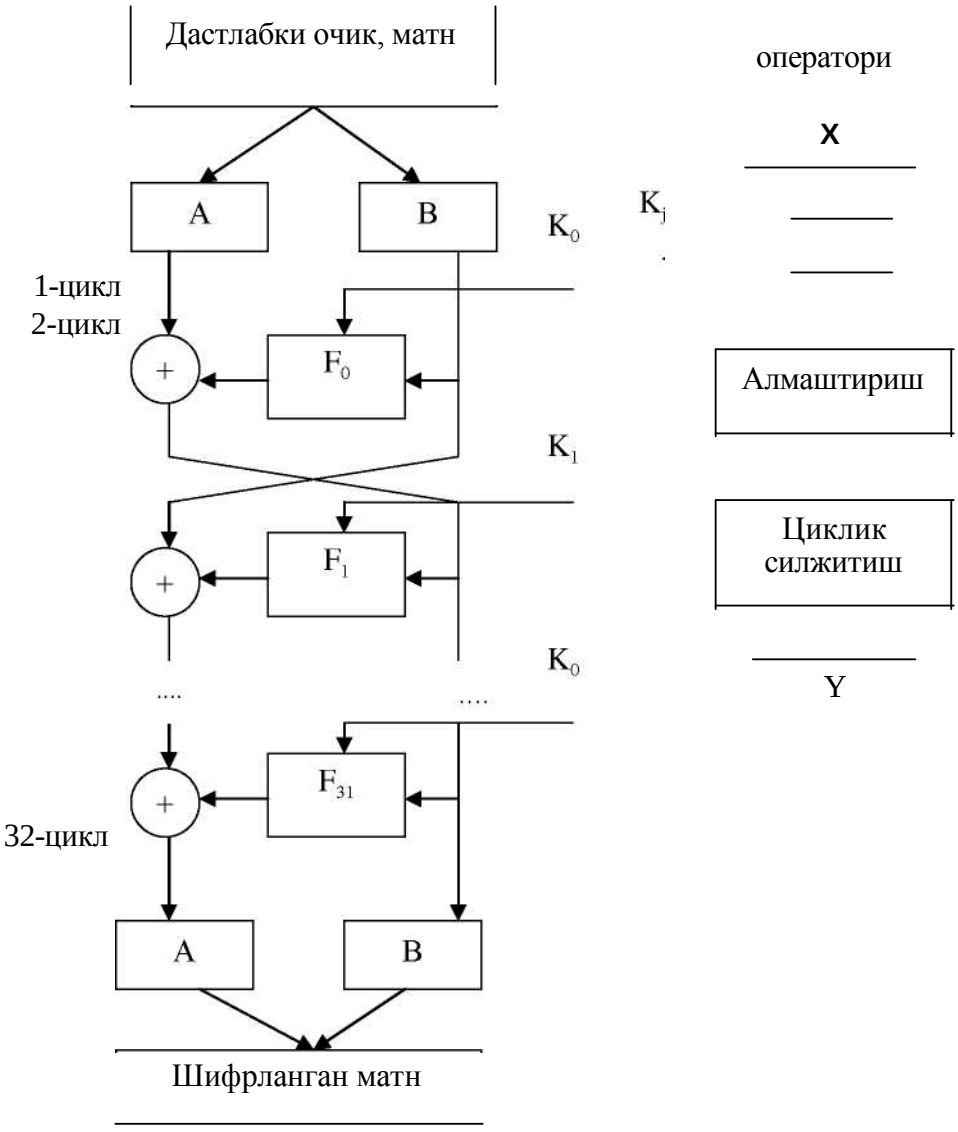
- оддий алмаштириш;
- гаммалаш;
- тескари богланишли гаммалаш;
- имитовставка.

Бу алгоритмлар учун 8 та 32 хонали иккили сузларга ажратилган 256 бит улчамли калитнинг ишлатилиши хамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий хисобланади.

Оддий аламштириш алгоритмининг мохияти куйидагича (5.12-расм).

Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали А ва В иккили сузларга ажратилади. А сузлар блокнинг кичик хоналарини В сузлар эса катта хоналарини ташкил этади. Бу сузларга сони /=32 булган циклик итерация оператори F_t кулланилади. Блокнинг кичик битларидаги суз (биринчи итерациядаги А сузи) калитининг 32 хонали сузи билан $\mathrm{mod} 2^{32}$ буйича жамланади; хар бири 4 битдан иборат кисмларга (4 хонали кириш йули векторлари) ажратилади; махсус алмаштириш узеллари ёрдамида х,ар бир вектор бошкаси билан алмаштирилади; олинган векторлар 32 хонали сузга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошка 32 хонали суз (биринчи итерациядаги *B* сузи) билан mod 2 буйича жамланади.

Биринчи итерация тугаганидан сунг кичик битлар урнида В суз жойланади, чап тарафда эса *A* суз жойланади. Кейинги итерацияларда сузлар устидаги амаллар такрорланади.



5.12-расм. Оддий алмаштириш алгоритмида шифрлаш жараёнининг блок-схемаси.

Хдр бир /-итерацияда K_j калитнинг (калитлар 8 та) 32 хонали сузи куйидаги кридага биноан танланади

(i-1) mod 8, l<i<24 булганда,

32-i, i>25 булганда,

0, *i=32 булганда.*

$$K_i = \begin{cases} |(-I) \bmod 8, & l < / < 24 \quad \textit{бўлганда,} \\ 32 - i, & i > 25 \quad \textit{бўлганда,} \\ 0, & i = 32 \quad \textit{бўлганда,} \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби куйидаги куринишда булади:

K0,K1, K_2, K_3, K_4, K_5, K_6, K_7, K0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,

K0,K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K0,.

Расшифровка килишда калитлар тескари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узеллари-дан иборат. Алмаштириш узели хар бирида алмаштириш вектори (4 бит) жойлашган 16 каторли жадвалдан иборат. Кириш нули вектори жадвалдаги катор адресини аникласа, катордаги сон алмаштиришнинг чикиш нули вектори хдсобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам узгартирилади.

Гаммалаш алгоритмида дастлабки битларнинг кетма-кетлиги гаммаининг битлари кетма-кетлиги билан mod2 буйича жамланади. Гамма опций алмаштириш алгоритмига биноан хрсил килинади. Гаммани шаклланти-ришда иккита махсус доимийлардан хамда 64-хонали иккили кетма-кетилик синхропосилкадан фойдаланилади. Ахборотни факат синхропосилка борли-гида расшифровка килиш мумкин.

Синхропосилка махфий булмайди ва очик, х,олда х,исоблаш машинаси хотирасида сакданиши ёки алок,а канали оркали узатилиши мумкин.

Тескари богланишли гаммалаш алгоритми гаммалаш алгоритмидан фак,ат шифрлаш жараёнининг биринчи кадамидаги х,аракатлар билан фаркланади.

Имитоестаека нотугри ахборотни зурлаб киритилишидан х,имоялашда ишлатилади. Имитовставка дастлабки ахборот ва махфий калитни узгартириш функцияси хисобланади. У *к* бит узунликдаги иккили кетма-кетликдан иборат булиб, *к* нинг к,иймати нотугри ахборотнинг зурлаб киритилиши эхтимоллиги $P_{ЗК}$ билан к,уйидаги муносабат билан богланган.

$$\mathbf{P}_{\text{ЗК}} = \mathbf{J}^{-k}$$

Имитоставкани шакллантириш алгоритми к,уйидаги харакатларнинг кетма-кетлигидан иборат. Очик, ахборот 64 битли *T(i)* (i=l,2,3v---,m) блок-ларга ажратилади, бу ерда m-шифрланувчи ахборот хажми оркали аникланади. Биринчи блок Г(1) оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан узгартирилади. Калит сифатида дастлабки ахбо-

рот шифрланищца ишлатиладиган калит олинади. Олинган 64 битли иккили суз иккинчи блок Г(2) билан mod2 буйича жамланади. Г(1) блок устида кандай итерация узгартиришлари бажарилган булса жамлаш натижаси устида хам шундай узгартиришлар амалга оширилади ва охирида Г(3) блок билан mod2 буйича жамланади. Бундай харакатлар дастлабки ахборотнинг *m-1* блоки буйича такрорланади. Агар охирги *T(m)* блок тулик, булмаса, у 64 хонагача ноллар билан тулдиради. Бу блок *T(m-1)* блок ишланиш натижаси билан mod2 буйича жамланади ва оддий алмаштириш алгоритмининг биринчи 16 итерациялари буйича узгартирилади. Хрсил булган 64 хонали блокдан к бит узунликдаги суз ажратиб олинади ва бу суз имитовставка хисобланади.

Имитовставка шифрланган ахборотнинг охирига жойлаштирилади. Бу ахборот олингандан сунг, у расшифровка килинади. Расшифровка килинган ахборот буйича имитовставка аникланади ва олингани билан солиштирилади. Агар имитовставкалар мое келмаса, расшифровка килинган ахборот нотуГри деб хисобланади.

АКШнинг ахборотни шифрлаш стандарты. АКШда давлат стандарти сифатида DES(Data Encryption Standart) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чик,илган булиб, АКД1 Миллий Хавфсизлик Агентлигининг мутахасислари томонидан текширилгандан сунг давлат стандарти макрмини олган. DES стандартидан нафак,ат федерал департаментлар, балки нодавлат ташкилотлар, нафакат АК,Шда, балки бутун дунёда фойдаланиб келинган.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик узгартирилади.

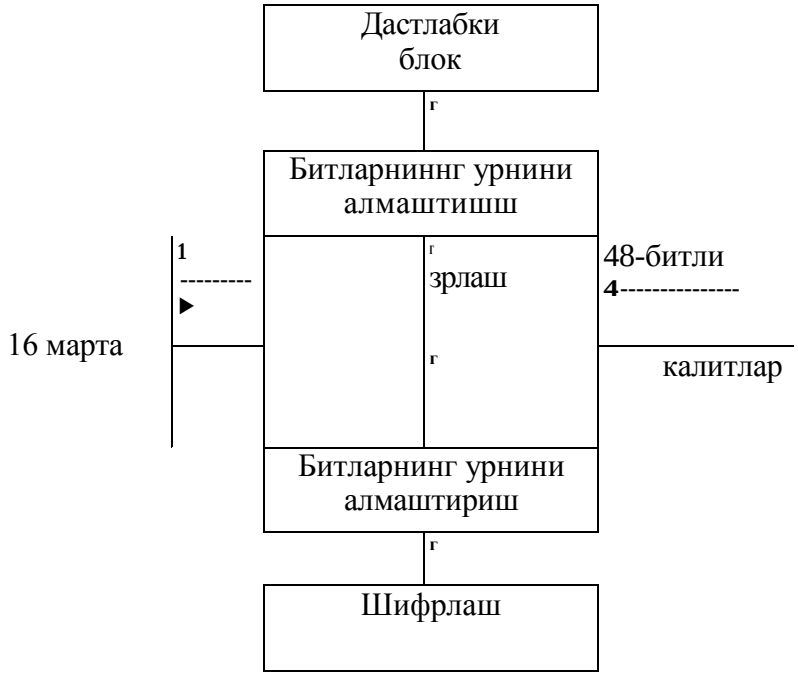
Дастлабки ахборот блоклари урин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини х,исоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга узгартириш ва 32-битли кет-макетликнинг урнини алмаштириш кузда тутилган.

DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 5.13-расмда келтирилган.

Расшифровка жараёни шифрлаш жараёнига инверс булиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.

Хрзирда бу стандарт куйидаги иккита сабабга кура фойдаланишга бутунлай яроксиз хисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу ЭХ,Млар-нинг замонавий ривожи учуй жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кузда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида куп вакт талаб килувчи амаллар бор эди (масалан, машина сузида маълум схема буйича битларнинг урнини алмаштириш каби).



5.13.-расм. DES алгоритмида шифрлаш жараёнининг блок-схемаси

Бу сабаблар АКД1 стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон килишига олиб келди. Танлов шартларига биноан алгоритмга к,уйидаги талаблар к,уйилган эди:

- алгоритм симметрик булиши керак;
- алгоритм блокли шифр булиши керак;
- блок узунлиги 128 бит булиб, 128, 192, ва 256 битли калит узунликларини таъминлаши лозим.

Ундан ташкари танловда иштирок этувчилар учун куйидаги тавсиялар берилган эди:

• хдм аппарат усулда хам программ усулда осонгина амалга оширилувчи амаллардан фойдаланиш;

• 32 хонали процессорлардан фойдаланиш;

• иложи борича шифр тузилмасини мураккаблаштирмаслик. Бу уз навбатида барча кизикувчиларнинг алгоритмни мустакил тарзда криптотахлил килиб, унда кандайдир хужжатсиз имкониятлар йуклигига ишонч хрсил к,илишлари учун зарур хисобланади.

2000 йил 2 октябрда танлов натижаси эълон килинди. Танлов Голиби деб Бельгия алгоритми RIJNDAEL топилди ва шу ондан бошлаб алгоритм-Голибдан барча патент чегараланишлари олиб ташланди.

Хрзирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж.Деймен (J. Daemen) ва В. Райджмен (V.Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокли шифр булиб, кодланувчи маълумотларнинг хар бир блоки кабул килинган блок узунлигига караб 4х4, 4х6 ёки 4х8 улчамдаги байтларнинг икки улчамли массивлари куринишига эга.

Шифрдаги барча узгартиришлар к,атъий математик асосга эга. Амалларнинг тузилмаси ва кетма-кетлиги алгоритмнинг х,ам 8-битли, хам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм тузилмасида баъзи амалларнинг параллел ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Узбекистоннинг ахборотни шифрлаш стандарти. Ушбу "Маълумотларни шифрлаш алгоритми" стандарти Узбекистон ал ока ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадк,ик,отлари маркази томонидан ишлаб чикилган ва унда Узбекистон Республикасининг "Электрон ракамли имзо хусусида"ги ва "Электрон хужжат алмашинуви хусусида"ги к,онунларининг меъёрлари амалга оширилган.

Ушбу стандарт - криптографик алгоритм, электрон маълумотларни химоялашта мулжалланган. Маълумотларни шифрлаш алгоритми симметрик блокли шифр булиб, ахборотни шифрлаш ва расшифровка килиш учун ишлатилади. Алгоритм 128 ёки 256 бит узунлигидаги маълумотларни

шифрлашда ва расшифровка килишда 128, 256, 512 битли калитлардан фойдаланиши мумкин.

Стандарт ЭХ,М тармокдарида, телекоммуникацияда, алохдда хисоблаш комплекслари ва ЭХ,Мда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш кридасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари куйидаги камчиликларга эга:

- ахборот алмашувчи икала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига куйиладиган талабларнинг катъийлиги;
- калитларни яратиш ва таксимлаш хизматига куйиладиган талабларнинг юкррилиги. Сабаби, узаро алоканинг «хар ким - хар ким билан» схемасида «л» та абонент учун *n(n-1)/2* та калит талаб этилади, яъни калитлар сонининг абонентлар сонига богликлиги квадратли. Масалан, л=1000 абонент учун талаб килинадиган калитлар сони л(л-1)/2=499500. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармогида симметрик шифрлаш тизимини к,ушимча усул ва воситаларсиз куллашнинг иложи йук,.

Асимметрик шифрлашнинг биринчи ва кенг таркалган криптоалгоритми RSA (5.3 га каралсин) 1993 йилда стандарт сифатида кабул килинди. Ушбу криптоалгоритм хар тарафлама тасдикданган ва калитнинг етарли узунлигида бардошлиги эътироф этилган. Хозирда 512 битли калит бардошликни таъминлашда етарли х,исобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор к,увватининг ошиши RSA криптоалгоритмининг тулик, саралаш хужумларга бардошлигининг йук,олишига олиб келади. Аммо, процессор кувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

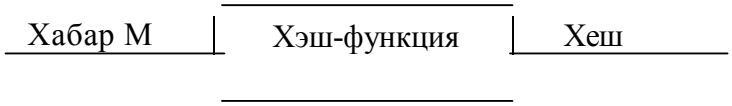
- калитларни махфий тарзда етказиш зарурияти йук,; асимметрик шифрлаш очик, калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса хдмояланган алока сеанси бошланишидан аввал махфий калитлар алмашиниши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли богланишлиги йукрлади; RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига богликдиги чизикди куринишга эга *(N* фойдаланувчиси булган тизимда *2N* калит ишлатилади).

Аммо асимметрик криптотизимлар, хусусан RSA криптотизими, камчиликлардан холи эмас:

- хрзиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг кайтарилмаслигининг математик исботи йук,;
- асимметрик шифрлаш симметрик шифрлашга нисбатан секин амалга оширилади, чунки шифрлашда ва расшифровка килишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, ЯБАда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;
- очик, калитларни алмаштириб куйилишидан химоялаш зарур. Фараз килайлик "А" абонентнинг компьютерида *"В"* абонентнинг очик, калиги *"$К_в$"* сакданади. "л" нияти бузук, одам "А" абонентда сакланаётган очик, калитлардан фойдалана олади. У узининг жуфт (очик, ва махфий) *"$К_п$"* ва *"$k_п$"* калитларини яратади ва "А" абонен тда сакланаётган *"В"* абонентнинг *"$К_в$"* калитини узининг очик, *"$К_п$"* калити билан алмаштиради. "А" абонент кандайдир ахборотни "В" абонентга жунатиш учун уни *"$К_п$"* калитда (бу *"$К_в$"* калит деб уйлаган х,олда) шифрлайди. Натижада, бу хабарни *"В"* абонент у кий олмайди, "л" абонент осонгина расшифровка килади ва укийди. Очик, калитларни алмаштиришни олдини олишда калит ларни сертификациялашдан фойдаланилади.

5.5. Хэшлаш функцияси

Хэшлаш функцияси (хэш-функцияси) шундай узгартиришки, кириш йулига узунлиги узгарувчан хабар М берилганида чикиш йулида белгиланган узунликдаги катор *h(M)* хрсил булади. Бошкача айтганда, хеш-функция *h(.)* аргумент сифатида узунлиги ихтиёрий хабар (хужжат) М ни кабул килади ва белгиланган узунликдаги хеш-киймат (хеш) /7=/г(М)ни кайтаради (5.14-расм).



5.14-расм. Хэшни шакллантириш схемаси

Хэш-киймат h(M) — хабар М нинг дайджести, яъни ихтиёрий узунликдаги асосий хабар Мнинг хичлантирилган иккилик ифодаси. Хэшлаш функцияси улчами мегабайт ва ундан катта булган имзо чекилувчи хужжат Мни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлаштиришга имкон беради. Таъкидлаш лозимки, хеш-функция *h(M)* кийматининг хужжат Мга богликдиги мураккаб ва хужжат Мнинг узини тиклашга имкон бермайди.

Хэшлаш функцияси куйидаги хусусиятларга эга булиши л озим:

1. Хэш-функция ихтиёрий улчамли аргументга к,улланиши мумкин.
2. Хэш-функция чикиш йулининг к,иймати белгиланган улчамга эга.
3. Хэш-функция *h(x)* ни ихтиёрий *"x"* учун етарлича осон х,исобланади. Хэш-функцияни х,исоблаш тезлиги шундай булиши керакки, хэш-функция ишлатилганида электрон ракамли имзони тузиш ва текшириш тезлиги хабарнинг узидан фойдаланилганига Караганда анчагина катта булсин.
4. Хэш-функция матн М даги орасига куйишлар (вставки), чикариб ташлашлар (выбросы), жойини узгартиришлар ва х,. каби узгаришларга сезгир булиши лозим.
5. Хэш-функция кайтарилмаслик хусусиятига эга булиши лозим.

6. Иккита турли хужжатлар (уларнинг узунлигига боглик, булмаган хрлда) хэш-функциялари кийматларининг мое келиши эхтимоллиги жуда кичкина булиши шарт, яъни хисоблаш нуктаи назаридан *h(x')=h(x)* буладиган xVxнн топиш мумкин эмас.

Иккита турли хабар бита тугунчага (свертка) зичлаштириш назарий жихатдан мумкин. Бу коллизия ёки тукнашиш деб аталади. Шунинг учуй хэшлаш функциясининг бардошлигини таъминлаш максадида тукнашишларга йул куймасликни кузда тутиш лозим. Тукнашишларга бутунлай йул куймаслик мумкин эмас, чунки умумий хрлда мумкин булган хабарлар сони хэшлаш функциялари чикиш йуллари кийматларининг мумкин булган сонидан ортик,. Аммо, тукнашишлар эхтимоллиги паст булиши лозим.

5-хусусият *h(.)* бир томонлама эканлигини билдирса, 6 хусусият бир бир хил тугунчани берувчи иккита ахборотни топиш мумкин эмаслигини кафолатлайди. Бу сохталаштиришни олдини олади.

Шундай к,илиб, хэшлаш функциясидан хабар узгаришини пайк,ашда фойдаланиш мумкин, яъни у *криптографии назорат uuFunducunu* (узгаришларни пайкаш коди ёки *хабарни аутентификациялаш коди* деб хам юритилади) шакллантиришга хизмат килиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон ракамли имзони шакллантаришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентифкациялашда хам кенг кулланилади. Ахборот хавфеизлигининг катор технологияларида шифрлашнинг узига хос усули *бир томонлама хеш-функция ёрдамида шифрлаш* ишлатилади. Бу шифрлашнинг узига хослиги шундан иборатки, у мохияти буйича, бир томонламадир, яъни тескари муолажа - кабул килувчи томонда расшифровка килиш билан бирга олиб борилмайди. Иккала тараф (жунатувчи ва к,абул к,илувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланади.

Энг оммабоп хэш-функциялар - MD2, MD4, MD5 ва SHA.

MD2, MD4 ва MD5 - Р.Райвест томонидан ишлаб чикилган ахборот дайджестини хисобловчи алгоритм. Уларнинг х,ар бири 128 битли хэш-

кодни тузади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тезкор ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси булиб, MD4 алгоритмида хавфсизликнинг оширилиши эвазига тезликдан ютказилган. SHA(Secure Hash Algorithm) - 160 битли *хэш-кодни* тузувчи ахборот дайджестини хисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбатан ишончлирок,.

5.6. Электрон ракамли имзо

Электрон хужжатларни тармок, оркали алмашишда уларни ишлаш ва саклаш харажатлари камаяди, кидириш тезлашади.Аммо, электрон хужжат муаллифини ва хужжатнинг узини аутентификациялаш, яъни муаллифнинг хакикийлигини ва олинган электрон хужжатда узгаришларнинг йуклигини аникдаш муаммоси пайдо булади.

Электрон хужжатларни ауентификациялашдан максад уларни мумкин булган жинояткорона харакатлардан химоялашдир. Бундай харакатларга куйидагилар киради:

- *фаол ушлаб колиш* - тармоккд уланган бузгунчи хужжатларни (файлларни) ушлаб крлади ва узгартиради.

- *маскарад* - абонент *С* хужжатларни абонент *В* га абонент *А* номидан юборади;

- *ренегатлик* - абонент *А* абонент *В* га хабар юборган булсада, юбормаганман дейди;

- *алмаштириш* - абонент *В* хужжатни узгартиради, ёки янгисини шакиллантирадива уни абонент *А* дан олганман дейди;

- *такрорлаш* - абонент *А* абонент *В* га юборган хужжатни абонент С такрорлайди.

Жинояткорона харакатларнинг бу турлари уз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат тузилмаларига, давлат корхона ва ташкилотларига хусусий шахсларга анча- мунча зарар етказиши мумкин.

Электрон ракамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хакикийлигини текшириш муаммосини самарали х,ал этишга имкон беради.

Электрон ракамли имзо телекоммуникация каналлари оркали узатилувчи матнларни аутентификациялаш учун ишлатилади. Ракамли имзо ишлаши буйича оддий кулёзма имзога ухшаш булиб, куйидаги афзалликларга эга:

- имзо чекилган матн имзо куйган шахсга тегишли эканлигини тасдикдайди;

- бу шахсга имзо чекилган матнга боглик, мажбуриятларидан тониш имкониятини бермайди;

- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон ракамли имзо-имзо чекилувчи матн билан бирга узатилувчи кушимча ракамли хабарнинг нисбатан катта булмаган сонидир.

Электрон ракамли имзо асимметрик шифрларнинг кайтарувчанлигига хамда хабар таркиби, имзонинг узи ва калитлар жуфтининг узаро богликдигига асосланади. Бу элементларнинг хатто бирининг узгариши ракамли имзонинг хакикийлигини тасдикдашга имкон бермайди. Электрон ракамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш-функциялари ёрдамида амалга оширилади.

Электрон ракамли имзо тизимининг кулланишида бир- бирига имзо чекилган электрон хужжатларни жунатувчи абонент тармогининг мавжудлиги фараз килинади. Хар бир абонент учун жуфт - махфий ва очик, калит генерацияланади. Мах,фий калит абонентда сир сакланади ва ундан абонент электрон ракамли имзони шакллантиришда фойдаланади.

Очик, калит бошк,а барча фойдаланувчиларга маълум булиб, ундан имзо чекилган электрон хужжатни кабул килувчи электрон ракамли имзони текширишда фойдаланади.

Электрон ракамли имзо тизими иккита асосий муолажани амалга оширади:

- ракамли имзони шакллантириш муолажаси;

- ракамли имзони текшириш муолажаси.

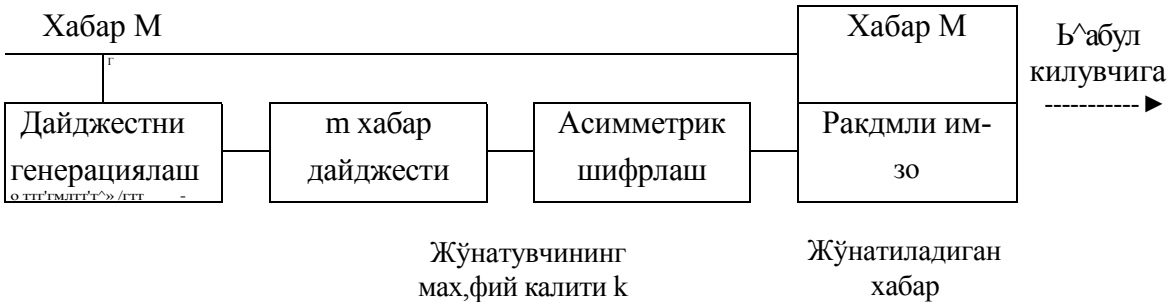
Имзони шакллантириш муолажасида хабар жунатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жунатувчининг очик, калитидан фойдаланилади.

Ракамли имзони шакллантириш муолажаси.

Ушбу муолажани тайёрлаш боскичида хабар жунатувчи абонент *А* иккита калитни генерациялайди: махфий калит $к_A$ ва очик, калит $К_A$. Очик, калит $К_A$ унинг жуфти булган махфий калити k_A дан хисоблаш оркали олинади. Очик, калит $К_A$ тармокнинг бошка абонентларига имзони текширишда фойдаланиш учун таркатилади.

Ракамли имзони шакллантириш учун жунатувчи *А* аввало имзо чекилувчи матн *М* нинг хеш функцияси *ЦМ)* к,ийматини х,исоблайди (5.15-расм).

Хеш-функция имзо чекилувчи дастлабки матн *"М"* ни дайджест *"m"* га зичлаштиришга хизмат к,илади. Дайджест М-бутун матн *"М"* ни характерловчи битларнинг белгиланган катта булмаган сонидан иборат нисбатан киск,а сондир. Сунгра жунатувчи *А* узининг махфий калити k_A билан дайджест *"m"* ни шифрлайди. Натижада олинган сонлар жуфти берилган *"М"* матн учун ракамли имзо х,исобланади. Хабар *"М"* рак,амли имзо билан биргаликда к,абул к,илувчининг адресига юборилади.

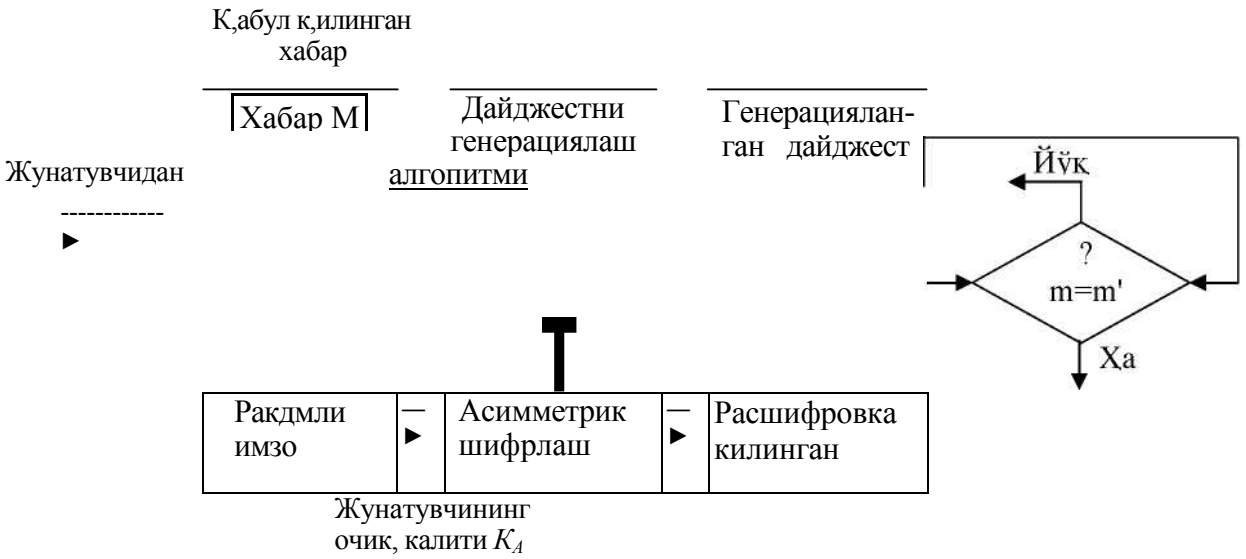


5.*15-расм. Электрон ракамли имзони шакллантириш схемаси.*

Ракамли имзони текшириш муолажаси.

Тармок, абонентлари олинган хабар *"М"* нинг рак,амли имзосини ушбу хабарни жунатувчининг очик калити $К_A$ ёрдамида текширишлари мумкин (5.16-расм).

Электрон ракамли имзони текширишда хабар "М"ни кабул килувчи "5" кабул килинган дайджестни жунатувчининг очик, калити *"K_A"* ёрдамида расшифровка килади. Ундан ташкари, кабул килувчини узи хеш-функция *h(M)* ёрдамида кабул килинган хабар *"M"* нинг дайджести *"m"* ни хисоблайди ва уни расшифровка килингани билан такдослайди. Агар иккала дайджест *"m"* ва *"m"'* мое келса рак,амли имзо хакикий х,исобланади. Акс х,олда имзо калбакилаштирилган, ёки ахборот мазмуни узгартирилган булади.



5.16-расм. Электрон рацамли имзони текшириш схемаси.

Электрон ракамли имзо тизимининг принципиал жихати- фойдаланувчининг электрон рак,амли имзосини унинг имзо чекишдаги махфий калитини билмасдан к,албакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни рухсатсиз фойдаланишдан химоялаш зарур. Электрон ракамли имзонинг махфий калитини, симметрик шифрлаш калитига ухшаб, шахеий калит элитувчисида, х,имояланган х,олда сакдаш тавфеия этилади.

Электрон рак,амли имзо имзо чекилувчи хужжат ва махфий калит орк,али аникданувчи ноёб сондир. Имзо чекилувчи хужжат сифатида х,ар кандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо кушилиши оркали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рак,амли имзо имзо чекилган хужжат муаллифини идентификацияловчи к,ушимча ахборот-

га эга. Бу ахборот хужжатга электрон ракамли имзо хисобланмасидан олдин кушилади. Хдр бир имзо куйидаги ахборотни уз ичига олади:

- имзо чекилган сана;
- ушбу имзо калиги таъсирининг тугаши муддати;
- файлга имзо чекувчи шахе хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);
- имзо чекувчининг индентификатори (очик, калит номи);
- ракамли имзонинг узи.

Асимметрик шифрлашга ухшаш, электрон ракамли имзони текшириш учун ишлатиладиган очик, калитнинг алмаштирилишига йул куймаслик лозим. Фараз килайлик, нияти бузук, одам "л" абонент "5" компьютерида сакданаётган очик, калитлардан, хусусан, абонент A нинг очик, калиги K_A дан фойдалана олади. Унда у куйидаги харакатларини амалга ошириши мумкин:

- очик, калит K_A сакданаётган файлдан абонент A хусусидаги инденцификация ахборотини укиши;
- ичига абонент A хусусидаги индентификация ахборотини ёзган хрлда шахеий жуфт калитлари k_n ва K_n ни генерациялаши;
- абонент Дда сакданаётган очик, калит ^Γ_Aни узининг очик, калити K_n билан алмаштириши.

Сунгра нияти бузук, одам "л" абонент B га хужжатларни узининг махфий калити k_n ёрдамида имзо чекиб жунатиши мумкин. Бу хужжатлар имзосини текширишда абонент B абонент A имзо чеккан хужжатларни ва уларнинг электрон ракамли имзоларини тугри ва хеч ким томонидан модификацияланмаган деб хисоблайди. Абонент А билан муносабатларини бевосита ойдинлаштирилишигача В абонентда олинган хужжатларнинг хакикийлигига шубх,а тугилмайди.

Электрон рак,амли имзонинг катор алгоритмлари ишлаб чик,илган. 1977 йилда АК.Ш да яратилган RSA тизими биринчи ва дунёда машхур электрон ракамли имзо тизими хисобланади ва юкррида келтирилган принципларни амалга оширади. Аммо рак,амли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузук, одамга махфий калитни билмасдан, хеш-

лаш натижасини имзо чекиб булинган хужжатларнинг хешлаш натижаларини купайтириш оркали хисоблаш мумкин булган хужжатлар имзосини шакллантиришга имкон беради.

Ишончлилигининг юкррилиги ва шахсий компьютерларда амалга оширилишининг кулайлиги билан ажралиб турувчи ракамли имзо алгоритмли 1984 йилда Эль Гамал томонидан ишлаб чикилди. Эль Гамалнинг ракамли имзо алгоритми (EGSA) RSA ракамли имзо алгоритмидаги камчиликлардан холи булиб, **АКТТТ** нинг стандартлар ва технологияларнинг Миллий университети томонидан ракамли имзонинг миллий стандартига асос каби кабул килинди.

5.7. Криптографик калитларни бошкариш

Хдр кандай криптографик тизим крпитографик калитлардан фойдаланишга асосланган. Калит ахбороти деганда ахборот тармокдари ва тизимларида ишлатилувчи барча калитлар мажмуи тушунилади. Агар калит ахборотларининг етарлича ишончли бошк,арилиши таъминланмаса, нияти бузук, одам унга эга булиб олиб тармок, ва тизимдаги барча ахборотдан х,охдаганича фойдаланиши мумкин. Калитларни бошкариш калитларни генерациялаш, сакдаш ва так,симлаш каби вазифаларни бажаради. Калитларни так,симлаш калитларни бошкариш жараёнидаги энг маъсулиятли жараён хисобланади.

Симметрик криптотизимдан фойдаланилганда ахборот алмашинувида иштирок этувчи иккала томон аввал махфий сессия калити, яъни алмашинув жараёнида узатиладиган барча хабарларни шифрлаш калити буйича келишишлари лозим. Бу калитни бошка барча билмаслиги ва уни вакти-вакти билан жунатувчи ва к,абул килувчида бир вактда алмаштириб туриш лозим. Сессия калити буйича келишиш жараёнини калитларни алмаштириш ёки таксимлаш деб хам юритилади.

Асимметрик криптотизимда иккита калит- очик, ва ёпик, (махфий) калит ишлатилади. Очик, калитни ошкор этиш мумкин, ёпик, калитни яши-

риш л озим. Хабар алмашинувида факат очик, калитни унинг хакикийлигини таъминлаган хрлда жунатиш лозим.

Калитларни таксимлашга куйидаги талаблар куйилади:

- таксимлашнинг оперативлиги ва аниклиги;
- таксимланувчи калитларнинг конфиденциаллиги ва яхлитлиги.

Компьютер тармокларидан фойдаланувчилар уртасида калитларни таксимлашнинг куйидаги асосий усулларидан фойдаланилади.

1. Калитларни таксимловчи битта ёки бир нечта марказлардан фойдаланиш.
2. Тармок, фойдаланувчилари уртасида калитларни тугридан-тугри алмашиш.

Биринчи усулнинг муаммоси шундаки, калитларни таксимлаш марказига кимга, кайси калитлар так,симланганлиги маълум. Бу эса тармок, буйича узатилаётган барча хабарларни укишга имкон беради. Булиши мумкин булган суиистеъмоллар тармок, хавфсизлигининг жиддий бузилишига олиб келиши мумкин.

Иккинчи усулдаги муаммо - тармок, субъектларининг хакикий экан-лигига ишонч хрсил к,илишдир.

Калитларни так,симлаш масаласи к,уйидагиларни таъминловчи калитларни таксимлаш протоколини куришга келтирилади:

- сеанс катнашчиларининг х,ак,ик,ийлигига иккала томоннинг тасдиги;
- сеанс х,ак,ик,ийлигининг тасдиги;
- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тарикасида Kerberos деб аталувчи калитларни аутентификациялаш ва так,симлаш тизимини курсатиш мумкин.

Иккинчи усулга-тармок, фойдаланувчилари уртасида калитларни тугридан-тугри алмашишга батафсил тухталамиз.

Симметрик калитли криптотизимдан фойдаланилганда криптографик х,имояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий махфий калитга эга булишлари лозим. Бу фойдаланувчилар умумий калит-

ни алока канали буйича хавфсиз алмашишлари лозим. Агар фойдаланувчилар калитни тез-тез узгартириб турсалар калитни етказиш жиддий муаммога айланади.

Бу муаммони ечиш учун куйидаги иккита асосий усул кулланилади:

1. Симметрик криптотизимнинг махфий калитини химоялаш учун очик, калитли асимметрик криптотизимдан фойдаланиш
2. Диффи-Хеллманнинг калитларни очик, таксимлаш тизимидан фой даланиш.

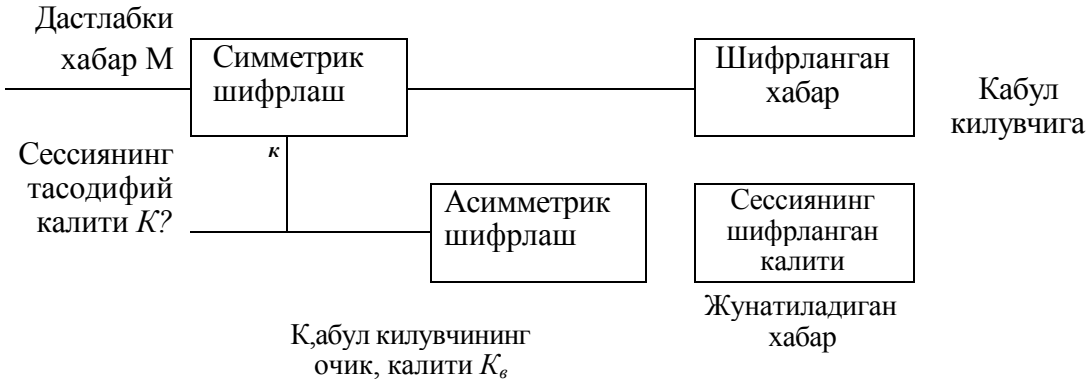
Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптотизим доирасида амалга оширилади. Бундай ёндашишда симметрик криптотизим дастлабки очик, матнни шифрлаш ва узатишда ишлатилса, очик, калитли асимметрик криптотизим факат симметрик криптотизимнинг махфий калитини шифрлаш, узатиш ва кейинги расшифровка килишда ишлатилади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очик, калитли асимметрик криптотизимнинг юкрри махфийлиги билан махфий калитли симметрик криптотизимнинг юкрри тезкорлигининг уйгунлашишга олиб келади. Бундай ёндашиш баъзида *электрон ракамли конверт* схемаси деб юритилади.

Фараз килайлик, фойдаланувчи *A* хабар *M* ни фойдаланувчи *B* га химояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмокчи. Унда фойдаланувчиларнинг харакатлари куйидагича булади.

Фойдаланувчи *A* нинг харакатлари:

1. Симметрик сеанс махфий калит K_s ни яратади (масалан, тасодифий тарзда генерациялайди).
2. Хабар *M* ни симметрик сеанс махфий калит $K_s m$ шифрлайди.
3. Махфий сеанс калит K_s ни фойдаланувчи (хабар кабул килувчи) 5нинг очик, калити $\Gamma_в$да шифрлайди.
4. Фойдаланувчи *B* адресига алоканинг очик, канали буйича шифрланган хабар *M* ни шифрланган сеанс калити K_s билан биргаликда узатади.

Фойдаланувчи *A* нинг харакаталарини 5.17-расмда келтирилган хабарларни комбинацияланган усул буйича шифрлаш схемаси оркали тушуниш мумкин.

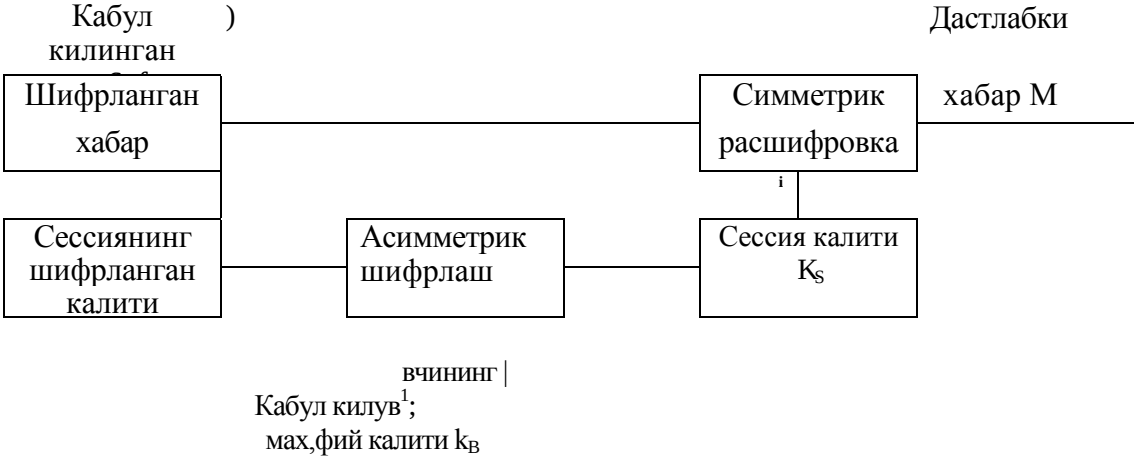


5.17-расм. Комбинацияланган усул бўйича хабарни шифрлаш схемаси.

Фойдаланувчи *B* нинг харакатлари (электрон ракамли конвертни-шифрланган хабар *M* ни ва шифрланган сеанс калити K_s ни олганидан сунгги) к,уйидагича:

1. Узининг махфий калити k_B буйича сеанс калити K_s ни расшифров ка килади.
2. Олинган сеанс калити K_s буйича олинган хабар *M* ни расшифров ка килади.

Фойдланувчи *B* нинг харакатларини 5.18-расмда келтирилган хабарларни комбинацияланган усул буйича расшифровка килиш схемаси оркали тушуниш мумкин.



5.18-расм. Комбинацияланган усул бўйича хабарни расшифровка цилиш.

Олинган электрон ракамли конвертни факат крнуний кабул килувчи-фойдаланувчи *B* очиши мумкин. Факат шахсий махфий калит $к_в$ эгаси булган фойдаланувчи *B* махфий сеанс калиги K_s ни тугри расшифровка килиш ва сунгра бу калит ёрдамида олинган хабар *M* ни расшифровка килиши ва укиши мумкин.

Ракамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари куйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини таркатиш муаммоси бартараф килинади, чунки хабарни шифрловчи сеанс калиги K_s очик, канал буйича шифрланган куринишда узатилади, калит $K_5яи$ расшифровка к,илиш учун асимметрик криптоалгоритмдан фойдаланилади;
- бу хрлда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо булмайди, чунки асимметрик алгоритм буйича факат киска калит K_s шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм буйича шифрланади.

Натижада тезкор шифрлаш билан биргаликда калитларнинг кулай так,симланиши амалга оширилади.

Шифрлашнинг комбинацияланган усулида симметрик хам асимметрик криптотизимларнинг криптографик калитларидан фойдаланилади. Равшанки, криптотизимнинг хар бир тури учун калитлар узунлигини шундай танлаш лозимки, нияти бузук, одамга комбинацияланган криптотизим химоясининг х,ар к,андай механизмига хужум килиш бир хил кийинчилик тугдирсин.

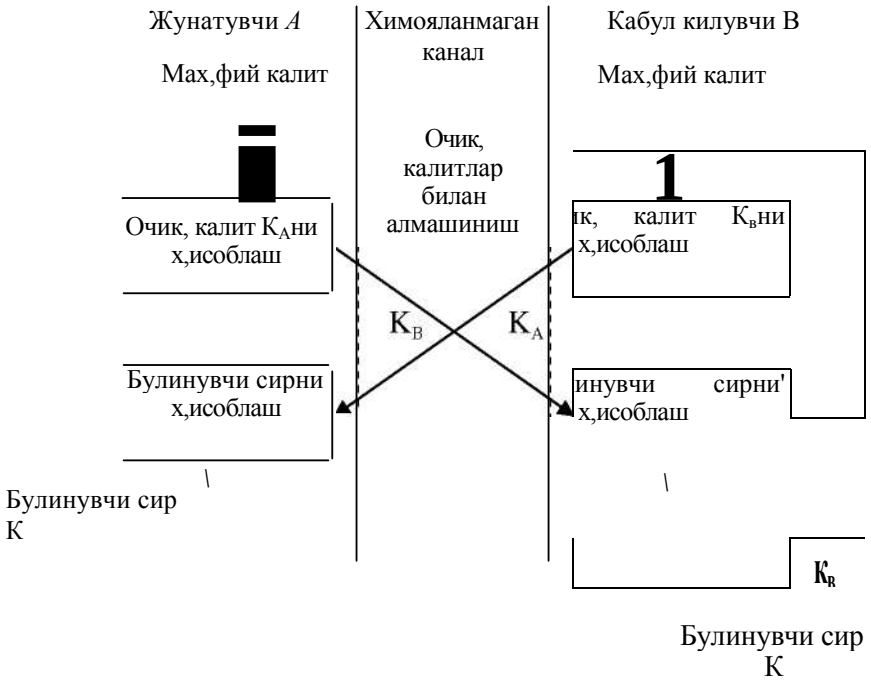
5.1-жадвалда куп учрайдиган симметрик ва асимметрик криптотизимлар калитларининг узунлиги келтирилган.

5.1-жадвал

Симметрик криптотизим калитлари узунлиги, битлар	Асимметрик криптотизим калитлари узунлиги, битлар
56	384
64	512
80	768
112	1792
128	2304

У. Диффи ва М.Хеллман томонидан кашф этилган *калитларни очщ тщсимлаш усули* фойдаланувчиларга калитларни хдмояланмаган алока каналлари оркали алмашишга имкон беради. Унинг хавфсизлиги чегараланган сохада дискрет логарифмларни хисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулининг мохдяти куйидагича (5.19-расм).



5.19-расм. Диффи-Хеллманнинг калитларни очщ тацсимлаш схемаси

Ахборот алмашинувида иштирок этувчи фойдаланувчилар А ва В мустак,ил равишда узларининг махфий калитларини $к_А$ ва $к_в$ ни генерация-лайдилар ($к_А$ ва $к_в$ калитлар фойдаланувчилар А ва В лар сир сакловчи тасодифий катта бутун сонлар).

Сунгра фойдаланувчи А узининг махфий калити $к_А$ асосида очик, калитни х,исоблайди:

$K_A=g^K A(modN).$

Вир вактнинг узида фойдаланувчи *В* узининг махфий калити k_B асосида очик, калитни х,исоблайди:

$K_B=g^{KB}(modN).$

Ву ерда *N ва g* - катта бутун оддий сонлар. Арифметик амаллар Л^нинг модулига келтириш орк,али бажарилади. *N ва g* сонларни сир сакдаш шарт эмас, чунки одатда, бу кийматлар тармок, ва тизимдан фойдаланувчиларнинг барчаси учун умумий х,исобланади.

Сунгра фойдаланувчилар А ва В узларининг очик, калитларини химояланмаган канал оркали алмаштирадилар ва умумий сессия махфий калити *Кии* (булинувчи сирни) хисоблашда ишлатадилар:

фойдаланувчи А: $K = (K_в)^{кл}(\text{modiV}) = (g^{kB} f^{A}(\text{modiV})$,

фойдаланувчи В: $K' = (K_A f^{B} (\text{mod\#}) = (g'^{A} f^{B} (\text{modJV})$,

бунда $K = K'$, чунки $(g^{kB} f^{A} = (g^{kA} f^{B} (\text{modN})$.

Шундай к,илиб, ушбу амаллар натижасида иккала махфий калит $к_A$ ва $к_в$ларнинг функцияси булган умумий сессия махфий калити хрсил к,илинади.

Очик, калитлар $К_A$ ва $К_в$ к,ийматларини ушлаб к,олган нияти бузук, одам сессия махфий калити $К$ ни хисоблай олмайди, чунки у махфий калитлар $к_A$ ва $к_в$ к,ийматларини билмайди. Вир томонлама функциянинг ишлатилиши сабабли очик, калитни х,исоблаш амали кайтарилмайдиган амал, яъни абонентнинг очик, калити киймати буйича унинг махфий калитини х,исоблаш мумкин эмас.

Диффи-Хеллман усулининг ноёблиги шундан иборатки, абонентлар жуфти тармок, орк,али очик, калитларни узатганларида фак,ат узларига маълум махфий сонни олиш имкониятига эга. Сунгра абонентлар узатилаётган ахборотни маълум текширилган усулни - олинган умумий сессия махфий калитидан фойдаланган х,олда симметрик шифрлашни ишлатиб химоялашга киришишлари мумкин.

Диффи-Хеллман схемаси маълумотларни хар бир сеансда янги калитларда шифрлаш имконини беради. Бу сирларни дискетларда ёки бошка элтувчиларда сакламасликка имкон беради, чунки бундай саклаш уларни рак,иблар ёки нияти бузук, одамлар к,улига тушиб к,олиш эхтимоллигини оширади.

Диффи-Хеллман схемаси *узатшаётган маълумотларнинг конфиденциаллигини ва аутентлигини (аслига тугрилигини) комплекс щмоялаш усулиши* хам амалга ошириш имконини беради. Алгоритм фойдаланувчига ракамли имзони ва симметрик шифрлашни бажаришда бир хил калитларни шакллантириш ва ишлатиш имконини беради.

Маълумотлар яхлитлигини ва конфиденциаллигини бир вакхда хдмоялаш учун шифрлаш ва электрон ракамли имзодан комплекс фойдаланиш максадга мувофик, хисобланади. Диффи-Хеллман схемаси ишлашининг оралик, натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллагини комплекс химоялаш усулини амалга оширишда фойдаланиш мумкин. Хакикатан, ушбу алгоритмга биноан фойдаланувчилар *А* ва *В* аввал узларининг махфий калитлари $к_А$ ва $к_в$ ни генерациялайдилар ва очик, калитлари $К_А$ ва $К_в$ ни хисоблайдилар. Су игра абонентлар *А* ва *В* бу оралик, натижалардан маълумотларни симметрик шифрлашда фойдаланилиши мумкин булган умумий булинувчи махфий калиги *К* ни бир вактда хисоблаш учун ишлатади.

Узатилаётган маълумотларнинг конфиденциаллигини ва аутентилигини комплекс химоялаш усули куйидаги схема буйича ишлайди:

- абонент *А* ракамли имзонинг стандарт алгоритмидан фойдаланиб, узининг махфий калити $к_А$ ёрдамида хабар *М* га имзо чекади;

- абонент *А* узининг махфий калити $к_А$ ва абонент *В* нинг очик, кали ти $К_в$ дан Диффи-Хеллман алгоритми буйича умумий булинувчи махфий калити *К* ни хисоблайди.

- абонент *А* олинган узаро булинувчи махфий калитда алмашинув буйича шериги билан келишилган симметрик шифрлаш алгоритмидан фойдаланган х,олда хабар *М* ни шифрлайди;

- абонент *В* шифрланган хабар *М* ни олиши билан узининг махфий калити $к_в$ ва абонент *А* нинг очик, калити $К_А$ дан Диффи-Хеллман алгорит ми буйича узаро булинувчи махфий калит *К* ни хисоблайди;

- абонент *В* олинган хабар *М* ни калити *К* да расшифровка килади;

- абонент *В* абонент *А* нинг очик, калит $К_А$ ёрдамида расшифровка килинган хабар *М* имзосини текширади.

Диффи-Хеллман схемаси асосида тармок, сатхида химояланган виртуал тармоклар VPN курилишида кулланилувчи криптокалитларни бошк,ариш протоколлари SKIP (Simple Key Management for Internet Protocols) ва IKE (Internet Key Exchange) ишлайди.

VI боб. ИНДЕНТИФИКАЦИЯ ВА АУТЕНТИФИКАЦИЯ 6.1.

Асосий тушунчалар ва туркумланиши

Компьютер тизимида руйхатга олинган хар бир субъект (фойдаланувчи ёки фойдаланувчи номидан харакатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боглик,.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри булиши мумкин. Бу ахборот субъект *индентификатори* деб юритилади. Агар фойдаланувчи тармокда руйхатга олинган индентификаторга эга булса у легал (крнуний), акс хрлда легал булмаган (нокрнуний) фойдаланувчи хисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан утиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) буйича аниклаш жараёни. Бу фойдаланувчи тармокдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сурови буйича узининг идентификаторини билдиради, тизим эса узининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) - маълум килинган фойдаланувчи, жараён ёки курилманинг хакикий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки курилма) хакикатан айнан узи эканлигига ишонч хосил килишига имкон беради. Аутентификация утказишда текширувчи тараф текширилувчи тарафнинг хакикий эканлигига ишонч хрсил килиши билан бир каторда текширилувчи тараф хам ахборот алмашинув жараёнида фаол катнашади. Одатда фойдаланувчи тизимга уз хусусидаги ноёб, бошкаларга маълум булмаган ахборотни (масалан, парол ёки сертификат) киритиши оркали идентификацияни тасдикдайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) х,ак,ик,ий эканлигини аниклаш ва текширишнинг узаро богланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боглик,. Субъектни

идентификациялаш ва аутентификациялашдан сунг уни авторизациялаш бошланади.

Авторизация (Authorization) - субектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект хдракати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлитлиги бузилиши мумкин. Аутентификация ва авторизация муолажалари билан фойдаланувчи харакатини маъмурлаш муолажаси узвий богланган.

Маъмурлаш (Accounting) - фойдаланувчининг тармокдаги харакатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини кайд этиш. Ушбу хисобот ахбороти хавфсизлик нуктаи назаридан тармокдаги хавфсизлик ходисаларини ошкор килиш, тахлиллаш ва уларга мое реакция курсатиш учун жуда мухимдир.

Маълумотларни узатиш каналларини химоялашда *субъектларнинг узаро аутентифшацияси,* яъни алока каналлари оркали богланадиган субъектлар хакикийлигининг узаро тасдиги бажарилиши шарт. Хакикийликнинг тасдиги одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. "Улаш" атамаси оркали тармокнинг иккита субъекти уртасида мантикий богланиш тушунилади. Ушбу муолажанинг максади - улаш крнуний субъект билан амалга оширилганлигига ва барча ахборот мулжалланган манзилга боришлигига ишончни таъминлашдир.

Узининг хак,ик,ийлигининг тасдикдаш учун субъект тизимга турли асосларни курсатиши мумкин. Субъект курсатадиган асосларга боглик, х,олда аутентификация жараёнлари к,уйидаги категорияларга булиниши мумкин:

бирор нарсани билиш асосида. Мисол сифатида парол, шахеий идентификация коди PIN (Personal Identification Number) хамда "суров жавоб" хилидаги протоколларда намойиш этилувчи махфий ва очик, калитларни курсатиш мумкин;

бирор нарсага эгалиги асосида. Одатда булар магнит карталар, смарт-карталар, сертификатлар ва touch memory курилмалари;

кандайдир дахлсиз характеристикалар асосида. Ушбу категория уз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кузининг рангдор пардаси ва тур пардаси, бармок, излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки кандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол — фойдаланувчи хамда унинг ахборот алмашинувидаги шериги биладиган нарса. Узаро аутентификация учун фойдаланувчи ва унинг шериги уртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул хисобланади. PIN - коднинг махфий киймати факат карта эгасига маълум булиши шарт.

Динамик - (бир марталик) парол - бир марта ишлатилганидан сунг бошка умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам узгариб турувчи киймат ишлатилади.

"Суров-жавоб" тизими - тарафларнинг бири ноёб ва олдиндан билиб булмайдиган "суров" кийматини иккинчи тарафга жунатиш оркали аутентификацияни бошлаб беради, иккинчи тараф эса суров ва сир ёрдамида хисобланган жавобни жунатади. Иккала тарафга битта сир маълум булгани сабабли, биринчи тараф иккинчи тараф жавобини тугрилигини текшириши мумкин.

Сертификатлар ва ракамли имзолар - агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда ракамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташки ишончли ташкилот томонидан берилади. Internet доирасида очик, калит сертификатларини тарк,атиш учун очик, калитларни бошк,арувчи к,атор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо булди. Фойдаланувчилар турли даража сертификатларини олишлари мумкин.

Аутентификация жарёнларини таъминланувчи хавфсизлик даражаси буйича хам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари куйидаги турларга булинади:

- пароллар ва ракамли сертификатлардан фойдаланувчи аутентифи кация;
- криптографик усуллар ва воситалар асосидаги катьий аутентифи кация;
- нуллик билим билан исботлаш хусусиятига эга булган аутентифи кация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуктаи назаридан юкррида келтирилганларнинг хар бири узига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир каторда таъкидлаш лозимки, нуллик билим билан исботлаш хусусиятига эга булган аутентификацияга кизикиш амалий характерга нисбатан купрок, назарий характерга эга. Балким, якин келажакда улардан ахборот алмашинувини химоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига буладиган асосий хужумлар куйидагилар:

маскарад (impersonation). Фойдаланувчи узини бошка шахе деб курсатишга уриниб, у шахе тарафидан харакатларнинг имкониятларига ва имтиёзларига эга булишни мулжаллайди;

аутентификация алмашинуви *тарафини алмаштириб купит* (interleaving attack). Нияти бузук, одам ушбу хужум мобайнида икки тараф орасидаги аутенфикацион алмашиниш жараёнида трафикни модификация-лаш ниятида к,атнашади. Алмаштириб к,уйишнинг куйидаги хили мавжуд: иккита фойдаланувчи уртасидаги аутентификация муваффак,иятли утиб, уланиш урнатилганидан сунг бузгунчи фойдаланувчилардан бирини чикариб ташлаб, унинг номидан ишни давом эттиради;

такрорий узатиш (replay attack). Фойдаланувчиларнинг бири томонидан аутентификация маълумотлари такроран узатилади;

узатишни цайтариш (reflection attak). Олдинги хужум вариантларидан бири булиб, хужум мобайнида нияти бузук, одам протоколнинг ушбу сессия доирасида ушлаб крлинган ахборотни оркага кайтаради.

мажбурий кечикиш (forced delay). Нияти бузук, одам кандайдир маълумотни ушлаб крлиб, бирор вактдан сунг узатади.

матн танлашли хужум (chosen text attack). Нияти бузук, одам аутентификация трафигини ушлаб крлиб, узок, муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юкррида келтирилган хужумларни бартараф килиш учун аутентификация протоколларини куришда куйидаги усуллардан фойдал анил ади:

"суров-жавоб", вакт белгилари, тасодифий сонлар, индентификаторлар, ракамли имзолар каби механизмлардан фойдаланиш;

аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги харакатларига богааш. Бундай мисол ёндашишга тарикасида аутентификация жараёнида фойдаланувчиларнинг кейинга узаро алокаларида ишлатилувчи махфий сеанс калитларини алмашишни курсатиш мумкин;

алоканинг ур^{натилган} сеанси доирасида аутентификация муолажасини вакти-вакти билан бажариб туриш ва х,.

"Суров-жавоб" механизми к,уйидагича. Агар фойдаланувчи *А* фойдаланувчи *В* дан оладиган хабари ёлгон эмаслигига ишонч хосил килишни истаса, у фойдаланувчи *В* учун юборадиган хабарга олдиндан билиб булмайдиган элемент - *X* суровини (масалан, к,андайдир тасодифий сонни) кушали. Фойдаланувчи В жавоб беришда бу амал устида маълум амални (масалан, кандайдир *f(X)* функцияни х,исоблаш) бажариши лозим. Буни олдиндан бажариб булмайди, чунки суровда к,андай тасодифий сон *X* келиши фойдаланувчи *В* га маълум эмас. Фойдаланувчи *В* харакати натижасини олган фойдаланувчи *А* фойдаланувчи *В* нинг хакикий эканлигига ишонч хосил к,илиши мумкин. Ушбу усулнинг камчилиги - суров ва жавоб уртасидаги крнуниятни аниклаш мумкинлиги.

Вактни белгилаш механизми хар бир хабар учун вактни кайдлашни кузда тутади. Бунда тармокнинг хар бир фойдаланувчиси келган хабарнинг канчалик эскирганини аниклаши ва уни кабул килмаслик карорига келиши мумкин, чунки у ёлгон булиши мумкин. Вактни белгилашдан фойдаланишда сеанснинг хакикий эканлигини тасдиклаш учун *кечикишнинг жоиз вакт оралиги* муаммоси пайдо булади. Чунки, "вакт тамгаси"ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташкари, кабул килувчи ва жунатувчининг соатлари мутлакр синхронланган булиши мумкин эмас.

Аутентификация протоколларини так,к,ослашда ва танлашда куйидаги характеристикаларни х,исобга олиш зарур:

узаро аутентификациянинг мавжудлиги. Ушбу хусусият аутентификацион алмашинув тарафлари уртасида иккиёкдама аутентификациянинг зарурлигини акс эттиради;

щсоблаш самарадорлиги. Протоколни бажаришда зарур булган амаллар сони;

коммуникацион самарадорлик. Ушбу хусусият аутентификацияни бажариш учун зарур булган хабар сони ва узунлигини акс эттиради;

учинчи тарафнинг мавжудлиги. Учинчи тарафга мисол тарикасида симметрик калитларни таксимловчи ишончли серверни ёки очик, калитларни так,симлаш учун сертификатлар дарахтини амалга оширувчи серверни курсатиш мумкин;

хавфсизлик кафолати асоси. Мисол сифатида нуллик билим билан исботлаш хусусиятига эга булган протоколларни курсатиш мумкин;

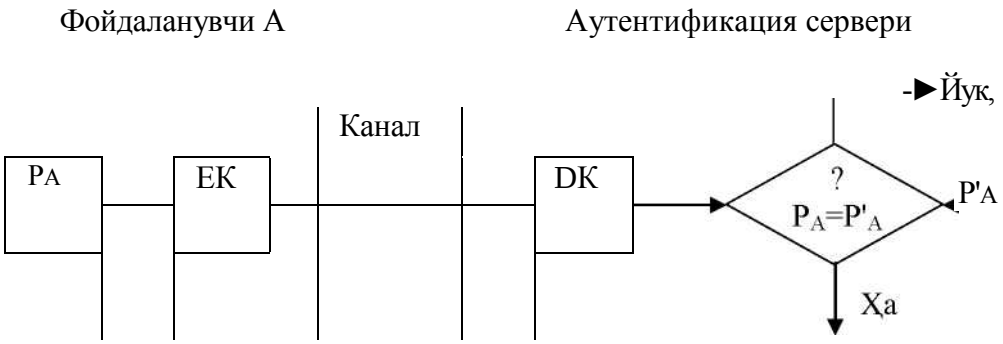
сирни сацлаш. Жиддий калитли ахборотни саклаш усули кузда тутилади.

6.2. Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарк,алган схемаларидан бири *оддий аутентификациялаш* булиб, у анъанавий куп мартали паролларни ишлатиши-

га асосланган. Тармокдаги фойдаланувчини оддий аутентификациялаш муолажасини дуйидагича тасаввур этиш мумкин. Тармокдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида узининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сакланаётган фойдаланувчи идентификатори буйича маълумотлар базасидан мое ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таддосланади. Агар улар мое келса, аутентификация муваффакиятли утган хисобланади ва фойдаланувчи легал (донуний) мадомини ва авторизация тизими ордали унинг мадоми учун анидланган худудларни ва тармод ресуреларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган хрлда оддий аутентификациялаш схемаси 6.1-расмда келтирилган.



Парол ^акдк,ий *6.1-*

раем. Паролдан фойдаланган уолда оддий аутентификациялаш.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш ордали аутентификациялаш варианти хавфеизликнинг хатто минимал даражасини кафолатламайди. Паролни химоялаш учун уни химояланмаган канал ордали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва расшифровка дилиш D_K воситалари киритилган. Бу воситалар булинувчи махфий калит К ордали бошдарилади. Фойдаланувчининг хадидийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида садланувчи дастлабки диймат P_A ни таддослашга асосланган. Агар P_A ва P_A дийматлар мое келса, парол P_A хадидий, фойдаланувчи A эса донуний хисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафакат паролларни узатиш, балки уларни саклаш ва текшириш турлари билан ажралиб туради. Энг кенг тарк,алган усул - фойдаланувчилар паролини тизимли файлларда, очик, хрлда сакдаш усулидир. Бунда файлларга укиш ва ёзишдан химоялаш атрибутлари урнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мое имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сакданаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги - нияти бузук, одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.

Хавфсизлик нуктаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сакдаш кулай хдеобланади. Бу хрлда фойдаланувчи паролнинг очик, шакли урнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу узгартириш ганим томонидан паролни унинг тасвири оркали ошкор кила олмаганлигини кафолатлайди, чунки ганим ечилмайдиган сонли масалага дуч келади.

Куп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сузларнинг нисбатан катта булмаган тупламидан жамланади. Куп мартали паролларнинг таъсир муддати ташкилотнинг хавфеизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар лугатда булмасин ва уларни топиш кийин булсин.

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга хар бир суров учун турли пароллар ишлатилади. Бир мартали динамик парол факат тизимдан бир марта фойдаланишга ярокди. Агар, хатто кимдир уни ушлаб крлса х,ам парол фонда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланувчиларни текширишда кулланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул ок,али амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташкаридан тулов пластик карточкаларига ухшаш микропроцессор урнатилган миниатюр курилмалар куринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта булмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни куллашнинг куйидаги усуллари маълум:

1. Ягона вакт тизимига асосланган вакт белгилари механизмидан фойдаланиш.
2. Легал фойдаланувчи ва текширувчи учун умумий булган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механиз мидан фойдаланиш.
3. Фойдаланувчи ва текширувчи учун умумий булган бир хил дастлабки кийматли псевдотасодифий сонлар генераторидан фойдала ниш.

Биринчи усулни амалга ошириш мисоли сифатида SecurlD аутентикациялаш технологиясини курсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чикилган булиб, катор компанияларнинг, хусусан Cisco Systems компаниясининг серверларида амалга оширилган.

Вакт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вактнинг маълум оралигидан сунг генерациялаш алгоритмига асосланган. Аутентификация схемаси куйидаги иккита параметрдан фойдаланади:

- хар бир фойдаланувчига аталган ва аутентификация серверида х,амда фойдаланувчининг аппарат калитида сакданувчи ноёб 64-битли сондан иборат махфий калит;
- жорий вакт киймати.

Масофадаги фойдаланувчи тармокдан фойдаланишга уринганида ундан шахсий идентификация номери РЕЧни киритиш таклиф этилади. PIN туртта унли ракамдан ва аппарат калити дисплейида аксланувчи тасодифий

соннинг олтита ракамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вакт киймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сунгра сервер генерацияланган сон билан фойдаланувчи киритган сонни такдослайди. Агар бу сонлар мое келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

Аутентификациянинг бу схемасидан фойдаланишда аппарат калит ва сервернинг катъий вактий синхронланиши талаб этилади. Чунки аппарат калит бир неча йил ишлаши ва демак сервер ички соати билан аппарат калитининг мувофиклиги аста-секин бузилиши мумкин.

Ушбу муаммони х,ал этишда Security Dynamics компанияси куйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чикилаётганида унинг таймер частотасининг меъёридан четлашиши аник, улчанади. Четлашишнинг бу киймати сервер алгоритми параметри сифатида хисобга олинади;
- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият тугилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боглик,. Аппарат калит генерациялаган тасодифий сон катта булмаган вакт оралиги мобайнида хакикий парол хисобланади. Шу сабабли, умуман, киска муддатли вазият содир булиши мумкинки, хакер PIN-кодни ушлаб крлиши ва уни тармокдан фойдаланишга ишлатиши мумкин. Бу вакт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи хисобланади.

Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант - «суров-жавоб» схемаси буйича аутентификациялаш. Фойдаланувчи тармокдан фойдаланишга уринганида сервер унга тасодифий сон куринишидаги суровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва сервернинг маълумотлар базасида сакланувчи махфий калити ёрдамида расшифровка килади. Тасодифий сон - суров шифрланган куринишда серверга кайтарилади. Сервер хам уз навбатида

уша DES алгоритми ва серверниг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида узи генерациялаган тасодифий сонни шифрлайди. Сунгра сервер шифрлаш натижасини аппарат калитидан келган сон билан такдослайди. Бу сонлар мое келганида фойдаланувчи тармокдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «суров-жавоб» аутентификациялаш схемаси ишлатишда вакт синхронизациясидан фойдаланувчи аутентификация схемасига Караганда мураккаброк,.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий булган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали парольларнинг булинувчи руйхати махфий пароллар кетма-кетлиги ёки туплами булиб, хар бир парол факат бир марта ишлатилади. Ушбу руйхат аутентификацион алмашинув тарафлар уртасида олдиндан таксимланиши шарт. Ушбу усулнинг бир вариантига биноан суров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи суровлар ва жавоблар мавжуд булиб, хар бир жуфт факат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий булган бир хил дастлабки кийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг куйидаги вариантлари мавжуд:

- *узгартирилувчи бир мартали пароллар кетма-кетлиги.* Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади;
- *бир томонлама функцияга асосланган пароллар кетма-кетлиги.* Ушбу усулнинг мохиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машхур схемаси) ташкил этади. Хавфсизлик нуктаи назаридан бу усул кетма-кет узгартирилувчи пароллар усулига нисбатан афзал х,исобланади.

Кенг тарк,алган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internet да стандартлаштирилган S/Key (RFC 1760) протоколидир. Ушбу протокол масофадаги фойдаланувчиларнинг хакикийлигини текширишни талаб этувчи купгина тизимларда, хусусан, Cisco компаниясининг TACACS+тизимида амалга оширилган.

Сертификатлар асосида аутентификациялаш

Тармокдан фойдаланувчилар сони миллионлаб улчанганида фойдаланувчилар паролларининг тайинланиши ва сакданиши билан боглик, фойдаланувчиларни дастлабки руйхатга олиш муолажаси жуда катта ва амалга оширилиши кийин булади. Бундай шароитда ракамли сертификатлар асосидаги аутентификациялаш пароллар кулланишига рационал альтернатива хисобланади.

Ракамли сертификатлар ишлатилганида компьютер тармоги фойдаланувчилари хусусидаги хеч кандай ахборотни сакламайди. Бундай ахборотни фойдаланувчиларнинг узи суров-сертификатларида такдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни саклаш вазифаси фойдаланувчиларнинг узига юкланади.

Фойдаланувчи шахсини тасдикдовчи рак,амли сертификатлар фойдаланувчилар сурови буйича махсус ваколатли ташкилот-сертификация маркази CA (Certificate Authority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг узи хам фойдаланувчининг хакикийлигини текшириш (яъни, аутентификациялаш) боскичини уз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази CA) булади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдикдовчи маълумотни ва очик, калитини такдим этиши лозим. Зарурий маълумотлар руйхати олинадиган сертификат турига боглик,. Сертификацияловчи ташкилот фойдаланувчининг хакикийлиги тасдигини текширганидан сунг узининг ракамли имзосини очик, калит ва фойдаланувчи хусусидаги маълумот булган файлга жойлаштиради х,амда ушбу очик, калитнинг му-

айян шахсга тегишли эканлигини тасдиклаган хрлда фойдаланувчига сертификат беради.

Сертификат электрон шакл булиб, таркибида куйидаги ахборот булади:

- ушбу сертификат эгасининг очик, калити;

- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта адреси, ишлайдиган ташкилот номи ва х,.;

- ушбу сертификатни берган ташкилот номи;

- сертификацияловчи ташкилотнинг электрон имзоси - ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармок, ресурсларига мурожаат этганида аутентификацияловчи восита хисобланади. Бунда текширувчи тараф вазифасини корпоратив тармокнинг аутентификация сервери бажаради. Сертификатлар нафакат аутентификациялашда, балки фойдаланишнинг маълум хукукларини такдим этишда ишлатилиши мумкин. Бунинг учун сертификатга кушимча хршиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги курсатилади.

Очик, калитларнинг сертификатлар билан узвий богликдигини алохида таъкидлаш лозим. Сертификат нафакат шахсни, балки очик, калит мансублигини тасдикдовчи хужжатдир. Ракамли сертификат очик, калит ва унинг эгаси уртасидаги мосликни урнатади ва кафолатлайди. Бу очик, калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви буйича шеригидан сертификат таркибидаги очик, калитни олса, у бу сертификатдаги сертификация марказининг ракамли имзосини ушбу сертификация марказининг очик, калити ёрдамида текшириш ва очик, калит адреси ва бошка маълумотлари сертификатда курсатилган фойдаланувчига тегишли эканлигига ишонч х,осил к,илиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар руйхатини уларнинг пароллари билан корпорация серверларида саклаш зарурияти йук,олади. Серверда сертификацияловчи ташкилотларнинг номлари ва очик, калитларининг булиши етарли.

Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очик, калитларидан кизиккдн барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган.

Сертификатлар асосида аутентификациялаш жараёнини амалга оширишда сертификацияловчи ташкилот вазифасини ким бажариши хусусидаги масалани ечиш мухим хисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг узи ечиши жуда табиий хисобланади. Корхона узининг ходимларини яхши билади ва улар шахсини тасдиклаш вазифасини узига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат курсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, Netscape Communications компанияси серверларини корхоналарга шахсий сертификатларини чикариш учун таклиф этади.

Сертификацияловчи ташкилот вазифасини бажаришда тижорат асосида сертификат бериш буйича мустакил марказлар хам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари х,алкаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар химоясининг катор махсулотларида, жумладан химояланган канал SSL протоколида ишлатилади.

6.4. К,атъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи к,атъий аутентификациялаш гояси к,уйидагича. Текширилувчи (исботловчи) тараф кандайдир сирни билишини намойиш этган хрлда текширувчига узининг х,ак,ик,ий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари уртасида олдиндан хавфсиз усул билан таксимланган булиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган хрлда суров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг мухдми, исботловчи тараф факдт сирни билишлигини намойиш этади, сирни узи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли суровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний суров факдт фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошлангач суровга боглик, булади.

Аксарият хрлларда кдтъий аутентификациялашга биноан хдр бир фойдаланувчи узининг махфий калитига эгалиги аломати буйича аутентификацияланади. Бошкдча айтганда фойдаланувчи унинг алокд буйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви буйича хдк,ик,ий шерик эканлигини исботлашга ишлата олиши мумкинлигини аникдаш имкониятига эга.

X.509 стандарти тавсияларига биноан кдтъий аутентификациялашнинг куйидаги муолажалари фаркданади:

- бир томонлама аутентификация;
- икки томонлама аутентификация;
- уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йуналтирилган ахборот алмашинувини кузда тутади. Аутентификациянинг бу тури куйидагиларга имкон яратади:

- ахборот алмашинувчининг факдт бир тарафини хак,ик,ийлигини тасдикдаш;
- узатилаётган ахборот яхлитлигининг бузилишини аникдаш;
- "узатишнинг такрори" типидаги хужумни аникдаш;
- узатилаётган аутентификацион маълумотлардан фак,ат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификацилаши бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг к,ушимча жавоби булади. Бу жавоб текширувчи томонни алокднинг айнан аутентификация маълумотлари мулжалланган тараф билан урнатилаётганига ишонтириш лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга к,ушимча маълумотлар узатиш мавжуд. Бундай ёндашиш аутентификация утказишда вакт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш л озимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар туплами аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боглик,. Кдтъий аутентификациянинг утказилиши ишлатиладиган криптографик алгоритмлар ва катор кушимча параметрларни тарафлар томонидан сузсиз мувофикдаштиришни талаб этади.

Кдтъий аутентификациялашнинг муайян вариантларини куришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тухташ лозим. Бир мартали параметрлар баъзида "nonces" - бир максадга бир мартадан ортик, ипшатилмайдиган катталик деб аталади.

Хрзирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вакт белгилари ва кетма-кетликларнинг номерларини курсатиш мумкин.

Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб куйишни ва очик, матнни танлаш билан хужум килишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вактий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алох,ида ишлатилиши, ёки бир-бирини тулдириши мумкин.

Бир мартали параметрларнинг куйидаги ишлатилиш мисолларини курсатиш мумкин:

- "суров-жавоб" принципида к,урилган протоколларда уз вактидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш билан вакт белгилари ёки муайян жуфт (текширувчи, исботловчи) учун кетма-кетликларнинг номерларидан фойдаланиш мумкин;

- уз вактидалигини ёки ноёблик кафолатини таъминлаш. Протоколнинг бир мартали параметрларини бевосита (тасодифий сонни танлаш нули билан) ёки билвосита (булинувчи сирдаги ахборотни тахлиллаш ёрдамида) назоратлаш орк,али амалга оширилади;

- хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир охангда усувчи кетма-кетликнинг бир мартали кийматини (масалан, серия номерлари ёки вакт белгилари кетма-кетлиги) ёки мое узунликдаги тасодифий сонларни тузиш оркали амалга оширилади.

Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошка вариантларида хам (масалан, калит ахборотини таксимлаш протоколларида) кенг кулланилади.

Кдтъий аутентификациялаш протоколларини кулланиладиган криптографик алгоритмларига боглик, хрлда куйидаги гурухдарга ажратиш мумкин:

- шифрлашнинг симметрик алгоритмлари асосидаги катъий аутенти фикациялаш протоколлари;
- бир томонлама калитли хеш-функциялар асосидаги катъий аутенти фикациялаш протоколлари;
- шифрлашнинг асимметрик алгоритмлари асосидаги катъий аутенти фикациялаш алгоритмлари;
- электрон ракамли имзо асосидаги катъий аутентификациялаш алго ритмлари.

Симметрик алгоритмларга асосланган катъий аутентификациялаш. Kerberos протоколи.

Симметрик алгоритмлар асосида курилган аутентификациялашнинг ишлаши учун текширувчи ва исботловчи айни бошидан битта махфий калитга эга булишлари зарур. Фойдаланувчилари куп булмаган ёпик, тизимлар учун фойдаланувчиларнинг хар бир жуфти махфий калитни узаро булиб олишлари мумкин. Симметрик шифрлаш технологиясини к,улловчи катта так,симланган тизимларда ишончли сервер к,атнашувидаги аутентификациялаш протоколларидан фойдаланилади. Бу сервер билан х,ар бир тараф калитни билишлигини уртокдашишади.

Ушбу ёндашиш содда булиб туюлсада, аслида бундай аутентификациялаш протоколини ишлаб чикиш мураккаб ва хавфеизлик нуктаи назаридан шубхасиз эмас.

Куйида шифрлашнинг симметрик алгоритмларига асосланган, 18ОЯЕС9798-2да спецификацияланган аутентификациялаш протоколлари-

нинг учта мисоли келтирилган. Бу протоколлар булинувчи махфий калитларни олдиндан таксимланишини кузда тутади. Аутентфикациялашнинг куйидаги вариантларини куриб чикамиз.

- вакт белгиларидан фойдаланувчи бир томонлама аутентификациялаш.

- тасодифий сонлардан фойдаланувчи бир томонлама аутентификациялаш.

- икки томонлама аутентификациялаш.

Бу вариантларнинг хдр бирида фойдаланувчи махфий калитни билишини намойиш к,илган хрлда, узининг хакикийлигини исботлайди, чунки ушбу махфий калит ёрдамида суровларни расшифровка килади. Аутентификациялаш жараёнида симметрик шифрлашни куллашда узатиладиган маълумотларнинг яхлитлигини таъминлаш механизмини раем булиб крлган усуллар асосида амалга ошириш хам зарур.

Куйидаги белгилашларни киритамиз:

$г_A$- катнашувчи А генерациялаган тасодифий сон;

$г_в$- катнашувчи В генерациялаган тасодифий сон;

t_A- катнашувчи А генерациялаган вакт белгиси;

$E_к$- калит Кда симметрик шифрлаш (калит К олдиндан А ва В уртасида таксимланиши шарт).

Вщт белгиларига асосланган бир томонлама аутентификациялаш:

$A^B:E_K (t_A, B)$ (1)

Ушбу хабарни олиб расшифровка килганидан сунг к,атнашувчи В вакт меткаси t_A х,акикий эканлигига ва хабарда курсатилган идентификатор узиники билан мое келишига ишонч хреил к,илади. Ушбу хабарни кайтадан узатишни олдини олиш калитни билмасдан туриб вакт меткаси t_A ни ва индентификатор Вни узгартириш мумкин эмаслигига асосланади.

Тасодифий сонлардан фойдаланишга асосланган бир томонлама аутентфикациялаш:

$A^B:г_в$ (1)

$A^B:E_к(г_в,B)$ (2)

Катнашувчи *B* катнашувчи *A* га тасодифий сон $г_в$ни жунатади. Катнашувчи *A* олинган сон $г_в$ ва идентификатор *B* дан иборат хабарни шифрлайди ва шифрланган хабарни катнашувчи *B* га жунатади. Катнашувчи *B* олинган хабарни расшифровка килади ва хабардаги тасодифий сонни катнашувчи Ага юборгани билан такдослайди. Кушимча у хабардаги исмни текширади.

Тасодифий цийматлардан фойдаланувчи икки томонлама аутентификациялаш:

$A \hat{} B: г_в$ (1)

$A \hat{} > B: E_к(г_A, г_в, B)$ (2)

$A \hat{} B: E_к(г_A, г_в)$ (3)

Иккинчи ахборотни олиши билан катнашувчи *B* олдинги протоколдаги текширишни амалга оширади ва катнашувчи *A* га аталган учунчи хабарга киритиш учун к,ушимча тасодифий сон $г_A$*яи* расшифровка к,илади. Кдтнашувчи *A* учинчи хабарни олганидан сунг $г_A$ ва $г_в$ларнинг кийматларини текшириш асосида айнан к,атнашувчи *B* билан ишлаётганига ишонч хрсил к,илади.

Аутентификация жараёнида учинчи тарафни жалб этиш билан фойдаланувчиларни аутентификациялашни таъминловчи протоколларнинг машх,ур намуналари сифатида Нидхэм ва Шредернинг махфий калитларни таксимлаш протоколини ва Kerberos протоколини курсатиш мумкин.

Kerberos протоколи "мижоз-сервер" ва хам локал ва х,ам глобал тармокдарда ишловчи абонентлар орасида алоканинг х,имояланган каналини урнатишга аталган калит ахборотини алмашиш тизимларида аутентификациялаш учун ишлатилади. Бу протоколнинг Microsoft Windows 2000 ва UNIX BSD операцион тизимларига аутентификациялашнинг асосий протоколи сифатида урнатилганлиги алох,ида кизикиш уйготади.

Kerberos ишонч к,озонмаган тармокдарда аутентификациялашни таъминлайди, яъни Kerberos ишлашида нияти бузук, одамлар к,уйидаги харакатларни бажаришлари мумкин:

- узини тармок, уланишининг эътироф этилган тарафларидан бири деб курсатиш;

- уланишда иштирок этаётган компьютерларнинг биридан фойдалана олиш;

- хдр кандай пакетни ушлаб крлиш, уларни модификациялаш ва/ёки иккинчи марта узатиш.

Kerberos протоколида хавфсизлик таъминоти юкррида келтирилган нияти бузук, одамларнинг харакатлари натижасида пайдо буладиган хар кандай муаммоларнинг бартарафланишини таъминлайди.

Kerberos протоколи олдинги асрнинг 80-йилларида яратилган ва шу пайтгача бешта версияда уз аксини топган катор жиддий узгаришларга дучор булди.

Kerberos ТСРЯР тармоклари учун яратилган булиб, протокол катнашчиларининг учинчи(ишонилган) тарафга ишонишлари асосига курилган. Тармокда ишловчи Kerberos хизмати ишонилган воситачи сифатида харакат килиб, тармок, ресурсларидан мижознинг (мижоз иловасининг) фойдалинишини авторизациялаш билан тармокда ишончли аутентификациялашни таъминлайди. Kerberos хизмати алохида махфий калитни тармокнинг хар бир субъекти билан булишади ва бундай махфий калитни билиш тармок, субъекти хакикийлигининг исботига тенг кучлидир.

Kerberos асосини Нидхем-Шредернинг учинчи ишонилган тараф билан аутентификациялаш ва калитларни таксимлаш протоколи ташкил этади. Нидхем-Шредер протоколининг ушбу версиясини Kerberosra татбик,ан курайлик. Kerberos протоколида (5-версия) алок,а к,илувчи иккита тараф ва калитларни таксимлаш маркази KDC(Key Distribution Center) вазифасини бажарувчи ишонилган сервер KS иштирок этади.

Чакирувчи объект А орк,али, чак,ирилувчи объект В орк,али белгиланади. Сеанс катнашчилари, мое х,олда Id_A ва Id_B ноёб идентификаторларга эга. А ва В тарафлар, хар бири алохида, узининг махфий калитини сервер KS билан булишади.

Айтайлик, А тараф В тараф билан ахборот алмашиш максадида сеанс калитини олмок,чи. А тараф тармок, оркали сервер KSra Id_A ва Id_B идентификаторларни юбориш билан калитлар так,симланиши даврини бошлаб беради:

$$A\text{^>}KS{:}Id_A{,}Id_B$$

Сервер KS вактий белги Г, таъсир мудцати *L,* тасодифий калит *К* ва идентфикатор $ЬI_A$ булган хабарни генерациялаб, бу хабарни *В* тараф билан булинган махфий калит ёрдамида шифрлайди.

Сунгра сервер KS *В* тарафга тегишли вактий белги Г, таъсир мудцати *L,* тасодифий калит *К,* идентификатор $ЬI_в$ ни олиб уни *А* тараф билан булинган махфий калит ёрдамида шифрлайди. Бу иккала шифрланган хабарларни *А* тарафга жунатади.

$$KS\ \text{^}A{:}E_A(T,L,K,Id_B),E_B(T,L,K,Id_A)$$

А тараф биринчи хабарни узининг махфий калиги билан расшифровка килаци ва ушбу хабар калитлар таксимотининг олдинги муолажасининг кайтарилиши эмаслигига ишонч хрсил килиш максацида вакт белгиси Г ни текширади. Сунгра *А* тараф узининг идентификатори Id_A ва вакт белгиси билан хабарни генерациялаб, уни сеанс калиги *К* ёрдамида шифрлайди ва *В* тарафга узатади. Ундан ташкари, *А* тараф *В* тараф учун KS дан *В* тараф калиги ёрдамида шифрланган хабарни жунатади:

$$A\text{^}B{:}E_K(Id_A,T),E_B(T,L,KJd_A)$$

Бу хабарни факат *В* тараф расшифровака килиши мумкин. *В* тараф вакт белгиси Г, таъсир мудцати *L,* сеанс калиги *К* ва идентификатор Id_A ни олаци. Сунгра *В* тараф сеанс калит *К* ёрцамида хабарнинг иккинчи кисмини расшифровка килаци. Хабарнинг иккала кисмидаги Г ва Id_A кийматларининг мое келиши *А* нинг *В* га нисбатан хакикийлигини тасциклайди.

Хакикийликни узаро тасцикдаш мак,сацида *В* тараф вакт белгиси Г плюс 1 цан иборат хабар яратаци, уни *К* калит ёрцамида шифрлайди ва *А* тарафга жунатаци.

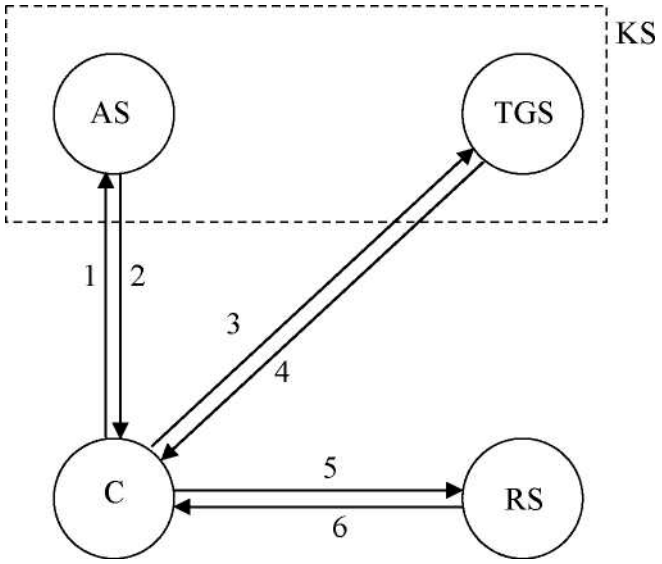
$$B\text{^}A{:}E_к(T + \backslash)$$

Агар бу хабар (4) расшифровка килингандан кейин *А* тараф кутилган натижани олса, у алока линиясининг бошка тарафида х,ак,ик,атан *В* турганлигига ишонч хрсил килаци.

Бу протокол барча катнашувчиларнинг соатлари сервер KS соатлари билан синхронланганида муваффакиятли ишлайди. Таъкидлаш л озимки, бу

протоколда *A* тарафнинг *B* тараф билан алока урнатишга *ДР бир хохдшида сеанс калитини олиш учун KS билан алмашинув зарур булади. Протоколнинг *A* ва *B* объектларни ишончли улаши учун, хеч бир калит обрусизланмаслиги ва сервер KS нинг хдмояланиши талаб этилади.

Умуман *Kerberos* тизимида (5 версия) фойдаланувчини идентификациялаш ва аутентификациялаш жараёнини куйидагича тавсифлаш мумкин (6.2-расм).



Белгилашлар:
KS - Kerberos тизими сервери
AS - аутентификация сервери
TGS - мандатларни ажратиш хизмати сервери
RS - ахборот ресурслари сервери
C - Kerberos тизимининг мижози

6.2-расм. Kerberos протоколининг ишлаш схемаси

Мижоз С, тармок, ресурсидан фойдаланиш максадида аутентификация сервери *AS* га суров йуллайди. Сервер *AS* фойдаланувчини унинг исми ва пароли ёрдамида идентификациялайди ва мижозга мандат ажратиш хизмати сервери *TGSRZH (Ticket Grating Service)* фойдаланишга мандат юборади.

Ахборот ресурсларининг муайян максадли сервери *RS* дан фойдаланиш учун мижоз *C TGS* дан максадли сервер *RS* га мурожаат килишга мандат сурайди. Хдмма нарса тартибда булса *TGS* керакли тармок, ресурсларидан фойдаланишга рухсат бериб, клиент *C* га мое мандатни юборади.

Kerberos тизими ишлашининг асосий кадамлари (6.2.-расмга каралсин):

1. *C ^ AS* - мижоз *C* нинг *TGS* хизматига мурожаат килишга рухсат сураб сервер А5дан сурови.

2. *AS -^ C* - сервер *AS* нинг мижоз *C* га *TGS* хизматидан фойдаланиш га рухсати (мандати).

3. *C^TGS* - мижоз *C* нинг ресурслар сервери *RS* дан фойдаланишга рухсат (мандат) сураб, *TGS* хизматидан сурови.

4. *TGS* -» С - *TGS* хизматининг мижоз *C* га ресурслар сервери *RS* дан фойдаланишига рухсати (мандата).

5. *C* -^*RS* - сервер *RS* дан ахборот ресурсининг (хизматнинг) сурови.

6. *RS* —» С - сервер і?5 нинг хакикийлигини тасдиклаш ва мижоз С га ахборот ресурсини (хизматни) такдим этиш.

Мижоз билан сервер алокасининг ушбу модели факдт узатиладиган бошк,арувчи ахборотнинг конфиденциаллиги ва яхлитлиги таъминланганида ишлаши мумкин. Ахборот хавфсизлигини кдтъий таъминламасдан *AS, TGS* ва *RS* серверларга мижоз *C* суров юбораолмайди ва тармок, хизматидан фойдаланишга рухсат ололмайди.

Ахборотнинг ушлаб к,олиниши ва рухсатсиз фойдаланиши имкониятларини бартараф этиш мак,садида Kerberos тармокда х,арк,андай бошкдриш ахбороти узатилганида махфий калитлар комплексини (мижознинг махфий калити, сервернинг махфий калиги, мижоз-сервер жуфтининг махфий сеанс калитлари) куп марта шифрлашни ишлатади. Kerberos шифрлашнинг турли алгоритмларидан ва хэш-функциялардан фойдаланиши мумкин, аммо мададлаш учун Triple DES ва MD5 алгоритмлари урнатилган.

Kerberos тизимида ишонч хужжатларининг икки туридан фойдаланилади: мандат (tricket) ва аутентификатор (authentifacator).

Мандат серверга мандат берилган мижознинг идентификацион маълумотларини хавфсиз узатиш учун ишлатилади. Унинг таркибида ахборот хам булиб, ундан сервер мандатдан фойдаланаётган мижознинг хак,ик,ий эканлигини текширишда фойдаланиши мумкин.

Аутентификатор - мандат билан бирга курсатилувчи кушимча атрибут(аломат). Куйида Kerberos хужжатларида ишлатилувчи белгилашлар тизими келтирилган:

C - мижоз;

S - сервер;

a - мижознинг тармок, адреси;

v - мандат таъсири вактининг бошланиши ва охири;

Г - вакт белгиси; $К_x$ - махфий

калит х; *Кф* - х ва у учун сеанс

калити;

{m}$К_x$ - субъект *х* нинг махфий калити $К_x$ билан шифрланган хабар *m;*

Т - *у* дан фойдаланишга мандат *х;*

$А_{XJ}$ - *х* ва *у* учун аутентификатор.

Kerberos мандаты.

Kerberos мандати куйидаги шаклга эга: $T_{cs} = S,\{C,a,v,K_{cS}\}K_S$.

Мандат битта мижозга катъий белгиланган сервердан фойдаланиш учун катъий белгиланган вактга берилади. Унинг таркибида мижоз исми, унинг тармок, адреси, мижоз харакатининг бошланиш ва тугаш вакти ва сервернинг махфий калити K_s шифрланган сеанс калити ^$_{C5}$булади. Мижоз мандатни расшифровка к,илаолмайди (у сервернинг махфий калитини билмайди), аммо у мандатни шифрланган шаклда сервер га курсатиши мумкин. Мандат тармок, оркали узатилаётганда тармокдаги яширинча эшитиб турувчиларнинг бирортаси х,ам уни укий олмайди ва узгартира олмайди.

Kerberos аутентификатори.

Kerberos аутентификатори куйидаги шаклга эга: A_{cs} ={*C,t,K.cuium*}K_{cs}

Мижоз максадли сервердан фойдаланишни хохдаганида аутентификаторни яратади. Унинг таркибида мижоз исми, вакт белгиси, мижоз ва сервер учун умумий булган сеанс калити K_{cs} шифрланган сеанс калити булади. Мандатдан фаркди х,олда аутентификатор бир марта ишлатилади.

Аутентификаторнинг ишлатилиши иккита мак,садни кузлайди. Биринчидан, аутентификаторда сеанс калитида шифрланган кандайдир матн булади. Бу калитнинг мижозга маълумлигидан далолат беради. Иккинчидан, шифрланган очик, матнда вакт белгиси мавжуд. Бу вакт белгиси аутентификатор ва мандатни ушлаб колган нияти бузук, одамга улардан бирор вакт утганидан сунг аутентфикациялаш муолжасини утишда ишлатишига имкон бермайди.

Kerberos хабарлари.

KerberosHHHr 5-версиясида хабарларнинг куйидаги турлари ишлатилади (6.3-расмга карал син).

1. Мижоз - Kerberos: *C, tgs*.
2. Kerberos - мижоз : $\{K_{c,tgs}\}K_c\{T_{cftgs}\}K_{tgs}$.
3. Мижоз- $TGS:\{A_{C,S}\}K_{C,tgs}(T_{C,tgs})K_{tgs,S}$.
4. TGS -мижоз: $\{K_{C,S}\}K_{C,tgs}\{T_{C,S}\}K_S$,.
5. Мижоз - сервер: $\{A_{C,S}\}K_{C,S}\{T_{C,S}\}K_S$.

Ушбу хабарлардан фойдаланишни батафсил курайлик.

Дастлабки мандатни олиш.

Мижоздан шахсини исботловчи ахборотнинг кисми - унинг пароли мавжуд. Мижозни паролини тармок, оркали жунатишига мажбур килиб булмайди. Kerberos протоколи паролни обрусизлантириш эхтимолини минималлаштиради, аммо агар фойдаланувчи паролни билмаса унга узини тугри идентификациялашга имкон бермайди.

Мижоз KerberosHHHr аутентификация серверига узининг исми, сервери *TGS* нинг (бир нечта сервер *TGS* булиши мумкин) булган хабарни жунатади. Амалда фойдаланувчи купинча исмини узини киритади, тизимга кириш дастури эса суров юборади.

KerberosHHHr аутентификациялаш сервери узининг маълумотлар базасида мижоз хусусидаги маълумотларни к,идиради. Агар мижоз хусусидаги ахборот маълумотлар базасида булса, Kerberos мижоз ва *TGS* орасида маълумот алмашиш учун ишлатиладиган сеанс калитини генерациялайди. Kerberos бу сеанс калитини мижознинг махфий калити билан шифрлайди. Сунгра у *TGS* хизматига мижознинг хакикийлигини исботловчи *TGT (Ticket Granting Ticket)* мандатининг ажратилиши учун мижозга мандат яратади. *TGS* нинг махфий калитида *TGT* шифрланади ва унинг таркибида мижоз ва сервер идентификатори, *TGS* - мижоз жуфтининг сеанс калити, хамда *TGT* таъсирининг бошланиш ва охирги вактлари булади. Аутентификациялаш сервери бу иккита шифрланган хабарни мижозга юборади.

Энди мижоз бу хабарларни кабул килади, биринчи хабарни узининг махфий калити K_c билан расшифровка килиб, сеанс калити $K_{c\ tgs}$ ни хрсил килади. Махфий калит мижоз паролининг бир томонлама хэш-функцияси

булганлиги сабабли крнуний фойдаланувчида хеч кандай муаммо тугилмайди. Нияти бузук, одам тугри паролни билмайди ва, демак, аутентификациялаш серверининг жавобини расшифровка кила олмайди. Шу сабабли нияти бузук, одам мандатни ёки сеанс калитини ола олмайди. Мижоз *TGT* мандатини ва сеанс калитини саклаб, парол ва хэш-кийматни, улар-нинг обрусизланиш эхтимолликларини пасайтириш максадида, учиради. Агар нияти бузук, одам мижоз хотираси таркибининг нусхасини олишга уринса, у факат *TGT* ва сеанс калитини олади. Бу маълумотлар факат *TGT* таъсири вактидагина мухим хисобланади. *TGT* таъсир муддати тугагунидан сунг бу маълумотлар маънога эга булмайди. Энди мижоз *TGT* дан олинган мандат ёрдамида унда курсатилган *TGT* таъсирининг бутун муддати мобай-нида сервер *TGS* да аутентификациялашдан утиш имкониятига эга.

Сервер мандатларини олиш.

Мижоз узига керак булган х,ар бир хизмат учун алох,ида мандат олиши мумкин. Шу максадда мижоз *TGS* хизматига *TGT* мандата ва аутентификатордан иборат суров юбориши лозим. (Амалда суровни дастурий таъминот автоматик тарзда, яъни фойдаланувчига билдирмасдан юборади.) Мижоз ва *TGS* сервери жуфтининг калитида шифрланган аутентификатор таркибида мижоз ва унга керакли сервернинг идентификатори, тасодифий сеанс калиги ва вакт белгиси булади.

TGS суровни олиб, узининг махфий калитида *TGT* ни расшифровка килади. Сунгра *TGS TGT* даги сеанс калитидан аутентификаторни расшифровка килишда фойдаланади. Них,оясида аутентификатордаги ахборотни мандат ахбороти билан так,к,осланади. Аник,роги, билетдаги мижознинг тармок, адреси суровда курсатилган тармок, адреси билан, х,амда вакт белгиси жорий вакт билан солиштирилади. Агар барчаси мое келса, *TGS* суровни бажаришга рухсат беради.

Вакт белгиларини текширишда барча компьютерларнинг соатлари, булмаганда, бир неча минут аниклигида синхронланганлиги кузда тутилади. Агар суровда курсатилган вакт жорий ондан анчагина фарк, к,илса, TGS бундай суровни олдинги суровни к,айтаришга уриниш деб хисоблайди.

TGS хизмати аутентификатор таъсири муддатининг тугрилигини кузатилиши лозим, чунки сервер хизмати битта мандат, аммо турли аутентификаторлар ёрдамида кетма-кет бир неча марта суралиши мумкин. Угла мандат ва аутентификаторнинг ишлатилган вакт белгиси билан килинган суров кайтарилади.

Тугри суровга жавоб тарикасида *TGS* мижозга максад сервердан фойдаланиш учун мандат такдим этади. *TGS* мижоз ва максад сервери учун мижоз ва *TGS* га умумий булган сеанс калитида шифрланган сеанс калитини хам яратади. Бу иккала хабар мижозга юборилади. Мижоз хабарни расшифровка килади ва сеанс калитини чикариб олади.

Хизмат сурови.

Энди мижоз узининг хакикийлигини максад серверига исботлаши мумкин. Максад серверида аутентификациядан муваффакиятли утиш учун мижоз таркибида узининг исми, тармок, адреси, вакт белгиси булган ва сеанс калити "мижоз-сервер"да шифрланган аутентификаторни яратади ва уни TGS хизматидан олиб берилган максад серверининг махфий калитида шифрланган мандат билан бирга жунатади.

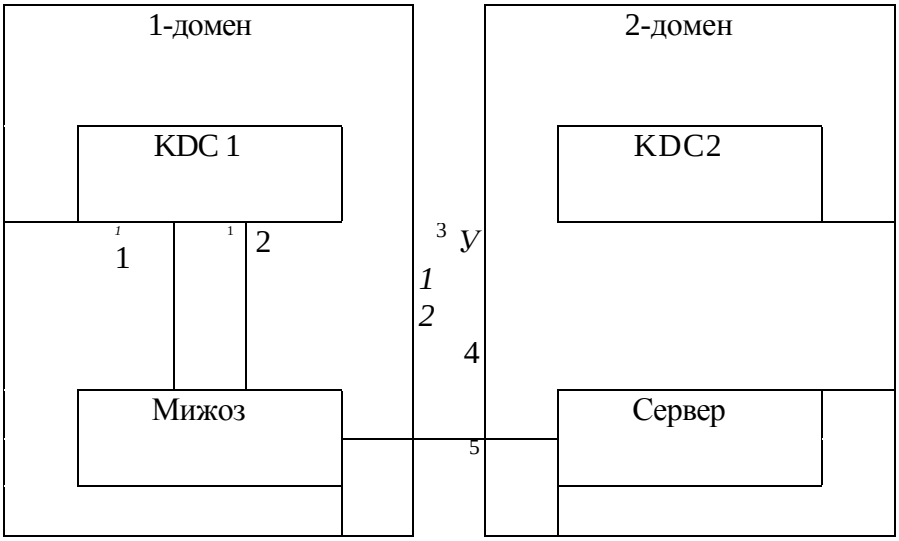
Максад сервери мижоздан маълумотларни олиб, аутентификаторни узининг махфий калитида расшифровка килади ва ундан "мижоз-сервер" сеанс калитини чикариб олади. Мандат хам текширилади. Текшириш муолажаси "мижоз-TGS" сессиясида утказиладиган муолажага ухшаш, яъни тармок, адреслари ва вакт белгисининг мослиги текширилади. Агар барчаси мое келса, сервер мижознинг хакикийлигига ишонч хреил килади.

Агар илова х,ак,ик,ийликнинг узаро текширилишини талаб этеа, сервер мижозга таркибида сеанс калитида шифрланган вакт белгиси булган хабарни юборади. Бу серверга тугри махфий калитнинг маълум эканлигини ва у мандат ва гувохномани расшифровка кила олишини исботлайди. Зарурият тугилганида мижоз ва сервер кейинги хабарларни умумий калитда шифрлашлари мумкин. Чунки бу калит факат уларга маълум, бу калит билан шифрланган охирги хабар иккинчи тарафдан юборилганига иккала тараф ишонч хреил килишлари мумкин. Амалда бу барча мураккаб муолажалар

автоматик тарзда бажарилади ва мижозга кандайдир нокулайликлар етказилмайди.

Доменлараро аутентификациялаш хусусиятлари.

Kerberos дан доменлараро аутентификациялашда хдм фойдаланиш мумкин. Мижоз бошка домендаги сервердан фойдаланиш максадида калит - ларни таксимлаш маркази *KDC* га мурожаат килса, *KDC* мижозга суралаётган сервер жойлашган доменнинг *KDC* ига мурожаат этишга *щита адреслаш мандатини* (referal ticket) такдим этади (6.4-расм).



6.4-расм. Kerberos протоколида доменлараро аутентификациялаш схемаси

Расмда куйидаги белгилапглар кабул килинган:

1. Аутентификациялашга суров.
2. *KDC1* учун *TGT*
3. *KDC2* учун *TGT.*
4. Сервердан фойдаланиш мандата.
5. Маълумотларни аутентификациялаш ва алмашиш.

Кдйта адреслаш мандата иккита домен КБССининг жуфтли алока калитида шифрланган ТСГдир. Бунда мижозга сервердан фойдаланишга мандатни суралаётган сервер жойлашган KDC такдим этади.

Жуда куп доменли тармокда аутентификациялаш учун KerberosflaH фойдаланиш назарий жихдтдан мумкин булсада, мурожаатлар сонининг доменлар сонига мутаносиб равишда ошиши сабабли, суровларни муайян

KDCnapra бир маънода кайта адресловчи кандайдир марказий домен куришга тугри келади.

Kerberos хаефсизлиги.

Kerberos, криптографик химоялашнинг бошка харкандай дастурий воситаси каби ишончсиз дастурий мухдтда ишлайди. Ушбу мухитнинг хужжатлаштирилмаган имкониятлари ёки нотугри конфигурацияси жиддий ахборотнинг чикиб кетишига олиб келиши мумкин. Хатто калитлар фойдаланувчи ишлаш сеансида факат оператив хотирада сакланса хам операцион тизимдаги бузилиш калитларнинг каттик, дискда нусхаланишига олиб келиши мумкин.

Kerberos дастурий таъминоти урнатилган ишчи станциясидан купчилик фойдаланувчи режимнинг ишлатилиши ёки ишчи станциялардан фойдаланишнинг назорати булмаслиги дастур-закладкани киритиш ёки криптографик дастурий таъминотни модификациялаш имкониятини тугдиради.

Шу сабабли, Kerberos хавфсизлиги куп жихатдан ушбу протокол урнатилган ишчи станцияси химоясининг ишончлигига боглик,.

Kerberos протоколининг узига к,уйидаги к,атор талаблар к,уйилади:

- Kerberos хизмати хизмат килишдан воз кечишга йуналтирилган хужумлардан химояланиши шарт;

- вакт белгиси аутентификация жараёнида к,атнашиши сабабли, тизимдан фойдаланувчиларининг барчаси учун тизимли вактни синхронлаш зарур;

- Kerberos паролни саралаш орк,али хужум к,илишдан химояламайди. Муаммо шундаки, *KDC* да сакланувчи фойдаланувчи калити унинг паролини хэш-функция ёрдамида кайта ишлаш натижасидир. Паролнинг бушлигида уни саралаб топиш мумкин.

- Kerberos хизмати рухсатсиз фойдаланишининг барча турларидан ишончли химояланиши шарт;

- мижоз олган мандатлар, хамда махфий калитлар рухсатсиз фойдаланишдан х,имояланиши шарт.

Юкррида келтирилган талабларнинг бажарилмаслиги муваффакиятли хужумга сабаб булиши мумкин.

Хрзирда Kerberos протоколи аутентификациялашнинг кенг тарк,алган воситаси хисобланади. Kerberos турли криптографик схемалар, хусусан, очик, калитли шифрлаш билан биргаликда ишлатилиши мумкин.

Бир томонлама калитли хэш-функциялардан фойдаланишга асосланган протоколлар.

Бир томонлама хэш-функция ёрдамида шифрлашнинг узига хос хусусияти шундаки, у мохияти буйича бир томонламадир, яъни тескари узгартириш-кабул килувчи тарафда расшифровка килиш билан бирга олиб борилмайди. Иккала тараф (жунатувчи ва кабул килувчи) бир томонлама шифрлаш муолажасидан фойдаланади.

Шифрланаётган маълумот *М* га кулланилган *К* параметр-калитли бир томонлама хэш-функция $h_k(.)$ натижада байтларнинг белгиланган катта булмагани сонидан иборат хэш-киймат (дайджест) *"m"* ни беради (6.4-расм).

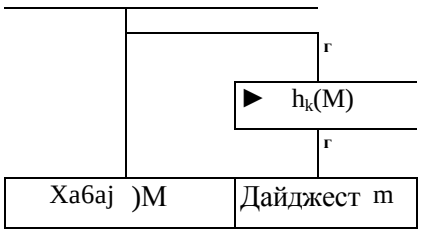
Жунатувчи (^

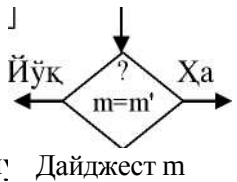
Хабар М

К,

6.4-расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатилиши (I-вариант).

Дайджест "т" кабул килувчига дастлабки хабар *М* билан бирга узатилади. Хабарни кабул килувчи, дайджест олинишида кандай бир томонлама хэш-функция ишлатилганлигини билган х,олда, расшифровка килинган хабар *М* дан фойдаланиб, дайджестни бошк,атдан х,исоблайди. Агар олинган дайджест билан хисобланган дайджест мое келса, хабар *М* нинг таркиби хеч кандай узгаришга дучор булмаганини билдиради.



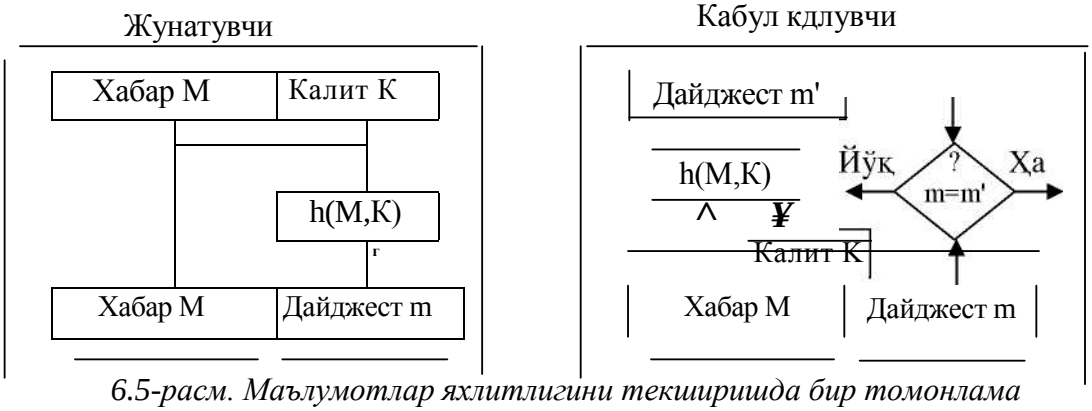


дХабар М mлу Дайджест m

Дайджестни билиш дастлабки хабарни тиклашга имкон бермайди, аммо маълумотлар яхлитлигини текширишга имкон беради. Дайджестга дастлабки хабар учун узига хос назорат йигиндиси сифатида караш мумкин. Аммо, дайджест ва оддий назорат йигиндиси орасида жиддий фарк, хам мавжуд. Назорат йигиндисидан алоканинг ишончсиз линияси буйича узатиладиган хабарларнинг ахлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузук, одамлар билан курашишга мулжалланмаган. Чунки, бу хрлда назорат йигиндисининг янги кийматини кушиб хабарни алмаштириб куйишга уларга хеч ким халакит бермайди. К,абул килувчи бунда хеч нарсани сезмайди.

Дайджестни хисоблашда, оддий назорат йигиндисидан фаркли равишда, махфий калитлар ишлатилади. Агар дайджест олинишида факат жунатувчи ва кабул килувчига маълум булган параметр-калитли бир томонлама хэш-функция ишлатилса, дастлабки хабарнинг хар к,андай модификацияси дархрл маълум булади.

6.5-расмда маълумотлар яхлитлигини текширишда бир томонлама хэш-функция ишлатилишининг бошка варианти келтирилган.



6.5-расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатиши (II-вариант).

Бу хрлда бир томонлама хэш-функция *h(.)* параметр-калитга эга эмас, аммо у махфий калит билан тулдирилган хабарга кулланилади, яъни жунатувчи дайджест m=h(M, К)ни х,исоблайди. К,абул к,илувчи дастлабки хабарни чикариб олиб, уни уша маълум махфий калит билан тулдиради. Сунгра олинган маълумотлар га бир томонлама хэш-функция п(.)ни

куллайди. Х,исоблаш натижаси - дайджест "т" тармок, оркали олинган дайджест "т" билан такдосланади.

Асимметрии алгоритмларга асосланган катъий аутентификациялаш.

Кдтъий аутентификациялаш протоколларида очик, калитли асимметрик алгоритмлардан фойдаланиш мумкин. Бу хрлда исботловчи махфий калитни билишлигини куйидаги усулларнинг бири ёрдамида намойиш этиши мумкин:

- очик, калитда шифрланган суровый расшифровка килиш;
- суров сузининг ракамли имзосини куйиш.

Аутентификацияга зарур булган калитларнинг жуфти, хавфсизлик мулохазасига кура, бошка максадларга (масалан, шифрлашда) ишлатилмаслиги шарт. Очик, калитли танланган тизим шифрланган матнни танлаш билан хужумларга, хатто бузгунчи узини текширувчи деб курсатиб ва унинг номидан х,аракат к,илганда х,ам, бардош бериши лозимлигига фойдаланувчиларни огохдантириш керак.

Шифрлашнинг асимметрия алгоритмларидан фойдаланиб аутентификациялаш.

Шифрлашнинг асимметрик алгоритмларидан фойдаланишга асосланган протоколга мисол тарикасида аутентификациялашнинг куйидаги протокол ини келтириш мумкин:

A<^B:h(r),B,P_A(r,B),

A^B-.г.

К,атнашувчи *B* тасодифий х,олда *г* ни танлайди ва *x=h(r)* к,ийматини х,исоблайди *(x* к,иймати г нинг к,ийматини очмасдан туриб г ни билишлигини намойиш этади), сунгра у *e = P_A(г,B)* кийматни хисоблайди. P_A орк,али асимметрик шифрлаш алгоритми фараз к,илинса, *h(.)* орк,али хэш-функция фараз к,илинади. Кдтнашувчи *B* ахборот хабарни к,атнашувчи *A* га жунатади. К,атнашувчи *A e = P_A(г,B)* ни расшифровка килади ва *г′* ва *B′* кийматларни олади, хамда х'=/г(г')ни х,исоблайди. Ундай кейин *x=x′* эканлигини ва *B′* идентификатор х,ак,ик,атан к,атнашувчи 5га курсатаётганини тасдикловчи к,атор так,к,ослашлар бажарилади. Так,к,ослаш муваффакиятли

утса катнашувчи *A* "г" катнашувчини *B* га узатади. Кдтнашувчи *B* "г"ни олганидан сунг уни биринчи хабарда жунатган киймати эканлигини текширади.

Кейинги мисол сифатида асимметрик шифрлашга асосланган Нидхем ва Шредернинг модификацияланган протоколини келтирамиз. Факат аутентификациялашда ишлатилувчи Нидхем ва Шредер протоколи вариантный куришда $Р_в$ оркали катнашувчи Внинг очик, калити ёрдамида шифрлаш алгоритми фараз килинади. Протокол куйидаги тузилмага эга:

Рацамли имзодан фойдаланиш асосидаги аутентификациялаш

Х.509 стандартининг тавсияларида ракамли имзо, вак,т белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун к,уйидаги белгилашларни киритамиз:

- t_A, $г_A$ ва $г_в$ — мое х,олда вак,т белгиси ва тасодифий сонлар;
- S_A - к,атнашувчи *A* генерациялаган имзо;
- $cert_A$ — к,атнашувчи *A* очик, калитининг сертификати;
- $cert_B$ - к,атнашувчи *B* очик, калитининг сертификати;

Мисол тарикасида аутентификациялашнинг куйидаги протоколларини келтирамиз:

1. В акт белгисидан фойдаланиб бир томонлама аутентфикациялаш:

$A^B:cert_A,t_A,B,S_A(f_A,B)$

К,атнашувчи *B* ушбу хабарни олганидан сунг вакт белгиси t_A нинг тугрилигини, олинган идентификатор *B* ни ва сертификат $cert_A$ даги очик, калитдан фойдаланиб рак,амли имзо $S_A(t_A,B)$ нинг корректлигини текширади.

2. Тасодифий сонлардан фойдаланиб бир томонлама аутентификация лаш:

$A <- B : г_в$

$A^B:cert_A,r_A,B,S_A(r_A,r_B,B)$

Кдтнашувчи *B* катнашувчи *A* дан хабарни олиб айнан у хабарнинг адресати эканлигига ишонч хрсил килади; сертификат $cert_A$ дан олинган катнашувчи *A* очик, калитидан фойдаланиб очик, куринишда олинган $г_A$ сони, биринчи хабарда жунатилган $г_в$ сони ва узининг идентификатори *B* остидаги имзо $S_A(r_A,r_B,B)$ нинг корректлигини текширади. Имзо чекилган тасодифий сон $г_A$ очик, матнни танлаш билан хужумни олдини олиш учун ишлатилади.

3. Тасодифий сонлардан фойдаланиб икки томонлама аутентификациялаш:

$A <- B : г_в$

$A \hat{} B: cert_A, r_A, B, S_A(r_A, r_B, B)$

$A <г- B: cert_B, A, S_B (r_A, r_B, A)$

Ушбу протоколдаги хабарларни ишлаш олдинги протоколдагидек бажарилади.

6.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш

Охирги вакхда инсоннинг физиологик параметрлари ва характеристикаларини, хулк,ининг хусусиятларини улчаш орк,али фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг таркалмокда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан куйидаги афзалликларга эга:

- биометрик аломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юк,ори;
- биометрик аломатларнинг соглом шахсдан ажратиб булмаслиги;
- биометрик аломатларни сохталаштиришнинг к,ийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биомет рик алгоритмлар к,уйидагилар:

- бармок, излари;
- к,ул панжасининг геометрик шакли;

- юзнинг шакли ва улчамлари;
- овоз хусусиятлари;
- куз ёйи ва тур пардасининг накхпи.

Аутентификациянинг биометрик кием тизими ишлашининг намунавий схемаси куйидагича. Тизимда руйхатга олинишида фойдаланувчидан узининг характерли аломатларини бир ёки бир неча марта намойиш килиниши талаб этилади. Бу аломатлар (хакикий сифатида маълум) тизим томонидан крнуний фойдаланувчининг киёфаси сифатида руйхатга Олинади. Фойдаланувчининг бу киёфаси тизимда электрон шаклда сакданади ва узини крнуний фойдаланувчи деб даъво килган хар бир одамни текширишда ишлатилади. Такдим этилган аломатлар мажмуаси билан руйхатга олинганларининг мослиги ёки мое келмаслигига караб карор кабул килинади. Истеъмолчи нуктаи назаридан биометрик аутенфикациялаш тизими куйидаги иккита параметр оркали характерланади:

- хатолик инкорлар коэффициенти FRR (false-reject rate);
- хатолик тасдиклар коэффициенти FAR (false-alarm rate).

Хатолик инкор тизим крнуний фойдаланувчи шахеини тасдикламаганда пайдо булади (одатда FRR киймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдик* тизим нокрнуний фойдаланувчи шахеини тасдиклаганида пайдо булади (одатда FAP киймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боглик,: хатолик инкор коэффициентининг хар бирига маълум хатолик тасдик, коэффициенти мое келади. Мукаммал биометрик тизимда иккала хатоликнинг иккала параметри нулга тенг булиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур курбон килишга тугри келади. Одатда тизимли параметрлар шундай созланадики, мое хатолик инкорлар коэффициентини аникловчи хатолик тасдикларнинг исталган коэффициентига эришилади.

Биометрик аутентификациялашнинг дактилосконик тизими. Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармок, изларидан фойдаланади (аутентификациянинг дактило-скопик тизими). Бундай тизимлар содда ва кулай, аутентификациялашнинг

юкрри ишончлилигига эга. Бундай тизимларнинг кенг тарк,алишига асосий сабаб бармок, излари буйича катта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

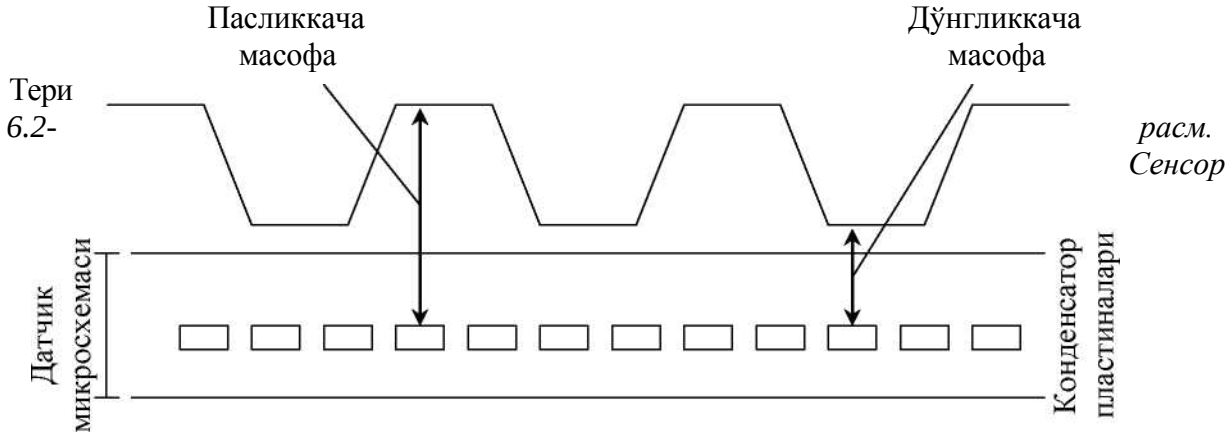
Аутентификациянинг дактилоскопик тизими куйидагича ишлайди. Аввал фойдаланувчи руйхатга олинади. Одатда, сканерда бармокнинг турли холатларида сканерлашнинг бир неча варианти амалга оширилади. Табиийки, намуналар бир-биридан бироз фаркданади ва кандайдир умумлаштирилган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутентификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармок, изи маълумотлар базасидаги «паспортлар» билан такдосланади.

Бармоц изларининг сканерлари. Бармок, изларини сканерловчи анъанавий курилмаларда асосий элемент сифатида бармокнинг характерли расмини ёзувчи кичкина оптик камера ишлатилади. Аммо, дактилоскопик курилмаларни ишлаб чикарувчиларнинг купчилиги интеграл схема асосидаги сенсорли курилмаларга эътибор бермокдалар. Бундай тенденция бармок, изларига асосланган аутентификациялашни куллашнинг янги сох,аларини очади.

Бундай технологияларни ишлаб чикувчи компаниялар бармок, изларини олишда турли, хусусан электрик, электромагнит ва бошка усулларни амалга оширувчи воситалардан фойдаланадилар.

Сканерлардан бири бармок, изи тасвирини шакллантириш максадида тери кисмларининг сигим к,аршилигини улчайди. Масалан, Veridicom компаниясининг дактилоскопик курилмаси ярим-утказгичли датчик ёрдамида сигим каршилигини аникдаш орк,али ахборотни йигади. Сенсор ишлашининг принципи к,уйидагича: ушбу асбобга куйилган бармок, конденсатор пластиналарининг бири вазифасини утайди (6.6-расм). Сенсор сиртида жойлашган иккинчи пластина конденсаторнинг 90000 сезгир пластинкали кремний микросхемасидан иборат. Сезгир сигим датчиклари бармок, сирти дунгликлари ва пастликлари орасидаги электрик майдон кучининг

узгаришини улчайди. Натижада дунгликлар ва пастликларгача булган масофа аникланиб, бармок, изи тасвири олинади.



6.2-ишлашининг принципига.

Интеграл схема асосидаги сенсорли текширишда AuthenTec компаниясида ишлатилувчи усул аникликни яна хам оширишга имкон беради.

К,атор ишлаб чикарувчилар биометрик тизимларни смарт-карталар ва карта-калитлар билан комбинациялайдилар.

Интеграл схемалар асосидаги бармок, излари датчикларининг кичик улчамлари ва юкрри булмаган нархи уларни химоя тизими учун идеал интерфейсга айлантиради. Уларни калитлар учун брелокларга урнатиш мумкин. Натижада фойдаланувчи компьютердан бошлаб то кириш нули, автомобиллар ва банкоматлар эшикларидан химояли фойдаланишни таъминлайдиган универсал калитга эга булади.

К,ул панжасининг геометрик шакли буйича аутентификациялаш тизимлари. Кул панжаси шаклини ук,увчи к,урилмалар бармокдар узунлигини, кул панжа к,алинлиги ва юзасини улчаш орк,али к,ул панжасининг хажмий тасвирини яратади. Масалан, Recognition Systems компаниясининг мах,сулотлари 90 дан ортик, улчамларни амалга оширади. Натижада кейинги так,к,ослаш учун 9-хонали намуна шакллантирилади. Бу натижа к,ул панжасини индивидуал сканерида ёки марказлаштирилган маълумотлар базасида сакданиши мумкин. К,ул панжасини сканерловчи курилмалар нархининг юк,орилиги ва улчамларининг катталиги сабабли тармок, мух,итида камдан-кам ишлатилсада, улар к,атъий хавфсизлик режимига ва шиддатли трафикка эга булган хисоблаш мух,ити (сервер хоналари хам

бунга киради) учуй кулай хисобланади. Уларнинг аниклиги юкрри ва инкор коэффициенти яъни инкор этилган крнуний фойдаланувчилар фоизи кичик.

Юзнинг тузилиши еа оеоз буйича аутентификациялоечи тизимлар. Бу тизимлар арзонлиги туфайли энг фойдаланувчан хисобланадилар, чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга. Бу синф тизимлари телекоммуникация тармокларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошка биометрик технологиялар яроксиз булган иловалар учун тугри келади. Бу хрлда шахсни идентификациялаш ва верификациялаш учун куз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аникловчи курилмаларни ишлаб чикарувчилар фойдаланувчини идентификациялашда хусусий математик алгоритмлардан фойдаланадилар.

Маълум булишича, купгина ташкилотларнинг хрдимлари юз тузилишини сканерловчи курилмаларга ишонмайдилар. Уларнинг фикрича камера уларни расмга олади, сунгра суратни монитор экранига чикаради. Камеранинг сифати эса паст булиши мумкин. Ундан ташкари юз тузилишини сканерлаш - биометрик аутентификациялаш усуллари ичида ягона, текширишга рухсатни талаб к,илмайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул хисобланали.

Таъкидлаш лозимки, юз тузилишини аникдаш технологияси янада такомиллаштирилишни талаб этади. Юз тузилишини аникловчи аксарият алгоритмлар куёш ёруглиги жадаллигининг кун буйича тебраниши натижасидаги ёруглик узгаришига таъсирчан буладилар. Юз х,олатининг узгариши х,ам аникдаш натижасига таъсир этади. Юз хрлатининг 45° га узгариши аниклашни самарасиз булишига олиб келади.

Оеоз буйича аутентификациялаш тизимлари. Бу тизимлар арзонлиги туфайли фойдаланувчан хисобланадилар. Хусусан уларни купгина шахсий компьютерлар стандарт комплектидаги ускуна (масалан микрофонлар) билан бирга урнатиш мумкин. Овоз буйича аутентификациялаш тизимлари хар бир одамга ноёб булган баландлиги, модуляцияси ва товуш частотаси каби овоз хусусиятларига асосланади.

Овозни аниклаш нуткни аниклашдан фаркланади. Чунки нуткни аникловчи технология абонент сузини изохласа, овозни аниклаш технологияси сузловчининг шахсини тасдиклайди. Сузловчи шахсини тасдиклаш баъзи чегараланишларга эга. Турли одамлар ухшаш овозлар билан гапириши мумкин, хар кандай одамнинг овози вакт мобайнида кайфияти, хиссиётлик хрлати ва ёшига боглик, хрлда узгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон оркали богланишларининг сифати сузловчи шахсини аниклашни кийинлаштиради. Шу сабабли овоз буйича аникдашни юз тузилишини ёки бармок, изларини аниклаш каби бошк,а биометриклар билан биргаликда амалга ошириш мак,садга мувофик, хисобланади.

Куз ёйи тур пардасининг шакли буйича аутентификациялаш тизими. Бу тизимларни иккита синфга ажратиш мумкин: куз ёйи расмидан фойдаланиш; куз тур пардаси кон томирлари расмидан фойдаланиш.

Одам куз пардаси аутентификация учун ноёб объект хисобланади. Куз туби кон томирларининг расми хатто эгизакларда хам фаркланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юкрри даражаси талаб этилганида (масалан х,арбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш "ким бу ким" эканлигини аниклаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аникдовчи курилмалардан фойдаланиш ходимларни тармок,к,а киришларида мураккаб паролларни эслаб к,олишдан халос этади. Катор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш тармок, маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар к,аторида кенг таркалган сох,аларидан бири мобил тизимлари булди. Муаммо фак,ат компьютер угирланишидаги йук,отишларда эмас, балки ахборот тизимининг бузилиши катта зарарга олиб келиши мумкин. Ундан ташк,ари, ноутбуклар

дастурий богааниш (мобил компьютерларда сакланувчи пароллар ёрдамида) оркали корпоратив тармокдан фойдаланишни тез-тез амалга оширади. Бу муаммоларни кичик, арзон ва катта энергия талаб этмайдиган бармок, излари датчиклари ечишга имкон беради. Бу курилмалар мое дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сакланаётган туртта сатхи - руйхатга олиш, экранни саклаш режимидан чикиш, юклаш ва файлларни дешифрациялаш учуй аутентификацияни бажаришга имкон беради.

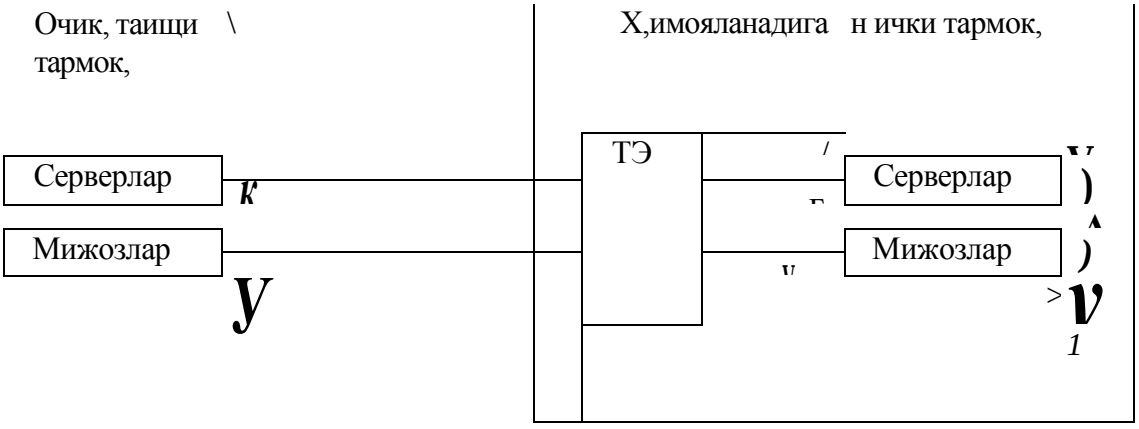
Фойдаланувчини биометрик аутентификациялаш махфий калитдан фойдаланишни модул куринишида шифрлашда жиддий ахамиятга эга булиши мумкин. Бу модул ахборотдан факат хакикий хусусий калит эгасининг фойдаланишига имкон беради. Сунгра калит эгаси узининг махфий калитини ишлатиб хусусий тармоклар ёки Internet орк,али узатилаётган ахборотни шифрлаши мумкин.

VII боб. ТАРМОКЛАРАРО ЭКРАН ТЕХНОЛОГИЯСИ

7.1. Тармоклараро экранларнинг ишлаш хусусиятлари

Тармокдарараро экран (ТЭ) - *брандмауэр* ёки *firewall системаси* деб хам аталувчи тармокдарараро химоянинг ихтисослаштирилган комплекси. Тармоклараро экран умумий тармокни икки ёки ундан куп кисмларга ажратиш ва маълумот пакетларини чегара оркали умумий тармокнинг бир кисмидан иккинчисига утиш шартларини белгиловчи кридалар тупламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоги ва Internet глобал тармок, орасида утказилади. Тармокдарараро экранлар гарчи корхона локал тармоги уланган корпоратив интратармогидан килинувчи х,ужумлардан химоялашда ишлатилишлари мумкин булсада, одатда улар корхона ички тармогини Internet глобал тармокдан сук,илиб киришдан х,имоялайди. Аксарият тижорат ташкилотлари учун тармокдарараро экранларнинг урнатилиши ички тармок, хавфсизлигини таъминлашнинг зарурий шарти хисобланади.

Рухсат этилмаган тармокдарараро фойдаланишга к,арши таъсир курсатиш учун тармокдарараро экран ички тармок, хисобланувчи ташкилотнинг химояланувчи тармоги ва ташк,и ганим тармок, орасида жойланиши лозим (7.1-раем). Бунда бу тармокдар орасидаги барча ал ока факат тармокдарараро экран орк,али амалга оширилиши лозим. Ташкилий нуктаи



7.1-расм. Тармоцлараро экранниулаш схемаси.

назаридан тармокдарарo экран химояланувчи тармок, таркибига киради.

Ички тармокнинг купгина узелларини бирданига хдмояловчи тармокдарарo экран куйидаги иккита вазифани бажариши керак:

- ташки (химояланувчи тармокка нисбатан) фойдаланувчиларнинг корпоратив тармокнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар каторига тармокдарарo экран хдмояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар, масофадаги фойдаланувчилар, хакерлар, хдтто компаниянинг ходимлари киритилиши мумкин;

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

Хрзирда ишлаб чикарилаётган тармокдарарo экранларнинг тавсифларига асосланган хрлда, уларни куйидаги асосий аломатлари буйича туркумлаш мумкин:

OSI модели ссжцларида ишлаши буйича:

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

Ишлатиладиган технология буйича:

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

Бажарилиши буйича:

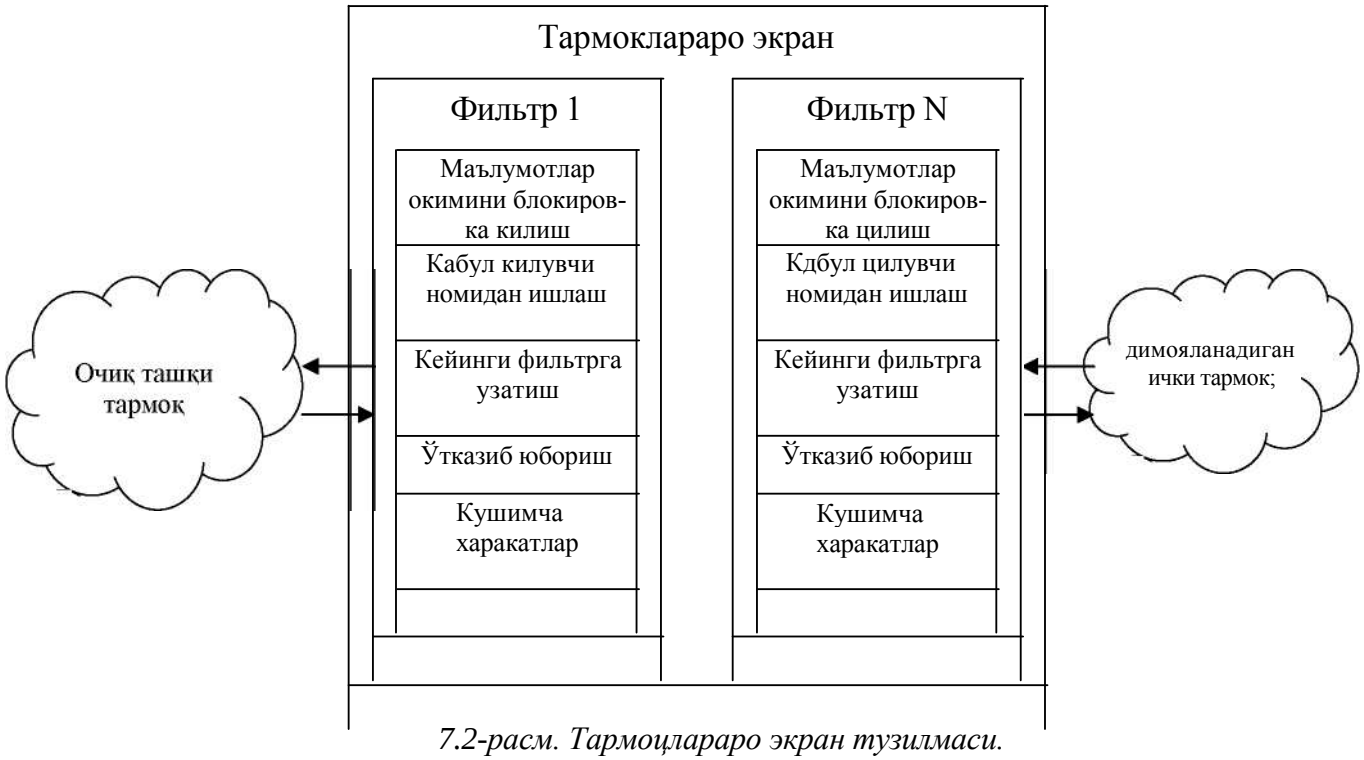
- аппарат-дастурий;
- дастурий;

Уланиш схемаси буйича;

- тармокни умумий химоялаш схемаси;
- тармок, сегментлари химояланувчи берк ва тармок, сегментлари химояланмайдиган очик, схема;

- тармокнинг берк ва очик, сегментларини алохдда химояловчи схема.

Трафикларни фильтрлаш. Ахборот окимларини фильтрлаш уларни экран оркали, баъзида кандайдир узгартиришлар билан, утказишдан иборат. Фильтрлаш кабул килинган хавфсизлик сиёсатига мое келувчи, экранга олдиндан юкланган кридалар асосида амалга оширилади. Шу сабабли тармоклараро экранни ахборот окимларини ишловчи фильтрлар кетма-кетлиги сифатида тасаввур этиш кул аи (7.2-расм).



7.2-расм. Тармоцлараро экран тузилмаси.

Фильтрларнинг х,ар бири куйидаги х,аракатларни бажариш орк,али фильтрлашнинг алох,ида к,оидаларини изохдашга аталган:

1. Ахборотни изохданувчи к,оидалардаги берилган мезонлар буйича тах,лиллаш, масалан, к,абул килувчи ва жунатувчи адреслари ёки ушбу ах борот аталган илова хили буйича.

2. Изохданувчи к,оидалар асосида куйидаги ечимлардан бирини к,абул килиш:

- маълумотларни утказмаслик;

- маълумотларни кабул килувчи номидан ишлаш ва натижани жунатувчига кайтариш;

- тахлиллашни давом эттириш учун маълумотларни кейинги фильтрга узатиш;

- кейинги фильтрларга эътибор килмай маълумотларни узатиш.

Фильтрлаш кридалари воситачилик функцияларига оид кушимча, масалан маълумотларни узгартириш, ходисаларни кайдлаш ва х,. каби харакатларни хам бериши мумкин. Мое хрлда, фильтрлаш кридалари куйидагиларнинг амалга оширилишини таъминловчи шартлар руйхатини аниклайди:

- маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

- химоялашнинг кушимча функцияларини бажариш.

Ахборот окимини тахлиллаш мезони сифатида куйидаги параметрлардан фойдаланиш мумкин:

- таркибида тармок, адреслари, идентификаторлар, интерфейслар адреси, портлар номери ва бошка мухим маълумотлар булган хабар пакетларининг хизматчи хошиялари;

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

- ахборот окимининг ташки характеристикалари, масалан, вакт ва частота характеристикалари маълумотлар хажми ва х,.

Ишлатилувчи тахлиллаш мезонлари фильтрлашни амалга оширувчи OSI моделининг сатхдарига боглик,. Умумий х,олда, пакетни фильтрлашни амалга оширувчи OSI моделининг сатхи канчалик юк,ори булса, таъминланувчи химоялаш даражаси х,ам шунчалик юк,ори булади.

Воситачилик функцияларининг бажарилиши. Тармокдараро экран воситачилик функцияларини *экранловчи агентлар* ёки *воситачи дастурлар* деб аталувчи махсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар хисобланади ва ташки ва ички тармок, орасида хабарлар пакетини бевосита узатишни такиклайди.

Ташки тармокдан ички тармокнинг ва аксинча фойдаланиш зарурияти тугилганда аввал тармокдараро экран компьютерида ишловчи воситачи-дастур билан мантик,ий уланиш урнатилиши лозим. Воситачи-дастур

суралган тармоклараро алоканинг жоизлигини текширади ва ижобий натижада у^{зи} суралган компьютер билан алохдда уланиш урнатади. Сунгра ташки ва ички тармок, компьютерлари орасида ахборот алмашиш, хабарлар окимини фильтрлашни хамда бошка химоялаш функцияларини бажарувчи дастурий воситачи оркали амалга оширилади.

Таъкидлаш лозимки, тармоклараро экран фильтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташки ва ички тармок, орасида узаро алоканинг шаффофлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар окимини фильтрлашни амалга оширмаслиги хам мумкин.

Умуман, воситачи-дастурлар, хабарлар окимини шаффоф узатилишини блокировка килган хрлда, куйидаги функцияларни бажариши мумкин:

- узатилувчи ва кабул килинувчи маълумотларнинг хакикийлигини текшириш;
- ички тармок, ресурсларидан фойдаланишни чегаралаш;
- ташки тармок, ресурсларидан фойдаланишни чегаралаш;
- ташки тармокдан суралувчи маълумотларни кэшлаш;
- хабарлар окимини фильтрлаш ва узгартириш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоф шифрлаш;
- фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- ички тармок, адресларини трансляциялаш;
- ходисаларни к,айдлаш, ходисаларга реакция курсатиш, хамда к,айдланган ахборотни тахлиллаш ва х,исоботларни генерациялаш.

Узатилувчи ва цабул цилинувчи маълумотларнинг щцщийлигини текшириш нафакат электрон хабарларни, балки сохталаштирилиши мумкин булган мигрцияланувчи дастурларни (Java, Active X Controls) аутентифкациялаш учун долзарб х,исобланади. Хабар ва дастурларнинг хакикийлигини текшириш уларнинг ракамли имзосини текширишдан иборатдир.

Ички тармок ресурсларидан фойдаланишни чегаралаш усуллари операцион тизим сатх,ида мададланувчи чегаралаш усулларидан фарк, к,илмайди.

Ташки тармок ресурсларидан фойдаланишни чегарлашш купинча куйидаги ёндашишлардан бири ишлатилади:

- факат ташки тармокдаги берилган адрес буйича фойдаланишга рухсат бериш;

- янгиланувчи ножоиз адреслар руйхати буйича суровларни фильтрлаш ва уринсиз калит сузлари буйича ахборот ресурсларини кидиришни блокировка килиш:

- маъмур томонидан ташки тармокнинг крнуний ресурсларини брандмауэрнинг дискли хотирасида туплаш ва янгилаш ва ташки тармокдан фойдаланишни тула такиклаш.

Ташки тармокдан суралувчи *маълумотларни кэшлаш* махсус воситачилар ёрдамида мададланади. Ички тармок, фойдаланувчилари ташки тармок, ресурсларидан фойдаланганларида барча ахборот, proxy-сервер деб аталувчи брандмауэр каттик, диски маконида тупланади. Шу сабабли, агар навбатдаги суровда керакли ахборот proxy-серверда булса, воситачи уни ташки тармоккд мурожаатсиз такдим этади. Бу фойдаланишни жиддий тезлаштиради. Маъмурга факат proxy-сервер таркибини вакти-вак,ти билан янгилаб туриш вазифаси к,олади.

Кэшлаш функцияси ташк,и тармок, ресурсларидан фойдаланишни чегаралашда муваффакиятли ишлатилиши мумкин. Бу хрлда ташки тармокнинг барча крнуний ресурслари маъмур томонидан proxy-серверда тупланади ва янгиланади. Ички тармок, фойдаланувчиларига фак,ат proxy-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташки тармок, ресурсларидан бевосита фойдаланиш эса манн килинади.

Хабарлар оцимини филътрлаш ва узгартириш воситачи томонидан коидаларнинг берилган туплами ёрдамида бажарилади. Бунда воситачидастурларнинг икки хили фаркланади:

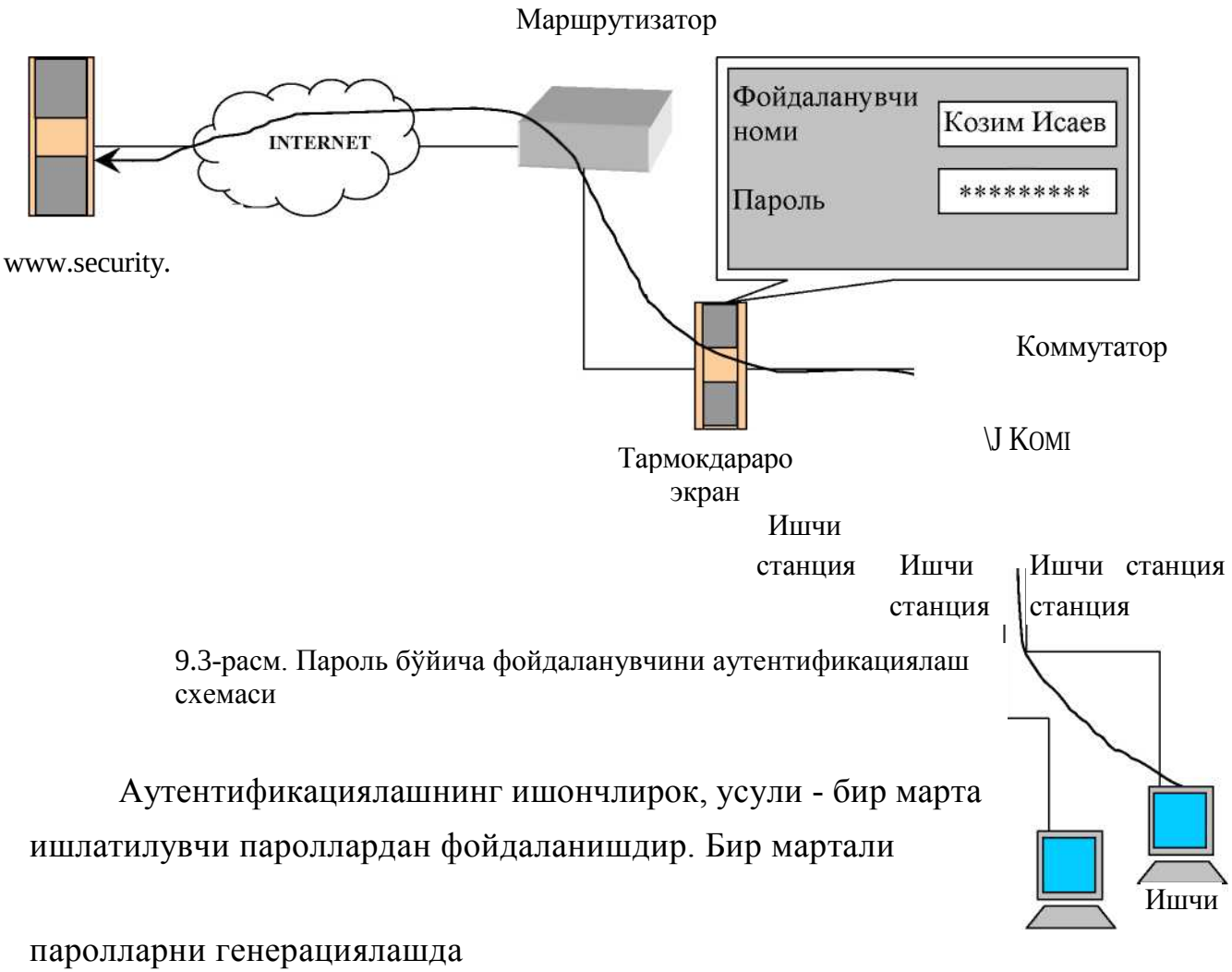
- сервис турини аникдаш учун хабарлар ок,имини тахлиллашга мулжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

- барча хабарлар окимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини кидириб зарарсизлантиришга ёки маълумотларни шаффоф шифрлашга мулжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини тахлиллайди ва агар кандайдир объект берилган мезонларга мое келмаса, воситачи унинг

кейинги силжишини блокировка килади ёки мое узгаришини, масалан, ошкор килинган компьютер вирусларни зарарсизлантиришни бажаради. Пакетлар таркибини тахлиллашда экранловчи агентнинг утувчи файлли архивларни автоматик тарзда оча олиши мухим хисобланади.

Фойдаланувчиларни идентификациялаш ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни такдим этиш билан амалга оширилади (7.3-расм). Аммо бу схема хавфсизлик нуктаи назаридан заиф хисобланади, чунки паролни бегона шахе ушлаб крлиб ишлатиши мумкин. Internet тармогидаги купгина можаролар кисман анъанавий куп марта ишлатилувчи паролларнинг заифлигидан келиб чикдан.



9.3-расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси

Аутентификациялашнинг ишончлирок, усули - бир марта ишлатилувчи пароллардан фойдаланишдир. Бир мартали

паролларни генерациялашда

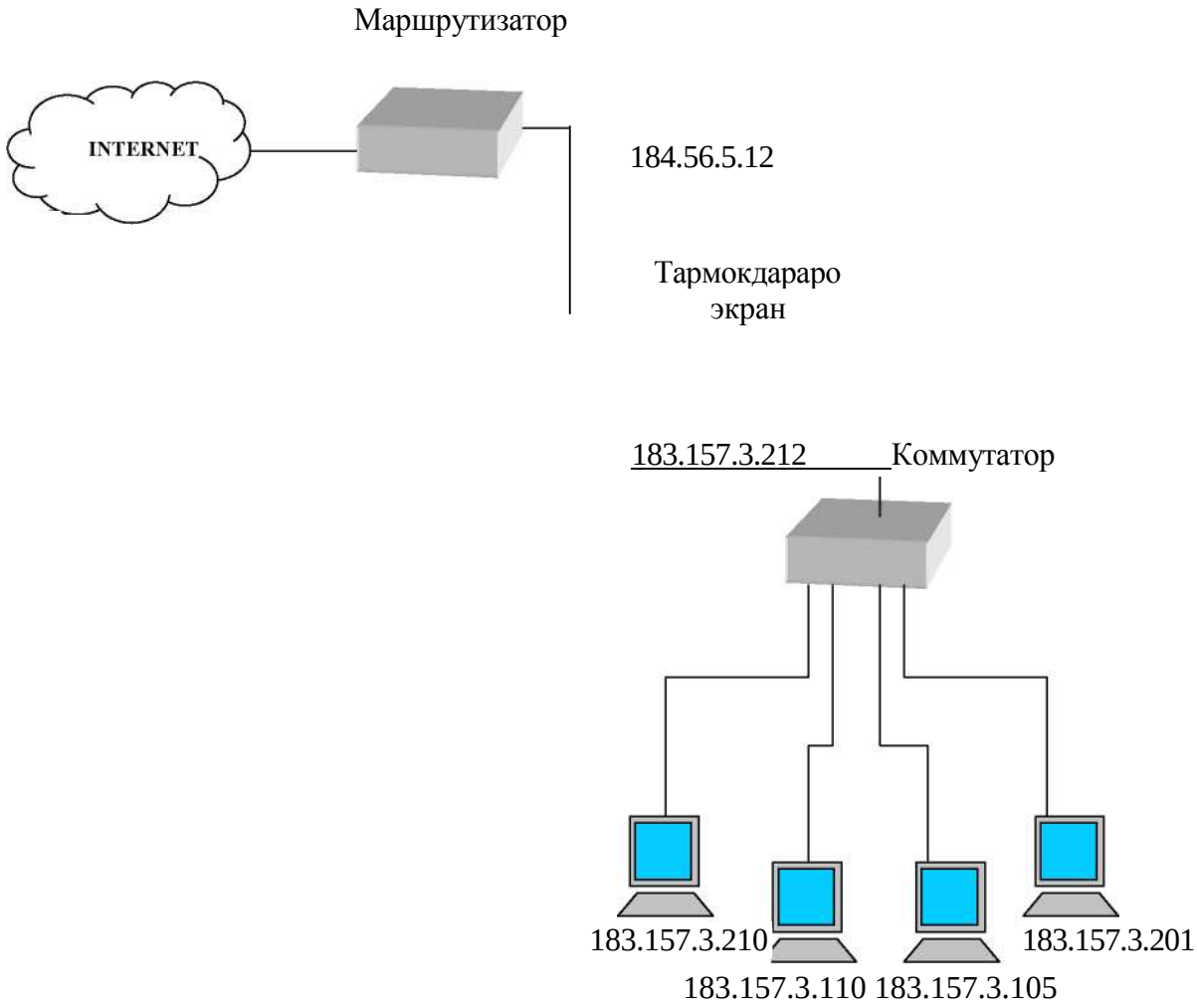
аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига урнатилувчи курилма булиб, уни ишга тушириш учун фойдаланувчи кандайдир махфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялайди ва бу ахборотни хост анъанавий парол урнида ишлатади. Смарт-карта ёки токен хостнинг аппарат ва дастурий таъминоти билан бирга ишлаши сабабли, генерацияланувчи парол хар бир сеанс учун ноёб булади.

Ишончли орган, масалан калитларни таксимлаш маркази томонидан берилувчи ракамли сертификатларни ишлатиш хам кулай ва ишончли. Купгина воситачи дастурлар шундай ишлаб чикиладики, фойдаланувчи факат тармокдарараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгиланган вакт мобайнида ундан кушимча аутентификацияланиш талаб этилмайди.

Тармокдарараро экранлар тармокдан фойдаланишни бошкаришни марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва курилмаларини урнатишга муносиб жой хисобланади. Гарчи кучайтирилган аутентификация воситалари хар бир хостда ишлатилиши мумкин булсада, уларнинг тармокдарараро экранларда жойлаштириш кулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармокдарараро экранлар булмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиги тармокнинг ички тизимларига тугридан-тугри утиши мумкин.

Катор тармокдарараро экранлар аутентификациялашнинг кенг тарк,алган усулларидан бири - KerberosHH мададлайди. Одатда, аксарият тижорат тармокдарараро экранлар аутентификациялашнинг турли схемаларини мададлайди. Бу эса тармок, хавфсизлиги маъмурига узининг шароитига к,араб энг макбул схемани танлаш имконини беради.

Ички тармок адресларини трансляциялаш. Купгина хужумларни амалга оширишда нияти бузук, одамга к,урбонининг адресини билиш керак булади. Бу адресларни хамда бутун тармок, топологиясини беркитиш учун тармокдарараро экранлар энг мухим вазифани - ички тармок, адресларини трансляциялашни бажаради (7.4-расм).



7.4-расм. Тармоқ адресларини трансляциялаш

Бу функция ички тармокдан ташки тармоккд узатилувчи барча пакет - ларга нисбатан бажарилади. Бундай пакетлар учун жунатувчи компьютер-ларнинг IP-адреслари битта "ишончли" IP адресга автоматик тарзда узгартирилади.

Ички тармок, адресларини трансляциялаш иккита усул-динамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда адрес узелга тармоклараро экранга мурожаат онида ажратилади. Уланиш тугалланганидан сунг адрес бушайди ва уни корпоратив тармокнинг бошка узели ишлатиши мумкин. Статик усулда узел адреси барча чикувчи пакетлар узатиладиган тармоклараро экраннинг битта адресига доимо богланади. Тармоклараро экраннинг IP-адреси ташки тармоккд тушувчи ягона фаол IP-адресга айланади. Натижада, ички тармокдан чикувчи барча пакетлар тармоклараро экрандан жунатилган булади. Бу авторизацияланган ички

тармок, ва хавфли булиши мумкин булган ташки тармок, орасида тугридан-тугри алокани истисно килади.

Бундай ёндашишда ички тармок, топологияси ташки фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи кийинлашади. Адресларни трансляциялаш тармок, ичида ташки тармок,, масалан Internetflara адреслаш билан келишилмаган адреслашнинг хусусий тизимига эга булишига имкон беради. Бу ички тармокнинг адрес маконини кенгайтириш ва ташки адрес танкислиги муаммосини самарали ечади.

Ходисаларни кайдлаш, ходисаларга реакция курсатиш, хамда кайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш тармоклараро экранларнинг мухим вазифалари х,исобланади. Корпоратив тармок,ни х,имоялаш тизимининг жиддий элементи сифатида тармокдараро экран барча харакатларни руйхатга олиш имкониятига эга. Бундай х,аракатларга нафак,ат тармок, пакетларини утказиб юбориш ёки блокировка килиш, балки хавфсизлик маъмури томонидан фойдаланишни к,оидасини узгартириш ва х,. х,ам тааллукди. Бундай руйхатга олиш зарурият тугилганда (хавфсизлик можароси пайдо булганида ёки суд инстанцияларига ёки ички тергов учун далилларни йигишда) яратилувчи журналларга мурожаат этишга имкон беради.

Шубх,али ходисалар (alarm) хусусидаги сигналларни к,айдлаш тизими тугри созланганида тармокдараро экран ёки тармок, хужумга дучор булганлиги ёки зондланганлиги тугрисидаги батафсил ахборотни бериши мумкин. Тармокдан фойдаланиш ва унинг зондланганлигининг исботи статистикасини йигиш к,атор сабабларга кура мухимдир. Аввало. тармокдараро экраннинг зондланишга ва хужумларга бардошлигини аник, билиш зарур ва тармокдараро экранни химоялаш тадбирларининг адэкватлигини аникдаш лозим. Ундан ташк,ари, тармокдан фойдаланиш статистикаси тармок, асбоб-ускуналарига ва дастурларига талабларни ифодалаш мак,садида хавф-хатарни тадкикдаш ва тахлиллашда дастлабки маълумотлар сифатида мухим хисобланади.

Купгина тармокдараро экранлар статистикани к,айдловчи, йигувчи ва тахлилловчи к,увватли тизимга эга. Мижоз ва сервер адреси, фойдаланувчилар идентификатори, сеанс вактлари, уланиш вактлари, узатилган ва к,абул

килинган маълумотлар сони, маъмур ва фойдаланувчилар харакатлари буйича хисоб олиб борилиши мумкин. Хисоб тизимлари статистикани тахлиллашга имкон беради ва маъмурларга батафсил хисоботларни такдим этади. Тармоклараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тугрисида реал вакт режимида масофадан хабар беришни бажариши мумкин.

Рухсатсиз харакатларни килишга уринишларни аникланишига буладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огохдантирувчи сигналларни бериш белгиланиши лозим. Хужум килинганлиги аникданганда огохдантирувчи сигналларни юборишга крдир булмаган тармокдараро экранни тармоклараро химоянинг самарали воситаси деб булмайди.

7.2. Тармоклараро экранларнинг асосий компонентлари

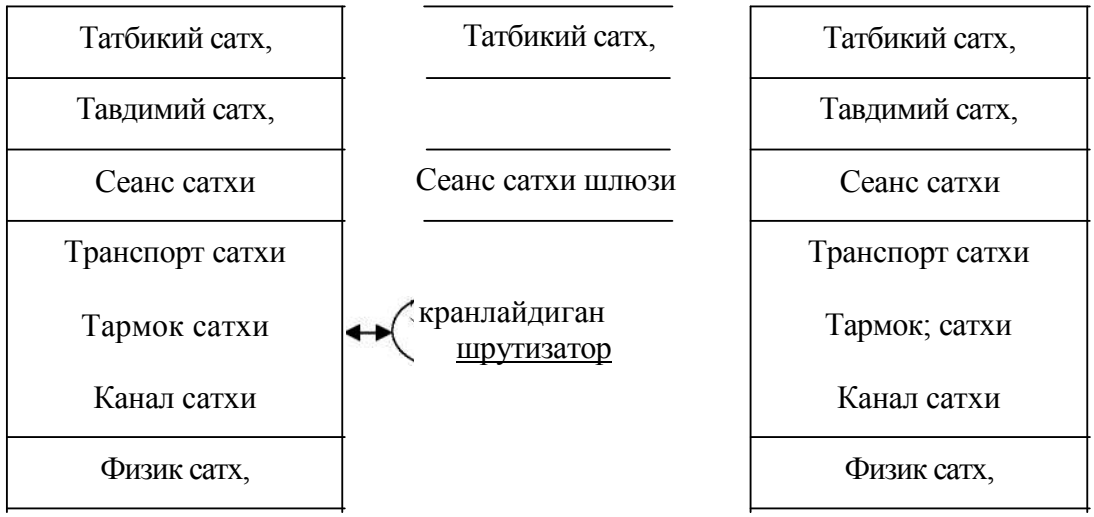
Тармокдараро экранлар тармокдараро алока хавфсизлигини OSI моделининг турли сатхдарида мададлайди. Бунда эталон моделнинг турли сатхдарида бажариладиган химоя функциялари бир-биридан жиддий фаркданади. Шу сабабли, тармокдараро экранлар комплексини, хар бири OSI моделининг алохида сатхига мулжалланган, булинмайдиган экранлар мажмуи куринишида тасаввур этиш мумкин.

Экранлар комплекси купинча эталон моделнинг тармок,, сеанс, татбик,ий сатхдарида ишлайди. Мое х,олда, к,уйидаги булинмайдиган брандмауэрлар фаркданади (7.5-расм).

- экранловчи маршрутизатор;
- сеанс сатхи шлюзи (экранловчи транспорт);
- татбикий сатх, шлюзи (экранловчи шлюз).

Тармокдарда ишлатиладиган протоколлар (ТСРЯР, БРХЯРХ) OSI эталон моделига батамом мое келмайди, шу сабабли санаб утилган экранлар хили функцияларини амалга оширишда эталон моделининг кушни сатхдарини хам камраб олишлари мумкин. Масалан, татбикий экран хабарларнинг ташк,и тармоккд узатилишида уларни автоматик тарзда шифрлаш-

ни, хдмда кабул к,илинувчи криптографик беркитилган маълумотларни автоматик тарзда расшифровка килишни амалга ошириши мумкин. Бу хрлда бундай экран OSI моделининг нафакат татбикий сатх,ида, балки такдимий сатхдда хам ишлайди.



7.5-расм. OSI моделининг алощда сатуларида ишлайдиган тармоцлараро экранлар тури

Сеанс сатхд шлюзи ишлашида OSI моделининг транспорт ва тармок, сатхдарини камраб олади. Экранловчи маршрутизатор хабарлар пакетини тахлиллашда уларнинг нафакат тармок,, балки транспорт сатхи сарлавх,аларини хам текширади.

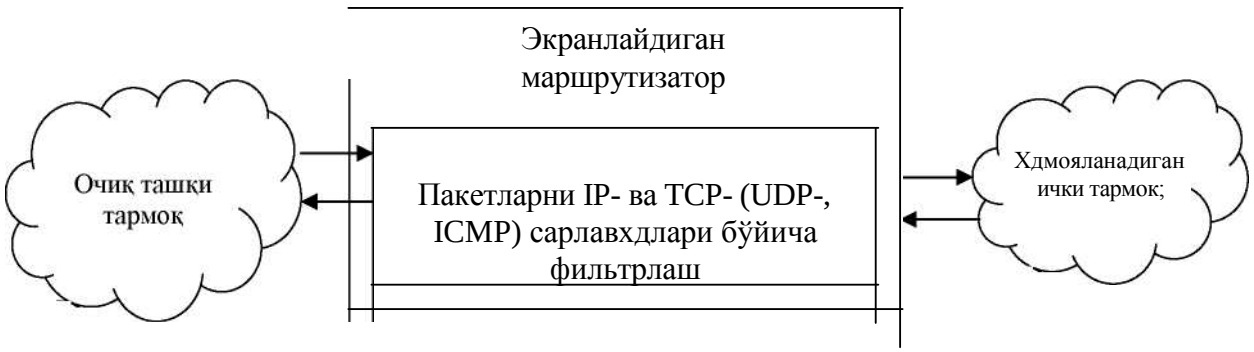
Юкррида келтирилган тармоклараро экранларнинг хиллари узининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмауэрларнинг купчилиги ёки татбик,ий шлюзлар, ёки экранловчи маршрутизаторлар булиб, тармоклараро алоканинг тулик, хавфсизлигини таъминламайди. Ишончли химояни эса фак,ат х,ар бири экранловчи маршрутизатор, сеанс сатхд шлюзи, хдмда татбикий шлюзни бирлаштирувчи тармоклараро экранларнинг комплекси таъминлайди.

Экранловчи маршрутизатор (screening router) (пакетли фильтр (packet filter) деб хам аталади) хабарлар пакетини фильтрлашга аталган ва ички ва ташки тармоклар орасида шаффоф алок,ани таъминлайди. У OSI моделининг тармок, сатх,ида ишлайди, аммо узининг айрим функцияларини ба-жаришида эталон моделининг транспорт сатхини х,ам к,амраб олиши мумкин.

Маълумотларни утказиш еки бракка чикариш хусусидаги карор фильтрлашнинг берилган коидаларига биноан хар бир пакет учун мустакил кабул килинади. Кдрор кабул килишда тармок, ва транспорт сатхдари пакетларининг сарлавх,алари тахлил этилади (7.6-расм).

Хар бир пакетнинг IP- ва TCP/UDP - сарлавх,аларининг тахлилланувчи хршиялари сифатида куйидагилар ишлатилиши мумкин:

- жунатувчи адреси;
- кабул килувчи адреси;
- пакет хили;
- пакетни фрагментлаш байроги;
- манба порти номери;
- кабул килувчи порт номери.



7.6-расм. Пакетли фильтрни ишлаш схемаси

Биринчи туртта параметр пакетнинг IP-сарлавхасига, кейингилари эса TCP-ёки UDP сарлавхасига тааллукди. Жунатувчи ва кабул килувчи адреслари IP-адреслар хисобланади. Бу адреслар пакетларни шакллантиришда тулдирилади ва уни тармок, буйича узатганда узгармайди.

Пакет хили хршиясида тармок, сатх,ига мое келувчи ICMP протокол коди ёки тахлилланувчи IP-пакет тааллукди булган транспорт сатх,и протоколининг (TCP ёки UDP) коди булади.

Пакетни фрагментлаш байроги IP-пакетлар фрагментлашининг борлиги ёки йуклигини аникдайди. Агар тах,лилланувчи пакет учун фрагментлаш байроги урнатилган булса, мазкур пакет фрагментланган IP-пакетнинг кием пакети хисобланади.

Манба ва кабул килувчи портлари номерлари TCP ёки UDP драйвер томонидан хар бир жунатилувчи хабар пакетларига кушилади ва жунатувчи иловасини, хамда ушбу пакет аталган иловани бир маънода идентификациялайди. Портлар номерлари буйича фильтрлаш имконияти учуй юкрри сатх, протоколларига порт номерларини ажратиш буйича тармокда кабул килинган келишувни билиш л озим.

Хдр бир пакет ишланишида экранловчи маршрутизатор берилган кридалар жадвалини, пакетнинг тулик, ассоциациясига мое келувчи кридани топгунича, кетма-кет куриб чикади. Бу ерда ассоциация деганда берилган пакет сарлавх,аларида курсатилган параметрлар мажмуи тушунилади. Агар экранловчи маршрутизатор жадвалдаги кридаларнинг бирортасига хам мое келмайдиган пакетни олса, у, хавфеизлик нуктаи назаридан, уни брака чикаради.

Пакетли фильтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли фильтр сифатида оддий маршрутизатор, хамда кирувчи ва чикувчи пакетларни фильтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар хар бир порт билан бир неча унлаб кридаларни боглаши ва киришда, хам чикишда пакетларни фильтрлаши мумкин.

Пакетли фильтрларнинг камчилиги сифатида к,уйидагиларни курсатиш мумкин. Улар хавфеизликнинг юкрри даражасини таъминламайди, чунки фак,ат пакет сарлавх,аларини текширадилар ва купгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охирги узелларни аутентификациялаш, хабарлар пакетларини криптографик беркитиш, х,амда уларнинг яхлитлигини ва хакикийлигини текшириш киради. Пакетли фильтрлар дастлабки адресларни алмаштириб к,уйиш ва хабарлар пакети таркибини рухсатсиз узгартириш каби кенг тарк,алган тармок, хужумларига заиф х,исобланадилар. Бу хил брандмауэрларни "алдаш" к,ийин эмас - фильтрлашга рухсат берувчи кридаларни крндирувчи пакет сарлавх,аларини шакллантириш кифоя.

Аммо, пакетли фильтрларнинг амалга оширилишининг соддалиги, юкрри унумдорлиги, дастурий иловалар учун шаффофлиги ва нархининг

пастлиги, уларнинг хдмма ерда тарк,алишига ва тармок, хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

Сеанс сагщи шлюзи, (экранловчи транспорт деб хдм юритилади) виртуал уланишларни назоратлашга ва ташки тармок, билан узаро алока килишда IP-адресларни трансляциялашга аталган. У OSI моделининг сеанс сатхдда ишлайди ва ишлаши жараёнида эталон моделнинг транспорт ва тармок, сатхдарини хам камраб олади. Сеанс сатхд шлюзининг химоялаш функциялари воситачилик функцияларига тааллукли.

Виртуал уланишларнинг назорати алокани квитирлашни кузатишдан хамда урнатилган виртуал каналлар буйича ахборот узатилишининг назоратлашдан иборат. Алокани квитирлашнинг назоратида сеанс сатх,ида шлюз ички тармок, ишчи станцияси ва тапщи тармок, компьютери орасида виртуал уланишни кузатиб, суралаётган алока сеансининг жоизлигини аниклайди.

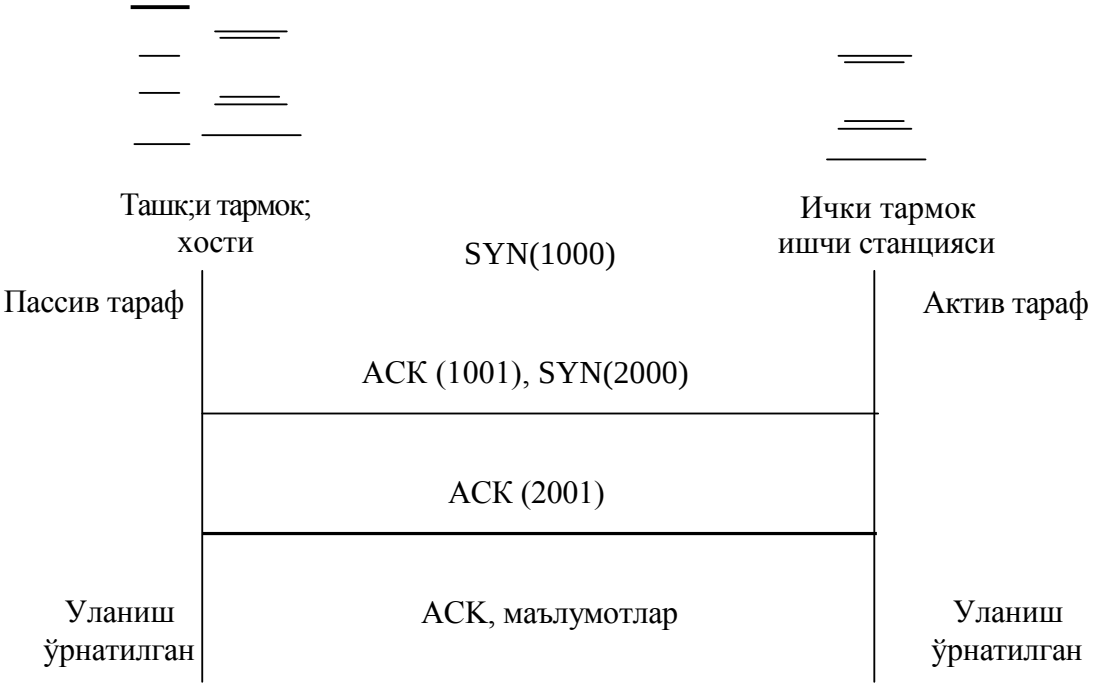
Бундай назорат TCP протоколининг сеанс сатхи пакетларининг сарлавхасидаги ахборотга асосланади. Аммо TCP-сарлавх,аларни тахлиллашда пакетли фильтр фак,ат манба ва кдбул к,илувчи портларининг номерини текширса, экранловчи транспорт алокани квиртирлаш жараёнига тааллукди бошк,а хршияларни тахдиллайди.

Алок,а сеансига суровнинг жоизлигини аниклаш учун сеанс сатх,и шлюзи куйидаги х,аракатларни бажаради. Ишчи станция (мижоз) ташки тармок, билан богланишни сураганида, шлюз бу суровни кабул килиб унинг фильтрлашнинг базавий мезонларни к,аноатлантиришини, масалан сервер мижоз ва у билан ассоциацияланган исмнинг IP-адресини аникдай олишини текширади. Сунгра шлюз, мижоз исмидан х,аракат к,илиб, ташки тармок, компьютери билан уланишни урнатади ва TCP протоколи буйича квитирлаш жараёнининг бажарилишини кузатади.

Бу муолажа SYN (Синхронлаш) ва АСК (Тасдиклаш) байрокдари орк,али белгиланувчи TCP-пакетларни алмашишдан иборат (7.7-расм).

SYN байрок, билан белгиланган ва таркибида ихтиёрий сон, масалан 1000, булган TCP сеансининг биринчи пакети мижознинг сеанс очишга сурови хисобланади. Бу пакетни олган ташки тармок, компьютери жавоб

тарикасида АСК байрок, билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг х,олда 1001) сон булган пакетни жунатади. Шу тарика, мижоздан SYN пакети олинганлиги тасдикланади. Сунгра, тескари муолажа амалга оширилади: ташки тармок, компьютери х,ам мижозга узатилувчи маълумотлар биринчи байтининг тартиб раками билан (масалан, 2000) SYN пакетини жунатади, мижоз эса уни олганлигини, таркибида 2001 сони булган пакетни узатиш оркали тасдиклайди. Шу билан алокани квиртирлаш жараёни тугалланади.



7.7-расм. TCP протоколи бўйича алокани квитирлаш схемаси. Сеанс сатх,и шлюзи (7.8-расм) учун суралган сеанс жоиз х,исобланади, к,ачонки алокани квиртирлаш жараёни бажарилишида SYN ва АСК байроклар, х,амда TCP-пакетлари сарлавх,аларидаги сонлар узаро мантик,ий богланган булса.

7.8-расм. Сеанс сатх,и шлюзи ишлаш схемаси

Ички тармокнинг ички станцияси ва ташки тармокнинг компьютери TCP сеансининг авторизацияланган катнашчилари эканлиги хамда ушбу сеанснинг жоизлиги тасдикланганидан сунг шлюз уланишни урнатади. Бунда шлюз уланишларининг махсус жадвалига мое ахборотни (жунатувчи ва кабул килувчи адреслари, уланиш хрлати, кетма-кетлик номери хусусидаги ахборот ва х,.) киритади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йуналтириб, урнатилган виртуал канал буйича ахборот узатилишини назорат килади. Ушбу назорат жараёнида сеанс сатхи шлюзи пакетларни фильтрламайди. Аммо у узатилувчи ахборот сонини назорат килиши ва кандайдир чегарадан ошганида уланишни узиши мумкин. Бу эса, уз навбатида, ахборотнинг рухсатсиз экспорт килинишига тусик, булади. Виртуал уланишлар хусусидаги кайдлаш ахборотининг тупланиши хам мумкин.

Сеанс сатхи шлюзларида виртуал уланишларни назоратлашда *канал воситачилари* (pipe proxy) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташк,и тармоклар орасида виртуал каналларни урнатади, сунгра TCPЯР иловалари генерациялаган пакетларнинг ушбу канал оркали узатилишини назоратлайди.

Канал воситачилари TCPЯРнинг муайян хизматларига мулжалланган. Шу сабабли ишлаши муайян иловаларнинг воситачи-дастурларига асосланган татбикий сатх, шлюзлари имкониятларини кенгайтиришда сеанс сатх, шлюзларидан фойдаланиш мумкин.

Сеанс сатхи шлюзи ташки тармок, билан узаро алок,ада тармок, сатх,и ички адресларини (IP-адресларини) трансляциялашни х,ам таъминлайди. Ички адресларни трансляциялаш ички тармокдан ташк,и тармок,к,а жунатилувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуктаи назаридан сеанс сатх,и шлюзи етарлича оддий ва нисбатан ишончли дастур хисобланади. У экранловчи маршрутизаторни виртуал уланишларни назоратлаш ва ички IP-адресларни трансляциялаш функциялари билан тулдиради.

Сеанс сатх,и шлюзининг камчиликлари - экранловчи маршрутизаторларнинг камчиликларига ухшаш. Ушбу технологиянинг яна бир жиддий

камчилиги маълумотлар хршиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузук, одамларга зарар келтирувчи дастурларни хдмояланувчи тармоккд узатиш имконияти тугилади. Ундан ташкари, TCP-сессиясининг (TCP hijacking) ушлаб крлинишида нияти бузук, одам хужумларини хатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатх, шлюзлари мустакил махсулот булмай, татбикий сатх, шлюзлари билан комплектда такдим этилади.

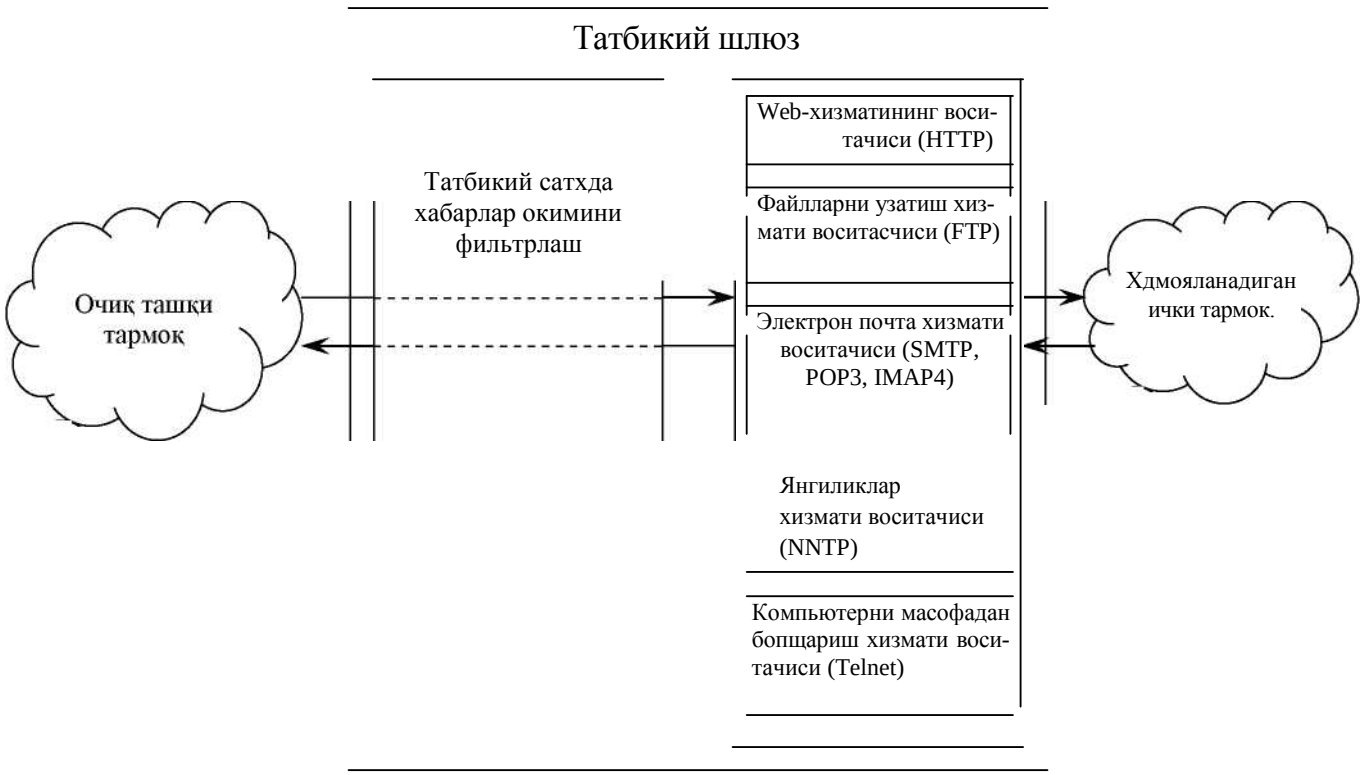
Татбщий сагщ шлюзи (экранловчи шлюз деб хам юритилади) OSI моделининг татбикий сатх,ида ишлаб, такдимий сатхни хам камраб олади ва тармоклараро алоканинг энг ишончли химоясини таъминлайди. Татбикий сатх, шлюзининг химоялаш функциялари, сеанс сатхи шлюзига ухшаб, воситачилик функцияларига тааллукди. Аммо, татбикий сатх, шлюзи сеанс сатхи шлюзига Караганда химоялашнинг анча куп функцияларини бажариши мумкин:

- брандмауэр орк,али уланишни урнатишга уринишда фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- шлюз оркали узатилувчи ахборотнинг х,ак,икийлигини текшириш;
- ички ва ташки тармок, ресурсларидан фойдаланишни чегаралаш;
- ахборотлар окимини фильтрлаш ва узгартириш, масалан, вирусларни динамик тарзда кидириш ва ахборотни шаффоф шифрлаш;
- ходисаларни к,айдлаш, ходисаларга реакция курсатиш, х,амда к,айдланган ахборотни тахлиллаш ва хисоботларни генерациялаш;
- ташки тармокдан суралувчи маълумотларни кэшлаш.

Татбикий сатх, шлюзи функциялари воситачилик функцияларига тааллукди булганлиги сабабли, бу шлюз универсал компьютер хисобланади ва бу компьютерда хар бир хизмат курсатилувчи татбикий протокол (HTTP, FTP, SMTP, NNTP ва х,.) учун биттадан воситачи дастур (экранловчи агент) ишлатилади. TCPЯРнинг хар бир хизматининг воситачи дастури (application proxy) айнан шу хизматга тааллукди хабарларни ишлашга ва химоялаш функцияларини бажаришга мулжалланган.

Татбикий сатх, шлюзи мое экранловчи агентлар ёрдамида кирувчи ва чикувчи пакетларни ушлаб крлади, ахборотни нусхалайди ва кайта

жунатади, яъни ички ва ташки тармоклар орасидаги тугридан-тугри уланишни истисно килган х,олда, сервер-воситачи функциясини бажаради (7.9-расм).



7.9-расм. Татбиций шлюз ишлаш схемаси.

Татбикий сатх, шлюзи ишлатадиган воситачилар сеанс сатхд шлюзларининг канал воситачиларидан жиддий фаркданади. Биринчидан, татбикий сатх, шлюзлари муайян иловалар (дастурий серверлар) билан богланган, иккинчидан улар OSI моделининг татбикий сатх,ида хабарлар окимини фильтрлашлари мумкин.

Татбик,ий сатх, шлюзлари воситачи сифатида мана шу максадлар учун махсус ишлаб чикилган ТСРЯРнинг муайян хизматларининг дастурий серверлари - HTTP, FTP, SMTP, NNTP ва х,. - серверларидан фойдаланади. Бу дастурий серверлар брандмауэрларда резидент режимида ишлайди ва ТСРЯРнинг мое хизматларига тааллукли х,имоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг махсус транслятори хизмат курсатади.

Ички тармок, ишчи сервери ва ташки тармок, компьютери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмауэргача ва брандмауэрдан белгиланган жойгача. Канал воситачиларидан фаркли х,олда,

татбикий сатх, шлюзининг воситачилари факат узлари хизмат килувчи иловалар генерациялаган пакетларни утказади. Масалан, HTTP хизматининг воситачи-дастури факат шу хизмат генерациялаган трафикни ишлайди.

Агар кандайдир иловада узининг воситачиси булмаса, татбикий сатхдаги шлюз бундай иловани ишлай олмайди ва у блокировка килинади. Масалан, агар татбикий сатхдаги шлюз факат HTTP, FTP ва Telnet восита-чидастурларидан фойдаланса, у факат шу хизматларга тегишли пакетларни ишлайди ва крлган хизматларнинг пакетларини блокировка килади.

Татбикий сатх, шлюзи воситачилари, канал воситачиларидан фаркли хрлда, ишланувчи маълумотлар таркибини текширишни таъминлайди. Улар узлари хизмат курсатадиган татбикий сатх, протоколларидаги командаларнинг алохдда хилларини ва хабарлардаги ахборотлани фильтрлашлари мумкин.

Татбикий сатх, шлюзини созлашда ва хабарларни фильтрлаш кридаларини тавсифлашда куйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жоиз вакт оралиги, ушбу сервисга боглик, хабар таркибига чегаралашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва х,.

Татбикий сатх, шлюзи куйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармок, х,имоясининг юк,ори даражасини таъминлайди;

- иловалар сатх,ида х,имоялаш купгина к,ушимча текширишларни амалга оширишга имкон беради, натижада дастурий таъминот камчиликларига асосланган муваффакиятли хужумлар утказиш эх,тимоллиги камаяди;

- татбик,ий сатх, шлюзининг ишга лаёкатлиги бузилса, булинувчи тармокдар орасида пакетларнинг туппа-тугри утиши блокировка килинади, натижада, рад килиниши туфайли химояланувчи тармок,нинг хавфсизлиги пасаймайди.

Татбик,ий сатх, шлюзининг камчиликларига куйидагилар киради:

- нархининг нисбатан юкррилиги;

- брандмауэрнинг узи, х,амда уни урнатиш ва конфигурациялаш муолажаси етарлича мураккаб;

- компьютер платформаси унумдорлигига ва ресурслари хджмига купиладиган талабларнинг юкррилиги;

- фойдаланувчилар учун шаффофликнинг йуклиги ва тармоклараро алока урнатилишида утказиш крбилиятининг сусайиши.

Охирги камчиликка батафсил тухталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралик, ролини бажаради. Аввал воситачи билан уланиш урнатилади, сунгра воситачи адресат билан уланишни яратиш ёки яратмаслик хусусида карор кабул к,илади. Мое хрлда татбикий сатх, шлюзи ишлаши жараёнида хар кандай рухсат этилган уланишни кайталайди. Натижада фойдаланувчилар учун шаффофлик йукрлади ва уланишга хизмат килишга кушимча харажат сарфланади.

Эксперт сатуи шлюзи. Татбикий сатх, шлюзининг фойдаланувчилар учун шаффофлигининг йукдиги ва тармоклараро алока урнатилишида утказиш крбилиятининг сусайиши каби жиддий камчиликларини бартараф этиш максадида пакетларни фильтрлашнинг янги технологияси ишлаб чикилган. Бу технологияни баъзида *уланиш холатини назоратлашли филътрлаш* (stateful inspection) ёки эксперт сатхддаги фильтрлаш деб юритишади. Бундай фильтрлаш пакетлар х,олатини куп сатхди тахдиллашнинг махсус усуллари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармок, сатх,ида пакетларни ушлаб крлиш ва ундан уланишни назорат килишда ишлатилувчи татбик,ий сатх, ахборотини чикариб олиш орк,али уланиш хрлатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоклараро экран *эксперт сатх брандмауэры* деб юритилади. Бундай брандмауэрлар узида экранловчи маршрутизаторлар ва татбик,ий сатх, шлюзлари элементларини уйгунлаштиради. Улар хар бир пакет таркибини берилган хавфеизлик сиёсатига мувофик, бахрлайдилар.

Шундай к,илиб эксперт сатх,идаги брандмауэрлар куйидагиларни назоратлашга имкон беради:

- мавжуд кридалар жадвали асосида хар бир узатилувчи пакетни;
- хрлатлар жадвали асосида хар бир сессияни;
- ишлаб чикилган воситачилар асосида хар бир иловани.

Эксперт сатх, тармокдарарo экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот окимини ишлашининг юкрри тезкорлигини хдмда улар оркали утувчи пакетларнинг IP-адресларини узгартирмаслигини курсатиш мумкин. Охирги афазаллик. IP-адресдан фойдаланувчи татбикий сатхнинг хар кандай протоколининг бундай брандмауэрлардан хеч кандай узгаришсиз ёки махсус дастурлашсиз бирга ишлай олишини англатади.

Бундай брандмауэрларнинг авторизацияланган мижоз ва ташки тармок, компьютери орасида тугридан-тугри уланишга йул кутили, химоянинг унчалик юк,ори булмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатх,ини фильтрлаш технологиясидан комплекс брандмауэрлар ипшаши самарадорлигини оширишда фойдаланилади. Эксперт сатх,нинг фильтрлаш технологиясини ишлатувчи комплекс брандмауэрларга мисол тарикасида Fire Wall-1 ва ON GuardnapHn курсатиш мумкин.

7.3. Тармо^лараро экранлар асосидаги тармок з^имоясининг схемалари

Тармокдарарo алокани самарали х,имоялаш учун брандмауэр тизими тугри урнатилиши ва конфигурацияланиши лозим. Ушбу жараён к,уйидагиларни уз ичига олади:

- тармокдарарo алока сиёсатини шакллантириш;
- брандмауэрни улаш схемасини танлаш ва параметрларини созлаш.

Тармоцлараро алоца сиёсатини шакллантириш

Тармокдарарo алока сиёсатини шакллантиришда куйидагиларни аниклаш лозим:

- тармок, сервисларидан фойдаланиш сиёсати;
- тармокдарарo экран ишлаши сиёсати.

Тармоц сервисларидан фойдаланиш сиёсати химояланувчи компьютер тармокнинг барча сервисларини такдим этиш, хамда улардан фойдаланиш кридаларини белгилайди. Ушбу сиёсат доирасида тармок, экрани орк,али такдим этилувчи барча сервислар ва х,ар бир сервис учун мижозларнинг жоиз адреслари берилиши лозим. Ундан ташк,ари, фойдаланувчилар учун

кдчон ва кайси фойдаланувчилар кайси сервисдан ва кайси компьютерда фойдаланишларини тавсифловчи кридалар курсатилиши лозим. Фойдаланиш усулларига чегаралашлар хам берилади. Бу чегаралашлар фойдаланувчиларнинг InternetHHHr ман этилган сервисларидан айланма йул оркали фойдаланишларига йул куймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш кридалари, хамда ташкилот локал тармога ташкарисидаги фойдаланувчиларнинг ишлаш шароитлари алохдда белгиланиши лозим.

ТармокларарО экран ишлаши сиёсатида тармокдарарО алокани бошкаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг куйидаги иккитасидан бири танланиши мумкин:

- ошкора рухсат этилмагани ман килинган;
- ошкора ман этилмаганига рухсат берилган.

"Ошкора рухсат этилмагани ман килинган" принципи танланганида тармокдарарО экран шундай созланадики, харкандай рухсат этилмаган тармокдарарО алок,алар блокировка к,илинади. Ушбу принцип ахборот хавфсизлигининг барча сох,аларида ишлатилувчи фойдаланишнинг мумтоз моделига мое келади. Бундай ёндашиш, имтиёзларни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфеизлик нуктаи назаридан яхширок, х,исобланади. Мох,ияти буйича "ошкора рухсат этилмагани ман к,илинган" принципи билмаслик зарар келтириши фактини эътироф этишдир. Таъкидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш к,оидалари фойдаланувчиларга маълум нок,улайликлар тугдириши мумкин.

"Ошкора ман этилмаганига рухсат берилган" принципи танланганида тармокдарарО экран шундай созланадики, факат ошкора ман этилган тармокдарарО алокалар блокировка килинади. Бу хрлда, фойдаланувчилар томонидан тармок, сервисларидан фойдаланиш к,улайлиги ошади, аммо тармокдарарО алока хавфеизлиги пасаяди. Фойдаланувчиларнинг тармокдарарО экранни четлаб утишларига имкон тугилади, масалан улар сиёсат ман килмаган (х,атто сиёсатда курсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички

тармок, хакерларнинг хужумларидан камрок, химояланган булади. Шу сабабли, тармокдарарo экранларни ишлаб чикарувчилари одатда ушбу принципдан фойдаланмайдилар.

Тармокдарарo экран симметрик эмас. Унга ички тармокнинг ташки тармокдан ва аксинча фойдаланишни чегараловчи кридалар алохида берилади. Умумий хрлда, тармокдарарo экраннинг иши куйидаги иккита гурух, функцияларни динамик тарзда бажаришга асосланган:

- у оркали утаётган ахборот окимини фильтрлаш;
- тармокдарарo алока амалга оширилишида воситачилик.

Оддий тармокдарарo экранлар бу функцияларнинг бирини бажаришга мулжалланган. Комплекс тармокдарарo экранлар химоялашнинг курсатилган функцияларининг биргаликда бажарилишини таъминлайди.

Тармоклараро экранларни улашнинг асосий схемалари. Корпора-тив тармокни глобал тармокдарга улаганда х,имояланувчи тармокнинг гло-бал тармокдан ва глобал тармокнинг химояланувчи тармокдан фойдалани-шини чегаралаш, х,амда уланувчи тармокдан глобал тармокнинг масофадан рухсатсиз фойдаланишидан химоялашни таъминлаш лозим. Бунда ташкилот узининг тармоги ва унинг компонентлари хусусидаги ахборотни глобал тармок, фойдаланувчиларидан беркитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш х,имояланувчи тармок, ресурсларидан фойдаланишнинг к,атъий чегараланишини талаб этади.

Ташкилотдаги корпоратив тармок, таркибида купинча х,имояланишнинг турли сатхди бирнечи сегментларга эга булиши эх,тиёжи тугилади:

- бемалол фойдаланилувчи сегментлар (масалан, реклама WWW-серверлари);
- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг ма софадаги узеллари ходимларининг фойдаланиши учун);
- ёпик, сегментлар (масалан, ташкилотнинг молия локал к,исм тармоги)

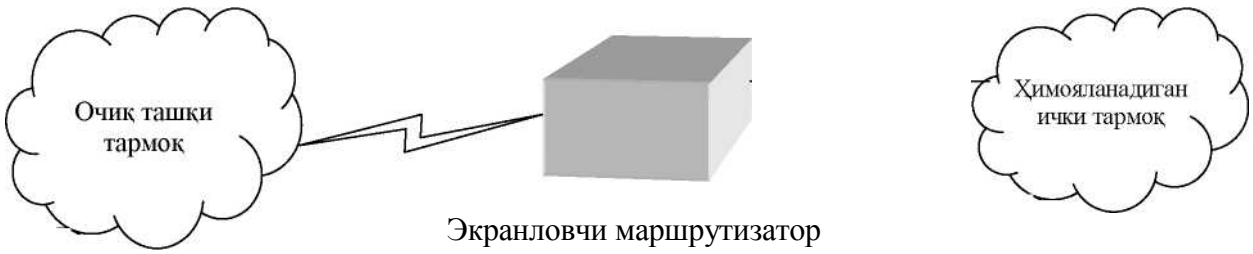
Тармокдарарo экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар х,имояланувчи тармок, ишлаши шароитига, хамда иш-

латиладиган брандмауэрларнинг тармок, интерфейслари сонига ва бошка характеристикаларига боглик,. Тармоклараро экранни улашнинг куйидаги схемалари кенг таркалган:

- экранловчи маршрутизатордан фойдаланилган химоя схемалари;
- л окал тармокни умумий химоялаш схемалари;
- химояланувчи ёпик, ва химояланмайдиган очик, кием тармокли схемалар;
- ёпик, ва очик, кием тармокдарни алохида химояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган химоя схемаси.

Пакетларни фильтрлашга асосланган тармоклараро экран кенг тарк,алган ва амалга оширилиши осон. У х,имояланувчи тармок, ва булиши мумкин булган ганим очик, тармок, орасида жойлашган экранловчи маршрутизатордан иборат (7.10-расм).



7.10-расм. Тармоцлараро экран - экранловчи маршрутизатор Экранловчи маршрутизатор (пакетли фильтр) кирувчи ва чикувчи пакетларни уларнинг адреслари ва портлари асосида блокировка килиш ва фильтрлаш учун конфигурацияланган.

Химояланувчи тармокдаги компьютерлар InternetflaH тугридан-тугри фойдаланаолади, InternetHHHr улардан фойдаланишининг куп к,исми эса блокировка килинади. Умуман, экранловчи маршрутизатор юкррида тавсифланган х,имоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йули ва чикиш йули портлари номери буйича фильтрламаса, "ошкора рухсат этилмагани ман килинган" сиёсатини амалга ошириш к,ийинлашади.

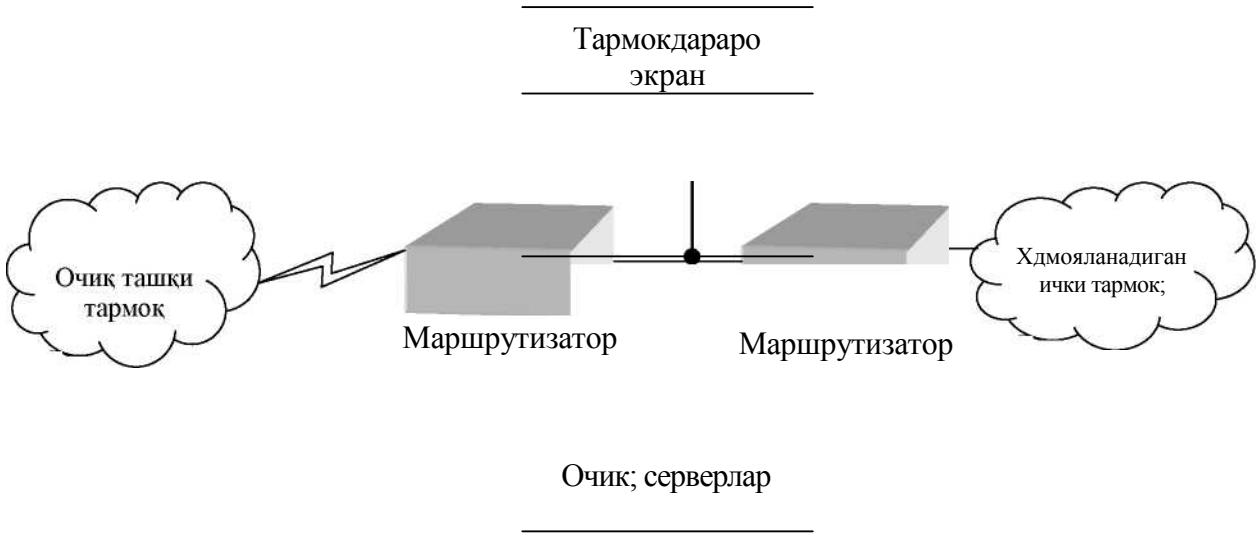
Пакетларни фильтрлашга асосланган тармоклараро экраннинг камчиликлари к,уйидагилар:

- фильтрлаш кридаларининг мураккаблиги; баъзи хрлларда бу кридалар мажмуи бажарилмаслиги мумкин;

- фильтрлаш кридаларини тулик, тестлаш мумкин эмаслиги; бу тармокни тестланмаган хужумлардан химояланмаслигига олиб келади;

- ходисаларни руйхатга олиш имкониятининг йуклиги; натижада маъмурга машрутизаторнинг хужумга дуч келганлигини ва обрусизлантирилганлигини аникдаш кийинлашади.

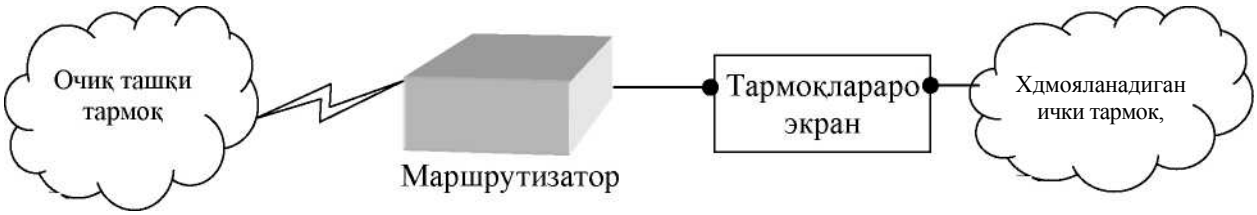
Локал тармоцни умумий химоялаш схемалари. Битта тармок, интерфейсли брандмауэрлардан фойдаланилган химоялаш схемалари (7.11-раем)



7.11-расм. Битта тармоц интерфейсли firewall ёрдамида локал тармоцни щмоялаш

хавфеизлик ва конфигурациялашнинг кулайлиги нуктаи назаридан самарасиз х,исобланади. Улар ички ва ташки тармокдарни физик ажратмайдилар, демак, тармоклараро алок,анинг ишончли х,имоясини таъминлай олмайдилар.

Локал тармок,ни умумий химоялаш схемаси энг оддий ечим булиб, унда брандмауэр локал тармокни ташк,и ганим тармокдан бутунлай экранлайди (7.12-расм). Маршрутизатор ва брандмауэр орасида факат битта йул



7.12-расм. Локал тармоцни умумий щмоялаш схемаси

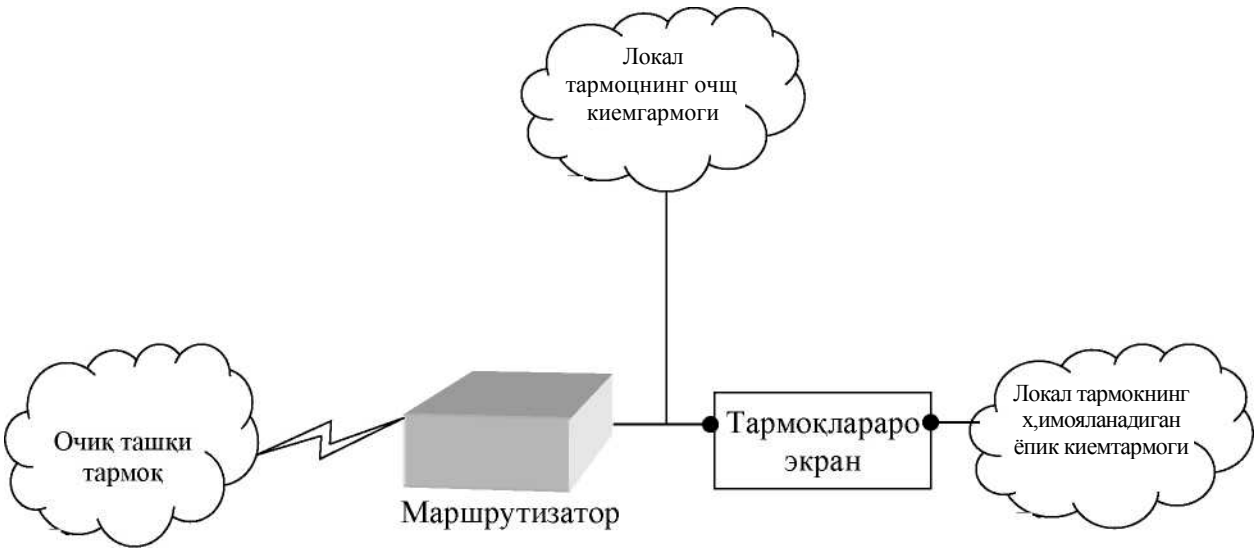
булиб, бу йул орк,али бутун трафик утади. Брандмауэрнинг ушбу варианти "ошкора рухсат этилмагани ман килинган" принципига асосланган химоялаш сиёсатини амалга оширади. Одатда маршрутизатор шундай созланадики, брандмауэр ташкаридан куринадиган ягона машина булади.

Локал тармок, таркибидаги очик, серверлар хам тармокдараро экранлар томонидан химояланади. Аммо, ташки тармок, фойдаланаоладиган серверларни химоялануvчи локал тармокларнинг бошка ресурслари билан бирлаштириш тармокдараро алока хавфсизлигини жиддий пасайтиради.

Тармокдараро экран фойдаланадиган хостга фойдаланувчиларни кучайтирилган аутентификациялаш учун дастур уранатилиши мумкин.

Х,имояланувчи ёпиц еа уимояланмайдиган очиц цисм тармоцли схемалар. Агар локал тармок, таркибида умумфойдаланувчи очик, серверлар булса уларни тармокдараро экрандан олдин очик, кием тармок, сифатида чик,ариш мак,садга мувофик, х,исобланади (7.13-расм).

Ушбу усул локал тармок, ёпик, к,исмининг кучли химояланишини, аммо тармокдараро экрангача жойлашган очик, серверларнинг пасайган х,имояланишини таъминлайди.

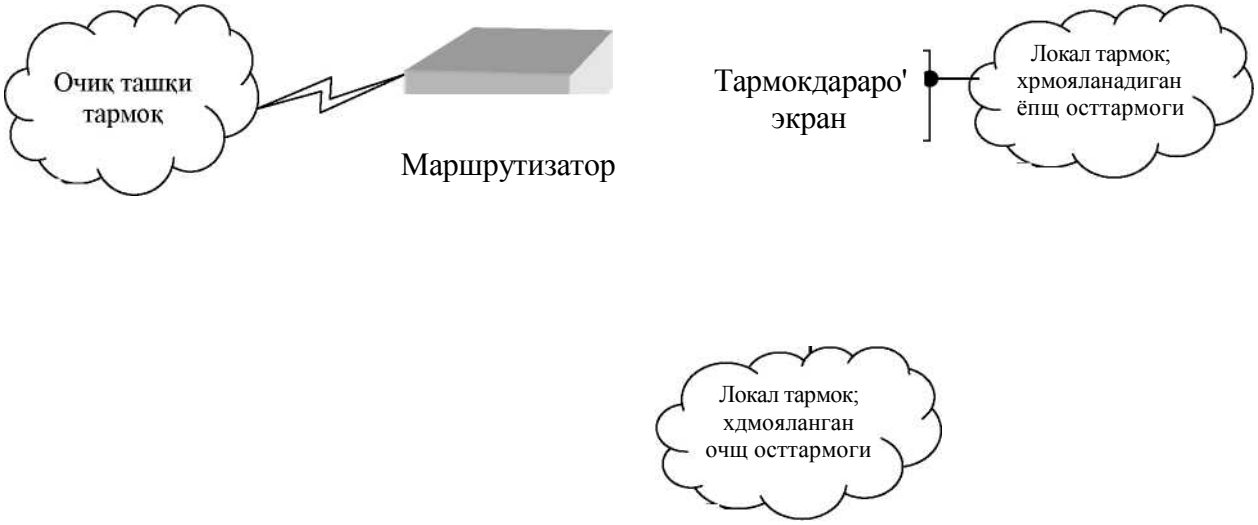


7.13-расм. Х,имояланадиган ёпиц ва щмояланмайдиган очиц циемтармоцли схема

Баъзи брандмауэрлар бу серверларни узида жойлаштиради. Аммо бу брандмауэрнинг хавфеизлиги ва компьютернинг юкланиши нуктаи назаридан яхши ечим хисобланмайди. Химоялануvчи ёпик, ва химояланмайдиган очик, к,исм тармокди схемани очик, кием тармок, хавфсизлигига куйиладиган

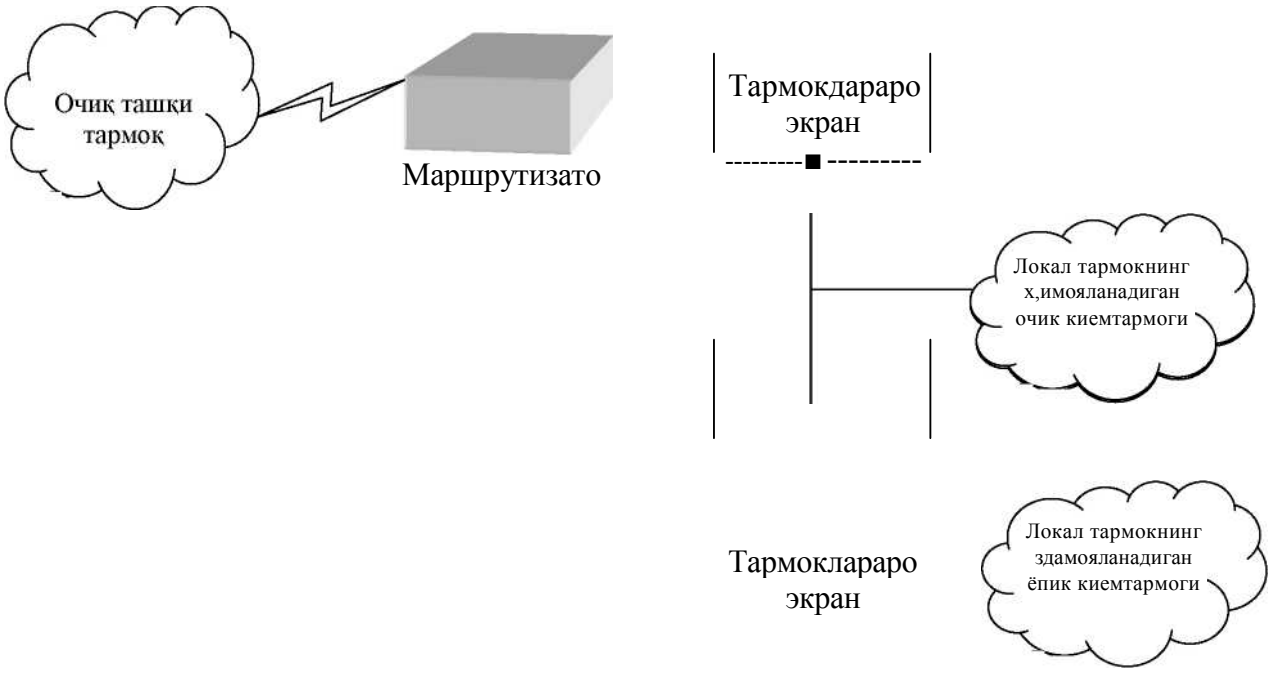
талабларнинг булмаган хрлларида ишлатилиши максадга мувофик, хисобланади. Агар очик, сервер хавфсизлигига юкрри талаблар куйилса, ёпик, ва очик, кием тармокларни алохдда химоялаш схемаларидан фойдаланиш зарур.

Ёпиц еа очиц цисм тармоцларни алоуида уимояловчи схемалар. Бундай схемалар учта тармок, интерфейсли битта брандмауэр (7.14-расм)



7.14 -расм. Учта тармоц интерфейсли бир брандмауэр асосида ёпиц ва очиц цисм тармоцларни алоуида щмоялаш схемаси

ёки иккита тармок, интерфейсли иккита брандмауэр (7.15-расм) асосида



7.15-расм. Иккита тармоц интерфейсли иккита брандмауэр асосида ёпиц ва очиц циемтармоцларни алоуида щмоялаш схемаси

курилиши мумкин. Иккала хрлда хам очик, ва ёпик, кием тармокдардан факат тармокдарарро экран оркали фойдаланиш мумкин. Бунда очик, кием тармокдан фойдаланиш ёпик, кием тармокдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармокдарарро алока хавфеизлигининг юкрри даражасини таъминлайди. Бунда хар бир брандмауэр ёпик, тармокни химоялашнинг алохида эшелонини хреил килади, химояланувчи очик, кием тармок, эса экранловчи кием тармок, сифатида иштирок этади.

Одатда экранловчи кием тармок, шундай конфигурацияланадики, кием тармок, компьютеридан ганим ташки тармок, ва локал тармокнинг ёпик, кием тармога фойдалана олеин. Аммо ташки тармок, ва ёпик, кием тармок, орасида тугридан-тугри ахборот пакетларини алмашиш мумкин эмас. Экранловчи кием тармокди тизимни хужум к,илишда, булмаганида х,имоянинг иккита мустак,ил чизигини босиб утишга тугри келади. Бу эса жуда мураккаб масала хисобланади. Тармокдарарро экран х,олатларини мониторинглаш воситалари бундай уринишни доимо аникдаши ва тизим маъмури уз вактида рухсатсиз фойдаланишга карши зарурий чоралар куриши мумкин.

Таъкидлаш лозимки, алок,анинг коммутацияланувчи линияси орк,али уланувчи масофадаги фойдаланувчиларнинг иши х,ам ташкилотда утказилувчи хавфеизлик сиёсатига мувофик, назорат к,илиниши шарт. Бундай масаланинг намунавий х,ал этилиши - зарурий функционал имкониятларга эга булган масофадан фойдаланиш серверини (терминал серверни) урнатиш. Терминал сервер бир неча асинхрон портларга ва локал тармокнинг битта интерфейсига эга булган тизим хисобланади. Асинхрон портлар ва локал тармок, орасида ахборот алмашиш факат ташки фойдаланувчини аутентификациялашдан кейин амалга оширилади.

Терминал серверни улаш шундай амалга ошириш лозимки, унинг иши факат тармокдарарро экран оркали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурелари билан ишлаш хавфеизлигининг керакли даражасини таъминлашга имкон беради.

Терминал серверни очик, кием тармок, таркибига киритилганида бундай уланиш жоиз хисобланади. Терминал сервернинг дастурий таъминоти

коммутацияланувчи каналлар оркали алока сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошкдриш модуллари серверни узини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш буйича етарлича ривожланган имкониятларга эга ва куйидаги функцияларни бажаради:

- кетма-кет портлардан, PPP протоколи буйича масофадан, хамда маъмур консолидан фойдаланишда л окал паролни ишлатиш;
- локал тармокнинг кандайдир машинасининг аутентификациялашга суровидан фойдаланиш;
- аутентификациялашнинг ташки воситаларидан фойдаланиш;
- терминал сервери портларидан фойдаланишни назоратловчи руйхатни урнатиш;
- терминал сервер оркали алока сеансларини протоколлаш.

Шахсий еа тацсимланган тармоц экранлари. Охирги бир неча йил мобайнида корпоратив тармок, тузилмасида маълум узгаришлар содир булди. Агар илгари бундай тармок, чегараларини аник, белгилаш мумкин булган булса, хрзирда бу мумкин эмас. Якиндаёк, бундай чегара барча маршрутизаторлар ёки бошк,а к,урилмалар (масалан, модемлар) орк,али утар ва улар ёрдамида тапщи тармокдарга чик,илар эди. Аммо хрзирда тармоклараро экран орк,али х,имояланувчи тармок,нинг тула х,ук,укди эгаси - химояланувчи периметр ташк,арисидаги ходим хисобланади. Бундай ходимлар сирасига уйдаги ёки мех,нат сафаридаги ходимлар киради. Шубхасиз, уларга хам химоя зарур. Аммо барча анъанавий тармоклараро экранлар шундай к,урилганки, х,имояланувчи фойдаланувчилар ва ресурслар уларнинг х,имоясида корпоратив ёки локал тармокнинг ички томонида булишлари шарт. Бу эса мобил фойдаланувчилар учун мумкин эмас.

Бу муаммони ечиш учун куйидаги ёндашишлар таклиф этилган:

- так,симланган тармоклараро экранлардан (distributed firewall) фойдаланиш;
- виртуал хусусий тармок, VPNnap имкониятидан фойдаланиш.

Тацсимланган тармоцлараро экран тармокнинг алох,ида компьютерини химояловчи марказдан бошк,арилувчи тармок, мини-экранлар мажмуидир.

Таксимланган брандмауэрларнинг катор функциялари (масалан марказдан бошкариш, хавфсизлик сиёсатини таркатиш) шахсий фойдаланувчилар учун ортикча булганлиги сабабли, таксимланган брандмауэр л ар модификацияланди. Янги ёндашиш *шахсий тармоцли экранлаш технологияси* номини олди. Бунда тармокли экран химояланувчи шахсий компьютерда урнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармокли экранлаш тизими деб аталувчи бундай экран, бошка барча тизимли химоялаш воситаларига боглик, булмаган хрлда бутун чикувчи ва кирувчи трафикни назоратлайди. Алохида компьютерни экранлашда тармок, сервисдан фойдаланувчанлик мададланади, аммо ташки фаолликнинг юкланиши пасаяди. Натижада, шу тарика химояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузук, одам олдин, химоялаш воситалари синчиклаб ва катъий конфигурацияланган, экранни босиб утиши лозим.

Таксимланган тармокдарараро экраннинг шахсий экрандан асосий фарк,и-так,симланган тармокдарараро экранда марказдан бошкариш функциясининг борлиги. Агар шахсий тармокли экранлар улар урнатилган компьютер орк,али бошк,арилса (уй шароитида к,улланишга жуда мое), таксимланган тармокдарараро экранлар ташкилотнинг бош офисида урнатилган бошк,аришнинг умумий консоли томонидан бошкарилиши мумкин.

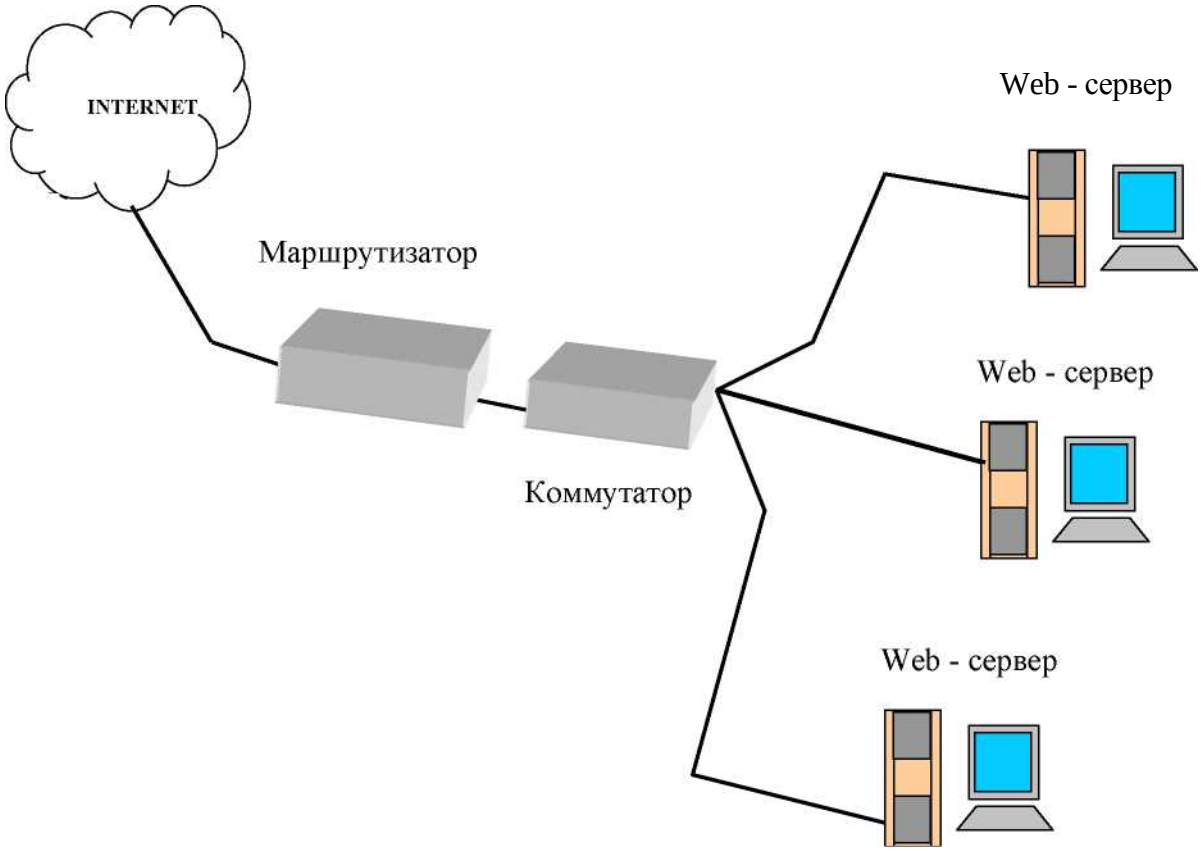
Корпоратив тармок, рухсатсиз фойдаланишдан х,ак,ик,атан х,ам химояланган х,исобланади, к,ачонки унинг InternetflaH кириш нуктасида х,имоя воситалари х,амда ташкилот локал тармоги фрагментларини, корпоратив серверларини ва алохида компьютерлар хавфеизлигини таъминловчи ечимлар мавжуд булса. Таксимланган ёки шахсий тармокдарараро экран асосидаги ечимлар алох,ида компьютерлар, корпоратив серверлар ва ташкилот локал тармок, фрагментлари хавфеизлигини таъминлашни аъло даражада бажаради.

Таксимланган тармокдарараро экранлар, анъанавий тармокдарараро экранлардан фаркли равишда, кушимча дастурий таъминот булиб, хусусан корпоратив серверларни, масалан Internet-серверларни ишончли химоялаши

мумкин. Корпоратив тармокни хдмоялашнинг окилона ечими - хдмоялаш воситасини у хдмоя килувчи сервери билан бир платформада жойлаштиришдир. 7.16-расмда корпоратив серверларни таксимланган тармокдараро экранлар ёрдамида хдмоялаш схемаси келтирилган.

Анъанавий ва таксимланган тармокдараро экранларни куйидаги курсаткичлари буйича таккрслайлик.

Самарадорлик. Анъанавий брандмауэр купинча тармок, периметрии буйича жойлаштирилади, яъни у хдмоянинг бир катламини таъминлайди холос. Агар бу ягона катлам бузилса, тизим хдркандай хужумга бардош бераолмайди. Шахсий брандмауэр операцион тизимнинг ядро сатхдда ишлайди ва барча кирувчи ва чикувчи пакетларни текшириб корпоратив серверларни ишончли хдмоялайди.



7.16 -расм. Таксимланган тармокдараро экранлар ёрдамида корпоратив серверларни х,имоялаш

Урнатилишининг осонлиги. Анъанавий брандмауэр корпоратив тармок, конфигурациясининг булими сифатида урнатилиши л озим. Таксимланган брандмауэр дастурий таъминот булиб, санокди дак,ик,аларда урнатилади ва олиб ташланади.

Бошқариш. Анъанавий брандмауэр тармок, маъмури томонидан бошкарилади. Таксимланган брандмауэр тармок, маъмури ёки локал тармок, фойдаланувчиси томонидан бошкарилиши мумкин.

Унумдорлик. Анъанавий брандмауэр тармоклараро алмашишни таъминловчи курилма булиб, унумдороиги (пакет/дакика буйича) белгиланган чегараланишга эга. У бир-бири билан коммутацияланувчи мах,аллий тармок, орк,али богланган усувчи сервер парклари учун тугри келмайди. Так,симланган брандмауэр к,абул к,илинган хавфсизлик сиёсатига зиён етказмасдан сервер паркларини усишига имкон беради.

Нархи. Анъанавий брандмауэр, одатда функциялари белгиланган, нархи етарлича юк,ори тизим х,исобланади. Брандмауэрнинг так,симланган махсулотлари дастурий таъминот булиб, анъанавий тармокдараро экранлар нархининг 1/5 ёки 1/10 га тенг.

VIII боб. ХИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОКЛАР 8.1.

Х,имояланган виртуал хусусий тармоцларни куриш концепцияси

Internet нинг гуриллаб ривожланиши натижасида дунёда ахборотни таркдтиш ва фойдаланишда сифатий узгариш содир булди. Internet фойдаланувчилари арзон ва кул аи коммуникацияга эга булдилар. Корхоналар Internet каналларидан жиддий тижорат ва бошкдрув ахборотларини узатиш имкониятларига к,изик,иб к,олдилар. Аммо InternetHHHr курилиши принципи нияти бузук, одамларга ахборотни угирлаш ёки атайин бузиш имкониятини яратди. Одатда ТСРЯР протоколлар ва стандарт Internet-иловалар (e-mail, Web, FTP) асосида курилган корпоратив ва идора тармокдари сук,илиб киришдан кафолатланмаганлар.

InternetHHHr хамма ерда таркдпишидан манфаат куриш мак,садида тармок, хужумларига самарали кдршилик курсатувчи ва бизнесда очик, тармокдардан фаол ва хавфсиз фойдаланишга имкон берувчи виртуал хусусий тармок, VPN яратиш устида ишлар олиб борилди. Натижада 1990 йилнинг бошида виртуал хусусий тармок, VPN концепцияси яратилди. "Виртуал" ибораси VPN атамасига иккита узел уртасидаги уланишни вак,тинча деб курилишини таъкидлаш мак,садида киритилган. Хдк,икдтан, бу уланиш доимий, кдтъий булмай, фак,ат очик, тармок, буйича трафик утганида мавжуд булади.

Виртуал тармок, УРМларни к,уриш концепцияси асосида етарлича оддий гоя ётади: агал глобал тармокда ахборот алмашинувчи иккита узел булса, бу узеллар орасида очик, тармок, орк,али узатилаётган ахборотнинг конфиденциаллигини ва яхлитлигини таъминловчи виртуал х,имояланган туннел к,уриш зарур ва бу виртуал туннелдан барча мумкин булган тапщи фаол ва пассив кузатувчиларнинг фойдаланиши хаддан ташкдри к,ийин булиши лозим.

Шундай к,илиб, VPN туннели очик, тармок, орк,али утказилган уланиш булиб, у оркдпи виртуал тармок,нинг криптографик х,имояланган ахборот

пакетлари узатилади. Ахборотни VPN туннели буйича узатилиши жараёнидаги химоялаш куйидаги вазифаларни бажаришга асосланган:

- узаро алокадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг хакикийлигини ва яхлитлигини текшириш.

Бу вазифалар бир бирига боглик, булиб, уларни амалга оширишда ахборотни криптографик химоялаш усулларидан фойдаланилади. Бундай химоялашнинг самарадорлиги симметрик ва асимметрик криптографик тизимларнинг биргаликда ишлатилиши эвазига таъминланади. VPN курилмалари томонидан шакллантирилувчи VPN туннели химояланган ажратилган линия хусусиятларига эга булиб, бу химояланган ажратилган линиялар умумфойдаланувчи тармок,, масалан Internet доирасида, сафланади. VPN курилмалари виртуал хусусий тармокдарда VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзи вазифасини уташи мумкин.

VPN-мижоз одатда шахсий компьютер асосидаги дастурий ёки дастурий-аппарат комплекси булиб, унинг тармок, дастурий таъминоти у бошка VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзлари билан алмашинадиган трафикни шифрлаш ва аутентификациялаш учун модификацияланади. Одатда VPN-мижознинг амалга оширилиши стандарт операцион тизим - Windows NT/2000 ёки UnixHH тулдирувчи дастурий ечимдан иборат булади.

VPN-сервер сервер вазифасини утовчи, компьютерга урнатилувчи дастурий ёки дастурий-аппарат комплексидан иборат. VPN-сервер ташк,и тармокдарнинг рухсатсиз фойдаланишидан серверларни х,имоялашни х,амда алох,ида компьютерлар ва мое VPN-мах.сулотлари оркали х,имояланган локал тармок, сегментларидаги компьютерлар билан х,имояланган уланишларни ташкил этишни таъминлайди. VPN-сервер VPN-мижознинг сервер платформалари учун функционал аналог хисобланади. У аввало VPN-мижозлар билан купгина уланишларни мададловчи кенгайтирилган ресурелари билан ажралиб туради. VPN-сервер мобил фойдаланувчилар билан уланишларни хам мададлаши мумкин.

VPN хавфсизлик шлюзи. (Security gateway) иккита тармоккд уланувчи тармок, курилмаси булиб, узидан кейин жойлашган куп сонли хостлар учун шифрлаш ва аутентификациялаш вазифаларини бажаради. VPN хавфсизлиги шлюзи шундай жойлаштириладики, ички корпоратив тармоккд аталган барча трафик у оркали утади. VPN хавфсизлиги шлюзининг адреси кирувчи туннелланувчи пакетнинг ташки адреси сифатида курсатилади, пакетнинг ички адреси эса шлюз оркасидаги муайян хост адреси хисобланади. VPN хавфсизлиги шлюзи алохида дастурий ечим, алохида аппарат курилмаси, хамда VPN вазифалари билан тулдирилган маршрутизаторлар ёки тармоклараро экран куринишида амалга оширилиши мумкин.

Ахборот узатишнинг очик, ташки мухити маълумот узатишнинг тезкор каналларини (Internet мухити) ва алоканинг секин ишлайдиган умумфойдаланувчи каналларини (масалан, телефон тармога каналларини) уз ичига олади. Виртуал хусусий тармок, VPNHHHr самарадорлиги алоканинг очик, каналлари буйича айланувчи ахборотнинг химояланиш даражасига боглик,. Очик, тармок, орк,али маълумотларни хавфсиз узатиш учун инкапсуляциялаш ва туннеллаш кенг ишлатилади. Туннеллаш усули буйича маълумотлар пакети умумфойдаланувчи тармок, орк,али худди оддий икки нуктали уланиш буйича узатилганидек узатилади. Хар бир "жунатувчи-к,абул к,илувчи" жуфтлиги орасига бир протокол маълумотларини бошкасининг пакетига инкапсуляциялашга имкон берувчи узига хос туннел-мантикий уланиш урнатилади.

Туннеллашга биноан, узатилувчи маълумотлар порцияси хизматчи х,ошиялар билан бирга янги "конверт"га "жойлаш" амалга оширилади. Бунда пастрок, сатх, протоколи пакети юкррирок, ёки худи шундай сатх, протоколи пакети маълумотлари майдонига жойлаштирилади. Таъкидлаш лозимки, туннелашнинг узи маълумотларни рухсатсиз фойдаланишдан ёки бузишдан химояламайди, аммо туннеллаш туфайли инкапсуляцияланувчи дастлабки пакетларни тула криптографик химоялаш имконияти пайдо булади. Узатилувчи маълумотлар конфиденциаллигини таъминлаш мак,садида жунатувчи дастлабки пакетларни шифрлайди, уларни, янги IP-

сарлавхд билан ташки пакетга жойлайди ва транзит тармок, буйича жунатади (8.1-раем).

Очик, тармок, буйича маълумотларни ташишда ташки пакет сарлавхдеининг очик, каналларидан фойдаланилади.

Янги пакет

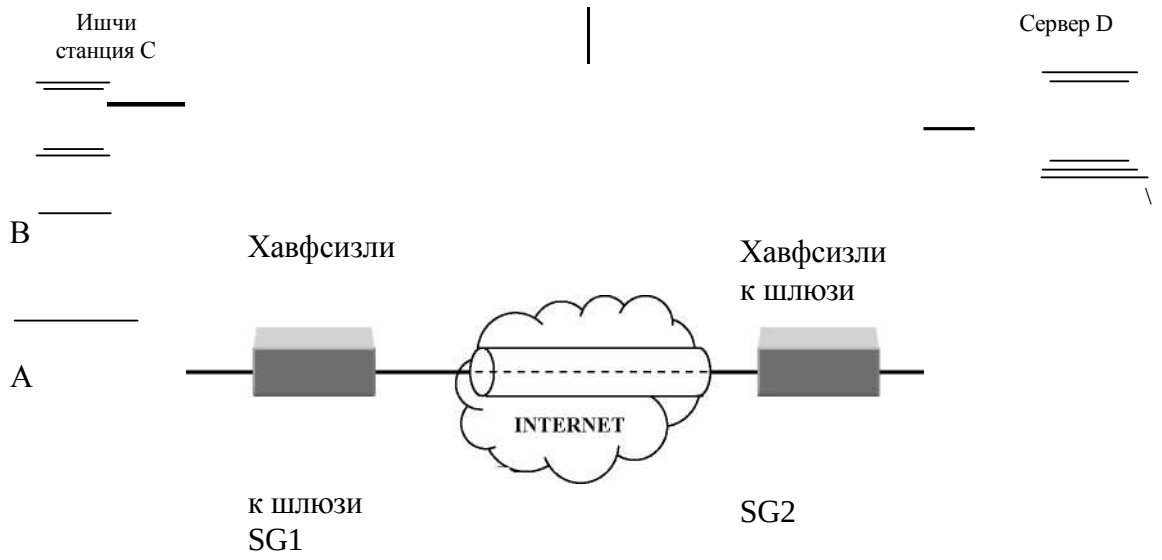
Янги IP-сарлав^а	АН - сарлав^а	ESP-сарлав^а	Дастлабки IP - сарлав^а	Маълумотлар

V

Дастлабки пакет

8.1-расм. Туннеллашга тайёрланган пакет мисоли

Ташки пакет химояланган каналнинг охирги нуктасига келиши билан ундан ички дастлабки пакет чикариб олиниб, расшифровка килинади ва унинг тикланган сарлавхаси ички тармок, буйича кейинги узатиш учун ишлатилади (8.2-расм)



8.2-расм. Виртуалъ щмояланган туннел схемаси.

Туннеллашдан пакет таркибини нафакат конфиденциаллигини, балки унинг яхлитлигини ва аутентилигини таъминлашда фойдаланилади. Бунда электрон ракамли имзони пакетнинг барча хршияларига тарк,атиш мумкин.

Internet билан богланмаган локал тармок, яратилганда компания узининг тармок, курилмалари ва компьютерлари учун хрхдаган 1Р-адресдан фойдаланиши мумкин. Олдин яккаланган тармокларни бирлаштиришда бу адреслар бир-бирлари ва Internets ишлатилаётган адреслар билан тукнашишлари мумкин. Пакетларни инкапсуляциялаш бу муаммони ечади, чунки у дастлабки адресларни беркитишга ва Internet IP адреслари маконидаги ноёб адресларни кушишта имкон беради. Бу адреслар кейин маълумотларни ажратилувчи тармокдар буйича узатишда ишлатилади. Бунга локал тармоккд уланувчи мобил фойдаланувчиларнинг IP-адресларини ва бошка параметрларини созлаш масаласи хам киради.

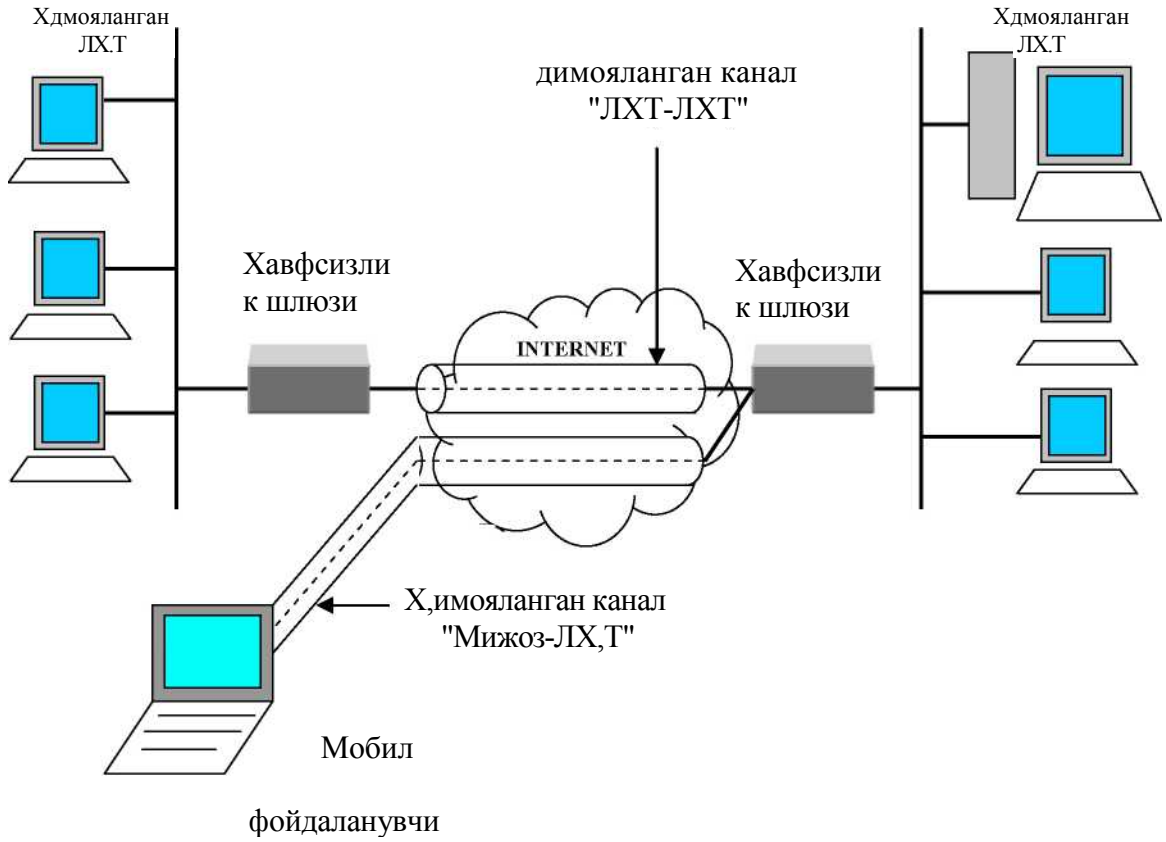
Тунеллаш механизми химояланувчи канални шакллантирувчи турли протоколларда кенг кулланилади. Одатда туннел факат маълумотларнинг конфиденциаллиги ва яхлитлигининг бузилиши хавфи мавжуд булган очик, тармок, кисмида, масалан, очик, Internet ва корпоратив тармок, кириш нукталари орасида, яратилади. Бунда ташки пакетлар учун ушбу икки нуктада урнатилган чегара маршрутизаторларининг адресларидан фойдаланилса, охирги узелларнинг ички адреслари ички дастлабки пакетларда химояланган хрлда сакланади. Таъкидлаш лозимки, тунеллаш механизмининг узи к,андай максадларда туннеллаш к,улланилаётганига боглик, эмас. Туннеллаш нафакат узатилаётган барча маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашда, балки турли протоколли (масалан IPv4 ва IPv6) тармокдар орасида утишни ташкил этишда хам кулланилади. Туннеллаш бир протокол пакетини бошка протоколдан фойдаланувчи мантикий мухитда узатишни ташкил этишга имкон беради. Натижада бир неча турли хил тармокдарнинг узаро алокалари муаммосини х,ал этиш имконияти пайдо булади.

Туннеллаш механизмини амалга оширилишига уч хил протоколлар: протокол-"йуловчи", протокол элтувчи ва туннеллаш протоколи ишлаши натижаси деб караш мумкин. Масалан, протокол - "йуловчи" сифатида битта корхона филиалларининг локал тармокдарида маълумотларни ташувчи транспорт протоколи IPX ишлатилиши мумкин. Элтувчи протоколнинг энг куп тарк,алган варианти Internet тармогининг IP протоколи

хдсобланади. Туннеллаш протоколи сифатида канал сатхи протоколари PPTP ва L2TP, хамда тармок, сатхи протоколи IPSec ишлатилиши мумкин. Туннеллаш туфайли Internet инфратузилмасини VPN-иловалардан беркитиш мумкин булади.

VPN туннеллари турли фойдаланувчилар учун яратилиши мумкин. булар хавфсизлик шлюзи булган *локал тармоқ* LAN ёки масофадаги ва мобил фойдаланувчиларнинг алохида компьютерлари булиши мумкин. Йирик корхонанинг виртуал хусусий тармогини яратиш учун VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар керак булади. VPN-шлюзларни корхона локал тармокларини химоялаш учун ишлатиш максадга мувофик, булса, VPN-серверлар ва VPN-мижозлардан масофадаги ва мобил фойдаланувчи-ларни Internet орк,али корпоратив тармок, билан химояланган уланишини ташкил этишда фойдаланилади.

Виртуал уимояланган каналларни цуриш еариантлари. VPN ни лойих,алашда одатда иккита асосий схема курилади (8.3-расм):



8.3-расм. "Л^Т-Л^Т" ва "Мижоз-Л^Т"хилидаги виртуал димояланган каналлар

- локал тармоклар орасидаги виртуал хдмояланган канал ("ЛХТ-ЛХТ" канал);

- узел ва локал тармок, орасидаги виртуал хдмояланган канал ("ми жоз-Л ХТ" канали).

Уланишнинг биринчи схемаси алохдда офислар орасидаги кимматли ажратилган линиялар урнига утади ва улар орасида доимо фойдаланувчан, х,имояланган каналларни яратади. Бу х,олда хавфсизлик шлюзи туннел ва локал тармок, орасида интерфейс вазифасини утайди ва локал тармок, фойдаланувчилари бир-бирлари билан мул окот килишда туннелдан фойдаланадилар. Аксарият компаниялар VPNHHHr бу хдлидан глобал тармокнинг мавжуд Frame Relay каби уланишларни алмаштириш учун ёки уларга кушимча сифатида фойдаланадилар.

VPN хдмояланган каналнинг иккинчи схемаси масофадаги ёки мобил фойдаланувчилар билан уланишни урнатишга аталган. Туннелни яратишни мижоз (масофадан фойдаланувчи) бошлаб беради. Масофадаги тармокни хдмояловчи шлюз билан богланиш учун у узининг компьютерида махсус мижоз дастурий таъминотини ишга туширади. VPNHHHr бу тури коммутацияланувчи уланишларни урнига утади ва масофадан фойдаланишнинг анъанавий усуллари билан бир каторда ишлатилиши мумкин.

Виртуал хдмояланган каналларнинг катор вариантлари мавжуд. Умуман, орасида виртуал хдмояланган канал шакллантирилувчи корпоратив тармокнинг х,ар к,андай иккита узели хдмояланувчи ахборот ок,имининг охирги ва оралик, нуктасига тааллукди булиши мумкин. Ахборот хавфсизлиги нуктаи назаридан х,имояланган туннел охирги нукталарининг х,имояланувчи ахборот ок,имининг охирги нукталарига мое келиши варианти маъкул х,исобланади. Бу х,олда каналнинг ахборот пакетлари утишининг барча йуллари буйлаб х,имояланиши таъминланади. Аммо бу вариант бошкаришнинг децентрализацияланишига ва ресурс сарфининг ошишига олиб келади. Агар виртуал тармокдаги локал тармок, ичида трафикни х,имоялаш талаб этилмаса, х,имояланган туннелнинг охирги нуктаси сифатида ушбу локал тармокнинг тармоклараро экрани ёки чегара маршрутизатори танланиши мумкин. Агар локал тармок, ичидаги ахборот окими

химояланиши шарт булса, бу тармок, охирги нуктаси вазифасини химояланган алокада иштирок этувчи компьютер бажаради.

Локал тармокдан масофадан фойдаланилганида фойдаланувчи компьютери виртуал химояланган каналнинг охирги нуктаси булиши шарт. Факат пакетларни коммутациялашли очик, тармок,, масалан Internet ичида утказилувчи химояланган туннел варианти етарлича кенг таркалган. Ушбу вариант ишлатилиши кулайлиги билан ажралиб турсада, нисбатан паст хавфсизликка эга. Бундай туннелнинг охирги нукталари вазифасини одатда Internet провайдерлари ёки локал тармок, чегара маршрутизаторлари (тармокдараро экранлар) бажаради.

Локал тармокдар бирлаштирилганида туннел факат InternetHHHr чегара провайдерлари ёки локал тармокнинг маршрутизаторлари (тармокдараро экранлари) орасида шакллантирилади. Локал тармокдан масофадан фойдаланилганида туннел Internet провайдерининг масофадан фойдаланиш сервери, хамда InternetHHHr чегара провайдери ёки локал тармок, маршрутизатори (тармокдараро экран) орасида яратилади. Ушбу вариант буйича курилган корпоратив тармокдар яхши масштабланувчанлик ва бошкарилувчанликка эга булади. Шакллантирилган х,имояланган туннеллар ушбу виртуал тармокдаги мижоз компьютерлари ва серверлари учун тула шаффоф хисобланади. Ушбу узелларнинг дастурий таъминоти узгармайди. Аммо бу вариант ахборот алокасининг нисбатан паст хавфсизлиги билан характерланади, чунки трафик кисман очик, алок,а канали буйича химояланмаган х,олда утади. Агар шундай VPNнн яратиш ва эксплуатация к,илишни провайдер ISP уз зиммасига олса, барча виртуал хусусий тармок, унинг шлюзларида, локал тармокдар ва корхоналарнинг масофадаги фойдаланувчилари учун шаффоф хрлда к,урилиши мумкин. Аммо бу хрлда провайдерга ишонч ва унинг хизматига доимо тулаш муаммоси пайдо булди.

Химояланган туннел, орасида туннел шакллантирилувчи узеллардаги виртуал тармок, компонентлари ёрдамида яратилади. Бу компонентларни туннел инициаторлари ва туннел терминаторлари деб юритиш кабул килинган.

Туннел инициаторы дастлабки пакетни янги пакетга жунатувчи ва кабул килувчи хусусидаги ахбороти булган янги сарлавх,али пакетга инкапсуляциялайди. Инкапсуляцияланган пакетлар хар кандай протокол турига, жумладан маршрутланмайдиган протоколларга (масалан Net BEUL) мансуб булишлари мумкин. Туннел буйича узатиладиган барча пакетлар IP пакетлари хисобланади. Туннелнинг инициатори ва терминатори орасидаги маршрутни одатда, InternetflaH фаркданиши мумкин булган, оддий маршрутланувчи тармок, IP аникдайди.

Туннелни инициаллаш ва узиш турли тармок, курилмалари ва дастурий таъминот ёрдамида амалга оширилиши мумкин. Масалан, туннел масофадан фойдаланиш учун улашни таъминловчи модем ва мое дастурий таъминот билан жихрзланган мобил фойдаланувчининг ноутбуки томонидан инициалланиши мумкин. Инициатор вазифасини мое функционал имкониятларга эга булган локал тармок, маршрутизатори хам бажариши мумкин. Туннел одатда, тармок, коммутатори ёки хизматлар провайдери шлюзи билан тугалланади.

Туннел терминатори инкасуляциялаш жараёнига тескари жараённи бажаради. Терминатор янги янги сарлавх,аларни олиб ташлаб, хар бир дастлабки пакетни локал тармокдаги адресатга йуллайди.

Инкапсулацияланувчи пакетларнинг конфиденциаллиги уларни шифрлаш, яхлитлиги ва хакикийлиги эса электрон ракамли имзони шакллантириш йули билан таъминланади. Маълумотларни криптографик химоялашнинг жуда куп усуллари ва алгоритмлари мавжуд булганлиги сабабли, туннел инициатори ва терминатори химоянинг бир хил усулларидан фойдаланишга уз вактида келишиб олишлари максадга мувофик, х,исобланади. Маълумотларни расшифровка килиш ва рак,амли имзони текшириш имкониятини таъминлаш учун туннел инициатор ива терминатори калитларни хавфеиз алмашиш вазифасини х,ам мададлашлари зарур. Ундан ташк,ари, VPN туннеларини ваколатли фойдаланувчилар томонидан яратилишини кафолатлаш максадида ахборот алок,асининг асосий тарафлари аутентификациялашдан утишлари лозим. Корпорациянинг мавжуд

тармок, инфратузилмалари УР1Чдан фойдаланишга хам дастурий, хам аппарат таъминот ёрдамида тайёрланишлари мумкин.

8.2. Хдмояланган виртуал хусусий тармоцларнинг туркумланиши

Химояланган виртуал хусусий тармокдар VPNнн туркумлашни турли вариантлари мавжуд. Купинча туркумлашнинг куйидаги учта аломати ишлатилади:

- OSI моделининг иш сатхи;
- VPN техник ечимининг архитектураси;
- VPNнн техник амалга ошириш усули.

OSI моделининг иш сатуи буйича VPNнинг туркумланиши. Ушбу туркумлаш анчагина кизикиш тугдиради, чунки амалга оширилувчи VPNннне функционаллиги ва унинг корпоратив ахборот тизимлари иловалари хамда химоянинг бошка воситалари билан биргаликда ишлатилиши куп хрлларда танланган OSI сатхига боглик, булади.

OSI моделининг иш сатх, аломати буйича канал сатхддаги VPN, тармок, сатх,идаги VPN ва сеанс сатхидаги VPN фаркланади. Демак, УРМлар одатда OSI моделининг пастки сатхдарида к,урилади. Бунинг сабаби шуки, х,имояланган канал воситалари канчалик пастки сатхда амалга оширилса, уларни иловаларга ва татбик,ий протоколларга шунчалик шаффоф к,илиш соддалашади. Тармок, ва канал сатхдарида иловаларнинг х,имоя протоколларига богликдиги умуман йукрлади. Шу сабабли, фойдаланувчилар учун универсал ва шаффоф х,имояни факат OSI моделининг пастки сатхдарида куриш мумкин. Аммо, бунда биз бошка муаммога-х,имоя протоколининг муайян тармок, технологиясига богликдиги муаммосига дуч келамиз.

Каналъ сатхидаги VPN. OSI моделининг канал сатх,ида ишлатилувчи VPN воситалари учинчи (ва юкррирок) сатхнинг турли хил трафигини инкапсулациялашни таъминлашга ва "нукта-нукта" тилидаги виртуал туннелларни (маршрутизатордан маршрутизаторга ёки шахсий компьтердан локал х,исоблаш тармогининг шлюзигача) куришга имкон беради. Бу гурухга L2F

(Layer 2 Forwarding) ва PPTP (Point-to-Point Tunneling Protocol) протоколлари хдмда Cisco Systems и MicroSoft фирмаларининг бирга ишлаб чикдан L2TP(Layer 2 Tunneling Protocol) стандартидан фойдаланувчи VPN-махсулотлар тааллукди.

Хдмояланган каналнинг протоколи PPTP "нукта-нукта" уланишларида, масалан, ажратилган линияларда ишлаганда кенг кулланилувчи PPP протоколига асосланган. PPTP протоколи иловалари ва татбикдй сатх, хизматлари учун хдмоя воситаларининг шаффофлигини таъминлайди ва тармок, сатхдда ишлатилувчи протоколга боглик, эмас. Хусусан, PPTP протоколи хам IP тармокдарида, хам IPX, DECnet ёки NetBEUL протоколлари асосида ишловчи тармокдарда пакетларни ташиши мумкин. Аммо, PPP протоколи хдмма тармокдарда хам ишлатилмаслиги сабабли (аксарият локал тармокдарида канал сатхдда Ethernet протоколи ишласа, глобал тармокдарда ATM, Frame Relay тармокдари ишлайди), уни универсал восита деб беулмайди. Йирик бирикма тармокнинг турли кисмларида, умуман айтганда, турли канал протоколлари ишлатилади. Шу сабабли бу гетероген мухдт оркали канал сатхднинг ягона протоколи ёрдамида хдмояланган каналнн утказиш мумкин эмас.

L2TP протоколи, эхтимол, локал хдсоблаш тармокдаридан фойдаланишни ташкил этишда устунлик к,илувчи ечим булиб крлиши мумкин (чунки у, асосан, Windows операцион тизимига таянади.)

Тармоц сатщдаги VPN. Тармок, сатх,идаги УР1Ч-мах,сулотлар 1Рни IPra инкапсуляциялашни бажаради. Бу сатхдаги кенг тарк,алган протоколлардан бири SKIP протоколидир. Аммо бу протоколни аутентификациялаш, туннеллаш ва IP-пакетларни шифрлаш учун аталган IPSec(IPSecurity) протоколи аста-секин суриб чикармокда.

Тармок, сатхдда ишловчи IPSec протоколи муросага асосланган вариант х,исобланади. Бир томондан у иловадар учун шаффоф, иккинчи томондан кенг таркалган IP протоколига асосланганлиги сабабли барча тармокдарда ишлаши мумкин. Шу орада эсдан чикармаслик лозимки, IPSecHHHr спецификацияси IPra мулжалланганлиги сабабли у тармок, сатхднинг бошка протоколлари трафиги учун тугри келмайди. IPSec прото-

коли L2TP протоколи билан биргаликда ишлаши мумкин. Натижада бу икки протокол ишончли идентификациялашни, стандартланган шифрлашни ва маълумотлар яхлитлигини таъминлайди. Иккита локал тармок, орасидаги 1P8естуннели маълумотлар узатувчи якка тармоклар тупламини мададлаши мумкин. Натижада бу хилдаги иловалар масштабланиш нуктаи назаридан иккинчи сатх, технологияларига нисбатан устунликка эга булади.

IPSec протоколи билан масофадаги курилмалар орасида криптографик калитларни хавфсиз бошкариш ва алмашиш масалаларини ечувчи IKE (Internet Key Exchange) протоколи богланган. IKE протоколи калитларни алмашишни автоматлаштиради ва химояланган уланишни уранатади, IPSec эса пакетларни кодлайди ва "имзо чекади". Ундан ташкари, IKE урнатилган уланиш учун калитни узгартириш имкониятига эга. Бу узатилувчи ахборотнинг конфиденциаллигини оширади.

Сеанс сстцидаги VPN. Баъзи VPNnap "канал воситачилари" (circuit proxy) деб аталувчи усулдан фойдаланади. Бу усул транспорт сатхи устида ишлайди ва хар бир сокет учун алохида трафикни химояланган тармокдан умумфойданувчи Internet тармогига ретрансляциялайди. (IP сокети TCP-уланишнинг ва муайян порт ёки берилган порт UDP комбинацияси оркали идентификацияланади. TCP/IP стекида бешинчи-сеанс сатхи булмайди, аммо сокетларга мулжалланган амалларни купинча сеанс сатх,и амаллари деб юритишади.)

Туннелнинг инициатори ва терминатори орасида узатилувчи ахборотни шифрлаш транспорт сатхи TLS(Transport Layer Security) ёрдамида амалга оширилади. Тармокдарарo экран орк,али аутентификацияланган у^{тишни} стандартлаш учун SOCKS деб аталувчи протокол аникланган ва хрзирда SOCKS протоколининг 5-версияси канал воситачиларини стандарт амалга оширилишида ишлатилади.

SOCKS протоколининг 5-версиясида мижоз компьютери воситачи (proxy) вазифаларини бажарувчи сервер билан аутентифкацияланган сокет (ёки сеанс) ур^{ната}ди- Бу воситачи-тармокдарарo экран оркали богланишнинг ягона усули. Воситачи, у^{3} навбатида, мижоз томонидан суралган х,ар к,андай амални бажаради. Воситачига сокет сатхидаги трафик

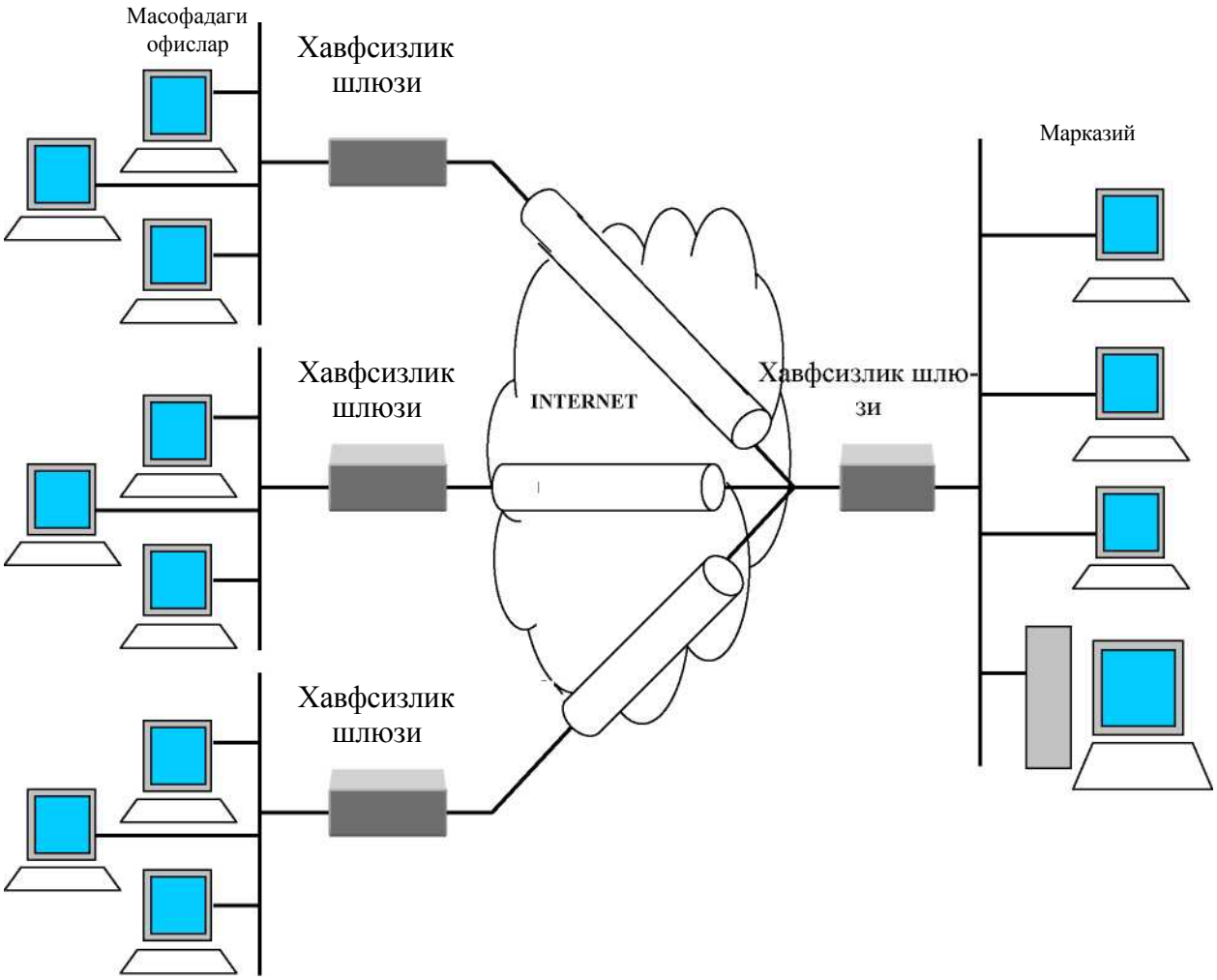
маълумлиги сабабли, у синчиклаб назорат килиши, масалан, муайян иловаларни, агар улар зарурий ваколатларга эга булмаса, блокировка килиши мумкин.

Агар IPSec протоколи мох,ияти буйича, IP тармокни химояланган туннелга таркатса, SOCKS протоколи асосидаги махсулотлар уни алохдда хар бир илова ва хар бир сокетга кенгайтиради. Иккинчи ва учинчи сатхнинг яратилган туннеллари иккала йуналишда бирдай ишласа, 5 сатхнинг VPN тармоги хар бир йуналишда узатишни мустакил бошкаришта рухсат беради. IPSec протоколга ва иккинчи сатх, протоколларига ухшаб 5 сатхнинг VPN тармогини виртуал хусусий тармокдарнинг бошка турлари билан бирга ишлатилиши мумкин, чунки бу технологиялар бир-бирини инкор килмайди.

Техник ечимининг архитектураси буйича VPNHUHZ туркумланиши. Ушбу туркумлаш буйича виртуал хусусий тармоклар куйидаги уч турга булинади:

- корпорация ичидаги VPN тармок,;
- масофадан фойдаланилувчи VPN тармок,;
- корпорацияларо VPN тармок,.

Корпорация ичидаги VPN тармоц. Корпорация ичидаги **VPN** тармоклар (Intranet VPN) корхона ичидаги булинмалар ёки алоканинг корпорация тармоклари (шу жумладан, ажратилган линиялар) ёрдамида бирлаштирилган корхоналар гурух,и орасида х,имояланган алок,ани ташкил этиш учун ишлатилади. Узининг филиаллари ва булимлари учун ахборотнинг марказлаштирилган омборидан фойдаланишга эх,тиёж сезган компаниялар масофадаги узелларни ажратилган линиялар ёки frame relay технологияси ёрдамида улайдилар. Аммо ажратилган линияларнинг ишлатилиши эгалланадиган утказиш полосасининг ва объектлар орасидаги масофанинг катталашгани сари жорий сарф-харажатларнинг ошишига сабаб булади. Буларни камайтириш учун компания узелларини виртуал хусусий тармок, ёрдамида улаши мумкин (8.4-расм).



8.4-расм. VPN intranet технологияси ёрдамида тармоқ узелларини улаш.

Intranet VPN тармокдар Шегпегдан ёки сервис-провайдерлар томонидан такдим этилувчи булинувчи тармок, инфратузилмаларидан фойдаланган хрлда курилади. Компания нархи кдммат ажратилган линиялардан воз кечиб, уларни арзонрок, Internet оркдпи алокд билан алмаштиради. Бу утказиш полосасидан фойдаланишдаги сарф-х,аражатни жиддий камайтиради, чунки Internetfla масофа уланиш нархига х,еч таъсир этмайди.

Intranet VPN учун куйидаги афзалликлар характерли:

- конфиденциал ахборотни химоялаш учун шифрлашнинг кучли криптографик протоколларидан фойдаланиш;

- автоматлаштирилган савдо тизими ва маълумотлар базасини бошк,ариш тизими каби жиддий иловаларни бажаришда ишлашининг ишончлилиги;

- сони тез усаётган фойдаланувчилар, янги офислар ва янги дастурий иловаларни самаралирок, жойлаштириш учун бошкаришнинг мослашувчанлиги.

InternetflaH фойдаланиб Intranet VPNнн куриш VPN-технологияни амалга оширувчи энг рентабел усули хдсобланади. Аммо Internets сервис даражаси умуман кафолатланмайди. Кафолатланган сервис даражасини хрхдовчи компаниялар узларининг VPNnapHHH сервер-провайдерлари томонидан такдим этилувчи булинувчи тармок, инфтузилмаларидан фойдаланиб сафлаш имкониятларини куришлари шарт.

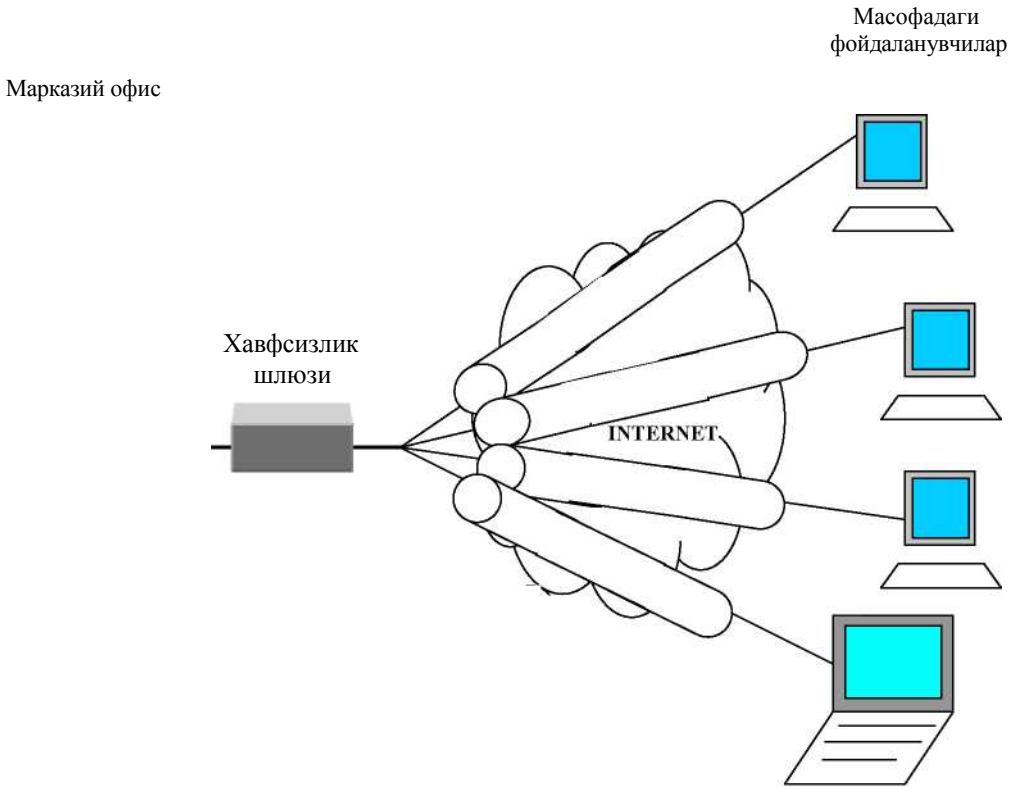
Масофадан фойдаланилувчи VPN тармоц. Масофадан фойдаланилувчи виртуал хусусий тармокдар VPN (Remote Access VPN) корпорациянинг мобил ёки масофадаги ходимларига (компания рахбарияти, мехнат сафаридаги ходимлар, касаначилар ва х,.) корхона ахборот ресурсларидан химояланган масофадан фойдаланишни таъминлайди.

Масофадан фойдаланувчи виртуал хусусий тармокдарнинг (8.5-расм) коммутацияланувчи ва ажратилган линиялардан фойдаланишнинг хар ойдаги сарф-х,аражатларини анчагина камайтиришга имкон бериши, уларнинг умумий эътироф этилишига сабаб булди. Уларнинг ишлаш принципи оддий: фойдаланувчилар глобал тармокдан фойдаланишнинг мах,аллий нуктаси билан уланишларни урнатади. Сунгра уларнинг суровлари Internet орк,али туннелланади. Бу шахарлараро ва халк,аро алок,а учун туловдан к,утилишга имкон беради. Ундан кейин барча суровлар мое узелларда тупланади ва корпорация тармокдарига узатилади.

Хусусий бошк,арилувчи тармокдардан (dial networks) масофадан фойдаланилувчи VPN тармокдарга (Remote Acces VPN) утиш куйидаги афзалликларни беради:

- шахарлараро номерлар урнига мах,аллий номерлардан фойдаланиш имконияти шах,арлараро телекоммуникацияга сарф-х,аражатларни анчагина камайтиради;

- аутентификациялаш жараёнини ишончли утказишни таъминловчи масофадаги ва мобил фойдаланувчилар хакикийлигини аникдаш тизимининг самарадорлиги;



7.5-расм. Масофадан фойдаланишли виртуаль хусусий тармоқ.

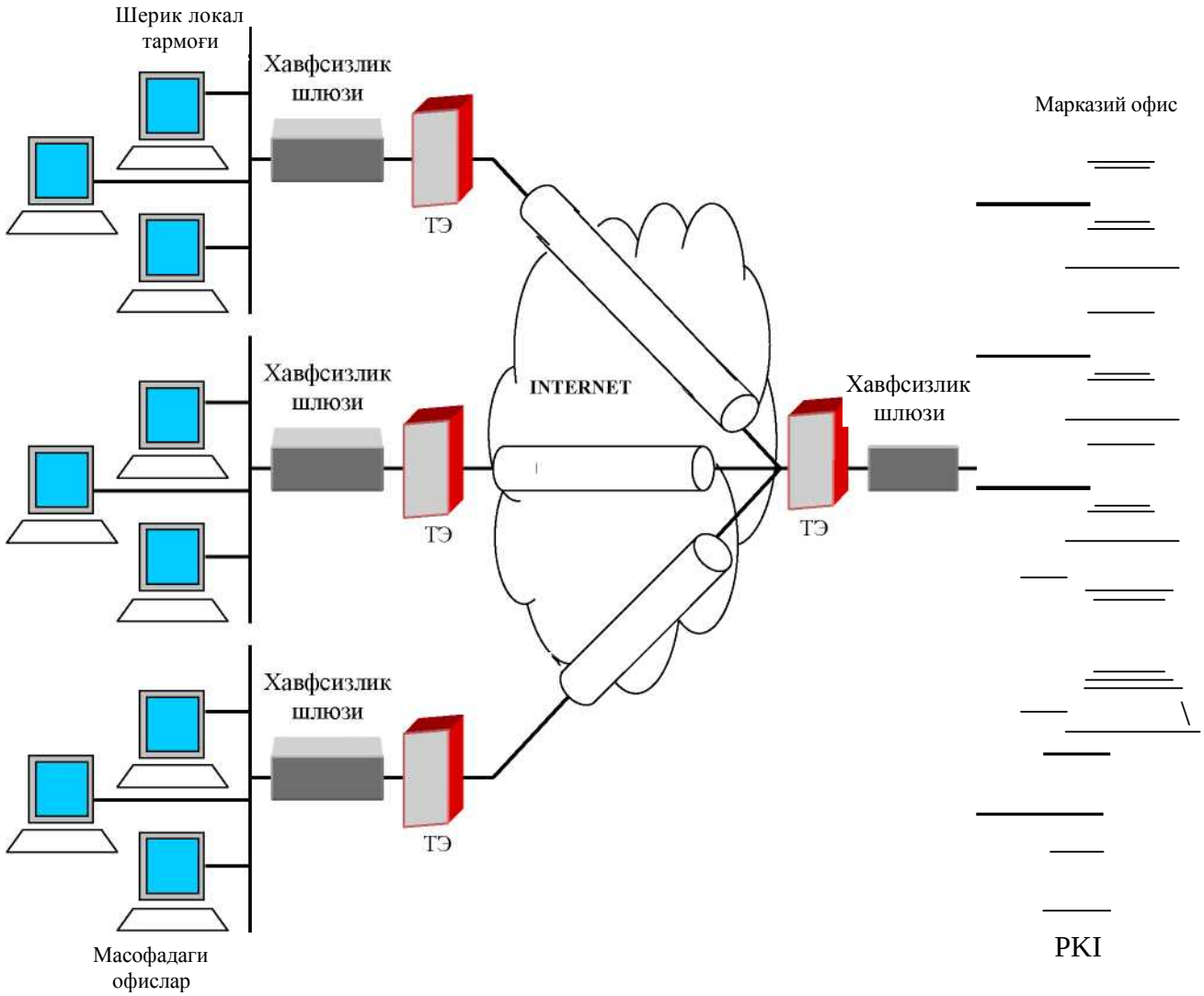
- масштабланишнинг янада юкррилиги ва тармоккд кушилувчи янги фойдаланувчилар сафланишининг оддийлиги;

- компания эътиборини тармок, ишлаши муаммолари урнига асосий корпорация бизнес-максадларига каратиш.

Таъкидлаш лозимки, сезувчан корпорация трафигини ташишда очик, тармок, InternetHHHr бирлаштирувчи магистрал сифатида ишлатилишининг масштаби ошиб бормокда. Бу ахборот химояси механизмини ушбу технологиянинг энг мухим элементига айлантиради.

Корпорацияларапо VPN тармоц. Корпорацияларапо VPN тармокдардан (Extranet VPN) бизнес буйича стратегик шериклар, хусусан чет эл асосий таъминотчилар, йирик буюртмачилар, мижозлар ва х,. билан самарали алокани ва ахборотни х,имояланган алмашинувини ташкил этишда фойдаланилади (8.6-расм).

Extranet - бир компания тармогидан иккинчи компания тармоганинг тугридан-тугри фойдаланишини таъминлаш орк,али иш юзасидан х,амкорлик жараёнида алок,а ишончлилигини оширишга имкон берувчи технологиядир.



8. 6-расм. Корпорацияларараро extranet VPN' тармоғи.

Extranet VPN тармоклари умуман корпорация ичидаги виртуал хусусий тармокдарга ухшаш, фарки шундаки, корпорацияларараро виртуал хусусий тармоклар учун ахборот химояси муаммоси кескинрокдир. Extranet VPN учун ишбилармон шериклар узларининг тармокдарида куллашлари мумкин булган турли VPN-ечимлар билан алока к,илиш имкониятларини кафолатловчи стандартлаштирилган VPN-махсулотлардан фойдаланиш характерлидир.

Бир неча компаниялар бирга ишлашга келишиб, бир-бирларига тармокларини очишганида, улар янги шерикларининг фак,ат маълум ахборотдан фойдаланишларига йул куйишлари лозим. Бунда конфиденциал ахборот рухсатсиз фойдаланишдан ишончли х,имояланиши зарур. Айнан, шу сабабли корпорацияларараро тармокларда очик, тармок, томонидан

тармокларарo экран (брандмауэр) ёрдамида назоратга катта ахамият берилади. Ахборотдан хакикий фойдаланувчининг фойдаланишини кафолатловчи аутентификациялаш хам мухим хисобланади. Шу билан бир каторда рухсатсиз фойдаланишдан химоялашнинг сафланган тизими узига эътиборни жал б килмаслиги шарт.

Extranet VPN уланишлари intranet VPN ва remote access VPN лар амалга оширилишидаги ишлатилган архитектура ва протоколлардан фойдаланиб сафланади. Асосий фарк, шундан иборатки, extranet VPN фойдаланувчиларига бериладиган фойдаланишга рухсат улар шеригининг тармоги билан боглик,.

Баъзида VPN тармоганинг локал варианти (Localnet VPN) алохдда гурухга ажратилади. Localnet VPN локал тармоги компания локал тармоги ичида (одатда, марказий офис) айланувчи ахборотлар окимидан компаниядан ишловчи "ортикча кизикувчи" ходимларнинг рухсатсиз фойдаланишидан химоялашни таъминлайди. Таъкидлаш лозимки, хрзирда VPNнн амалга оширувчи турли усулларнинг конвергенцияси гояси кузга ташланмокда.

Техник амалга ошириш буйича VPNнинг туркумланиши. **Виртуал** хусусий тармок,нинг конфигурацияси ва характеристикалари куп жихатдан ишлатиладиган VPN-к.урилмаларининг турига боглик,.

Техник амалга ошириш буйича VPNHHHr к,уйидаги гурухдари фаркданади:

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

Маршрутизаторлар асосидаги VPN. VPN куришнинг ушбу усулига биноан химояланган каналларни яратишда маршрутизаторлардан фойдаланилади. Локал тармокдан чик,увчи барча ахборот маршрутизатор оркали утганлиги сабабли, унга шифрлаш вазифасини юклаш табиий. Маршрутизатор асосидаги VPN асбоб-ускуналарига мисол тарикасида Cisco-Systems компаниясининг к,урилмаларини курсатиш мумкин.

Тармоцлараро экранлар асосидаги VPN. Аксарият ишлаб чикарувчиларнинг тармоклараро экрани туннеллаш ва маълумотларни шифрлаш вазифаларини мададлайди. Тармоклараро экранлар асосидаги ечимга мисол тарикасида Check Point Software Technologies компаниясининг Fire Wall-1 махсулотини курсатиш мумкин. Шахсий компьютер асосидаги тармоклараро экранлар факат узатилувчи ахборот хажми нисбатан кичик булган тармокларда кулланилади. Ушбу усулнинг камчилиги бита ишчи урнига хисобланганда ечим нархининг юкррилиги ва унумдорликнинг тармокдараро экран ишлайдиган аппарат таъминотига богликдиги.

Даспгурий таъминопг асосидаги VPN. Дастурий усул буйича амалга оширилган VPN махсулотлар унумдорлик нуктаи назаридан ихтисослаштирилган курилмадан крлишсада, VPN-тармокдарни амалга оширилишида етарли к,увватга эга. Таъкидлаш лозимки, масофадан фойдаланишда зарурий утказиш полосасига талаблар катта эмас. Шу сабабли, дастурий махсулотларнинг узи масофадан фойдаланиш учун етарли унумдорликни таъминлайди. Дастурий махсулотларнинг шубхдсиз афзаллиги-к,улланилишининг мосланувчанлиги ва к,улайлиги, х,амда нархининг нисбатан юкрри эмаслиги.

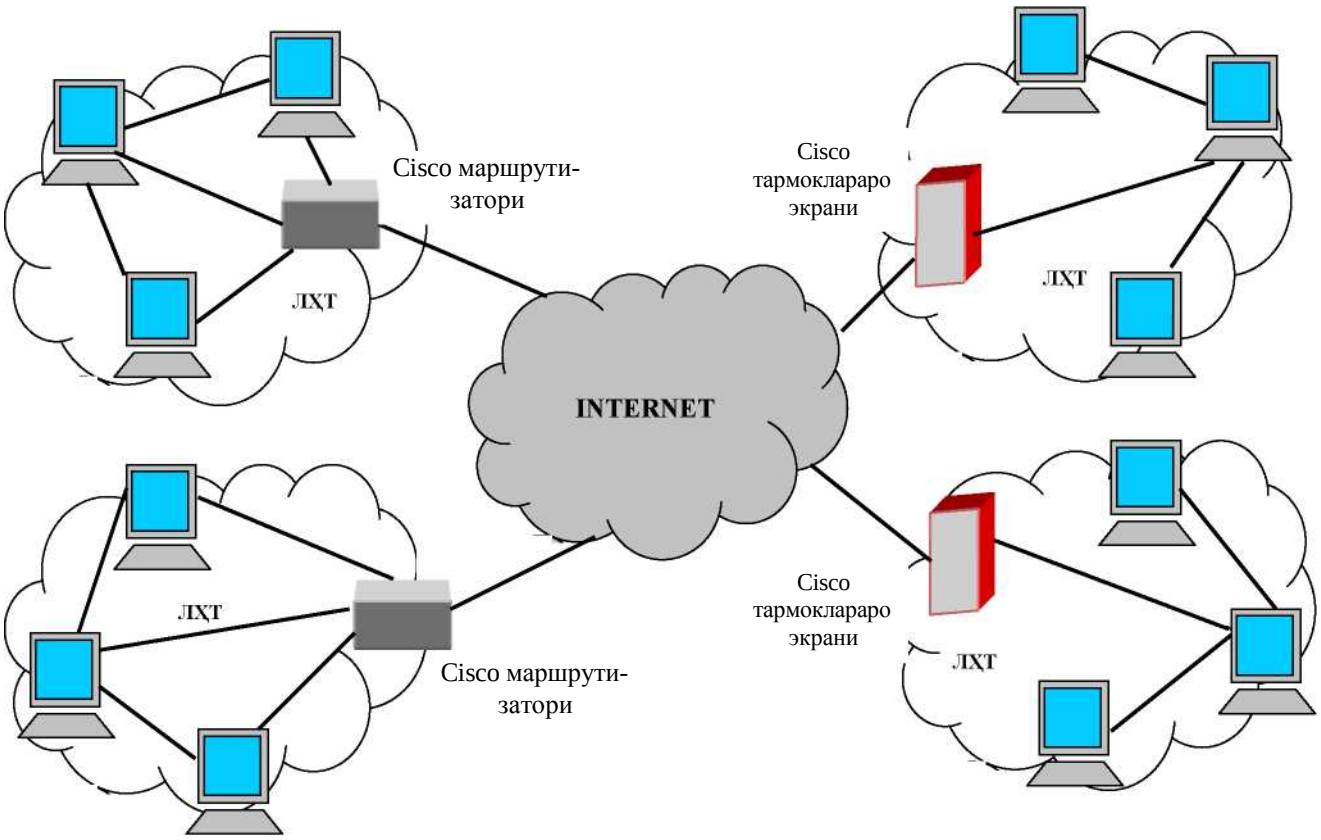
Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат воситалари асосидаги УРМларнинг энг мухим афзаллиги унумдорлигининг юкррилигидир. Ихтисослаштирилган VPN тизимларда шифрлашнинг микросхемаларда амалга оширилиши тезкорликнинг таъминланишига сабаб булади. Ихтисослаштирилган УРМ-к,урилмалар хавфсизликнинг юк,ори даражасини таъминлайди, аммо уларнинг нархи анчагина юкрри.

8.3. Х,имояланган корпоратив тармо^ларни куриш учун VPN ечимлар

Маршрутизаторлар асосидаги VPN. Ташки дунё билан локал тармок, алмашадиган барча ахборот машрутизатор оркали утади. Бу маршрутизаторларни чикувчи пакетларни шифрловчи ва кирувчи пакетларни расшифровка килувчи табиий платформага айлантиради. Бошк,ача айтганда,

маршрутизатор, умуман, маршрутлаш вазифасини VPN вазифасини мададлаш билан бирга олиб бориши мумкин. Бундай ечим узининг афзалликлари ва камчиликларига эга. Афзаллиги - маршрутлаш ва VPN вазифаларини биргаликда маъмурлаш кулайлигидир. Корхона тармоклараро экранни ишлатмасдан корпоратив тармок, химоясини факат хам тармокдан фойдаланиш буйича, хам узатиладиган трафикни шифрлаш буйича химоялаш вазифаларини биргаликда х,ал этувчи маршрутизатор ёрдамида ташкил этган хрлларда машрутизаторларни VPNнн мададлашда ишлатилиши айникса фойдалидур. Ушбу ечимнинг камчилиги маршрутлаш буйича асосий амалларнинг трафикни куп мехдат сарфини талаб этувчи шифрлаш ва аутентификациялаш амаллари билан бирга олиб борилиши натижасида маршрутизатор унумдорлигига куйиладиган талабларнинг ошиши билан боглик,. Маршрутизаторларнинг унумдорлигини оширишга шифрлаш вазифаларини аппарат мададлаш оркали эришилади. Хрзирда барча маршрутизатор ва бошка тармок, курилмаларини етакчи ишлаб чикарувчилар узларининг махсулотларида турли VPN-протоколларини мададлайдилар. Бу сохада Cisco Systems ва 3Com компаниялари лидер хдсобланадилар. Cisco Systems компанияси узлари ишлаб чиккдн маршрутизаторларга энг кенг тарк,алган стандартлар асосида УРМларни к,уришга имкон берувчи канал сатх,и протоколини мададловчи IOS 11.3(Internetwork Operation System 11.3) ва тармок, сатхи протоколи IPSecHH киритди. L2F протоколи аввалрок, IOS операцион тизимнинг компонентига айланди ва Cisco ишлаб чикарадиган барча тармоклараро алок,а ва масофадан фойдаланиш курилмаларида мададланади. Cisco маршрутизиторларида VPN вазифалари бутунлай дастурий йул билан ёки шифрлаш сопроцессори булган махсус кенгайтириш платасидан фойдаланилган х,олда амалга оширилиши мумкин. Охирги вариант VPN амалларида маршрутизатор унумдорлигини анчагина оширади. Cisco Systems компанияси томонидан ишлаб чикилган VPN к,уриш технологияси юкрри унумдорлиги ва мосланувчанлиги билан ажралиб туради. Унда "тоза" ёки инкапсуляция килинган куринишда узатилувчи х,ар кандай 1Р-ок,им учун шифрлаш билан туннеллаш таъминланади. Cisco компаниясининг маршрутизаторлари асосида VPN-каналларини куриш операционтизимининг

воситалари ёрдамида Cisco IOS 12.x. версиясидан бошлаб амалга оширилади. Агар мазкур операцион тизим компаниянинг бошка булимларидаги Cisco чегара маршрутизаторларида урнатилган булса, бир маршрутизатордан иккинчисига "нукта-нукта" туридаги виртуал химояланган туннеллар мажмуасидан иборат булган корпоратив VPN тармокни шакллантириш имконияти булади (8.7-расм).



8.7-расм. Cisco маршрутизаторлари асосида корпоратив VPN тармоғини куришнинг намунавий схемаси.

Маршрутизаторлар асосида УР1Чларни куришда эсда тутиш лозимки, бундай ёндашишнинг узи компаниянинг умумий ахборот хавфеизлигини таъминлаш муаммосини х,ал этмайди, чунки барча ички ахборот ресурелар барибир ташкаридан хужум килиш учун очик, к,олади. Бу ресуреларни химоялаш учун, одатда, чегара маршрутизаторларидан кейин жойлашган тармокдарарo экранлардан фойдаланилади.

Cisco 1720 VPN Access Router маршрутизатори катта булмаган ва уртача корхоналарда химояланган фойдаланишини ташкил этишга аталган.

Бу маршрутизатор Internet ва интратармоклардан фойдаланишни ташкил этишга зарур булган имкониятларни таъминлайди ва Cisco IOS дастурий таъминот асосидаги виртуал хусусий тармокларни ташкил этиш вазифаларини мададлайди. Cisco IOS операцион тизими маълумотларни химоялаш, хизмат сифатини бошкариш ва юкрри ишончилиликни таъминлаш буйича VPN вазифаларининг жуда кенг тупламини таъминлайди.

Cisco 1720 маршрутизатори маълумотлар химоясининг куйидаги вазифаларини бажаради:

- *тармоцлараро экранлаш.* Cisco IOS Firewall компонента локал тармокларни хужумлардан химоялайди. *Фойдаланишнинг контекстли назорати* CBAC (Context-based access control) функцияси маълумотларни дина мик ёки холатларга асосланган, иловалар буйича дифференциалланган фильтрлашни бажаради. Бу функция самарали тармокдарараро экранлаш учун жуда мухим хисобланади. Cisco IOS Firewall компонента катор бошка фойдали вазифаларни хам, хусусан, "хизмат килишдан воз кечиш" каби хужумларни аникдаш ва олдини олиш, JavaHH блокировка этиш, аудит ва вактнинг реал масштабида огохдантиришларни таркатиш вазифаларини ба жаради.

- *шифрлаш.* IPSec протоколидаги DES ва Triple DES шифрлаш алгоритмларини мададлаш маълумотларни конфиденциаллиги ва яхлитлигини ва маълумотлар манбаини аутентификациялашни (маълумотлар глобал тармокдан утганидан сунг) таъминлаш максадида ишончли ва стандарт шифрлайди.

- *туннеллаш.* Туннеллашнинг IPSec, GRE (Generic Routing Encapsula tion), L2F ва L2TP стандартлари ишлатилади. L2F ва L2TP стандартлари масофадаги фойдаланувчиларнинг корхона локал тармогида урнатилган Cis co 1720 маршрутизаторгача виртуал туннел утказганларида ишлатилади. Бундай к,улланишда корхонада масофадан фойдаланиш серверига эх,тиёж колмайди ва шах,ларарараро ёки халк,аро кунгироклар учун тулови тежалади.

- *цурилмаларни аутентификациялаш ва калитларни бошцариш.* IPSec катта тармокларда маълумотлар ва курилмаларни масштабланувчи аутенти фикациялашни таъминловчи калитларни бошкариш протоколи IKE,

ракамли сертификатлар X.509 версия 3, сертификатларни бошкарувчи протокол CEP, хдмда Verisign ва Entrust компания сертификат серверлари мададланади.

- *VPNнинг мижоз дастурий таъминоти.* IPSec ва L2TP протоколларининг стандарт версиялари билан ишловчи харкандай мижоз Cisco ЮБбилан узаро ал ока к,илиши мумкин.

- *фойдаланувчиларни аутентификациялаш.* Бунинг учун PAP, CHAP протокллари, TACACS"[1]" ва RADIUS тизимлари, фойдаланиш токенлари каби воситалардан фойдаланилида.

Виртуал хдмояланган тармокдар нафакат маълумотларни химоялаш, балки хдмоялашнинг юкрри савияси QoSнн (Quality of Service) таъминлаши лозим. Cisco 1720 маршрутизатори QoSнн куйидаги бошкариш механизмларини мададлайди:

- *фойдаланишнинг келишилган тезлиги CAR* (Committed Access Rate) иловалар ёки фойдаланувчилар базисида куийдаги учта мухим вазифани бажаради:

  - трафик турини туркумлайди;
  - берилган иловага рухсат этилган утказиш крбилиятининг максимал даражасини урнатади;
  - трафикнинг хар бир тури устиворлигини белгилайди;

- *сиёсат асосида маршрутлаш* (Policy Routing) хам трафикни туркумлайди ва устиворлайди хамда трафикнинг кайси турини маршрутизаторнинг мое чикиш йули портига жунатиш лозимлигини х,ал этади;

- *мулощзали одилона навбат* WFQ (Weighted Fair Queneing) трафик ни хисобга олган хрлда макбул жавоб вактини таъминлайди;

- *протокол RSVP* иловаларга йулнинг бошидан охиригача кафолатланган утказиш кобилиятини резервлашга имкон беради.

Маршрутизаторнинг мослашувчанлиги модулли конструкция ва иккита слотда урнатилувчи интерфейс WAN-карталари туплами орк,али таъминланади. Cisco 1720 моделида Cisco 1600, 2800, ва 3600 моделларда ишлатиладиган WAN-карталардан фойдаланилади.

Компания 3Com VPN технология™ амалга оширишда бошидан стандартларни кузга тутган эди. VPN ни мададлаш унинг NetBuilder II, Super Stack II NetBuilder маршрутизаторларига Office Connect Net Builder Platform ларида урнатилган.

3Com компанияси PPTP ва L2TP протоколларни мададловчи масофадан фойдаланилувчи концентраторларни йирик ишлаб чикарувчиларидан биридир. 3Com компаниясининг VPN тармоклари IPSec билан бирга ишлатилади ва ташки каталоглар, жумладан Novell NDS ва Windows NT Directory 8епасе8лар билан узаро алока килиш учун ишлаб чикилган.

Компания Web-технологияга асосланган ва VPN юкланганлигини назоратлашга, хамда юз берувчи ходисалар асосида статистика ва ахборотни йигишга аталган дастурий илова Transcend Ware Secure VPN Manager ни хам ишлаб чикди. Ундан ташкари 3Com криптохимояланган туннелларни осонгина яратишга имкон берувчи Web асосидаги инструментарийни ишлаб чикаради.

Internet Devices компаниясининг Fort Knox маршрутизаторларида тезлик ва кувват уйгунлашган. Ундаги тармокни химоялашни таъминлашга йуналтирилган IP-трафикни ишлаш вазифалари руйхатининг кенглиги унинг афзаллигидир. Fort Knox маршрутизатори тармоклараро экран режимида ишлаши, NAT стандарти буйича адресларни трансляциялаши, хавфсизлик сиёсатини бошкариши, Web-сахифалар ва DNS жадвал ёзувларини кэшлаши, аудитни бажариши мумкин. Одатда Fort Knox корпоратив тармок, чегарасида, корпоратив тармокни глобал тармок, билан уловчи маршрутизатордан кейин урнатилади. Демак, у бошк,а локал тармоклар билан VPN-алок,ани урнатиш ва тармоклараро экранлар каби фойдаланишни назоратлашнинг турли к,оидаларини шакллантириши мумкин. Fort Кпохда NAT адресларини трансляциялаш функциясининг мавжудлиги, унга ички IP-адресларни беркитиш ва маршрутизаторлар трафигини кайта йуналтириш имконини беради. Бу корпоратив тармок, маъмурларини VPNнн к,уришда маршрутизаторларни янгидан конфигурациялашдан озод этади. Fort Knox функциялари тупламининг кенглигига карамай унинг нархи одций маршрутизатор нархига тенг.

Тармоқлараро экранлар асосидаги VPN. Локал тармокнинг тармокдараро экрани оркали, худди маршрутизатордагидек, бутун трафик утади. Шу сабабли, тармоклараро экран хам чикувчи трафикни шифрлаш, кирувчи трафикни расшифровка килиш вазифасини бажариши мумкин. Хрзирди катор VPN-ечимлар тармокдараро экранларни VPNHHHF кушимча мадад функциялари билан тулдирилишига таянади. Бу Internet орк,али бошка тармокдараро экранлар билан шифрланган уланишни урнатишга имкон беради. Ахборот хавфсизлиги буйича катор мутахассисларнинг фикрича VPNHH тармокдараро экранлар асосида куриш, корпоратив тармокдарни очик, тармокдар хужумларидан комплекс химоялаш нуктаи назаридан, тула асосланган ечимдир. Хдкикатан, тармокдараро экран ва VPN-шлюз функциялари бир нуктада, ягона бошкариш ва аудит тизими назоратида бирлаштирилса, корпоратив тармокни х,имоялаш функциялари битта курилмада тупланади. Натижада х,имоя воситаларини маъмурлаш сифати ошади.

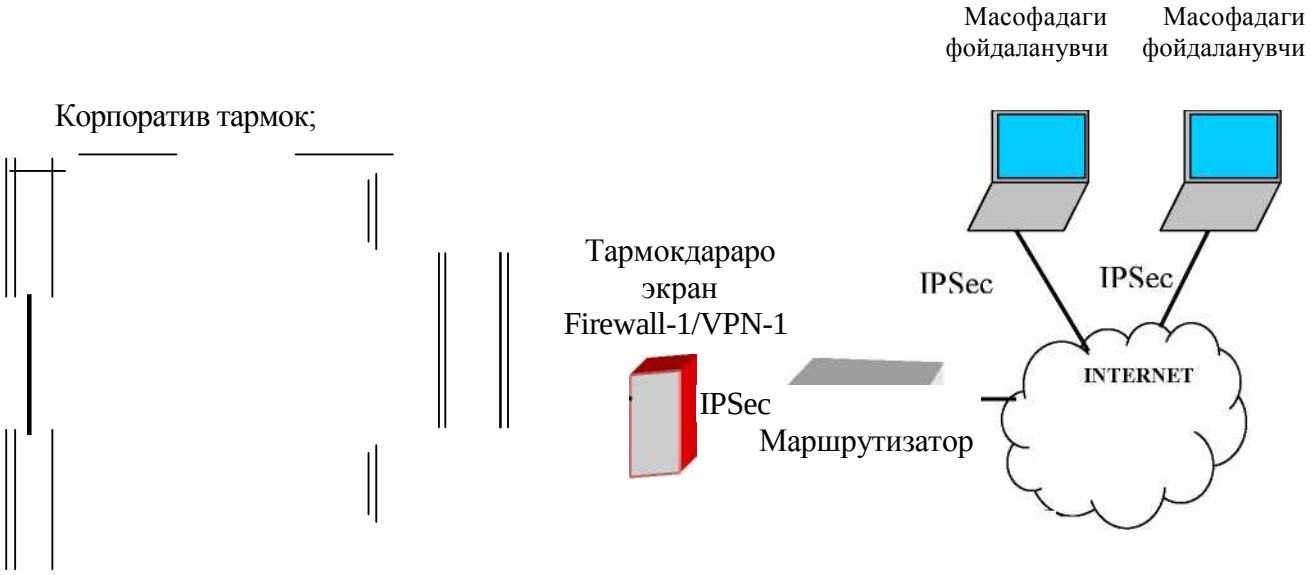
Аммо, химоялаш воситаларининг бундай универсаллаштирилиши, х,исоблаш воситаларининг мавжуд имкониятлари даражасида нафак,ат ижобий, балки салбий томонига х,ам эга. Шифрлаш ва аутентификациялаш амалларини хисоблаш мураккаблиги тармокдараро экран учун анъанавий булган пакетларни фильтрлаш амалларига нисбатан анча юкрри. Шу сабабли, VPNHHHF к,ушимча вазифаларини амалга оширишда мураккаблиги катта булмаган амалларни бажаришга мулжалланган тармокдараро экран купинча керакли унумдорликни таъминламайди. Корпоратив тармок, тезкор канал орк,али очик, тармок,к,а уланганида сифатли х,имояни таъминлаш учун алох,ида аппарат, дастурий ёки комбинацияланган курилма куринишидаги VPN-шлюздан фойдаланиш лозим.

Аксарият тармокдараро экранлар сервер дастурий таъминотидан иборат, шу сабабли унумдорликни ошириш муаммоси юкрри унумдорликка эга булган компьютер платформасидан фойдаланиш эвазига ечилиши мумкин.

Check Point Software Technologies компанияси Internet билан ишлаганда ахборот хавфсизлигини комплекс таъминлаш махсулотларини ишлаб чикариш сох,асидаги етакчилардан бири х,исобланади. Check Point Fire Wall-1 тармокдараро экран корпоратив ахборот ресурслари учун ягона

комплекс доирасида хдмоянинг чукур эшелонланган чегарасини куришга имкон беради. Бундай комплекс таркибига Check Point FW-1 нинг узи ва корпоратив VPN тармок, (химояланган туннеларни шакллантирувчи кием тизим) куриш учун махсулотлар туплами Check Point VPN-1, хдмда сукилиб киришни пайкаш воситалари Flood Gate ва х,. киради.

Дастурий таъминотлар Check Point Fire Wall-1/VPN-l асосида корпоратив тармок, куриш мисоли 8.8-расмда келтирилган.



8.8-расм. Check Point FW-1/VPN-1 асосида корпоратив VPN тармоғини куриш схемаси.

Check Point VPN-1 кием тизим таркибидаги барча махсулотлар хдм узаро, хам оммавий брандмауэр Fire Wall-1 билан узвий интеграцияланган. Check Point компанияси "тармок-тармок," (VPN-1 Gateway) ва "тармок-масофадаги фойдаланувчи" (VPN-1 Gateway+VPN-1 Secu Remote) типидаги хдмояланган тармокларни ташкил этиш учун воситаларни такдим этади.

Check Point VPN-1 махсулотлари очик, стандартлар (IPSec) асосида амалга оширилган, фойдаланувчиларни аутентификациялашнинг ривожланган тизимига эга, очик, калитларни (PKI) таксимлашнинг ташки тизимлари билан узаро алокани мададлайди, бошк,ариш ва аудитнинг марказлаштирилган тизимини куришта имкон беради ва х,.

Check Point Fire Wall-1/VPN-1 нафакат очик,, балки криптохимояланган трафикни х,ам назоратлайди. Тармокдарарo экран FW-1га келган маълумотлар VP-1 воситалари ёрдамида расшифровка килинади, сунгра ахборотлар пакети яна шифрланади ва утказиб юборилади.

VPN-1 кием тизими трафикни нафакат криптографик беркитади, балки ахборотлар пакетини аутентификациялайди хам.

Check Point Fire Wall-1/VPN-1 каналларида трафикни шифрлашда машхур алгоритмлар DES, 3-Des, CAST, IDEA, FWZ1 ва х,. алгоритмлардан фойдаланилади. FWZ1 криптотизими Check Point компаниясининг ишланмасидир. Ахборот пакетларини аутентификациялашда MD5, SHA-1, CBC DES ва MAC алгоритмлари ишлатилади.

VPN Gateway шлюзи - шифрлашнинг дастурий модули тармокларарo экран Fire Wall - 1 билан узвий интеграцияланган. Бу махсулот корхонага узатилувчи маълумотларнинг тула конфиденциаллигини, аутентификацияланганлиги ва яхлитлигини кафолатлаган хрлда Internet оркали алока каналларини куришта имкон беради. VPN функциялари корхонанинг умумий хавфсизлик сиёсатига тула интеграцияланганлиги сабабли, брандмауэр ва VPN-махсулотларни алохдда бошкаришта эхтиёж крлмайди.

VPN Gateway шлюзи химояланган VPN-туннелни урнатган хрлда тармокдар орасида Intrenet оркали узатилаётган конфиденциал маълумотларни шифрлайди. Бу шлюз уни жавобгарлик доирасига, яъни унинг доменига кирувчи компьютерлардан келадиган маълумотлар окимини шифрлайди. Бу л окал тармок, ёки ушбу шлюз оркасидаги оддий хостлар гурухи булиши мумкин. Бу маълумотлар тармокнинг оммавий кисми буйича шифрланган куринишда узатилади, ички тармок, буйича узатилганда шифрланмайди. VPN-амалларининг барчаси охирги фойдаланувчи ва барча иловалар учун шаффофдир.

VPN-1 Gateway шлюзи шифрлашнинг бир неча алгоритмини ва бир неча калитларни бошкариш протоколини мададлайди. Бу шлюз IKE (Internet Key Exchange) каби индустриал стандарт VPN-протоколларни мададлаши сабабли, экстратармокларни ташкил этишда к,уллаш к,улай х,исобланади. Экстратармокдарда VPN бизнес-шериклар орасида хавфсиз алок,ани таъминлайди. Check Point компаниясининг УРМ-мах,сулотлари IKE стандартига амал к,илади. Шу сабабли улар карши томон билан музокаралар жараёнида автоматик тарзда шифрлашнинг энг криптобардош алгоритмини (DES ва Triple DES) ва аутентификациялашнинг энг катъий алгоритмини

(SHA-1 ва MD5) танлайди. Ундан ташкари, шифрлашнинг махфий калитлари, максимал химояланишни кафолатлаган хрлда, тез-тез янгиланади.

VPN-1 Gateway шлюзи виртуал хусусий тармокдаги иккита охирги узелларга хам шифрланган, хам шифрланмаган маълумотларни алмашишга имкон берувчи шифрлашнинг танлов режимини мададлайди. Бунинг учун тармок, маъмури трафиги учун химоялашнинг алох,ида шартлари таъминланадиган иловаларни беради. Сунгра VPN-1 Gateway ушбу иловалар маълумотларини шифрланган, крлган конфиденциал булмаган маълумотларни очик, куринишда узатишни бошлайди. Бундай мосланувчанлик VPN-1 Gateway шлюзининг унумдорлигини оширади.

VPN-1 Gateway шлюзи калитларни бошкаришнинг куйидаги механизмларини мададлайди: IPSec учун стандарт булган IKE, калитларни бошкаришнинг саноат стандарти FWZ, оммавий протокол SKIP ва калитларни кул билан таркатиладиган усули. У X.509 сертификатлари ва Entrus Technologies компаниясининг сертификатлар серверлари технологияси асосида очик, PKI калитларни бошкариш инфратузилмасини мададлайди.

VPN-1 Secu Remote мижоз дастурий таъминоти VPN-1 Gateway Шлюзи ёрдамида "тармок-масофадаги фойдаланувчи" х,илидаги химояланган уланишларни ташкил этишда ишлатилади. Windows 9X/XP/NT/2000 бошкарувида ишловчи масофадаги компьютерларга VPN-lSecu RemoteHHHr урнатилиши Мобил ходимларнинг ёки телекомпьютерларнинг корхона бош тармоги билан Internet оркали х,имояланган богланишини таъминлайди. VPN-1 Secu RemoteHHHr мах,сулотларни OSI моделининг тармок, сатх,ида шифрлаши ва расшифровка килиши ушбу амалларнинг барча иловалар учун шаффофлигини, мавжуд иловаларга узгартириш киритишни талаб к,илмаган хрлда, таъминлайди. SecuRemote фойдаланувчиларга VPN-воситалар урнатилган бир неча турли тармоклар билан богланишига имкон беради.

VPN-1 Accelator Card к,урилмаси Chrysalis-ITS компанияси томонидан ишлаб чик,илган аппарат криптографик тезлатгичдир. VPNHHHr х,имояланган каналларида трафикни шифрлаш ва калитларни генерацияловчи амаллар анчагина х,исоблаш мураккаблигига эга ва VPN орк,али узатилувчи тра-

фикнинг хажми ошган сари компьютернинг процессори ва хотирасининг хадцан ортик, юкланиши руй бериши мумкин. VPN-1 Accelator махсулоти бу муаммони х,ал этиши мумкин.

VPN-1 Accelator Card тезлатгичи VPN-1 Gateway шлюзи билан биргаликда ишлашга аталган ва IKE ва IPSeanap талаб этадиган барча криптографик амалларни бажаради. VPN-1 Accelator Card бевосита шлюз оркали маъмурланади.

VPN функциялари урнатилган SecureZone тармокдарарo экрани Secure Computing компанияси томонидан ишлаб чикилган ва асосий характеристикалари куйидагича:

- VPNнн мададлаш функциялари - IPSec стандарти, DES ва Triple DES, PKI бошкариш ва Netscape, Entrust ва Verisign компаниялардан X.509 сертификатлари;

- ихтисослаштирилган операцион тизими Secure OS (11шхнинг химояланган варианти) бошкарувида ишлайди;

- куйидагиларни каноатлантирувчи аппарат платформалар: процессор Intel Pentium, Pentium Pro, ёки Pentium II; RAM-камида 64Мбайт; ташки курилмалар каттик, диск 4 Гбайт SCSI-2, кайишкрк, дисклар 3,5", СОКОМ, стриммер DAT; SVGA video, PS/2- билан бирга ишлай олувчи сичкрн.

- стандарт тармок, интерфейслари: 2-4 Ethernet, FAST Ethernet, Token Ring ёки FDDI;

- бузилишга бардошлик хоссасига эга.

Secure Computing компанияси MicroSoft Windows мухитида ишловчи, алохида фойдалунувчиларга ТСРЯР протоколлари буйича телефон тармоги ёки пакетларни коммутацияловчи, оммавий тармокдан х,имояланган масофавий фойдаланишни таъминловчи, IPSec билан бирга ишлайолувчи мижоз дастурий таъминотини (SecureClient) хам тавсия этади.

VPN функциялари урнатилган Raptor Firewall 5.0 тармокдарарo экрани Axent Technologies компанияси томонидан ишлаб чикилган ва Eagle FirewallHHHr модификацияланган мах,сулоти хисобланади. Бу тармокдарарo экраннинг характеристикалари куйидагича:

- VPN мадади тармокдарарo экранга урнатилган;

- IPSec стандарта мададланади, дастурий шифрлаш IP (текин таркатилувчи шифрлаш усули swIPe);

- хавфсизликнинг умумий сиёсати тармокдарарo экран функцияларига ва VPN функцияси ёрдамида туннелланувчи трафикка тааллукди;

- Windows NT/2000 ва Solaris операцион тизимлар бошкарувида ишлайди.

Axent компанияси масофадаги фойдаланувчилар учун VPNННҢ МИЖОЗ дастурий таъминотини хам такдим этади. Raptor Firewall 5.0 версияси IPSec протоколи буйича химояланган виртуал тармок, курилишини таъминлайди.

Gauntlet Global VPN махсулоти Network Associates компанияси таркибига кирувчи Trusted Information Systems компаниясининг Gauntlet Firewall тармокдарарo экрани учун, ушбу тармокдарарo экран мухдтида узвий интеграцияланувчи, кушимча дастурий махсулот хисобланади.

IPSec протоколига асосланган Gauntlet Global VPN кием тизими трафикни криптографик химоялашнинг куйидаги иккита режимини мададлайди:

Smart Gate шлюзлари ёрдамида амалга оширилувчи тармокдарарo экрандан тармоклараро экрангача; масофадаги мижоз дастурий таъминоти Gauntlet PC Extender ёрдамида амалга оширилувчи тармокдарарo экрандан масофадаги фойдаланувчи компьютеригача.

Gauntlet Global VPNfla шифрлашнинг DES алгоритми ишлатилади. Gauntlet Global VPN сертификация марказининг дастурий таъминоти билан хам такдим этилади. Ушбу дастурий таъминот ёрдамида ташкилотлар X.509 стандартига мое келувчи ракамли сертификатларни генерациялаши ва текшириши мумкин.

VPN куриш функциясини мададловчи BorderManager тармокдарарo экрани Novell компаниясининг махсулоти булиб, нафак,ат VPN куриш имкониятини, балки фойдаланишни чегаралашни, пакетларни фильтрлаш ва тармок, адресларини трансляциялашни таъминлайди, воситачи HTTPнинг хизматларини тавсия этади, Web сах,ифаларини кешлайди, канал сатх,ида

шлюзларга эга, куп протоколли маршрутлашни бажаради ва масофадан фойдаланишни мададлайди.

Border Manager тармоклараро экраннинг NDS (Novell Directory Service) каталоглари хизмати билан узвий интеграцияси химояланган виртуал тармокдарни самарали бошкаришта имкон беради. Шифрлаш калитининг таксимоти RSA криптотизими ва Диффи-Хеллман алгоритми буйича амалга оширилади. Ахборот пакетларини криптографик беркитиш ва аутентификациялашда RC2 ва RSA криптотизимлардан фойдаланилади. Border ManagerHHHr бир версиясида IPSec протоколи мададланади. Border Manager тармоклараро экран асосида курилган химояланган виртуал тармокдарда брандмауэрлардан бирининг асосий булиши, бошкариш маркази ролини бажариши лозим.

Ихтисослаштирилган дастурий таъминот асосидаги VPN. **VPN** куришда ихтисослаштирилган дастурий воситалар кенг кулланилади. VPN куришнинг дастурий воситалари химояланган туннелларни факат дастурий шакллантиришга имкон беради ва улар ишлайдиган компьютерни ТСРЯР маршрутизаторига айлантиради. Бу маршрутизатор шифрланган пакетларни кабул килади, расшифровка килади ва локал тармок, оркали тайинланган нуктага узатади. Охирги вактда бундай махсулотларнинг етарлича сони пайдо булди. Ихтисослаштирилган дастурий таъминот куринишида VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар бажарилиши мумкин.

Дастурий усул буйича амалга оширилган VPN-махсулотлар унумдорлик нуктаи-назаридан ихтисослаштирилган аппарат курилмалардан к,олишсада, дастурий мах,сулотлар масофадаги фойдаланувчиларга етарли унумдорликни осонгина таъминлайди. Дастурий маъсулотларнинг шубхасиз афзаллиги ишлатилишида мосланувчанлиги ва к,улайлиги, х,амда нисбатан юкрри булмаган нархидир. Аппарат шлюзларни ишлаб чикарувчи купгина компаниялар (масалан, Time Step, VPNet, Shiva) узларининг махсулотларига стандарт операцион тизимда ишлашга мулжалланган VPN-мижознинг дастурий амалга оширилишини к,ушадилар.

MicroSoft компаниясининг RAS ва RRAS дастурий маусулотлари. **MicroSoft** компаниясининг масофадан фойдаланувчи дастурий сервери RAS

(Remote Access Service) машхур PPP (Point to Point Protocol) протоколнинг кенгайтирилган варианта-химояланган канал протоколи PPTPни (Point-to-Point Tunneling Protocol) урнатилиши эвазига VPN технологияни мададлайди. Трафикни туннеллаш очик, IP-тармок, буйича узатиладиган стандарт PPP- фреймларни IP-датаграммаларга инкапсуляциялаш ва кейин шифрлаш оркали амалга оширилади.

RASHHHr асосий афзаллиги - тежамлилиги, камчилиги - унумдорлигининг пастлиги. Хрзирда бу махсулотнинг такомиллаштирилган версияси - RRAS (Routing and Remote Acces Service) пайдо булди. RRAS таркибидаги такомиллаштирилган дастурий куп протоколли маршрутизатор маршрутлашнинг RIP (Routing Information Protocol) ва OSFP (Open Shortest Path First) протоколларини мададлайди. RRASHHHr бу хусусиятлари ундан VPN шлюзи каби "тармок-тармок," узаро алокасида фойдаланишга имкон яратади. RAS хизмати масофадан фойдаланувчиларнинг купчилигига (256 тагача) битта Windows NT серверига уланиш ва локал тармок, ресурсларидан IPX ва TCPЯP протоколлари буйича фойдаланиш имкониятини беради.

Alta Vista Tunnel 98 маусулотлари оиласи учта махсулотни уз ичига олади: Telecommuter Server, Extranet Server, AltaVista Tunnel Client. Telecommuter Server сервери Internet корпоратив фойдаланувчилар орасида химояланган туннеларни Internet оркали ташкил этишга аталган. Extranet Server сервери ёрдамида тармокдар орасида химояланган канални хрсил килинади. Бу иккала сервер умумий Alta Vista Tunnel Server номига эга. Alta Vista Tunnel Client VPN клиентнинг дастурий таъминотидир.

Alta Vista Tunnel 98 оиласининг барча махсулотлари фойдаланувчиларни аутентификациялашда ва RSA криптографик тизимнинг сессия калитларини алмашишда ишлатилади. Фойдаланувчиларни аутентификациялашда Security Dynamics компаниясининг аппарат калити SecurlD х,ам ишлатилиши мумкин. Мижоз ва сервер янги сессия калитлари билан хар 30 минутда алмашишади.

Маълумотларни шифрлашда RC4 алгоритмидан фойдаланилади. Мах,сулотларнинг х,алкаро версияси RC4 алгоритми буйича шифрлашда 56 ёки 4 битли калитлардан фойдаланади. Маълумотларни аутентификациялаш

ва яхлитлигини таъминлаш учун MD5 хэш-функцияси ишлатилади. Alta Vista Tunnel 98 оиласининг махсулотлари LZO алгоритми буйича маълумотларни зичлаштириши мумкин.

Ушбу оила махсулотлари аксарият замонавий операцион тизимлар - Windows NT/2000, Unix BSD/OS, Unix BSD ва Digital UNIX бошкарувида ишлаши мумкин. Windows NT/2000 операцион мухитда Alta Vista Tunnel Server махсулоти бир вактнинг узида 200 туннел уланишларини, UNIX операцион мухитда эса 2000гача туннел уланишларни мададлайди.

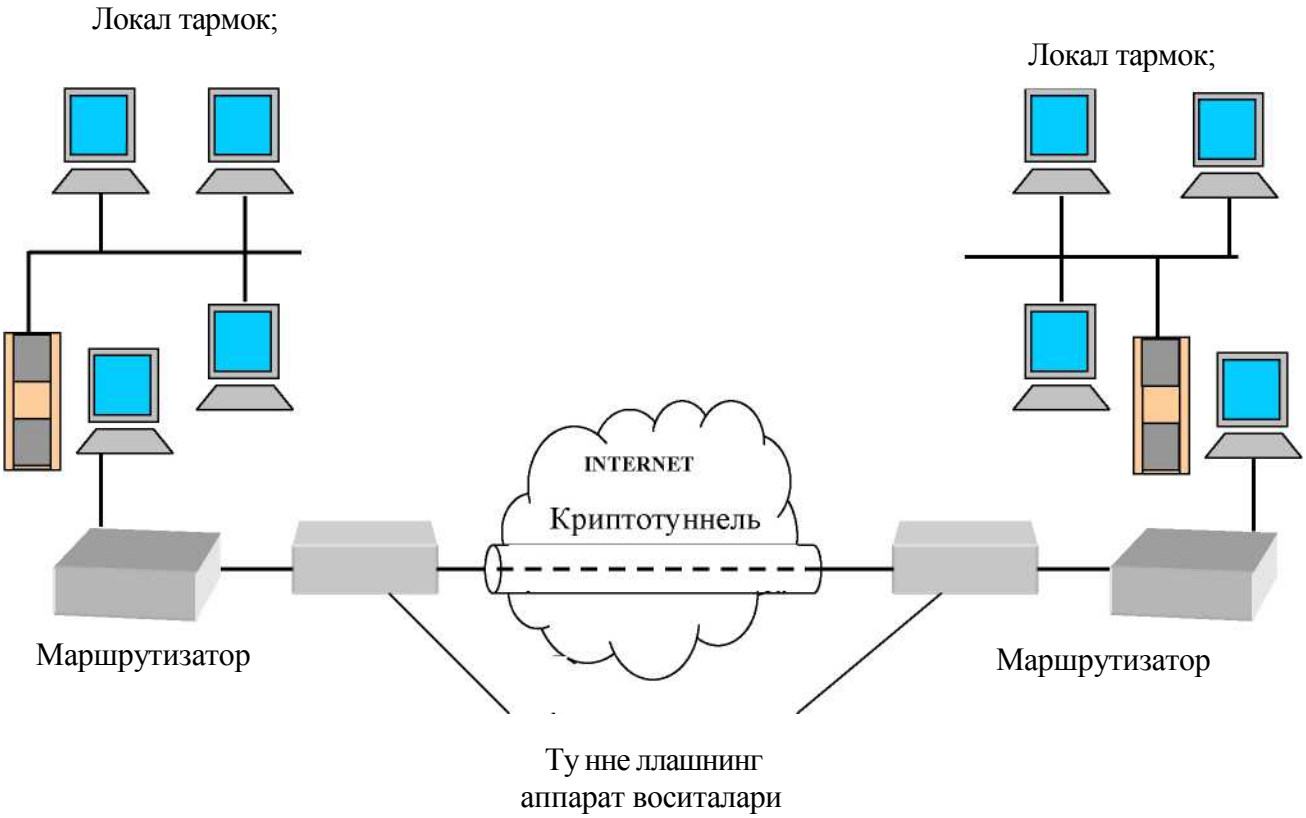
Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат курилмалари асосидаги VPN-воситаларнинг асосий афзаллиги-юкрри унумдорлиги. VPN-пакетларни ишлашда керакли хисоблашлар хажми оддий пакетларни ишлашдагига нисбатан 50-100 марта ошади. Аппарат воситалари асосидаги VPNnapfla юкрри тезликка уларда шифрлашнинг ихтисослаштирилган микросхемаларда амалга оширилиши эвазига эришилади. Бундай VPN-воситалар купинча IPSec протоколи билан бирга ишлайолади ва локал тармокдар орасида криптохимояланган туннелларни шакллантиришда ишлатилади. Баъзи ишлаб чикарувчиларнинг VPNнн шакллантирувчи асбоб-ускуналари бир вактнинг узида "масофадаги компьютер-локал тармок," режимида химояланган богланишни хам мададлайди.

Аппарат VPN-шлюзлар алохдда аппарат курилмаси куринишида булади. Уларнинг асосий вазифаси - трафикни юкрри унумдорлик билан шифрлаш. Бу VPN-шлюзлар X.509 ракамли сертификатлари PKI очик, калитларни бошкариш инфратузилмалари билан ишлайди, LDAP буйича маълумот берадиган хизматлар билан ишлашни мададлайди.

Аппарат химояланган туннел ишлашининг энг оддий варианти - аппарат шифрлашдан фойдаланиб уланишларни яратиш. Туннеллашнинг аппарат воситалари одатда локал ва глобал тармокларнинг туташган жойида, маршрутизатордан кейин урнатилади (8.9-расм) ва автоматик тарзда берилган трафикни шифрлайди. Бундай ёндашишнинг асосий афзаллиги шундаки, ишчи станциялар ва маршрутизаторларнинг шакллантирилувчи крипто-

туннеллар билан хеч кандай богликлиги йук,, VPN урнатилганида уларни конфигурациясини узгартириш талаб этилмайди.

Аппарат шлюзларни инсталляциялаш дастурий шлюзлар ва маршрутизаторлар ва брандмауэрлар асосидаги шлюзларга нисбатан жуда осон амалга оширилади. Бундай курилмаларни бошкариш иккита асосий масалани ечишни талаб этади: сертификация маркази оркали калитларни бошкариш ва химояланган туннеллашни бошкариш. Аксарият аппарат туннеллаш воситаларида сертификация марказлари Windowsra мослашган дастурий иловалардир. Аппарат туннелларини марказлашган хрлда бита иш жойида туриб бошкариш мумкин. Бошкарувчи дастурлар туннелнинг асосий х,имоялаш функцияларининг бажарилишини ва хатоликларни ишлашни таъминлайди.



8.9-расм. Ихтисослаштирилган аппарат воситалар асосида туннеллаш схемаси.

Ихтисослаштирилган аппарат VPN-воситалар нархидан ташкари барча булиши мумкин булган курсаткичлари буйича лидер х,исобланади.

TimeStep компанияси корхоналарда кенг масштабли ахборот алмашинуви учун IPSec билан бирга ишлайолувчи PERMIT Enterprise Snite деб аталувчи VPN-махсулотни ишлаб чикди. Ушбу махсулот Internet оркали ма-

софадан фойдаланишни ташкил этиш, корпоратив интратармок, ва экстратармокдарни куриш учун тулик, ечим хисобланади. PERMIT Enterprise мавжуд тармокдарда тармок, ва охирги фойдаланувчи унумдорлигига жиддий таъсир килмаган хрлда, осонгина сафланади, унинг масштабланувчи архитектураси бирнеча УРМларни яратиш ва уларни бошкариш имкониятини беради.

Компания томонидан шлюзнинг куйидаги туртта модификацияси такдим этилади:

- PERMIT/Gate 1520 нархи киммат булмаган автоном курилма булиб, кувватли телекомпьютерлар ёки SOHO синфидаги катта булмаган офислар учун ишлатилади;

- PERMIT/Gate 2520 ва PERMIT/Gate 4520 утказиш крбилияти, мое хрлда 4 ва 1- Мбит/с, булинмалар офислари ва кичик локал хисоблаш тармокдарига мулжалланган, масофадаги юзлаб фойдаланувчиларни мададлайди;

- PERMIT/Gate 7520 (70 Мбит/с) ички локал хисоблаш тармокдарида ишлатилади ва масофадаги минглаб фойдаланувчиларни мададлайди.

PERMIT/Gate шлюзларининг мухим афзаллиги - трафик ишланишининг юкрри унумдорлигини таъминлш максадида DES ва 3-DES шифрлаш алгоритмининг аппарат амалга оширилиши.

PERMIT/Gate7520 шлюзи IPSecHHHr амалга оширилишининг аппарат воситаси билан хам жихрзланганлиги, унумдорликка таъсир килмаган х,олда минглаб VPN уланишларни мададлашга имкон беради. Бу, зарурият тугилганда, корпоратив тармок,ни осонгина кенгайтириш имконини яратади.

Мижоз дастурий таъминоти PERMIT/Client IPSec протоколини мададлайди ва масофадаги фойдаланувчиларга узининг тармоги билан хавфсиз богланиш имконини беради. Ушбу дастурий таъминот Windows95/98/XP/NT ёки MAC OS 7.1. бошкарувида ишловчи алохдда ишчи станция томонидан адресланган тармок, трафигини химоялайди.

PERMIT/Gate шлюзларининг хар бири дастурли утилита PERMIT/Config билан бирга такдим этилади. Бу дастурли утилита виртуал хусусий тармокнинг хар кандай нук,тасидан бир неча шлюзларнинг дасту-

рий таъминотини масофадан конфигурациялаш, бошкариш ва модиифкациялашга имкон яратади.

VPNet компанияси VPN курит учун дастлабки интеграцияланган ечимлардан бири - VPNwareim таклиф этди. Бу ечим уз ичига куйидаги махсулотларни олади:

- учта VPN-шлюз: штаб кароргохи ва йирик локал тармоклар учун VSU.1100, булинмалар учун VSU-1010 ва катта булмаган офислар учун VSU-10;
- iPass компаниясидан дастурий сервер RoamServer;
- мижоз дастурий таъминоти VPNremote;
- бошкаришнинг дастурий тизими VPNmanager.

VPNet асбоб-ускуналари, "тармок-тармок," ва "тармок, - масофадаги фойдаланувчи" хилидаги уланишларга мулжалланган VPNнн мададлайди. Ишлатиладиган махсулотларга боглик, хрлда VPNware тизими IPSecHHHr стандарт амалга оширилиши ёрдамида оммавий IP тармок, оркали узатилаётган маълумотларни химоялаш билан 25дан 5000тача фойдаланувчиларни мададлаши мумкин. Бу тизим турли масштабли тармокларда йирик корхонанинг марказий локал тармогида, булинма ва катта булмаган офис локал тармогида ва масофадаги фойдаланувчиларни химоялашда ишлатилиши мумкин.

VSU-1010 ва VSU-10 шлюзлар IPSec билан бирга ишлай олади ва DES ва 3-DES алгоритмлари буйича маълумотларни шифрлашни аппарат мададлашга эга. VPNHHHr бошк,арувчи иловаси статистикани йигишга ва VPNflara ходисаларни к,айдлашга имкон беради. Хар хил VPNnapHH бошк,аришни марказлаштириш эвазига химояни бошк,аришнинг бошк,а функцияларини соддалаштириш ва марказлаштириш, масалан, корпоратив браднмауэр яхлитлигини бузилишини назоратини таъминлаш мумкин. VPNet махсулотларининг афзаллиги-мавжуд тармок, билан интеграциялашининг соддалиги, унумдорлигининг нисбатан юкррилиги ва IPSecHHHr тула амалга оширилиши.

Мижоз дастурий таъминоти VPNremote IPSec протоколини мададлайди ва Windows NT мухитида хамда телефон тармоклари оркали фойдала-

нилганда масофадаги ва мобил фойдаланувчилар, телекомпьютерлар ва бизнес-шерикларнинг маълумотларини химоялашда Windows95/98/XP мухдтида ишлайди.

Бошкарув тизими VPNmanager виртуал хусусий тармокларни яратиш, конфигурациялаш ва бошкариш учун махсус ишлаб чикилган. Тармок, маъмури ушбу тизим ёрдамида, график интерфейсни ишлатиб масофадаги фойдаланувчиларни ва бизнес-шерикларни VPNra осонгина кушиши мумкин. VPN мижозларини масофадан маъмурлашга Dyna-Policy функцияси аталган.

LanRover VPN Gateway шлюзи Shiva компанияси тоомнидан такдим этилган булиб, ICSA томонидан сертификацияланган. Бу шлюз очик, тармок, оркали узатиладиган маълумотларни химоялаш технологияларининг кенг тупламини мададлайди. Яхлитликни ва конфиденциалликни таъминлаш, фойдаланишнинг назорати, X.509нинг ракамли сертификатларига, Security Dynamics аппарат калитларига, RADIUS протоколи ёки доменли схемага асосланган аутентификациялашнинг турли схемалари бу тупламга киради.

Маълумотларни аппарат шифрлаш DES ёки 3-DES алгоритмлари асосида амалга оширилади. LanRover VPN Gateway шлюзлари Pentium-технологиянинг тезлиги, шифрловчи ихтисослаштирилган интеграл схемаларининг тезкорлиги ва реал вактнинг куп вазифали операцион тизимнинг реактивлигининг ноёб бирикмасидан фойдаланади. Бу шлюзлар ишлатишда кулай ва уларнинг ишлаши охирги фойдаланувчилар учун шаффоф. Бу шлюзлар билан ишлаш кулайлигини таъминлаш максадида график фойдаланувчи интерфейсли утилита VPN manager такдим этилади. Бу утилита маъмурга хар к,андай Windows 95/NT тизимидан бирданига бир неча шлюзларни бошк,аришни таъминлайди.

8.4. Канал ва сеанс сатзутрда з^имояланган виртуал каналларни куриш

Канал сатуида уимояланган виртуал каналларни шакллантириш протоколлари.

PPTP, L2F ва L2TP протоколлар OSI модели канал сатхднинг тунеллаш протоколлари хдсобланади. Ушбу протоколларнинг умумий хусусияти шундан иборатки, улар очик, тармок,, масалан Internet оркали корпоратив тармок, ресурсларидан химояланган куп протоколли масофадан фойдаланишни ташкил этишда ишлатилади. Уччала протоколни, одатда, химояланган канални шакллантириш протоколларига мансуб деб хисоблайдилар. Аммо бу таърифга узатиладиган маълумотларни туннеллашни ва шифрлашни таъминловчи факат PPTP протоколи аник, мое келади, чунки L2F ва L2TP протоколлар факат туннеллаш функцияларини мададлайди. Туннелланган маълумотларни хдмоялаш (шифрлаш, яхлитлик, аутентифкация) учун бу протоколларда кушимча, протокол, хусусан IPSec протоколи ишлатилади.

PPTP протоколи маълумотларни IP, IPX ва NetBEUI протоколлари буйича алмашиш учун химояланган каналларни яратишга имкон беради. Ушбу протоколлар маълумотлари PPP кадрларига жойланади ва сунгра PPTP протоколи воситасида IP протоколининг пакетларига инкапсуляцияланади ва шу протокол ёрдамида шифрланган куринишда х,ар к,андай TCPЯP тармоги орк,али ташилади.

PPP сессияси доирасида узатилувчи пакетлар куйидаги тузилмага эга (8.10-расм):

- Internet ичида ишлатилувчи канал сатхининг сарлавхаси, масалан Ethernet кадрининг сарлавхаси;
- таркибида пакетни жунатувчи ва кабул килувчи адреслари булган IP сарлавхаси;

маршрутлаш учун инкапсуляциялашнинг умумий усулининг сарлавхаси GRE(Generic Routing Encapsulation);

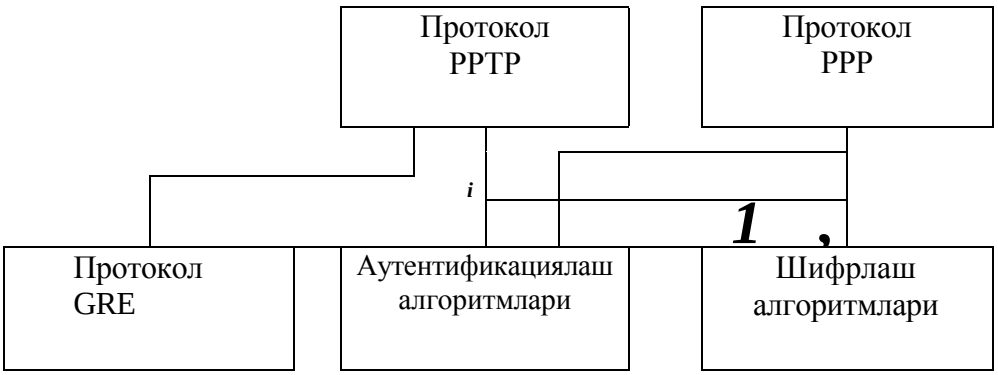
- таркибида IP, IPX ёки NetBEUI пакетлари булган дастлабки пакет PPP.

Узатиладиган кадр сарлавхаси	П>-сарлавхд	GRE-сарлавхд	PPP-сарлавхд	Шифрланган маълумотлар PPP	Узатиладиган кадр охири

8.10-расм. PPTP туннели бўйича жўнатилади пакет тузилмаси

Тармокнинг кабул килувчи узели IP пакетлардан PPP кадрларни чикариб олади, сунгра PPP кадрдан дастлабки пакет IP, IPX ёки NetBEUI пакетини чикариб олиб уни локал тармок, буйича муайян адресатга жунатади. Канал сатхининг инкапсуляцияловчи протоколларининг куп протоколлилиги (унга PPTP протокол хам тааллукди), уларнинг янада юкррирок, сатхнинг хдмояланган канал протоколларидан афзаллигидир. Масалан, агар корпоратив тармокда IPX ёки NetBEUI ишлатилса, IPSec ёки БББпротоколларини ишлатиб булмайди, чунки улар IP тармок, сатхининг факат битта протоколига мулжалланган.

Инкапсуляциялашнинг мазкур усули OSI моделининг тармок, сатхд протоколларига боглик, булмасликни таъминлайди ва очик, 1P-тармокдар оркали х,ар к,андай локал тармокдардан (IP, IPX ёки NetBEUI) хдмояланган масофадан фойдаланишни амалга оширишга имкон беради. PPTP протоколига мувофик,, химояланган виртуал канал яратишда масофадаги фойдаланувчини аутентификациялаш ва узатилувчи маълумотларни шифрлаш амалга оширилади (8.11-расм).



8.11-расм. PPTP протоколи архитектураси

Масофадаги фойдаланувчини аутентификациялашда PPP учун к,улланиладиган турли протоколлардан фойдаланиш мумкин. Microsoft компанияси томонидан Windows 98/XP/NT/2000 га киритилган PPTPнинг амалга оширилишида аутентификациялашнинг к,уйидаги протоколлари мададланади: парол буйича аникдаш протоколи PAP(Pasword Athentication Protocol), к,ул беришишда аникдаш протоколи MS CHAP (Microsoft Challenge - Handshaking Authentication Protocols) ва аникдаш протоколи EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP про-

токолидан фойдаланилганда идентификаторлар ва пароллар алока линиялари оркали шифрланмаган куринишда узатилади, бунда аутентификациялашни факат сервер утказади. MSCHAP ва EAP-TLS протоколларидан фойдаланилганда нияти бузук, одамнинг ушлаб крлинган шифрланган паролли пакетдан кайта фойдаланишидан химоялаш ва мижоз ва VPN-серверни аутентификациялаш таъминланади.

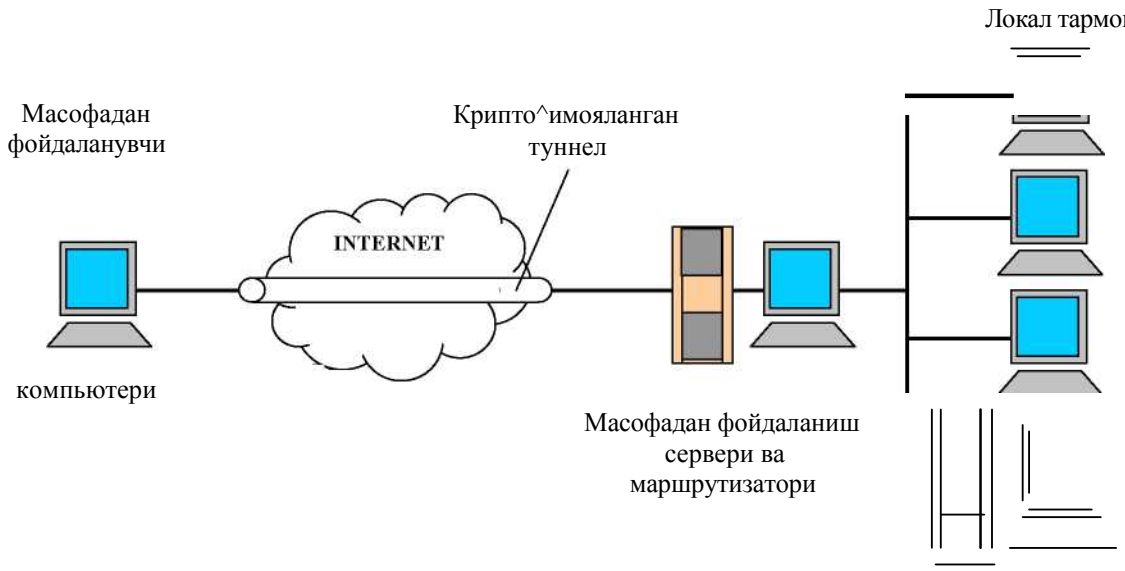
PPTP ёрдамида шифрлаш Internet оркали жунатишда маълумотлардан хеч ким фойдаланаолмаслигини кафолатлайди. Шифрлаш протоколи MPPE (Microsoft Point-to-Point Encryption) факат MSCHAP(1 ва 2 версиялари) ва EAP-TLS билан бирга ишлайолади ва мижоз ва сервер орасида параметрлар мувофиклаштирилишида шифрлаш калитининг узунлигини автоматик тарзда танлай олади. MPPE протоколи узунлиги 40, 56 ёки 128 бит булган калитлар билан ишлашни мададлайди.

PPTP протоколи хар бир олинган пакетдан сунг шифрлаш калиги кийматини узгартиради. MMPE протоколи "нукта-нукта" хилидаги алока каналлари учун ишлаб чик,илган булиб, бу ал ока каналларида пакетлар кетма-кет узатилади ва малумотлар йук,отилиши жуда кам. Бу вазиятда навбатдаги пакет учун калит киймати олдинги пакетнинг расшифровкаси натижасига боглик,. Умумфойдаланувчи тармок, орк,али виртуал тармок, к,уришда бу шартларга риоя килиш мумкин эмас, чунки маълумотлар пакети купинча к,абул к,илувчига жунатилган кетма-кетликда келмайди. Шунинг учун PPTP шифрлаш калитини узгартиришда пакетларнинг тартиб рак,амидан фойдаланади. Бу расшифровка к,илишни олдинги кабул килинган пакетларга боглик, булмаган хрлда амалга оширишга имкон беради.

PPTP протоколи учун куллашнинг куйидаги иккита асосий схемаси аникданган:

- масофадан фойдаланувчининг Internet билан тугридан-тугри уланишидаги туннеллаш схемаси;
- масофадан фойдаланувчининг Internet билан провайдер оркали телефон линияси буйича уланишидаги туннеллаш схемаси.

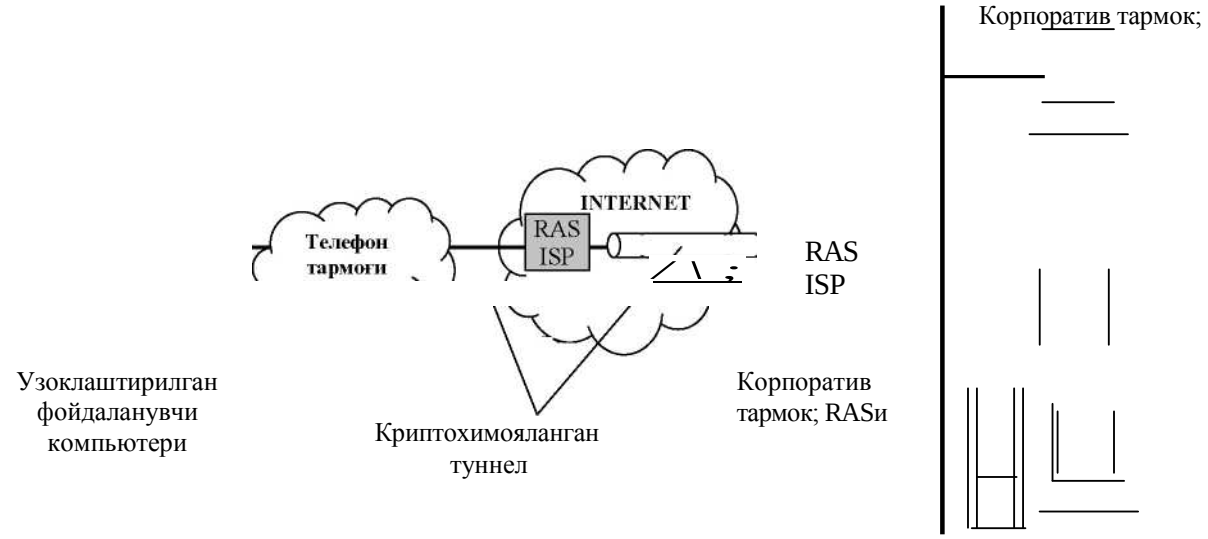
Туннеллашнинг биринчи схемаси амалга оширилганида (8.12-расм) масофадан фойдаланувчи Windows 98/XP/NT таркибидаги масофадан фой-



8.12 -расм. Масофадан фойдаланувчи компьютерини Internetга тўғридан-тўғри уланишидаги туннеллаш схемаси. даланиш сервиси RAS (Remote Access Service)HHHr мижоз кисми ёрдамида локал тармок, билан масофавий богаанишни урнатади. Сунгра фойдаланувчи локал тармокдан масофадан фойдаланиш серверига, унинг IP адресини курсатиб мурожаат этади ва у билан PPTP протоколи буйича алока урнатади.

Масофадан фойдаланиш сервери вазифасини локал тармокнинг чегара маршрутизатори бажариши мумкин. Масофадан фойдаланувчининг компьютерида Windows 98/XP/NT таркибидаги RAS сервернинг мижоз кисми ва PPTPнинг драйвери, масофадан фойдаланувчи локал тармогининг серверида эса Windows NT Server таркибидаги RAS сервери ва PPTP драйвери урнатилиши шарт. PPTP протоколи узаро алокадаги томонлар алмашадиган бир нечта хизматчи хабарни аниклайди. Хизматчи хабарлар TCP протоколи буйича узатилади. Муваффак,иятли аутентификациялашдан сунг х,имояланган алмашиш жараёни бошланади. Локал тармокнинг ички серверлари PPTP протоколини мададламаслиги мумкин, чунки чегара маршрутизатор IP пакетлардан PPP кадрларини чикариб олиб уларни локал тармок, оркали керакли IP, IPX ёки NetBIOS форматида жунатади.

Масофадаги компьютерни Internetra телефон линияси буйича провайдер ISP (Internet Service Provider) оркали улашда туннеллаш схемасининг иккита варианти булиши мумкин (8.13-расм).



8.13-расм. Масофадан фойдаланувчи компьютерини ISP провайдери орцали телефон линиясидан фойдаланиб Internetга уланишини туннеллаш схемасининг иккита варианти.

Схеманинг биринчи вариантининг курилиши протокол PPTPнинг провайдер ISPmnrr масофадан фойдаланиш сервери ва чегара корпоратив маршрутизатор оркали мададланиши тахминига асосланган. Сервер одатда фойдаланувчиларнинг уланишини таъминловчи куп сонли тезкорлиги паст портларга эга. Провайдер КРнинг сервери RAS ва маршрутизатор орасида химояланган канал хрсил булади. Мох,ияти буйича бу - "шлюз-шлюз" хилидаги химояланган канал варианти.

Бу вариантда масофадан фойдаланувчининг компьютери протокол PPTPни мададламаслиги мумкин. Масофадаги фойдаланувчи стандарт протокол PPP ёрдамида провайдер К>Рда урнатилган масофадан фойдаланиш сервери RAS билан богланади ва аутентификациялашни провайдерда утайди.

Провайдернинг сервери RAS фойдаланувчининг исми буйича фойдаланувчиларнинг хисоб маълумотлари базасидан маршрутизаторнинг IP-адресини топади. Бу маршрутизатор чегара маршрутизатори ва ушбу фойдаланувчининг локал тармокдан масофадан фойдаланиш сервери хисобланади. Бу маршрутизатор билан провайдер сервери RAS Intrenet оркали PPTP протоколи буйича сессия утказади. Провайдернинг сервери

RAS локал тармокдан масофадан фойдаланиш серверига фойдаланувчининг идентификаторини ва бошка маълумотларни узатади. Улар асосида бу сервер CHAP протоколи буйича фойдаланувчини яна аутентификациялайди. Агар фойдаланувчи иккинчи аутентификациялашдан (бу унинг учун шаффоф булади) муваффакиятли утса, провайдернинг RASн бу тугрида фойдаланувчини PPP протокол буйича огохдантиради ва сунгра, провайдернинг масофадан фойдаланувчи сервери ва локал тармок, орасида химояланган виртуал канал шаклланади.

Масофадан фойдаланувчининг компьютери локал тармок, IP, IPX, ёки NetBIOS билан узаро алока пакетларини PPP кадрларига жойлаб провайдернинг масофадан фойдаланувчи сервери RASra узатади. Провайдернинг RASн аталган адрес сифатида чегара маршрутизатори адресини, манба адреси сифатида узининг шахсий IP-адресини курсатган хрлда PPP кадрларининг IP пакетларга инкапсуляциясини амалга оширади. Провайдернинг масофадан фойдаланувчи сервери ва локал тармок, орасида узатишга аталган PPP пакетлари симметрик шифрда шифрланади. Бунда симметрик махфий калит сифатида CHAP протоколи буйича аутентификациялаш учун провайдер RASnHHHr хисоб маълумотларни базасида сакланувчи фойдаланувчи паролининг дайджести ишлатилади. Симметрик шифрлаш алгоритмлари сифатида DES ёки RC-4 алгоритм ишлатилади.

Тавсиф этилган вариант кенг таркалмади, чунки протокол PPTP, асосан, Microsoft компаниясининг махсулотларида - RAS Windows NT 4.0 нинг мижоз ва сервер кисмларида, хамда RAS Windows 98/XPнинг мижоз кисмида амалга оширилган. Провайдерлар масофадан фойдаланиш сервери сифатида одатда RAS Windows NTra нисбатан кувватлирок, воситалардан фойдаланади. Бунда протокол PPTP Internet провайдерларининг масофадан фойдаланиш серверлари RAS оркали доимо мададланмайди. Ундан ташк,ари бу схемада маълумотлар фойдаланувчи компьютери ва Intrenet провайдери орасида х,имояланмаган х,олда узатилади, натижада унинг хавфсизлиги жиддий ёмонлашади.

Microsoft компанияси томонидан PPTP протоколини куллашнинг яна бир бошк,а схемаси таавсия этилган. Бу схемага биноан PPTP протоколи-

нинг провайдернинг масофадан фойдаланиш сервери томонидан мададланиши талаб этилмайди. Туннеллашнинг бу варианти (8.13-расм) кенг таркалди.

Таъкидлаш лозимки, бу схемада корпоратив тармокнинг чегара маршрутизатори, олдинги схемадагидек PPTP протоколни мададлаши шарт. Бундай маршрутизатор сифатида, хусусан, RAS хизмати урнатилган дастурий маршрутизатор Windows NT 4.0 ишлатилиши мумкин. Умуман, RAS хизмати ва PPTP протоколи ишлайдиган, масофадаги мижоз компьютер ива корпоратив тармок, ичидаги компьютер орасида химояланган канални яратиш мумкин.

Ушбу схемага биноан фойдаланувчи икки марта масофадан уланишни урнатиши лозим. Биринчи марта фойдаланувчи провайдернинг масофадан фойдаланиш серверига модем буйича кунгирок, килиб, PPP протоколи буйича у билан алока урнатади ва провайдер ISP томонидан мададланувчи протоколларнинг бирига (PAP ёки CHAP) ёки терминал диалогига мувофик, аутентификациядан утади. ISP провайдерида аутентификациядан муваффак,иятли уттанидан сунг фойдаланувчи локал тармокдан масофадан фойдаланиш сервери билан, унинг IP-адресини курсатиб уланишни урнатади. Натижада масофадаги компьютер ва локал тармок, RAS орасида PPTP протоколи буйича сессия урнатилади. Мижоз яна, энди узининг корпоратив тармоги серверида аутентификацияланади. Масофадан фойдаланиш сервери фойдаланувчининг хакикийлигини узининг х,исоб маълумотлари базаси асосида текширади. Муваффакиятли аутентификациялашдан сунг ахборотни х,имояланган алмашиш жараёни бошланади.

Криптохимояланган туннелнинг чегара курилмаларининг узаро алок,аси учун PPTP протоколида бошк,арувчи хабарлар кузда тутилган булиб, бу бошк,арувчи хабарлар туннелни урнатиш, мададлаш ва узиш учун аталган. Бошк,арувчи хабарларни алмашиш мижоз ва PPTPнинг сервери орасида урнатилувчи TCP-уланиш буйича амалга оширилади. Бу уланиш буйича узатиладиган пакетларда канал сатхи сарлавх,аси билан бир к,аторда IP протоколининг сарлавхаси, TCP протоколининг сарлавхаси ва пакет маълумотлари сох,асидаги PPTPнинг бошкарувчи хабари булади.

L2F протоколы Cisco System компанияси томонидан OSI моделининг канал сатхида химояланган виртуал тармок, куриш учун, PPTP протоколига альтернатива сифатида ишлаб чикилган. L2F протоколи турли тармок, протоколлари томонидан мададланиши билан ажралиб туради ва Internet провайдерлари учун фойдаланишда анча кулай. L2F протоколи масофадаги фойдаланувчи компьютери билан провайдер сервери алокасини ташкил этишда масофадан фойдаланишниниг турли протоколларини (PPP, SLIP ва х,.) ишлатишга йул куяди. Туннел оркали пакетларни ташишда ишлатилувчи очик, тармок, IP протоколи асосида ва бошка, хусусан X.25 протоколи асосида ишлаши мумкин.

L2F протоколи куйидаги хусусиятларга эга:

хакикийликни текширувчи муайян протоколга катъий богланмаганликни тахминловчи аутентификациялаш муолажаларининг мосланувчанлиги;

- охирги тизимлар учун шаффофлиги, яъни локаль тармокнинг ишчи станциялари ва масофадаги тизимга химоялаш серверидан фойдаланиш учун махсус дастурий таъминот талаб этилмайди;

- воситалар учун шаффофлиги, яъни масофадаги фойдаланувчиларни авторизациялаш локал тармокнинг масофадан фойдаланиш серверига фой даланувчиларни бевосита уланишига ухшаб амалга оширилади;

- аудитнинг туликлиги, яъни локал тармок, серверидан фойдаланиш ходисасини кайдлаш нафак,ат масофадан фойдаланиш сервери тмонидан, балки провайдер сервери томонидан хам амалга оширилади.

L2F протоколининг спецификациясига мувофик, химояланган туннелни хосил килишда куйидаги протоколлар ишлатилади:

- дастлабки инкапсуляцияланувчи протокол - бу протокол (IP, IPX, ёки NetBEUI) асосида локал тармок, ишлайди;

- протокол - "пассажир" - бу протоколга дастлабки протокол инкапсуляцияланади ва бу протоколнинг узи хам очик, тармок, оркали масофадан фойдаланганда инкапсуляцияланаши мумкин; PPP протоколи тавсия этилади;

- бошкарувчи (инкапсуляцияловчи) протокол, туннелни яратишда, мададлашда ва узишда ишлатилади (бундай протокол сифатида L2F ишлатилади);

- провайдер протоколи, инкапсуляцияланувчи протоколларни (даст-лабки протокол ва протокол - "пассажир") ташишда ишлатилади; энг куп таркалган провайдер протоколи IP протоколидир.

Таъкидлаш лозимки, L2F технологиясидан фойдаланилганда провайдернинг масофадан фойдаланиш сервери фойдаланувчини аутентификациялашни факат виртуал канал яратилиши зарурлигини аникдаш ва исталган локал тармокнинг масофадан фойдаланиш сервери адресини топишда ишлатади. Хдкикийликни якуний текшириш локал тармокнинг масофадан фойдаланиш сервери томонидан, у билан провайдер сервери уланганидан сунг, бажарилади.

L2F протоколининг куйидаги камчиликларини курсатиш мумкин:

- унда IP протоколининг жорий версияси учун ахборот алмашинувининг охирги нукталари орасида криптохимояланган туннел яратиш кузда тутилмаган;

- виртуал химояланган канал факат провайдернинг масофадан фойдаланиш сервери ва локал тармокнинг чегара маршрутизатори орасида яратилиши мумкин, бунда масофадаги фойдаланувчи компьютери билан провайдер сервери орасидаги жой очик, крлади.

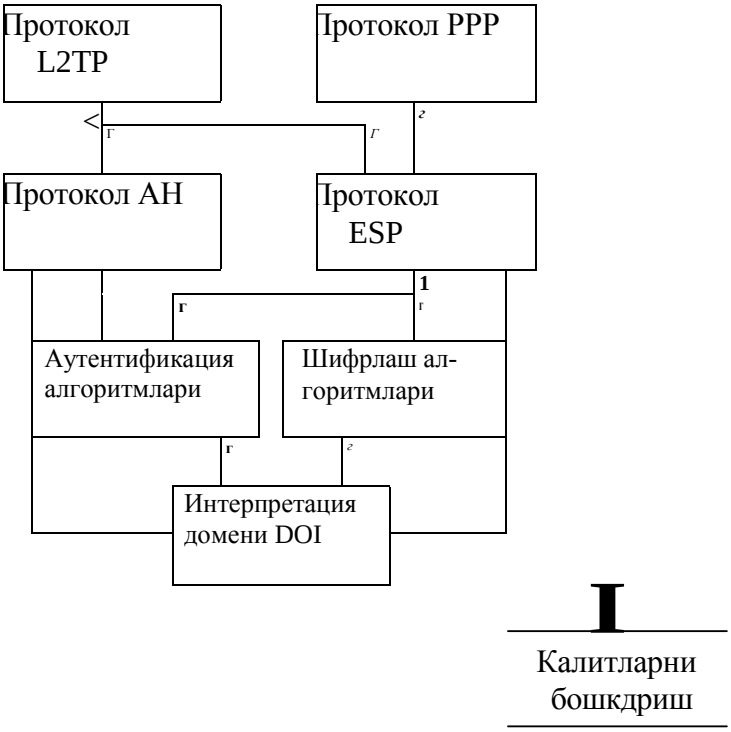
Хрзирда L2F протоколи Internet стандарта лойихаси макрмига эга булган L2TP протоколига сингдирилган.

L2TP протоколи IETF ташкилотида Microsoft ва Cisco Systems компаниялари мададида ишлаб чик,илган. L2TP протоколи ихтиёрий мухитли умуммак,сад тармок, орк,али PPP-трафикни х,имояланган туннеллаш протоколи сифатида ишлаб чикилган.

PPTPдан фаркли х,олда L2TP протоколи IP протоколига богланган эмас, шу сабабали ундан пакетларни коммутацияловчи тармокдарда, масалан ATM (Asynchronous Transfer Mode) ёки кадрларни ретрансляцияловчи (frame relay) тармокдарда фойдаланиш мумкин.

L2TP протоколида PPTP ва L2F протоколларининг нафакат яхши хусусиятлари бирлаштирилган, балки янги функциялар, жумладан IPSec протоколлари стекининг AH ва ESP протоколлари билан ишлаш имконияти кушилган.

L2TP протоколининг архитектураси 8.14-расмда келтирилган.



8.14 -расм. L2TP протоколининг архитектураси

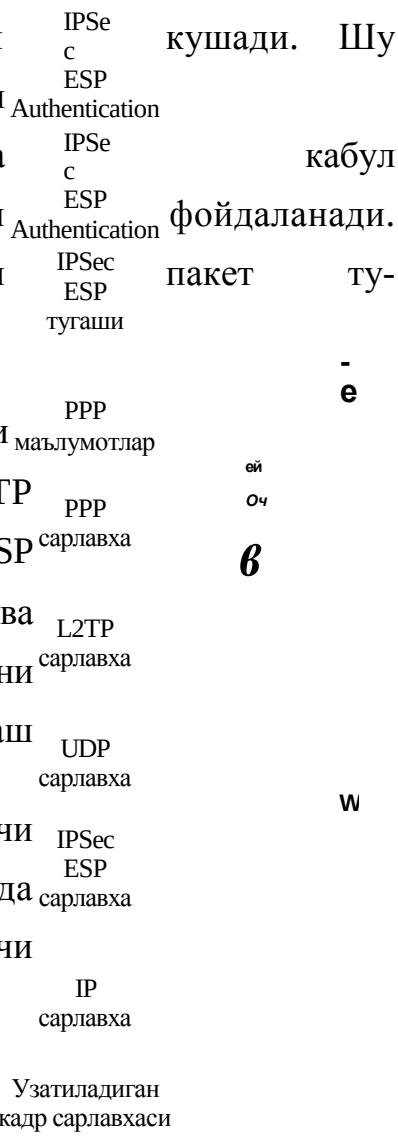
AH ва ESP протоколлари фойдаланувчиларнинг, келишилган хрлда, шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларини ишлатишларига йул куяди. Интерпретация домени DOT (Domain of Interpretation) ишлатилувчи ва алгоритмларнинг бирга ишлашини таъмиМавджги буйича, гибрид протокол L2TP масофадаги фойдаланувчиларни аутентификациялаш, химояланган виртуал уланишни яратиш ва маълумотлар окимларини бошк,ариш функциялари билан кенгайтирилган PPP протоколидир.

L2TP протоколи транспорт сифатида UDP протоколини ишлатади ва туннелни бошкаришда ва маълумотларни ташишда хабарларнинг бир хил форматидан фойдаланади.

PPTP протоколидагидек, L2TP протоколи туннелга узатиш учун пакетни йигишда аввал PPP ахборот маълумотлари майдонига PPP сарлавхдсини, сунгра L2TP сарлавхасини кушади. Шу тарика олинган пакет UDP протокол томонидан инкапсуляцияланади. L2TP протокол жунатувчи ва кабул килувчи порти сифа-тида UDP-портдан фойдаланади. 8.15-расмда L2TP туннели буйича жунатилувчи пакет тузилмаси келтирилган.

IPSec протоколлар стеки хавфсизлиги сиёсатининг танланган хилига боглик, хрлда L2TP протоколи UDP-хабарни шифрлаши ва унга ESP (Encapsulation Security Pay1oac1)нинг сарлавхасини ва охирини хамда IPSec ESP AuthenticationHHHr охирини кушиши мумкин. Сунгра IPra инкапсуляциялаш бажарилади. Таркибида жунатувчи ва кабул килувчи адрес-лари булган IP-сарлавха кушилади. Охирида L2TP маълумотларни узатишга тайёрлаш учун иккинчи PPP-инкапсуляциялашни бажаради.

Компьютер - кабул килувчи маълумотларни кабул килади. PPPнинг сарлавхаси ва охирини ишлайди. IP сарлавхани олиб ташлай-ди. IPSec ESP Authentication ёрдамида IP нинг ахборот майдони аутентификацияланади. IPSec ESP протоколи эса пакетнинг расшифровкасида ёрдам беради. Кейин компьютер UDP сарлавхасини ишлайди ва туннелни идентификациялаш учун L2TP сарлавхасидан фойдаланади. Энди PPP пакетнинг таркибида факат фойдали маълумотлар булади, улар ишланади ва курсатилган кабул килувчига юборилади.



8.15-расм. L2TP туннели бўйлаб жўнатиладиган пакет тузилмаси

L2TP протоколи "фойдаланувчи" ва "компьютер" сатхдарда аутентификациялашни таъминлайди, х,амда маълумотларни аутентификациялайди ва

шифрлайди. Мижозларни ва VPN серверларини аутентификациялашнинг биринчи боскичида L2TP сертификация хизматидан олинган локал сертификатлардан фойдаланади. Мижоз ва сервер сертификатлар билан алмашишади ва химояланган уланиш ESP SA (Security Association)НН яратишади.

L2TP компьютерни аутентификациялашни тугатганидан сунг, фойдаланувчи сатхда аутентификациялашда фойдаланувчи исмини ва паролни очик, куринишда узатувчи хар кандай протокол, хатто PAP, ишлатилиши мумкин. Бу тамомила хавфсиз, чунки L2TP бутун сессияни шифрлайди. Аммо фойдаланувчини аутентификациялашни, компьютер ва фойдаланувчини аутентификациялашда турли калитлардан фойдаланувчи MS CHAP ёрдамида утказиш хавфсизликни ошириш мумкин.

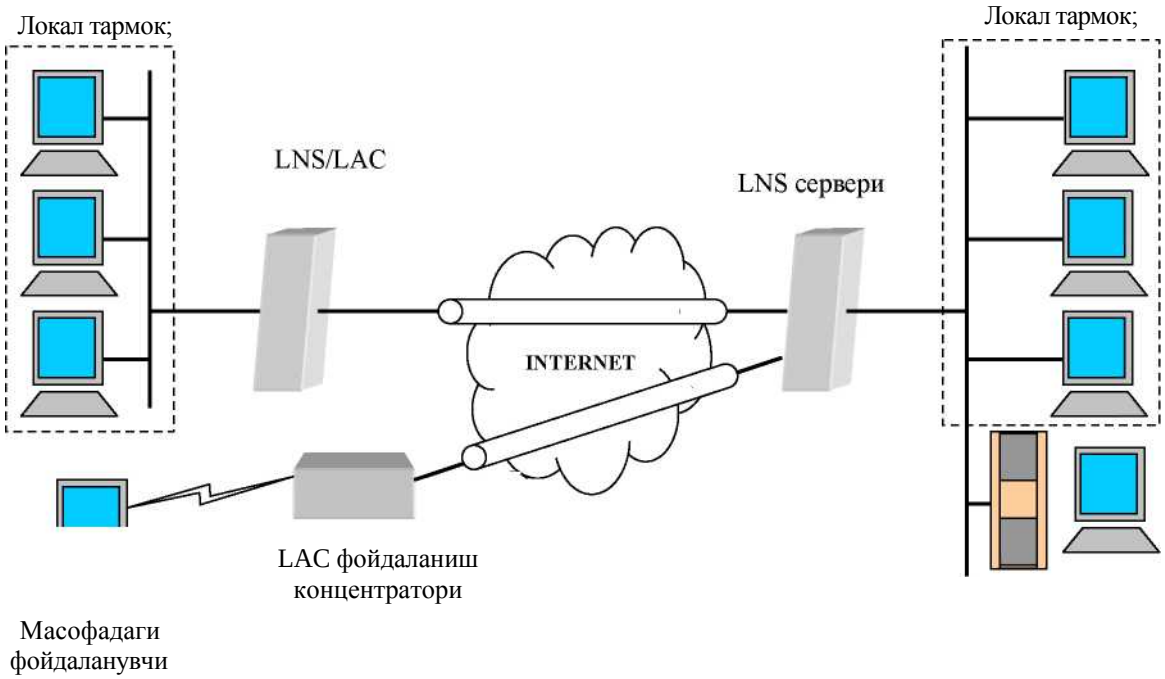
L2TP протоколининг тахмини буйича провайдернинг масофадан фойдаланиш сервери ва корпоратив тармок, маршрутизатори орасида туннел хрсил килувчи схемалардан фойдаланилади. Бу протокол олдингиларидан (PPTP ва L2F протоколларидан) фаркди хрлда охирги абонентлар орасида, хар бири алохида иловага ажратилиши мумкин булган, бир неча туннелни бирданига очиш имкониятини такдим этади. Бу хусусият туннеллашнинг мосланувчанлигини ва хавфсизлигини таъминлайди.

L2TP протоколининг спецификациясига биноан провайдернинг масофадан фойдаланиш сервери ролини, L2TP протоколининг мижоз кисмини амалга оширувчи ва масофадаги фойдаланувчига унинг локал тармогидан Internet оркали тармокди фойдаланишни таъминловчи, фойдаланишнинг концентратори LAC (L2TP Access Concentrator) бажариши лозим. Локал тармокнинг масофадан фойдаланиш сервери сифатида PPP протоколи билан бирга ишлай олувчи платформаларда ишловчи тармок, сервери LNS (L2TP Network Server)flaH фойдаланилади (8.16-расм).

PPTP ва L2F протоколларидек L2TP протоколида химояланган виртуал канални шакллантириш уч боск,ичда амалга оширилади:

- локал тармок,нинг масофадан фойдаланиш сервери билан уланишни урнатиш;
- фойдаланувчини аутентификациялаш;

- хдмояланган туннелни конфигурациялаш.



8.16-расм. L2TP протоколи асосида туннеллаш схемаси.

Биринчи боскичда локал тармокнинг масофадан фойдаланиш сервери билан уланишни урнатиш учун масофадаги фойдаланувчи провайдер ISP билан PPP - улашни бошлаб беради. Провайдер сервери КРда ишловчи фойдаланиш концентратори бу уланишни кабул килади ва канал PPPни урнатади. Сунгра фойдаланувчи концентратори LAC охирги узел ва унинг фойдаланувчисини кисман аутентификациялайди. Провайдер ISP факат фойдаланувчининг исмидан фойдаланган хрлда унга L2TP туннеллаш сервисининг кераклигини х,ал килади. Агар бундай сервис керак булса, фойдаланиш концентратори LAC туннели уланиш урнатилиши лозим булган тармок, сервери LNS адресини аниклашга утади. Фойдаланувчи ва фойдаланувчи тармогига хизмат курсатувчи сервер LNS орасидаги мувофикликни аниклашнинг кулайлигини таъминлаш мак,садида провайдер ISP томонидан узининг мижозлари учун мададланувчи маълумотлар базасидан фойдаланиш мумкин.

LNS серверининг IP-адреси аникланганидан сунг Ь2ТРнинг бу сервер билан туннели бор ёки йуклиги текширилади. Агар бундай туннел булмаса, у урнатилади. Провайдернинг фойдаланиш концентратори LAC ва локал

тармокнинг тармок, сервери LNS орасида L2TP протокол буйича сессия урнатилади.

Транспортга узаро алоканнинг "нукта-нукта" пакет режимини мададалаши талаби куйилади. LAC ва LNS орасида туннел яратишда бу туннел доирасида янги уланишга чакириш идентификатори Call ID деб аталувчи идентификатор берилади. Концентратор LAC тармок, серверига ушбу Call ID билан чакирик, хусусидаги билдириш булган пакет жунатади. LNS сервери чакирикни кабул килиши ёки рад этиши мумкин.

Иккинчи боскичда локал тармокнинг тармок, сервери LNS фойдаланувчини аутентификациялаш жараёнини бажаради. Бунинг учун аутентификациялашнинг стандарт алгоритмларидан бири, хусусан CHAP алгоритми ишлатилиши мумкин. Таъкидлаш лозимки, L2TP протоколининг спецификациясида аутентификациялаш усулларининг тавсифи келтирилмаган. Чакирик, хусусидаги билдириш таркибида тармок, сервери LNS томонидан фойдаланувчини аутентификациялаш учун ахборот булиши мумкин. Бу ахборотни концентратор LAC фойдаланувчи билан мулок,от жараёнида йигади. Аутентификациялашнинг CHAP протоколидан фойдаланилганда билдириш пакетида чак,ириш-сузи, фойдаланувчи исми ва унинг жавоби булади. PAP протоколи учун бу ахборот фойдаланувчи исми ва шифрланмаган паролдан иборат булади. Тармок, сервери LNS бу ахборотдан, масофадаги фойдаланувчини уз маълумотларини кайтадан киритишга мажбур килмаслик ва аутентификациялашнинг к,ушимча циклини бажармаслик максадида, бирданига фойдаланиш мумкин.

Аутентификация натижаси жунатилишида тармок, сервери LNS хам фойдаланиш концентратори LACra фойдаланувчи узелининг 1P-адресини узатиши мумкин. Мохияти буйича фойдаланиш концентратори LAC масофадаги фойдаланувчи узели ва локал тармокнинг тармок, сервери орасида воситачи вазифасини бажаради. Масофадаги узелга корпоратив тармокнинг адреслар пулидан адреснинг ажратилиши фойдаланувчига провайдер адреслар пулидан оддий адрес олинишидаги нок,улайликлардан кутилишига имкон беради.

Учинчи боскичда провайдернинг фойдаланиш концентратори LAC ва локал тармокнинг сервери LNS орасида химояланган туннел яратилади. Натижада инкапсуляцияланган кадрлар PPP туннел орк,али концентратор LAC ва тармок, сервери LNS орасида икала йуналишда узатилиши мумкин. Масофадаги фойдаланувчидан PPP кадри келганида концентратор LAC ундан кадрни крплаган байтларни, назорат йигинди байтларини чикариб ташлайди, сунгра уни L2TP протокол ёрдамида тармок, протоколига инкапсуляциялайди ва туннел оркали тармок, сервери LNSra жунатади. LNS сервер L2TP протоколдан фойдаланиб, келган пакетдан PPP кадрни чикариб олиб ипшайди.

Туннелнинг зарурий кийматларини созлаш бошкариш хабарлари ёрдамида амалга оширилади. L2TP протоколи хар кандай пакетни коммутацияловчи транспорт устидан ишлаши мумкин. Умумий хрлда, бу транспорт, масалан UDP протоколи, пакетларни кафолатли етказиш ни таъминламайди. Шу сабабли L2TP протоколи бу масалаларни хар бир масофадаги фойдаланувчи учун туннел ичида уланишларни урнатиш муолажаларидан фойдаланиб, мустакил х,ал этади.

Таъкидлаш лозимки, L2TP протоколи криптох,имоянинг муайян усулларини белгиламайди ва шифрлашни турли стандартларидан фойдаланиш мумкинлигини фараз килади. Агар х,имояланган туннелнинг 1P-тармокда шакллантирилиши режалаштирилган булса, криптох,имояни амалга оширишда IPSec протоколидан фойдаланилади. L2TP протоколи PPP алгоритмига нисбатан маълумотларни химоялашнинг юк,ори савиясини таъминлайди, чунки унда 3DES (Triple Data Encryption Standard) шифрлаш алгоритми ишлатилади. Агар х,имоянинг бундан юк,ори савияси керак булмаса битта 56 хонали калитли DES алгоритмидан фойдаланиш мумкин. Ундан ташк,ари L2TP протоколи HMAC (Hash Massage Authentication Code) алгоритми ёрдамида маълумотларни аутентификациялашни таъминлайди. Аутентификациялаш учун бу алгоритм узунлиги 128 хонага тенг булган "хэш"ни яратади.

Шундай к,илиб, PPTP ва L2TP протоколларининг функционал имкониятлари турлича, PPTP протоколи факат IP-тармокдарда ишлатилиши

мумкин ва унга туннелни яратиши ва ишлатиши учун алохида TCP уланиш зарур. L2TP протоколи нафакат IP-тармокларда ишлатилиши мумкин, туннелни яратиш ва у оркали маълумотларни ташишда хизматчи хабарлар бир хил формат ва протоколлардан фойдаланади. L2TP протоколи ташкилот учун мухим булган маълумотларнинг карийб 100%ли хавфсизлигини кафолатлаши мумкин.

L2TP протоколининг камчилиги сифатида куйидагиларни курсатиш мумкин:

- L2TP протоколини амалга оширишда ISP провайдерларнинг мадади зарур;

- L2TP трафикни танланган туннел доирасида чегаралайди ва фойдаланувчиларнинг InternetHHHr бошка кисмларидан фойдаланишига имкон бермайди;

- L2TP протоколида IP протоколининг жорий версияси учун ахборот алмашинувнинг охирги нукталари орасида криптохимояланган туннел яра тиш кузда тутилмаган;

- Ь2TPнинг таклиф этилган спецификацияси стандарт шифрлашни факат IP-тармокдарда IPSec протоколи ёрдамида таъминлайди.

Сеанс сатуида уимояланган еиртуал каналларни шакллантириш протоколлари

Химояланган виртуал каналларини шакллантириш мумкин булган OSI моделининг энг юкрри сатхи - бешинчи - сеанс сатхддир. Сеанс сатхдда химояланган виртуал тармокни куришда ахборот алмашинувини криптографик химоялаш, жумладан, аутентификациялаш х,амда узаро алок,а томонлари орасида воситачиликнинг к,атор функцияларини амалга ошириш имконияти пайдо булади. Ха^ик,атан, OSI моделининг сеанс сатхи мантик,ий уланишларни урнатишга ва бу уланишларни бошкаришга жавобгар. Шу сабабли, бу сатхда суралган уланишларнинг жоизлигини текширувчи ва тармоклараро х,аракатлар х,имоясининг бошк,а функцияларининг бажарилишини таъминлаовчи дастур-воситачилардан фойдаланиш имконияти мавжуд.

Сеанс сатх,ида х,имояланган виртуал канални шакллантириш протоколи химоянинг татбик,ий протоколлари х,амда турли сервисларни такдим

этувчи юкрри сатх, протоколлари (HTTP, FTP, POPS, SMTP ва х,. протоколлар) учуй шаффофдир. Аммо, сеанс сатх,ида юкрри сатхди протоколларни амалга оширувчи иловаларга бевосита богликлик бошланади. Шунинг учуй мазкур сатхга мое келувчи ахборот алмашиш протоколини амалга ошириш куп хрлларда юкрри сатхди иловаларга узгартиришлар киритилишини талаб этади.

Сеанс сатх,ида ахборот алмашишда SSL протоколи кенг таркалган. Сеанс сатхида узаро алока томонлари орасида воситачилик функцияларини бажариш учун IETF ташкилоти томонидан стандарт сифатида SOCKS протоколи кабул килинган.

SSL протоколи Netscape Communication компанияси томонидан мижоз-сервер иловаларида ахборотни химояланган алмашишни амалга ошириш учун ишлаб чикилган. Хрзирда SSL протоколи OSI моделининг сеанс сатхида ишловчи химояланган канал протоколи сифатида ишлатилади. Бу протокол ахборот алмашиш хавфеизлигини таъминлашда ахборотни химоялашнинг криптографик усулларидан фойдаланади. 88Ьпротоколи тармокнинг иккита абоненти орасида химояланган канал к,уришнинг барча функцияларини жумладан, уларни аутентификациялаш, узатилувчи маълумотларнинг конфиденциаллигини ва яхлитлигини таъминлаш функцияларини бажаради. Асимметрик ва симметрик криптотизимлардан комплекс фойдаланиш технологияси SSL протоколининг ядроси х,исобланади.

SSLfla иккала томоннинг узаро аутентификациялаш фойдаланувчиларнинг (мижоз ва сервер) махсус сертификация марказларининг ракамли имзоси билан тасдикланган очик, калитларининг рак,амли сертификатлари билан алмашиш орк,али бажарилади. SSL протоколи хамма к,абул к,илган X.509 стандартларга мое келувчи сертификатларни, хамда сертифкатларни беришда ва х,ак,ик,ийлигини текширишда ишлатилувчи PKI очик, калитлари инфратузилмаларининг стандартини мададлайди.

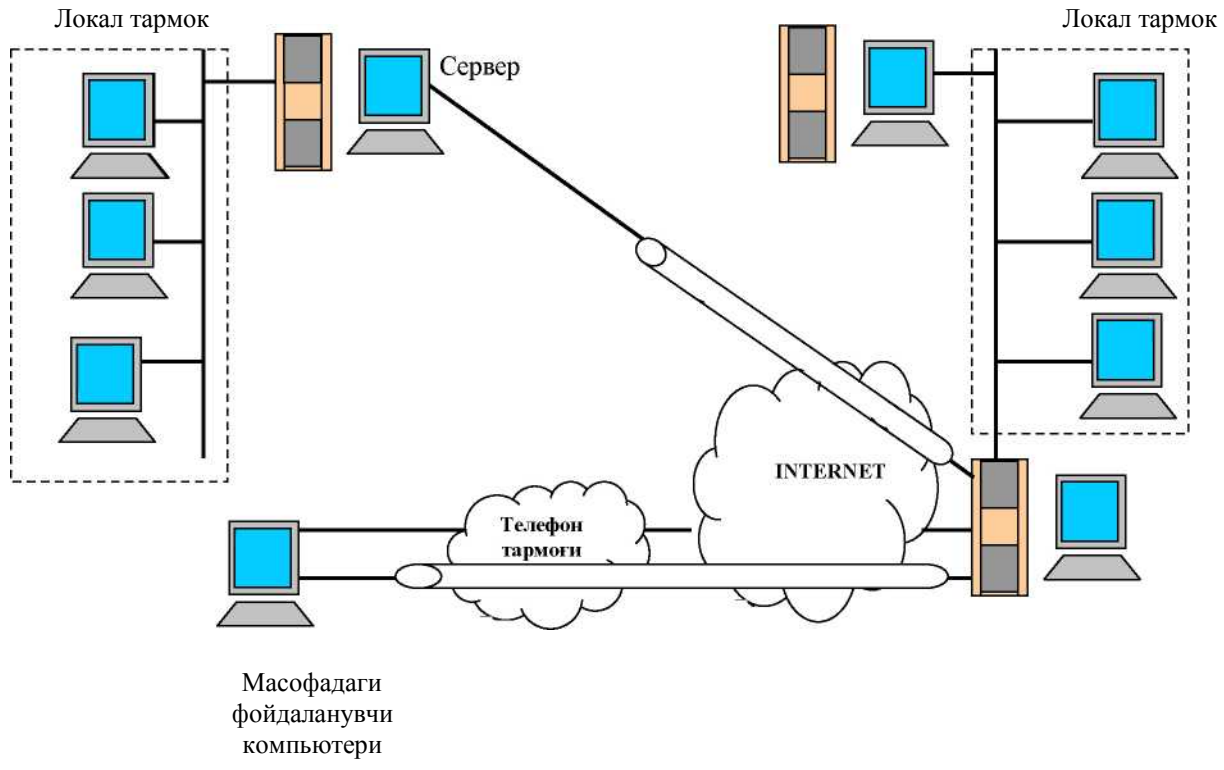
Конфиденциаллик уланиш урнатилишида томонлар алмашинадиган симметрик сессия калитларида узатилувчи хабарларни шифрлаш орк,али таъминланади. Сессия калитлари хам шифрланган куринишда узатилади. Бунда улар абонентларнинг сертификатларидан чикариб олинган очик, ка-

литларда шифрланади. Ахборотларни шифрлашда симметрик калитларнинг ишлатилишига асосий сабаб-симметрик калитларда шифрлаш ва расшифровка килиш жараёнининг тезлиги асимметрик калитлар ишлатилишидагига Караганда юкррилиги.

Айланувчи ахборотнинг хакикийлиги ва яхлитлиги электрон ракамли имзони шакллантириш ва текшириш эвазига таъминланади.

Асимметрик шифрлаш алгоритмлари сифатида RSA, хамда Диффи-Хеллман алгоритмлари ишлатилади. Симметрик шифрлаш алгоритмлари сифатида эса RC2, RC4, DES хамда Triple DES алгоритмлари ишлатилади. Хэш функцияларини хисоблашда MD5 ва SHA-1 стандартлари ишлатилиши мумкин. SSL протоколининг 3.0 версиясида криптографик алгоритмлари туплами кенгайтирилувчи хисобланади.

SSL протоколига мувофик, криптохимояланган туннеллар виртуал тармокнинг охирги нукталари орасида яратилади. Хар бир химояланган туннелни бошлаб берувчилари-туннел охирги нукталаридаги компьютерларда ишловчи мижоз ва сервер (8.17-расм).



8.17-расм. SSL протоколи асосида шаклланган криптощмояланган туннеллар.

Хдмояланган уланишни шакллантиришда ва мададлашда SSL протоколи мижоз ва сервер узаро алокасининг куйидаги боскичларини кузда тутади:

SSL сессиясини урнатиш; химояланган узаро алока. SSL сессияни урнатиш жараёнида куйидаги масалалар ечилади:

- томонларни аутентификациялаш;
- химояланган ахборот алмашинувида ишлатилувчи криптографик алгоритмлар ва зичлаштириш алгоритмларини мувофиклаштириш;
- умумий махфий мастер-калитни шакллантириш;
- ахборот алмашишни криптографик химоялаш учуй шакллантирилган мастер-калит асосида умумий махфий сеанс калитларини генерациялаш.

Кул беришиш муолажаси деб хам аталувчи SSL-сессияни урнатиш муолажаси ахборот алмашишни бевосита химоялашдан олдин пухта ишланади ва SSL протоколи таркибига кирувчи бошлангич саломлаш (Hand-Shake Protocol) протоколи буйича бажарилади.

Мижоз ва сервер орасида кайта уланиш урнатилишида томонлар, узаро келишув буйича, олдинги умумий сир асосида янги сеанс калитларини шакллантиришлари мумкин (ушбу муолажа SSL-сессиянинг давоми деб аталади).

SSL 3.0 протоколи аутентификациялашнинг к,уйидаги учта режимини мададлайди:

- томонларни узаро аутентификациялаш;
- мижозни аутентификацияламасдан серверни бир томонлама аутен тификациялаш ;
- тулик, анонимлик.

Охирги вариантдан фойдаланилганда томонларнинг х,ак,ик,ийлигини кафолатламасдан ахборот алмашиш хавфсизлиги таъминланади. Бу х,олда узаро алокадаги томонлар, алок,а к,атнашчиларини алмаштириб куйиш билан боглик, хужумлардан химояланмайдилар.

SSL протоколига мувофик, узаро алокадаги томонларни аутентификациялашда ва умумий махфий калитни шакллантиришда купинча RSA алгоритмидан фойдаланилади.

Очик, калитлар ва уларнинг эгалари орасидаги мувофиклик махсус сертификация марказлари томонидан берилувчи ракамли сертификатлар ёрдамида урнатилади. Сертификат таркибида куйидаги ахборот булган маълумотлар блокидир:

- сертификация марказининг номи;
- сертификат эгасининг исми;
- сертификат эгасининг очик, калиги;
- сертификатнинг таъсир муддати;
- идентификатор ва сертификатни ишлашда фойдаланиладиган криптоалгоритмнинг параметрлари;
- сертификат таркибидаги барча маълумотларни тасдикдовчи серти фикация марказининг ракамли имзоси.

Сертификат таркибидаги сертификация марказининг ракамли имзоси очик, калит ва унинг эгасининг хакикийлигини ва бир маънода мослигини таъминлайди. Сертификация маркази очик, калитларнинг хакикийлигини тасдикдовчи нотариус ролини утайди. Натижада бу калит эгаларига химояланган узаро алока хизматидан, олдиндан шахсий учрашувсиз фойдаланишларига имкон беради.

1999 йили SSL 3.Оверсияси урнига, SSL протоколига асосланган ва хрзирда Internet стандарта хисобланган TLS протоколи келди. SSL 3.0 ва TLS протоколлари орасидаги фарк, жуда хам жиддий эмас.

SSL ва TLS протоколларининг камчилиги - узларининг хабарларини ташишда тармок, сатх,идаги фак,ат битта - IP-протоколидан фойдаланишлари ва, демак, факат IP-тармокдарда ишлайолишлари. Ундан ташк,ари, SSL/TLSHHHr амалда к,улланиши татбик,ий протоколлар учун тула шаффоф эмас.

SSLHHHr яна бир салбий томони шундай иборатки, агар мижоз ва сервер уланишни узсалар, улар уни маълумотларнинг минимал хажмини алмашиш йули билан тиклашлари ва Session ID нинг эски параметрларидан

фойдаланишлари мумкин. Нияти бузук, одам олдинги сессиялардан бирини обрусизлантириб уни тиклаш муолажасини сервер билан утказиши мумкин. Натижада бу сессияда узатиладиган кейинги барча маълумотлар обрусизлантирилади.

Ундан ташкари, SSLfla аутентификациялашда ва ширфлашда бир хил калитдан фойдаланилади. Бу эса маълум бир хрлатларда заифликка олиб келиши мумкин. Бундай ечим турли калитлар ишлатилганига нисбатан куп статистик маълумотларни йигашта имкон беради.

SOCKS протокли OSI моделининг сеанс сатхида мижоз-сервер иловаларининг узаро алока муолажасини сервер-воситачи ёки proxy-сервер оркали ташкил этади.

Умумий хрлда, тармоклараро экранларда анъанавий ишлатилувчи дастур-воситачилар куйидаги функцияларни бажариши мумкин:

- фойдаланувчини идентификациялаш ва аутентификациялаш;
- узатилувчи маълумотларни криптохимоялаш;
- ички тармок, ресурсларидан фойдаланишни чегаралаш;
- ахборотлар окимини фильтрлаш ва узгартириш, масалан, вирусларни кидириш ва ахборотни шаффоф шифрлаш;
- чикадиган ахборот окимлари учун ички тармок, адресларини трансляциялаш.

Аввал SOCKS протоколи факат мижоз иловаларининг серверга суровларини к,айта йуналтириш, х,амда бу иловаларга олинган жавобни к,айтариш учун ишлаб чикилган эди. Ушбу муолажаларнинг узи тармок, IP-адреслари NATнн (Network Address Translation) трансляциялаш функцияларини амалга ошириш имкониятини беради. Чикувчи пакетлардаги жунатувчиларнинг IP-адресларини шлюзининг битта IP-адреси билан алмаштириш ички тармок, топологиясини ташк,и фойдаланувчилардан беркитишга имкон беради ва натижада, рухсатсиз фойдаланиш масаласи мураккаблашади. Тармок, адресларини трансляциялаш хавфсизликни ошириш билан бир каторда хусусий адреслаш тизимини мададлаш имконияти х,исобига тармок, ички адреси маконини кенгайтиришга имкон беради.

SOCKS протоколи асосида тармокди узаро алокани химоялаш буйича воситачиликнинг бошка функциялари хам амалга оширилиши мумкин. Масалан, SOCKS ахборот окимлари йуналишни назоратлашда ва фойдаланувчилар ва ахборотлар атрибутларига боглик, хрлда фойдаланишни чегаралашда ишлатилиши мумкин. SOCKS протоколининг воситачилик функцияларини бажаришдаги самарали ишлатилиши унинг OSI моделининг сеанс сатхига мулжалланганлиги билан таъминланади. Татбикий сатхдаги воситачиларга Караганда, сеанс сатхида энг юкрри тезкорликка, юкрри сатх, протоколларига (HTTP, FTP, POPS, SMTP ва х,.) боглик, булмасликка эришилади. Ундан ташкари SOCKS протоколи IP протоколга богланмаган ва операцион тизимга боглик, эмас. Масалан, мижоз иловалари ва воситачи орасида ахборот алмашишда IPX протоколи ишлатилиши мумкин.

SOCKS протоколи туфайли тармокдараро экранлар ва виртуал хусусий тармокдар турли тармокдар орасида хавфсиз узаро алокани ва ахборот алмашинувини ташкил этишлари мумкин. SOCKS протоколи ушбу тизимларни хавфсиз бошк,аришни унификацияланган стратегия асосида амалга оширишга имкон беради. Таъкидлаш лозимки, SOCKS протоколи асосида хар бир илова ва хар бир сеанс учун алох,ида х,имояланган туннел яратилиши мумкин.

SOCKS протоколи спецификациясига мувофик, тармок, шлюзига (тармокдараро экранга) урнатилувчи SOCKS - *сервер* ва хар бир фойдаланувчи компьютерга урнатилувчи SOCKS - *мижоз* фаркданади. SOCKS-сервер хар кандай татбик,ий сервер билан бу серверга мое келувчи татбикий мижоз номидан узаро алок,ани таъминлайди. SOCKS-мижоз мижоз томонидан татбик,ий серверга булган барча суровларни ушлаб крлиб уларни SOCKS-сервер узатишга аталган. Таъкидлаш лозимки, мижоз иловаларининг суровларини ва SOCKS-сервер билан узаро алокани ушлаб крлишни бажарувчи SOCKS-мижозлар универсал мижоз дастурларига урнатилиши мумкин. SOCKS-серверга сеанс (сокет) сатх,идаги трафик маълум, шунинг учун у синчиклаб назоратлаши, хусусан, фойдаланувчиларнинг муайян иловалари ишини, агар уларнинг ахборот алмашишга зарур ваколатлари булмаса, блокировка килиши мумкин. SOCKS протоколининг 4- ва 5- вер-

сиялари кенг таркалган. Хрзирда SOCKS протоколининг 5-версияси IETF ташкилоти томонидан InternetHHHr стандарти сифатида маъкулланган.

SOCKS протоколининг 4-версиясига биноан уланишни урнатишнинг умумий схемаси куйидагича:

- тармокдаги кандайдир сервер билан богланишни истаган мижоз SOCKS-сервер (ихтисослаштирилган proxy-сервер) билан уланиб унга махсус суров юборади. Бу суровда IP-адрес ва у уланиши керак булган масофадаги сервер порти булади;

- SOCKS-сервер масофадаги сервер-адресат билан уланади;

- мижоз ва масофадаги сервер уланиш занжири буйича узаро алока килади, SOCKS-сервер маълумотларни ретрансляциялайди;

SOCKS протоколининг 5-версияси туртинчи версиянинг жиддий ривожи хисобланади. У куйидаги кушимча имкониятларни амалга оширади:

- номларидан SOCKS-мижозлар мурожаат этувчи фойдаланувчиларни аутентификациялаш кузда тутилган. SOCKS-сервер SOCKS-мижоз билан аутентификациялаш усулини келишиб олишлари мумкин. Аутентификация лаш компьютер ресурсларидан фойдаланишни чегаралашга имкон беради. Икки томонлама аутентификациялаш хам жоиз хисобланади, яъни фойдаланувчи, уз навбатида, керакли SOCKS-сервер билан уланганига ишонч хрсил к,илиши мумкин;

- доменли исмларни ишлатиш жоиз хисобланади: SOCKS-мижоз SOCKS-серверга нафак,ат уланишни урнатишда керак булган компьютернинг IP-адресини, балки унинг DNS исмини хам узатиши мумкин;

- нафакат TCP-протокол, балки UDP протокол хам мададланади;

SOCKS протоколининг 5-версиясига биноан уланишни урнатишнинг умумий схемаси куйидагича тавсифланиши мумкин:

- тармокдаги кандайдир татбикий сервер билан уланиш урнатишни истаган татбикий мижознинг суровини мана шу компьютерда урнатилган SOCKS-мижоз ушлаб крлади;

- SOCKS-сервер билан уланган SOCKS-мижоз унга узи мададловчи аутентификациялашнинг барча усулларининг идентификаторларини билдиради;

- SOCKS-сервер аутентификациялашнинг кайси усулидан фойдаланишни х,ал килади (агар SOCKS-сервер SOCKS-мижоз томонидан таклиф этилган аутентификациялаш усулларидан бирортасини хам мададламаса, уланиш узилади);

- таклиф этилган аутентификациялаш усулидан бирортаси мададланса SOCKS сервер танланган усул буйича фойдаланувчини (унинг номидан SOCKS-мижоз катнашади) аутентификациялайди; муваффакиятсиз аутентификациялашда SOCKS-сервер уланишни узади;

муваффакиятли идентификациялашдан кейин SOCKS-мижоз SOCKS-серверга тармокдаги суралаётган татбикий сервер DNS исмини ёки IP-адресини узатади, сунгра SOCKS-сервер фойдаланишни чегаралашнинг мавжуд кридалари асосида ушбу татбикий сервер билан уланишни урнатиш буйича карор кабул килади;

- уланиш урнатилган хрлда татбикий мижоз ва татбикий сервер бир-бирлари билан уланиш занжири орк,али алока к,иладилар; SOCKS-сервер маълумотларни ретрансляциялайди, х,амда тармокди узаро алока хавфсизлиги буйича воситачилик функцияларини бажариши мумкин; масалан, аутен тификациялаш жараёнида SOCKS-мижоз ва SOCKS-сервер сеанс калитларини алмаштиришган булсалар, улар орасидаги барча трафик шифрланиши мумкин.

Фойдаланувчиларни SOCKS-сервер томонидан аутентификациялаш X.509 форматидаги ракамли сертификатларга ёки паролларга асосланиши мумкин. SOCKS-мижоз ва SOCKS-сервер орасидаги трафикни шифрлаш учун OSI моделининг сеансли ёки пастрок, сатхдарига мулжалланган протоколлар ишлатилиши мумкин. SOCKS-сервер фойдаланувчиларни аутенти фикациялаш, IP-адресларини трансляциялаш ва трафикни криптох,имоялашдан бошка яна к,уйидаги функцияларни бажариши мумкин:

- ички тармок, ресурсларидан фойдаланишни чегаралаш;

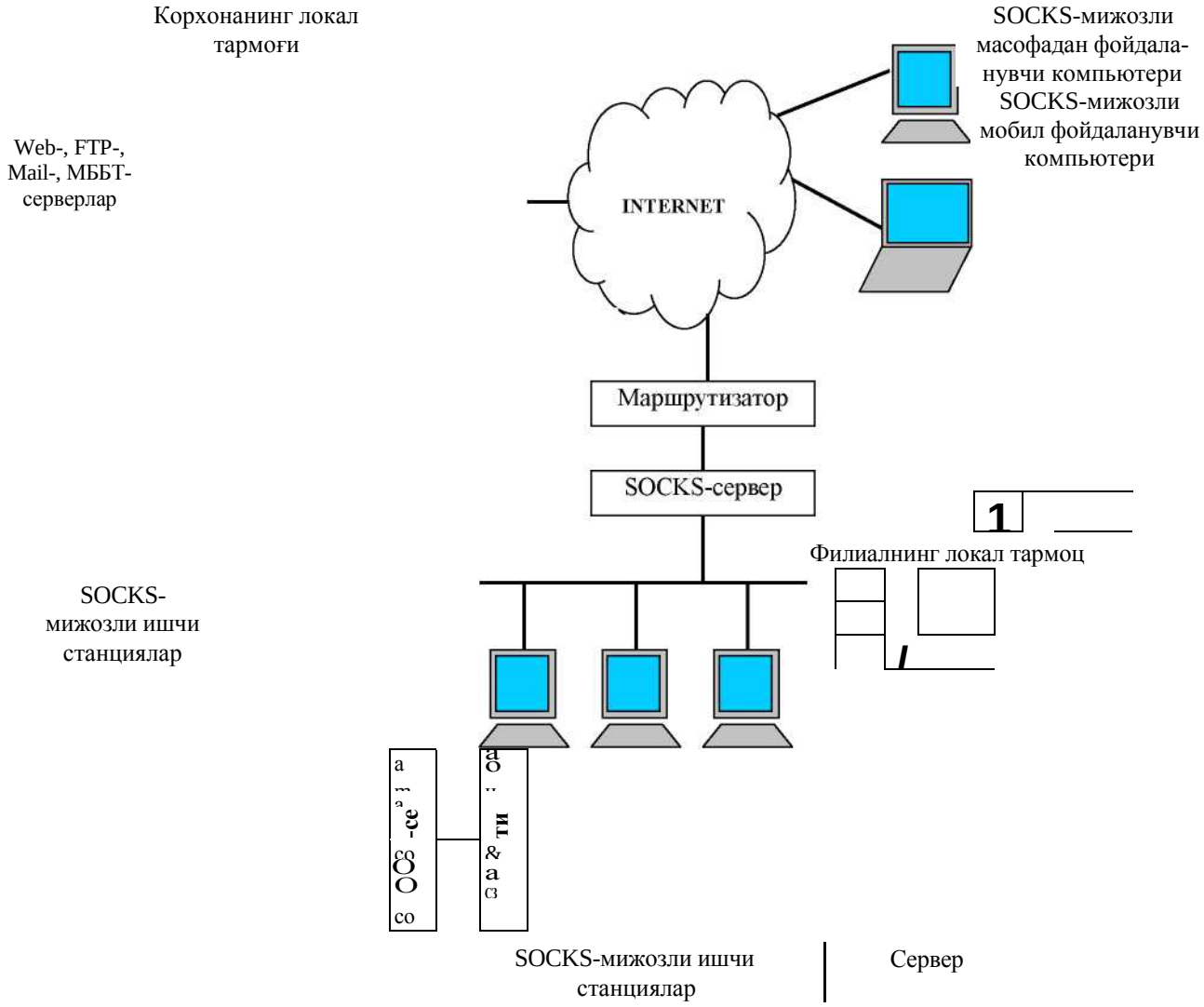
- ташк,и тармок, ресурсларидан фойдаланишни чегаралаш;

-хабарлар окимини фильтрлаш, масалан вирусларни динамик к,идириш;

- ходисаларни к,айдлаш ва уларга реакция курсатиш;

- ташки тармокдан суралган маълумотларни кэшлаш.

Шундай килиб, SOCKS протоколи буйича хдмояланган виртуал тармокларни шакллантириш учун хдр бир локал тармок, билан Internet уланган нуктадаги компьютер-шлюзда SOCKS-сервер, локал тармокдаги ишчи станцияларда ва масофадан фойдаланувчиларнинг компьютерларида эса SOCKS-мижоз урнатилади. Мох,ияти буйича, SOCKS-серверга SOCKS протоколини мададловчи тармокдараро экран сифатида караш мумкин (8.18-расм).



8.18-расм. SOCKS протоколи бўйича ўзаро алоца схемаси.

Масофадаги фойдаланувчилар Internetra коммутацияланувчи ёки аж-ратилган линиялар орк,али уланишлари мумкин. Х,имояланган виртуал тармок, фойдаланувчиси кандайдир татбик,ий сервер билан уланишга урин-ганида SOCKS-мижоз SOCKS-сервер билан узаро алокани бошлайди. Узаро

алоканинг биринчи боск,ичи тугаганидан сунг фойдаланувчи аутентифка-цияланади, фойдаланиш к,оидаси эса унинг курсатилган адресдаги компью-

терда ишлайдиган муайян тармок, иловаларига уланиш хукукига эга эканлигини курсатади. Кейинги узаро алокалар криптографик хдмояланган канал буйича юз бериши мумкин.

SOCKS-серверга, локал тармокдарни рухсатсиз фойдаланишдан химоялашдан ташкари, бу локал тармок, фойдаланувчиларининг InternetHHHr очик, ресурсларидан (Telnet, WWW, SMTP, POP ва х,.) фойдаланишларининг назорати хам юкланиши мумкин. Фойдаланиш бутунлай авторизацияланган, чунки фойдаланувчининг компьютери эмас, балки узи идентификацияланади ва аутентификацияланади. Фойдаланиш кридалар муайян ходимнинг ваколатига кура InternetHHHr маълум ресурслари билан богааништа рухсат бериши ёки бермаслиги мумкин. Фойдаланиш кридаларининг таъсири бошка параметрлар, масалан, аутентификациялаш усули ёки сутка вактига богаик, булиши мумкин. Тармокди узаро алока хавфсизлигининг янада юк,ори даражасига эришиш учун Internet томонидан фойдаланишга рухсат берилган локал тармок, серверлари, SOCKS-серверга уланувчи, химояланган очик, кием тармокни хреил к,илувчи алох,ида сегментга ажратилишлаш лозим.

8.5. IPSec протоколлар стекини химояланган виртуал хусусий тармоцлар куришда ишлатилиши

IPSec протоколи (Internet Protocol Security) асосан IP тармокларда маълумотларни хавфеиз узатишни таъминлашга аталган. IPSecHHHr ишлатилиши к,уйидагиларни кафолатлайди:

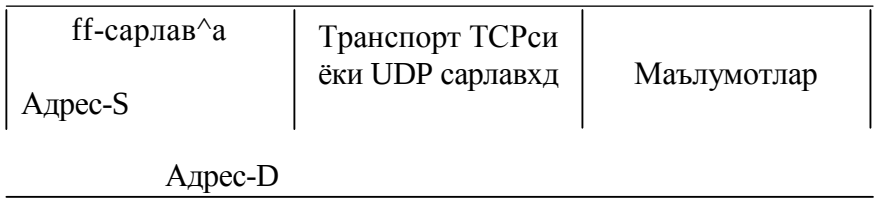
- узатилаётган маълумотларнинг яхлитлигини, яъни маълумотлар узатилишида бузилмайди, йукрлмайди ва такрорланмайди;

- жунатувчининг аутентлигини, яъни маълумотлар х,ак,ик,ий жунатувчи томонидан узатилган;

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

Таъкидлаш лозимки, маълумотлар хавфсизлиги тушунчасига одатда, яна бир талаб-маълумотларнинг фойдаланувчанлиги киритилади. Маълумотларнинг фойдаланувчанлиги деганда маълумотлар етказилишининг кафолати тушунилади. IPSec протоколлари бу масалани х,ал этмайди ва уни транспорт сатхд ISPra крлдиради. IPSec протоколлар стеки тармок, сатхида ахборот химоясини таъминлайди. Бу химоянинг ишловчи иловаларга куринмаслигига олиб келади.

IP-пакет IP тармокларда коммуникациянинг фундаментал бирлиги хисобланади. Унинг тузилмаси 8.19-расмда келтирилган. IP-пакет таркибида манба адреси S ва ахборот кабул килувчинининги адреси D, транспорт сарлавхаси, бу пакетда ташилувчи маълумотлар хили хусусидаги ахборот ва маълумотларнинг узи булади.



8.19-расм. IP-пакет тузилмаси

Аутентификациялашни, узатилувчи маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлаш максадида, IPSec протоколларининг стеки катор стандартлаштирилган криптографик технологиялар асосида курилган:

- калитларни алмаштириш очик, тармокдан фойдаланувчилар орасида махфий калитларни так,симлашнинг Диффи-Хеллман алгоритми буйича амалга оширилади;

- иккала томоннинг х,ак,ик,ийлигини кафолатлаш ва main-in-the-midle хилидаги хужумларни олдини олиш максадида Диффи-Хеллман алгоритми буйича алмашишларни имзолашда очик, калитлар криптографиясидан фойдаланилади;

- очик, калитларнинг х,ак,ик,ийлигини тасдиклашда рак,амли сертификатлар ишлатилади;

- маълумотларни шифрлашда блокли симметрик алгоритмлардан фойдаланилади;

- хэшлаш функциялари асосида ахборотларни аутентификациялаш алгоритмлари ишлатилади.

Хдмояланган канални урнатиш ва мададлашдаги асосий масалалар куйидагилар:

- фойдаланувчилар ёки компьютерларни аутентификациялаш;

- химояланган каналнинг охирги нукталари орасида узатилувчи маълумотларни шифрлаш ва аутентификациялаш;

- каналнинг охирги нукталарини маълумотларни аутентификациялашда ва шифрлашда керак буладиган махфий калитлар билан таъминлаш.

Юкррида санаб утилган масалаларни х,ал этишда IPSec тизими ахборот алмашиш хавфсизлиги воситаларининг комплексидан фойдаланади.

IPSec протоколининг аксарият амалга оширилишида куйидаги компонентлардан фойдаланилади:

- IPSecHHHr асосий протоколи. Ушбу компонент химояни инкапсуляцияловчи протокол ESP (Encapsulation Security Pay1oac1)ни ва сарлавхани аутентификацияловчи протоколи AH(Authentication Header)НН амалга оширади. У сарлавх,аларни ишлайди; пакетга кулланиладиган хавфсизлик сиёсатини аникдаш учун SPD ва SAD маълумотлар базаси билан узаро алока килади;

- калит ахборотларини алмашишни бошкариш протоколи IKE. IKE одатда фойдаланиш сатхида кулланилади (операцион тизимга урнатилгани бундан истисно);

- хавфсизлик сиёсатларининг маълумотлар базаси SPD (Security Poli су Database). Бу энг мухим компонентлардан бири булиб, пакетга кулланиладиган хавфсизлик сиёсатини белгилайди. SPD дан асосий прото кол IPSec томонидан кирувчи ва чикувчи пакетларни ишлашда фойдалани лади;

- хавфсиз ассоциацияларнинг маълумотлар базаси SPD (Security Assocition Database). Бу маълумотлар базаси кирувчи ва чикувчи ахборотни ишлаш учун хавфсиз ассоциациялар SA(Security Association) руйхатини саклайди. Чик,увчи 8Алардан чикувчи пакетларни химоялашда, кирувчи 8Алардан эса IPSec сарлавх,али пакетларни ишлашда фойдаланилади. SAD маълумотлар базаси SA билан кулда ёки калитларин бошк,ариш протоколлари IKE ёрдамида тулдирилади;

- хавфсизлик сиёсатини ва хавфсиз ассоцияцияларни бошкариш. Бу - хавфсизлик сиёсатини ва SAHH бошкарувчи иловалар.

Асосий протокол IPSec (ESP ва АНни амалга оширувчи) ТСРЯР протоколларининг транспорт ва тармок, стеклари билан узаро узвий алокада булади. IPSecHH тармок, сатхининг кисми дейиш мумкин. IPSecHHHr асосий модули иккита интерфейсни - кириш йули ва чикиш йули интерфейсларни таъминлайди. Кириш йули интерфейси кирувчи пакетлар томонидан, чикиш йули интерфейси эса чикувчи пакетлар томонидан фойдаланилади. IPSecHHHr амалга оширилиши ТСРЯР протоколлар стекининг транспорт ва тармок, сатхдари орасидаги интерфейсга боглик, булмаслиги лозим.

SPD ва SAD маълумотлар базаси IPSec ишлашига жиддий таъсир курсатади. Улардаги маълумотлар тузилмасини танлаш IPsec ишлашининг унумдорлигига таъсир этади.

1P8есдаги барча протоколларни иккита гурухга ажратиш мумкин:

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

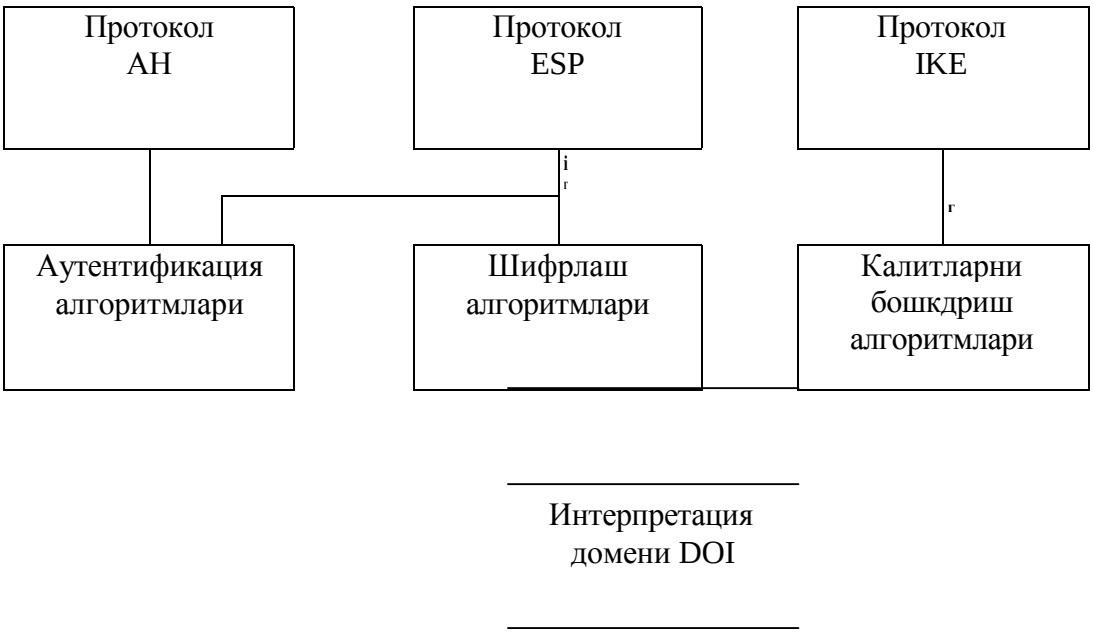
- биринчи гурух, протоколларига керакли химояланган уланишлар параметрларини автоматик тарзда мувофиклаштиришга имкон берувчи прото коллар.

IPSec ядросини учта АН, ESP ва виртуал канал ва калитларни бошк,ариш IKE параметрларини мувофикдаштирувчи протоколлар ташкил этади.

IPSecHHHr хавфсизлик воситаларининг архитектураси 8.20-расмда келтирилган.

Архитектуранинг *юцори сагщида* куйидаги протоколлар жойлашган:

- виртуал канал параметрларини мувофикдаштирувчи ва калитларни бошкариш протоколи IKE. Бу протокол химояланган каналнн инициализациялаш усулини, жумладан ишлатилувчи криптох,имоялаш алгоритмларини мувофикдаштиришни х,амда х,имояланган уланиш доирасида махфий калит ларни алмашиш ва бошкариш муолажаларини белгилайди;



8.20-расм. IP Sec протоколлари стекининг архитектураси

- сарлавхдни аутентификацияловчи протокол AH. Бу протокол маълумотлар манбаини аутентификациялашни, уларнинг, кабул килинганидан сунг, яхлитлигини ва хакикийлигини текшириш ва такрорий ахборотларнинг тикиштирилишидан химояни таъминлайди;

- химояни инкапсуляцияловчи протокол ESP. Бу протокол узатилувчи маълумотларни криптографик беркитишни, аутентификациялашни ва яхлитлигини таъминлайди хамда такрорий ахборотларнинг тикиштирилишидан химоялайди.

AH ва ESP протоколлари хар бири алохида ва биргаликда ишлатилиши мумкин. Бу протоколлар вазифаларининг кискача баёнидан куриниб турибдиики, уларнинг имкониятлари кисман бир хил.

AH протоколи факат маълумотларни яхлитлигини ва аутентификациялашни таъминлашга жавоб беради. ESP протоколи кувватлирок, хисобланади, чунки у маълумотларни шифрлаши мумкин, ундан ташкари AH протоколи вазифасини х,ам бажариши мумкин.

IKE, AH ва ESP протоколларининг узаро алок,алари к,уйидагича кечади. Аввал IKE протоколи буйича иккита нукта орасида мантик,ий уланиш урнатилади. Бу уланиш IPSec стандартларида "хавфсиз ассоциация"-Security Association, SA номини олган. Ушбу мантикий канал урнатилишида канал-

нинг охирги нукталарини аутентификациялаш бажарилади хамда маълумотларни химоялаш параметрлари, масалан, шифрлаш алгоритми, сессия махфий калиги ва х,. танланади. Сунгра хавфсиз ассоциация SA томонидан урнатилган доирада АНва ESP протоколи ишлай бошлайди. Бу протоколлар ёрдамида узатилувчи маълумотларнинг исталган химояси, танланган параметрлардан фойдаланилган хрлда, бажарилади.

IPSec архитектурасининг *урта сагщини* IKE протоколида кулланилувчи параметрларни мувофикдаштириш ва калитларни бошкариш алгоритмлари хамда АН ва ESP протоколларида ишлатилувчи аутентификациялаш ва шифрлаш алгоритмлари ташкил этади.

Таъкидлаш лозимки, IPSec архитектурасининг юкрри сатх,идаги виртуал канални химоялаш протоколлари (АН ва ESP) муайян криптографик алгоритмларга боглик, эмас. Аутентификациялаш ва шифрлашнинг куп сонли турли-туман алгоритмларидан фойдаланиш имконияти туфайли IPSec тармокни химоялашни ташкил этишнинг юкрри даражада мосланувчанлиги таъминлайди. IPSecHHHr мосланувчанлиги деганда хар бир масала учун унинг ечилишининг турли усуллари тавсия этилиши тушунилади. Бир масала учун танланган усул, одатда, бошка масалаларни амалга ошириш усулларига боглик, эмас. Масалан, шифрлаш учун DES алгоритмининг танланиши маълумотларни аутентификациялашда ишлатилувчи дайджестни хисоблаш функциясини танлашга таъсир к,илмайди.

IPSec архитектурасининг *пастки сатщ* интерпретациялаш домени DOI (Domain of Interpretation)flaH иборат. Интерпретациялаш доменининг кулланиш заруриятига куйидагилар сабаб булди. АН ва ESP протоколлари модулли тузилмага эга, яъни фойдаланувчилар узаро келишилган х,олда 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 IPSecfla ишлатиладиган протоколлар ва алгоритмлар, уларнинг параметрлари, протокол идентификаторлари ва х,. хусусидаги ахборотларни сакдайди. Мохияти

буйича интерпретациялаш домени IPSec архитектурасида фундамент ролини бажаради. AH ва ESP протоколларида аутентификациялаш ва шифрлаш алгоритмлари сифатида миллий стандартларга мое келувчи алгоритмлардан фойдаланиш учун бу алгоритмларни интерпретациялаш доменида руйхатдан утказиш лозим.

AH ёки ESP протоколлари узатилувчи маълумотларни куйидаги иккита режимда химоялаши мумкин:

- туннел режимда; IP пакетлар бутунлай, уларнинг сарлавхаси билан бирга химояланади.

траспорт режимида; IP пакетларнинг факат ичидагилари химояланади.

Туннел режими асосий режим хисобланади. Бу режимда дастлабки пакет янги IP пакетга жойланади ва маълумотлар тармок, буйича узатиш янги IP-пакет сарлавхаси асосида амалга оширилади. Туннел режимида ишлашда хар бир оддий IP-пакет криптохдмояланган куринишда бутунлайча IPSec конвертига жойланади. IPSec конверти, уз навбатида бошка химояланган IP-пакетга инкапсуляцияланади. Туннел режими одатда махсус ажратилган хавфеизлик шлюзларида - маршрутизаторлар ёки тармоклараро экранларда амалга оширилади. Бундай шлюзлар орасида химояланган туннеллар шакллантирилади.

Туннелнинг бошка томонида кабул килинган химояланган 1P-пакетлар "очилади" ва олинган дастлабки IP-пакетлар кабул килувчи локал тармок, компьютерларига стандарт кридалар буйича узатилади. IP-пакетларни туннеллаш туннелларни эгаси булмиш локал тармокдаги оддий компьютерлар учун шаффоф хисобланади. Охирги тизимларда туннел режими масофадаги ва мобил фойдаланувчиларни мададлаш учун ишлатилиши мумкин. бу хрлда фойдаланувчилар компьютерида IPSecHHHr туннел режимини амалга оширувчи дастурий таъминот урнатилиши лозим.

Транспорт режимида тармок, оркали IP-пакетни узатиш бу пакетнинг дастлабки сарлавхаси ёрдамида амалга оширилади. IPSec конвертига криптохдмояланган куринишда факат IP-пакет ичидаги жойланади ва олинган конвертга дастлабки IP-сарлавха кушилади. Транспорт режими туннел

режимига нисбатан тезкор ва охирги тизимларда кулланиш учун ишлаб чикилган. Ушбу режим масофадаги ва мобил фойдаланувчиларни хамда локал тармок, ичидаги ахборот окимини химоялашни мададлашда ишлатилиши мумкин. Таъкидлаш лозимки, транспорт режимида ишлаш химояланган узаро алока гурухига кирувчи барча тизимларда уз аксини топади ва аксарият хрлларда тармок, иловаларини кайта дастурлаш талаб этилади.

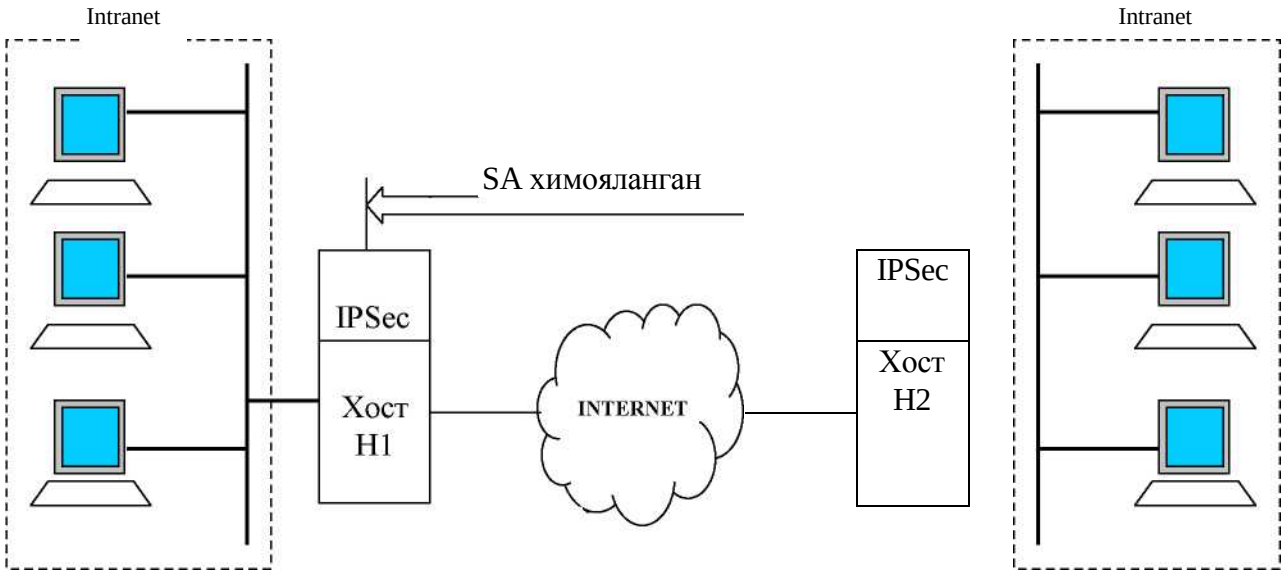
Туннел ёки транспорт режимидан фойдаланиш маълумотларни химоялашга куйиладиган талабларга хамда IPS ее ишловчи узел ролига боглик,. Химояланувчи канални тугалловчи узел-хост(охирги узел) ёки шлюз (ораликдаги узел) булиши мумкин. Мое хрлда, IPSecHH к,уллашнинг к,уйидагиучта асосий схемаси фаркланади:

- "хост - хост";
- "шлюз - шлюз";
- "хост - шлюз";

Биринчи схемада химояланган канал тармокнинг охирги иккита узели, яъни HI ва H2 хостлар орасида урнатилади (8.21-расм), IPSecHH мададловчи хостлар учун транспорт, хам туннел режимларидан фойдаланишга рухсат берилади.

8.21 расм. "Хост-хост " схемаси

Иккинчи схемага биноан, химояланган канал хар бирида IPSec протоколи ишловчи, *хавфеизлик шлюзлари SG1 ва SG2* (Security Gateway) деб аталувчи ораликдаги иккита узеллар орасида урнатилади (8.22-расм).

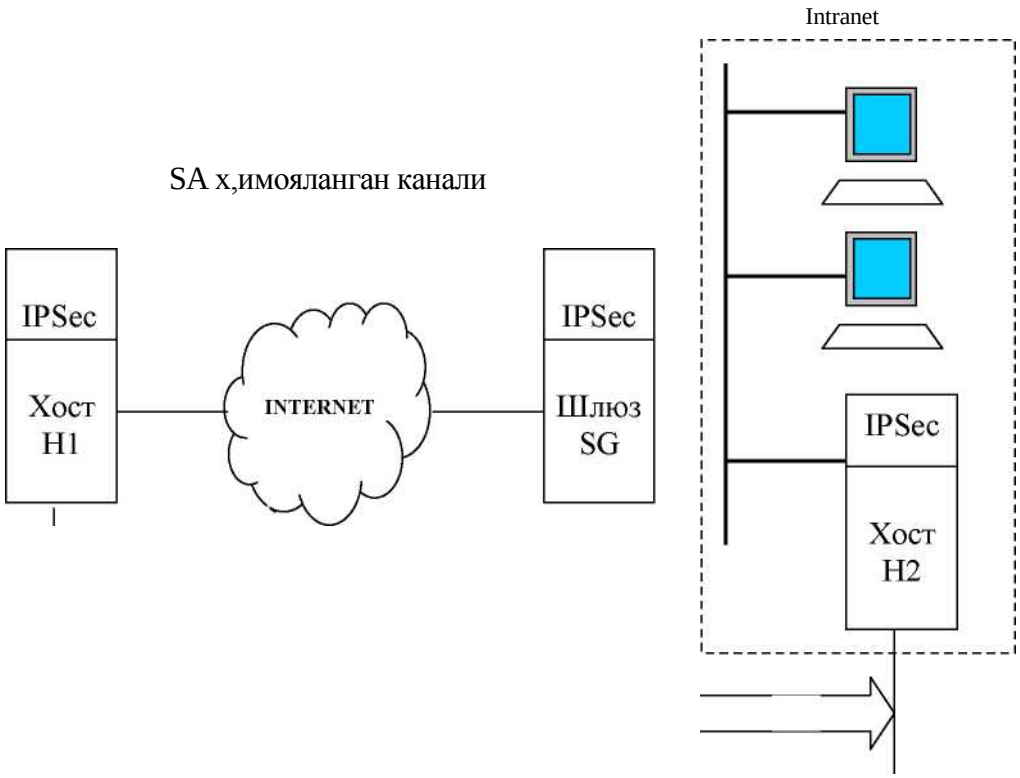


8.22-расм. "Шлюз-шлюз" схемаси

Хавфсизлик шлюзи иккита тармоккд уланувчи тармок, курилмаси булиб, узидан кейин жойлашган хостлар учун шифрлаш ва аутентификациялаш функцияларини бажаради. VPNнннғ хавфсизлик шлюзи алохида дастурий махсулот, алох,ида аппарат курилма хамда VPN функциялари билан тулдирилган маршрутизатор ёки тармоклараро экран куринишида амалга оширилиши мумкин.

Маълумотларни химояланган алмашиш тармокдарга уланган, хавфсизлик шлюзларидан кейин жойлашган х,ар кандай иккита охирги узеллар орасида руй бериши мумкин. Охирги узеллардан IPSec протоколни мададлаш талаб килинмайди, улар узларининг трафигини х,имояланмаган хрлда корхонанинг ишончли тармоги Intranet оркали узатади. Умумфойдаланувчи тармок,к,а юборилувчи трафик хавфсизлик шлюзи оркали утади ва бу шлюз узининг номидан IPSec ёрдамида трафикни х,имоялашни таъминлайди. Шлюзларга факат туннел режимида ишлашга рухсат берилади, гарчи улар транспорт режимини хам мададлашлари мумкин (бу хрлда самара кам булади).

"Хост - шлюз" схемаси купинча х,имояланган масофадан фойдаланишда ишлатилади (8.23-раем).



8.23-расм. "Хост-хост"канали билан тўлдирилган "хост-шлюз" схемаси Бу ерда хдмояланган канал IPSec ишловчи масофадаги HI хост ва корхона Intranet тармогига кирувчи барча хостлар учун трафикни химояловчи SG шлюз орасида ташкил этилади. Масофадаги хост шлюзга пакетларни жунатишда хам транспорт ва хам туннел режимларидан фойда-ланиши мумкин, шлюз эса хостга пакетларни факат туннел режимида жунатади.

Бу схемани масофадаги HI хост ва шлюз томонидан химояланувчи ички тармоккд тегишли бирор H2 хост орасида параллел яна бир химояланган канални яратиб модификациялаш мумкин. Иккита БАдан бундай комбинациялаб фойдаланиш ички тармокдаги трафикни хам ишончли химоялашта имкон беради.

Курилган IPSec асосида х,имояланган канални к,уриш схемалари тур-ли-туман виртуал х,имояланган тармокдарни (VPN) яратишда кенг кулланилади. IPSec асосида турли архитектурага эга булган виртуал химояланган тармокдар, жумладан масофадан фойдаланувчи VPN(Remote Access VPN), корпорация ичидаги VPN(Intranet VPN) ва корпорацияларарo VPN(Extranet VPN) к,урилади.

IPSec асосидаги VPN-технологияларининг жозибалилигини куйидаги сабаблар орк,али изохдаш мумкин:

- тармок, сатхининг химояси тармокда ишловчи барча татбикдш тизимлар учун шаффоф, яъни барча иловалар химояланган тармокда хеч кдндай тузатишсиз ва узгаришсиз худди очик, тармокда ипшаганидек ишлайверади;

- хдмоялаш тизимининг масштабланувчанлиги таъминланади, яъни мураккаблиги ва унумдорлиги турли булган объектларни х,имоялаш учун мураккаблиги, унумдорлиги, нархи даражаси буйича адэкват булган х,имоялашнинг дастурий ёки дастурий-аппарат воситаларидан фойдаланиш мумкин;

- масштабланувчи кдтордаги ахборотни х,имоялаш махсулотлари бирга ипглай оладилар, шу сабабли уларни турли сатхдаги объектларда (масофадаги ягона терминаллардан то ихтиёрий масштабли локал тармокдаргача) ресурсларидан ва трафигидан барча бегоналар фойдаланаоломайдиган ягона корпоратив тармок,к,а бирлаштириш мумкин.

IX боб. ОЧИК, КАЛИТЛАРНИ БО11ЩАРИШ ИНФРАТУЗИЛМАСИ РКІ

9.1. РК1нинг ишлаш принципи

Тарихан ахборот хавфсизлигини бошкарувчи хар кандай марказнинг вазифалари доирасига ахборот хавфсизлигининг турли воситалари томонидан ишлатилувчи калитларни бошкариш кирган. Бу-калитларни бериш, янгилаш, бекор килиш ва таркатиш.

Симметрик криптографиядан фойдаланилганда калитларни таркатиш масаласи энг мураккаб муаммога айланган, чунки:

- N фойдаланувчи учуй химояланган N(N-l)/2 калитни таркатиш лозим эди. N бир неча юзга тенг булганида бу сермашаккат вазифага айланиши мумкин;
- бундай тизимнинг мураккаблиги (калитларнинг куплиги ва таркатиш каналининг махфийлиги) хавфсизлик тизимини куриш кридаларининг биритизим оддийлигига тугри келмайди, натижада заиф жойларнинг пайдо булишига олиб келади.

Асимметрик криптография факат N махфий калитни тавсия этиб, бу муаммони четлаб утишга имкон яратади. Бунда хар бир фойдаланувчида факат битта махфий калит ва махсус алгоритм буйича махфий калитдан олинган очик, калит булади.

Очик, калитдан мах,фий калитни олиб булмаслиги сабабли очик, калитни химояланмаган х,олда барча узаро алок,а катнашчиларига тарк,атиш мумкин. Узининг мах,фий калиги ва узаро алокадаги шеригининг очик, калиги ёрдамида х,ар кандай фойдаланувчи х,ар к,андай криптоамалларни бажариши мумкин: булинувчи сирни хисоблаш, ахборотнинг конфиденциаллиги ва яхлитлигини х,имоялаш, электрон рак,амли имзони яратиш.

Шундай к,илиб, симметрик криптографиянинг иккита асосий муаммоси х,ал этилади:

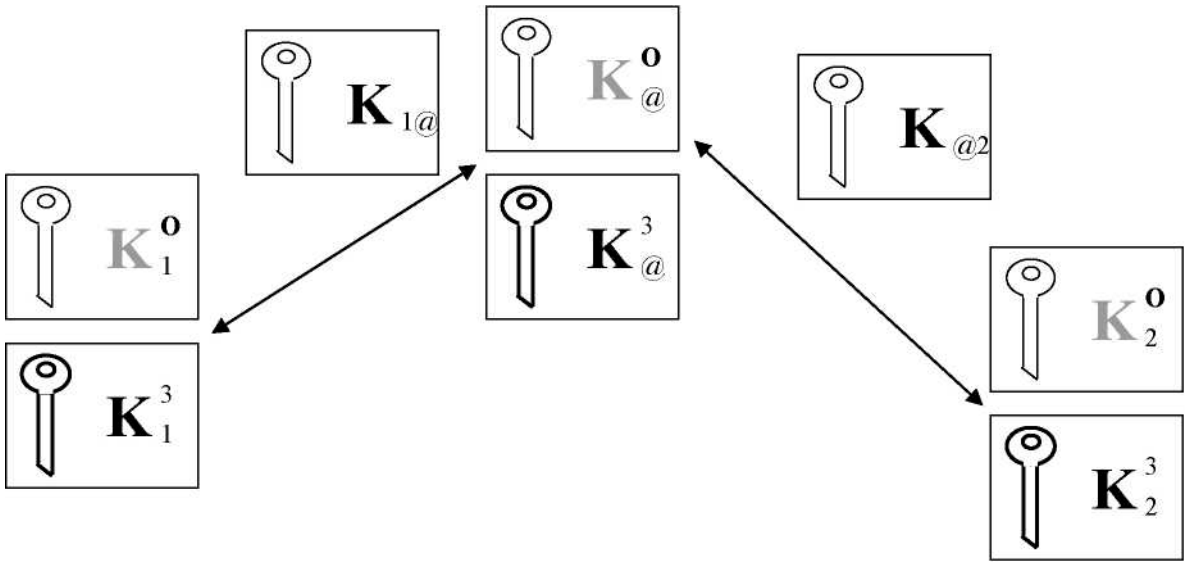
- калитлар сонининг куплиги - улар энди атиги NTa;
- таркатишнинг мураккаблиги - уларни очик, таркатиш мумкин.

Аммо бу технологиянинг битта камчилиги - хужум килувчи нияти бузук, одам узаро алока катнашчилари уртасида жойлашганида man-in-the-middle (уртадаги одам) хужумига мойиллиги.

Очик, калитларни бошкариш инфратузилмаси PKI ушбу камчиликни бартараф килишта имкон беради ва man-in-the-middle хужумидан самарали химояланишни таъминлайди. Очик, калитлар инфратузилмаси корпоратив ахборот тизимларининг ишончли ишлаши учуй аталган ва ички ва ташки фойдаланувчиларга ишончли муносабатлар занжири ёрдамида хавфсиз ахборот алмашишга имкон беради. Очик, калитлар инфратузилмаси фойдаланувчининг шахсий махфий калитини унинг очик, калити билан богловчи электрон паспортга ухшаб ишловчи ракамли сертификатларга асосланади.

Man-in-the-middle хужумидан химоялаш. Man-in-the-middle хужуми амалга оширилганида нияти бузук, одам очик, канал оркали узатилувчи узаро алоканинг крнуний иштирокчилари калитларини секингина узининг очик, калитига алмаштириб, крнуний иштирокчиларнинг хар бири билан булинувчи сир яратиши ва сунгра уларнинг барча ахборотларини ушлаб крлиши ва расшифровка килиши мумкин.

Хужум к,илувчининг х,аракатини ва бу хужумдан х,имояланиш усулини мисол оркали (9.1-раем) куриб чик,айлик. Фараз килайлик, фойдаланувчилар 1 ва 2 узларига умумий булган булинувчи сирни Диффи-Хеллман схемаси буйича х,исоблаб, химояланган уланишни урнатишга к,арор к,илдилар. Аммо 1- ва 2- фойдаланувчиларнинг Kj ва $К_2$ калитлари узатилаётган онда нияти бузук,, одам @ адресатга етказмай ушлаб к,олди. Нияти бузук, одам узининг махфий ва очик, калитини яратиб, очик, К калитини 1 ва 2-фойдаланувчиларга секингина уларнинг хакикий очик, Kj ва $К_2$ калитларининг урнига жунатади. Натижада 1 ва 2 - фойдаланувчилар булинувчи сирни узаро эмас, балки 1-@ ва 2-@ схемалари буйича яратадилар, чунки улар узларининг махфий калитларидан ва нияти бузук, одам @нинг очик, калити К@ дан фойдаланадилар.



9.1-расм. "Man-in-the-middle " атакасини амалга ошириш. 1-

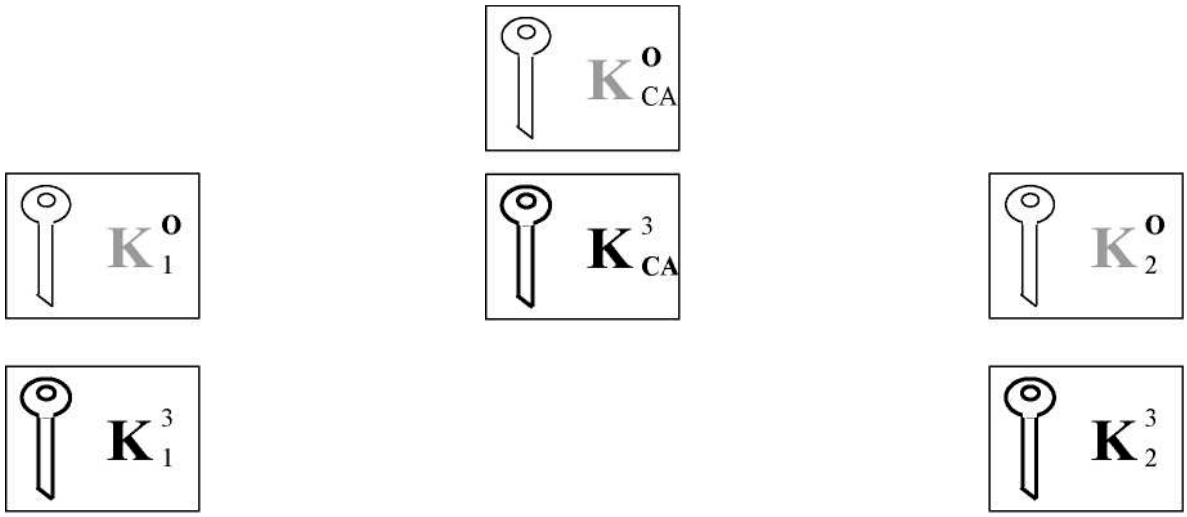
фойдаланувчи 2-фойдаланувчига шифрланган ахборотни жунатган вактида нияти бузук, одам @ уни ушлаб крлиши ва расшифровка килиши мумкин (унда 1-фойдаланувчи билан булинувчи сир $К_{1@}$ бор). Сунгра нияти бузук, одам @ ахборотни (узгартирилгани булиши мумкин) узи ва 2-нчи фойдаланувчи хисоблаган булинувчи сир $К_{@2}$ дан фойдаланиб янгидан шифрлайди. Натижада 2-фойдаланувчи 1-фойдаланувчи билан химояланган каналга эгаман деб уйлаб, нияти бузук, одам жунатган ахборотни олади, расшифровка килади ва ишлатади.

Бу хужумга карши самарали восита нотариус ёки сертификациялаш идораси С А (Certificate Authority). Очик, калитларнинг нотариал тасдикданган сертификатларини куллаш man-in-the-middle хужумини олдини олишга имкон беради.

1-фойдаланувчи нотариусга боради, нотариус 1-фойдаланувчининг очик, калитини узининг махфий калитидан фойдаланиб, электрон ракамли имзоси билан имзолайди. Бунда нотариус ракамли имзоси билан нафакат 1-фойдаланувчининг очик, калитини, балки фойдаланувчи хусусидаги к,атор аник, ахборотни (Ф.И.Ш., иш жойи ва х,.) х,амда имзонинг таъсир муддатини имзолайди. Хрсил булган хужжат (файл) 1-фойдаланувчи *очщ калитининг сертификаты* деб аталади. Нотариусдан узининг очик, калити учун сертификат олишнинг худци шу муолажасини 2-фойдаланувчи хам бажаради.

1 ва 2-фойдаланувчи имзо чекилган очик, калитларини алмашишганидан сунг, улар нотариуснинг электрон ракамли имзосини ва сертификат хакикатан 1- ёки 2- фойдаланувчига берилганлигини текширади. Нотариуснинг электрон ракамли имзосини текшириш фойдаланувчилар нотариусга ташриф буюрганларида эхтиётдан олиб куйилган нотариусни очик, калити ёрдамида шеригидан олган сертификатни расшифровка килиш оркали бажарилади. Натижада нотариус СА орк,али фойдаланувчилар орасида оддий ишонч занжири пайдо булади (9.2-расм).

Нияти бузук, одам @ нотариусга бориб 1-фойдаланувчининг сертификатини ололмайди, чунки унга бу сертификатни олиш вактида паспортини курсатишига ва у 1- фойдаланувчи эканлигини исботлашига тугри келади.



9.2-расм. Нотариус СА орцали фойдаланувчилар орасидаги оддий ишонч занжири

Очщ калит сертификатлари. Очик, калит сертификатларини шакллантириш X.509 стандарт тарафидан тавсия этилган *цатьий аутентификациялаш* принципига ва очик, калитли криптотизим хусусиятларига асосланади.

Очщ калит сертикати деганда маълумотлар булими ва имзо булимидан ташкил топган маълумотлар тузилмаси тушунилади. Маълумотлар булимида очик, калит хусусидаги ва калит эгасини идентификацияловчи маълумотлар булади. Имзо булимида очик, калитли маълумотлар булими учун генерацияланган очик, калит эгасини аутентификацияловчи электрон ракамли имзо булади. Сертификация маркази СА сертификатлардаги очик.

калитларни аутентификациялашни таъминловчи ишончли учинчи томон хдсобланади.

Сертификациялаш маркази узининг жуфт (очик,-махфий) калитига эга булиб, махфий калит сертификатларни имзолаш учун ишлатилса, очик, калит чоп этилади ва ундан фойдаланувчилар сертификатдаги очик, калитнинг хакикийлигини текширишда фойдаланадилар. Таъкидлаш л озимки, сертифкация марказининг очик, калитини хавфсиз узатиш нафакат сертифкация марказига шахсан мурожаат асосида, балки бу очик, калитни керакли ваколатга эга булган бошка сертифкация маркази томонидан сертификациялаш асосида хам амалга ошириш мумкин. Сертификация маркази фойдаланувчининг очик, калити сертификатини маълумотларнинг маълум тупламини ракамли имзо билан тасдикдаш оркали шакллантиради.

Одатда, маълумотларнинг бу тупламига куйидагилар киради:

- очик, калитнинг таъсир даври: даврининг бошланиши ва нихряси саналарини уз ичига олади;
- калитнинг номери ва серияси;
- фойдаланувчининг ноёб исми;
- фойдаланувчининг очик, калити хусусидаги ахборот: ушбу калит аталган алгоритмнинг идентификатори ва очик, калитнинг узи;
- электрон ракамли имзони текшириш муолажасида ишлатилувчи ал горитм (масалан, электрон ракамли имзони генерацияловчи алгоритм иден тификатори);
- сертификация марказининг ноёб исми;

Очик, калит сертификати куйидаги хусусиятларга эга:

- сертификация марказининг очик, калитидан фойдаланувчининг хар бири сертифкатга киритилган очик, калитни чикариб олиши мумкин;
- сертифкация марказидан ташкари хеч бир томон сертификатни билинтирмасдан узгартираолмайди (сертификатларни сохталаштириш мумкин эмас).

Сертифкатларни сохталаштириш мумкин эмаслиги, уларни умумфойдаланувчи маълумотномаларда, х,имояламасдан чоп этишга имкон тугдиради.

Очик, калит сертифкатини яратиш жуфт калитни (очик-махфий) яратишдан бошланади. Калитни генерациялаш муолажаси куйидаги иккита усул оркали амалга оширилиши мумкин:

- сертификация маркази калитлар жуфтини яратади. Очик, калит сертифкатга киритилади, унинг жуфти-махфий калит эса фойдаланувчига узатилади (фойдаланувчини аутентификациялашни ва калит узатилишининг конфиденциаллигини таъминлаган хрлда).

- фойдаланувчи калитлар жуфтини узи яратади. Махфий калит фойдаланувчида сакданади, очик, калит эса химояланган канал оркали сертифкация марказига юборилади.

Хдр бир фойдаланувчи сертифкация маркази томонидан шаклланти-рилган битта ёки бир нечта калитларнинг эгаси булиши мумкин. Фойдаланувчи бир неча турли сертифкация марказидан олинган сертификатларга хам эга булиши мумкин.

Амалда бошка сертификация марказидан сертифкат оладиган фойдаланувчиларни аутентификациялаш эхтиёжи тугилади.

Сертификатларни бошцариш тизимларининг базавий тузилмалари. Сертифкатларни бошкариш тизими-узаро ахборот алмашишда хавфсизликни таъминлаш максадида очик, калитли криптографик технологиялардан фойдаланишга зарур булган дастурий-аппарат воситалари хамда ташкилий-техник тадбирлар комплекси.

Очик, калитларни бошк,ариш инфратузилмаси PKI man-in-the-middle хужумларидан ишончли х,имоялашни амалга оширишга имкон берувчи нотариуслар тармогидан иборат. Нотариус орк,али фойдаланувчилар орасидаги оддий ишонч занжири (9.2-расм) битта нотариусга, унга ташриф буюрган фойдаланувчиларнинг очик, калитларини, имзоланган сертификатларни яратиш нули билан х,имоялашга имкон беради.

Бу тизимнинг самарали ишлаши куйидагиларга боглик,:

- узаро алока иштирокчилари сертификация маркази очик, сертификатининг х,ак,ик,ий нусхасига эга булишлари шарт;

- узаро алок,а иштрокчилари ишлатадиган ахборотни х,имоялаш воси талари узаро алокадаги шеригининг х,ар кандай сертификатини сертифика-

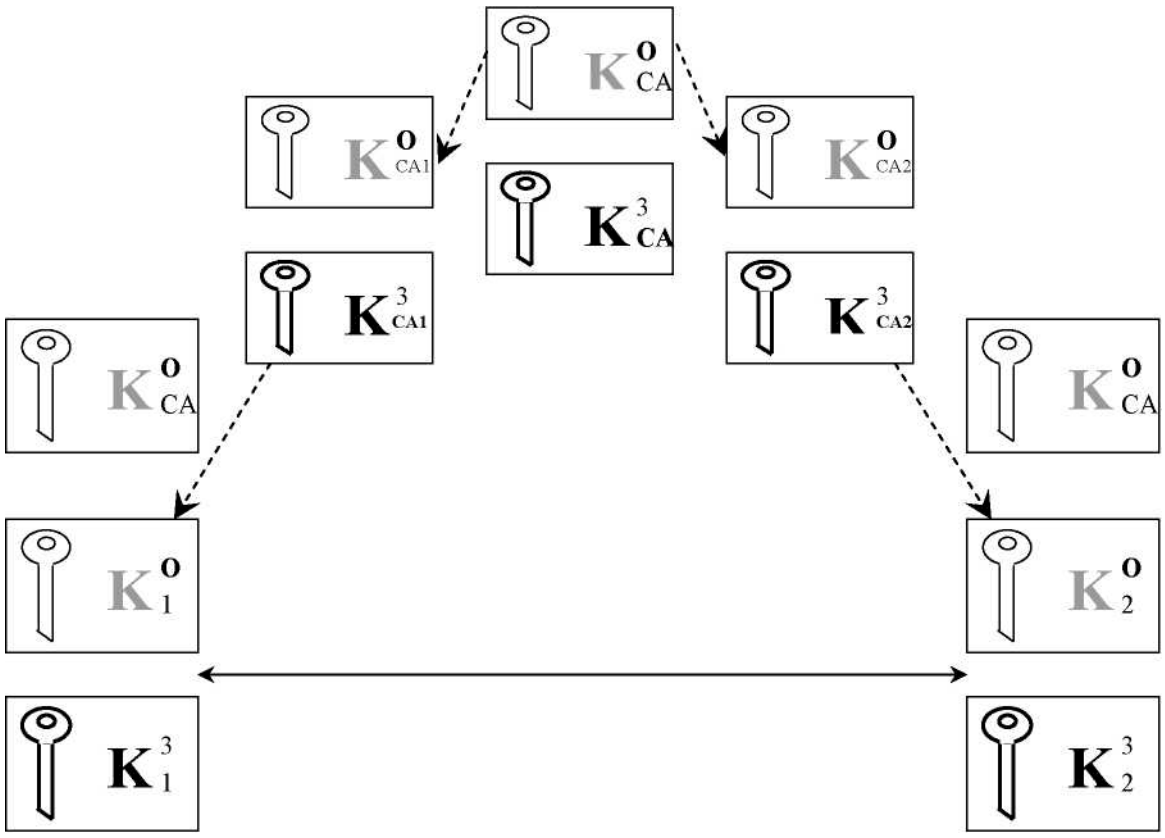
ция марказининг очик, сертификатидан фойдаланиб автоматик тарзда текшира олиши лозим.

Баъзида узаро алокадаги шериклар сертификация марказидан жуда узокда булишлиги мумкин. Бу хрлда СА нотариусларининг таксимланган катламлари яратилади.

Сертификациялашнинг учта базавий модели фаркланади:

- сертификатларнинг иерархик (шажара) занжирига асосланган сертификациялашнинг иерархик модели;
- кросс-сертификациялаш модели (узаро сертификациялашни кузда тутади);
- сертификациялашнинг тармок, (гибрид) модели (иерархик ва узаро сертификациялаш элементларини уз ичига олади);

Иерархик моделда СА лар бошка СА ларга сертификатлар берувчи илдиз сертификация марказига иерархик тобеликда жойлашган (9.3-расм).



9.3-расм. САнинг икки сатзрш иерархияси

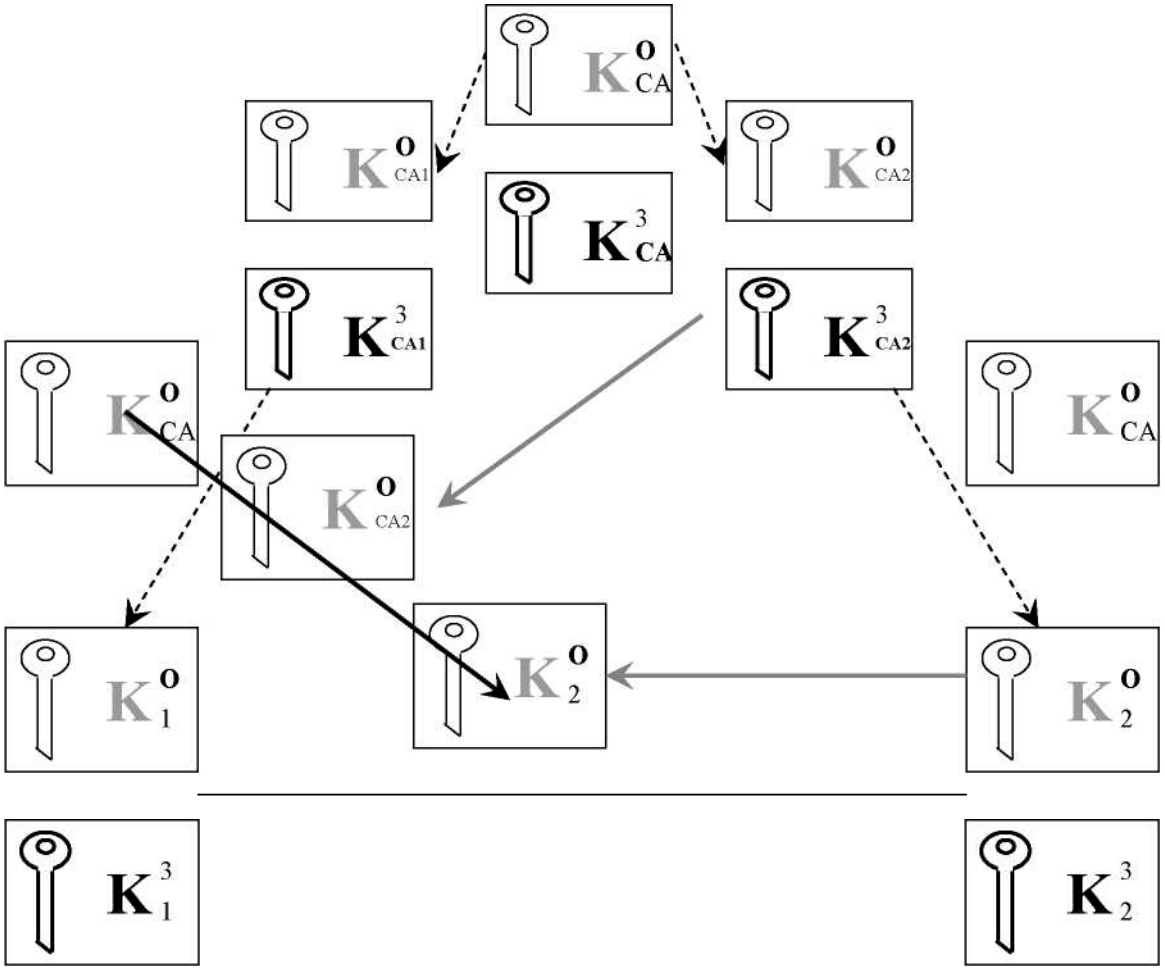
Илдиз сертификация марказининг вазифаси тобе СА1 ва СА2ларни кайдлашдан иборат. Хдр бир СА хавфсизликнинг ягона даражасини

таъминлаш максадида сертификациялашнинг берилган сиёсатига мувофик, ишлайди. 9.3-расмда келтирилган мисолда С А нотариусларнинг яна бир иерархик сатхи яратилади. Нотариуслар:

- фойдаланувчиларга ухшаб сертификатларини марказий САда имзолашади;

- марказий САга ухшаб оддий фойдаланувчиларнинг сертификатларини махфий калитлари билан, имзолайдилар.

Масофадаги шерикнинг хакикийлигини текшириш мантики куйидагиича курилади (9.4-расм)



9.4-расм. Масофадаги абонент сертификатини текшириш схемаси.

- фойдаланувчи шеригининг сертификатини олиб, уни нотаниш СА имзолаганини аниклайди;

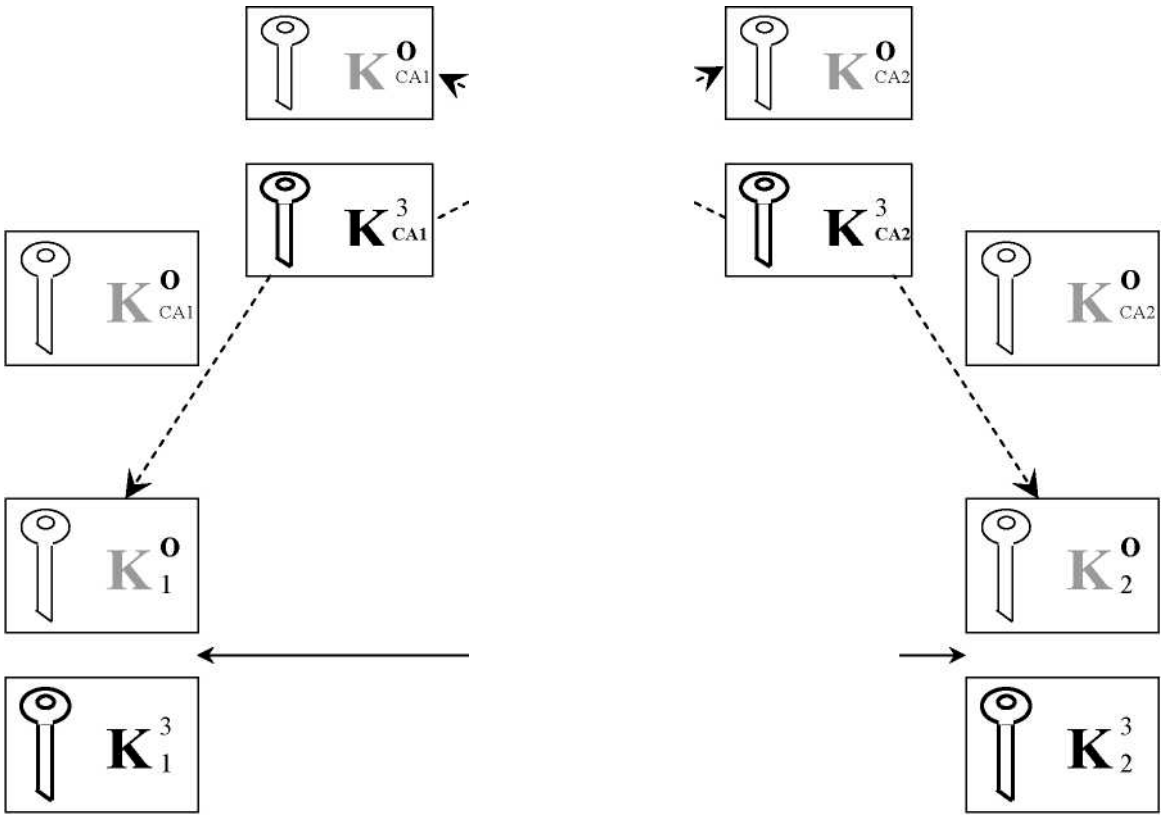
- у шеригидан ушбу САнинг сертификатини сурайди;

- САнинг сертификатини олиб, уни марказий СА сертификати билан текширади;

- муваффакиятли текширишдан сунг фойдаланувчи бу САга ишона бошлайди ва унинг сертификати билан масофадаги фойдаланувчи сертификатини текширади.

Худди шундай текширишни иккинчи шерик хам бажаради. Мухими, ишлатиладиган ахборотни химоялаш тизимлари бундай мураккаб иерархик текширишларни автоматик тарзда бажараолсинлар. Тавсифланган иерархик схемани, зарурият тугилганда иерархиянинг янги сатхдарини киритиб, давом эттириш мумкин.

Кросс-сертификациялаш моделида иерархиянинг бир шохдда булмаган мустакил САлар сертификация марказлари тармогида узаро сертификацияланадилар. Текшириш схемаси узгармайди, чунки фойдаланувчига бегона нотариус унинг нотариусига тобедек туюлади (9.5-расм).



9.5-расм. Кросс-сертификатлаш схемаси.

Таъкидлаш лозимки, кросс-сертификациялаш модели сертификатларни бошкариш тизимининг тармокди архитектурасининг хусусий холи хисобланади.

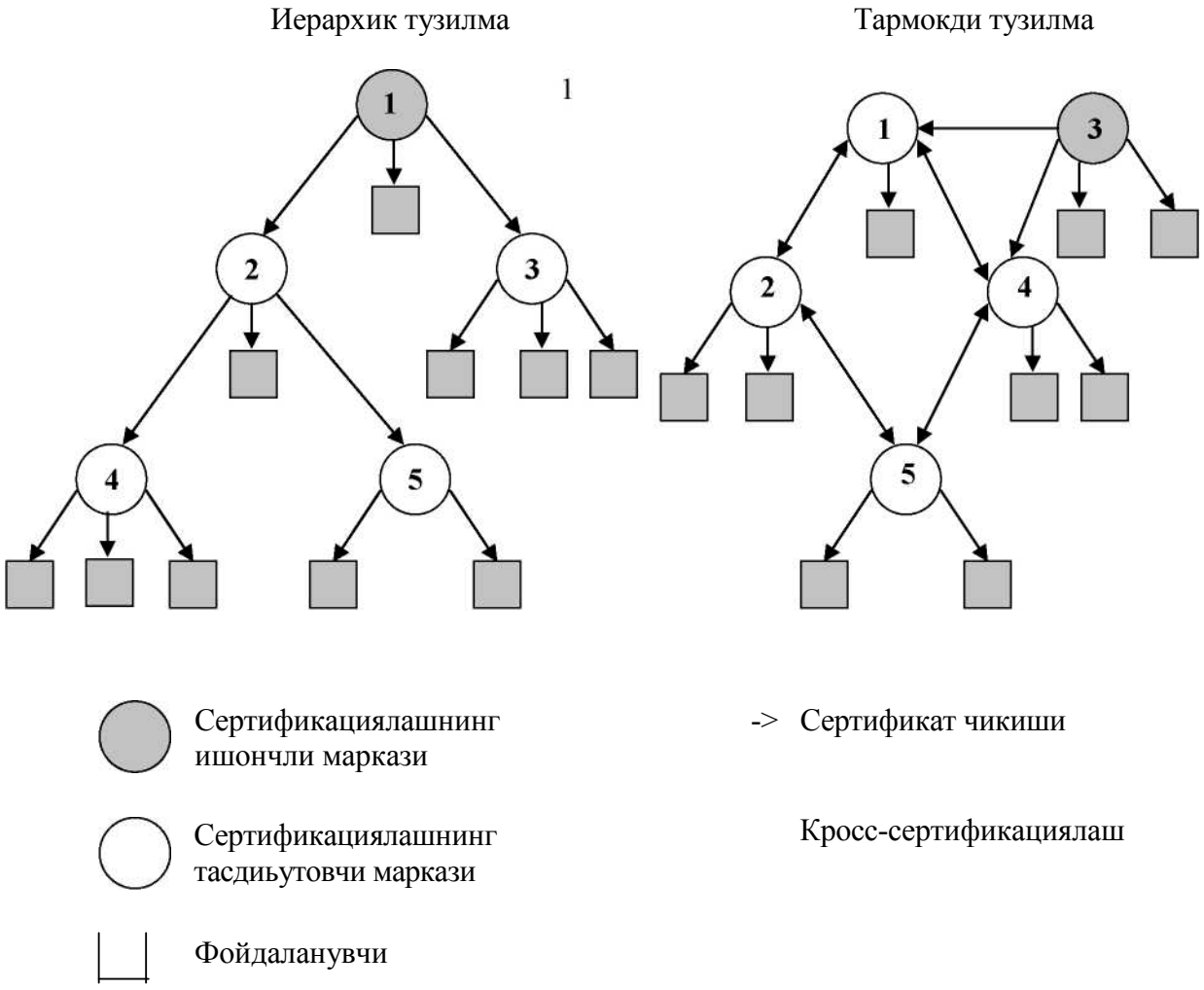
Сертификатларни бошк,ариш тизимининг иерархик ва тармок, архитектураларининг умумлаштирилган схемалари 9.6-расмда келтирилган.

Сертификатларни бошкариш тизимининг *иерархик тузилмаси* куйидаги афзалликларга эга:

- у мавжуд федерал ва идора ташкилий-бошкарув тузилмаларга ухшаш ва уларнинг принциплари буйича курилиши мумкин;

- у исмларнинг иерархик дарахтига осонгина богланиши мумкин;

- у узаро алокадаги барча томонлар учуй сертификатлар занжирини кидириш, куриш ва верификациялашнинг оддий алгоритмини аникдайди;



9. 6-расм. Сертификатларни бошкариш тизимининг иерархик ва тармокли архитектуралари

- иккита фойдаланувчининг узаро алокани таъминлаши учуй улардан бирининг иккинчисига узининг сертификатлар занжирини такдим этиши кифоя, бу узаро алока билан боглик, муаммоларни камайтиради.

Иерархик архитектурага куйидаги камчиликлар характерли:

- барча охирги фойдаланувчиларнинг узаро алок,ани таъминлаш учун фак,ат битта илдизли ишончли С А булиши шарт;

- тижорат тузилмаларининг узаро алокаси иерархикдан кура купрок, тугри характерга эга.

Сертификататларни бошкариш тизимининг *тармоқ архитектураси* куйидаги афзалликларга эга:

- у анчагина мослашувчан ва замонавий бизнесда мавжуд булган бевосита ишончли узаро муносабатларнинг урнатилишига имкон беради;

- охирги фойдаланувчи хеч булмаганда унинг сертификатный босиб чикарган марказга ишониши шарт ва тизимдаги ишонч муносабатлари мана шунга асосланган;

- фойдаланувчилари узаро тез-тез алока килувчи турли тасдикдовчи САларни бевосита кросс-сертификациялаш мумкин, бу занжирларни верификациялаш жараёнини кискартиради;

- тасдикдовчи СА калиги обрусизлантирилганидан сунг тиклаш жараёни иерархик тузилмага Караганда тармок, тузилмасида оддийрок,.

Аммо сертификатларни бошкаришнинг тармок, архитектураси куйидаги камчиликларга эга:

- барча узаро алока томонлар учуй сертификатлар занжирини кидириш ва куриш алгоритми жуда мураккаб булиши мумкин;

- фойдаланувчи унинг сертификатини бошка барча фойдаланувчилар томонидан текширилишини таъминловчи занжирни такдим этаолмайди.

Эхтимол, як,ин орада сертификациялаш иерархиясининг энг юкрри сатх,ида турли ташкилотларнинг ишонч занжирлари алокасини таъминловчи давлат нотариуси булиши л озим.

9.2. Очик калитларни бошкариш инфратузилмасининг мантикий тузилмаси ва компонентлари

Очик, калитларни бошкариш инфратузилмаси РК1нинг асосий вазифалари к,уйидагилар:

- рак,амли калитлар ва сертификатларнинг хаёт циклини мададлаш (яъни калитларни генерациялаш, сертификатларни яратиш ва имзолаш, уларни таксимлаш ва х,.);

- обрусизлантириш фактларини кайдлаш ва чакириб олинган сертификатларнинг "кора" руйхатини чоп этиш;

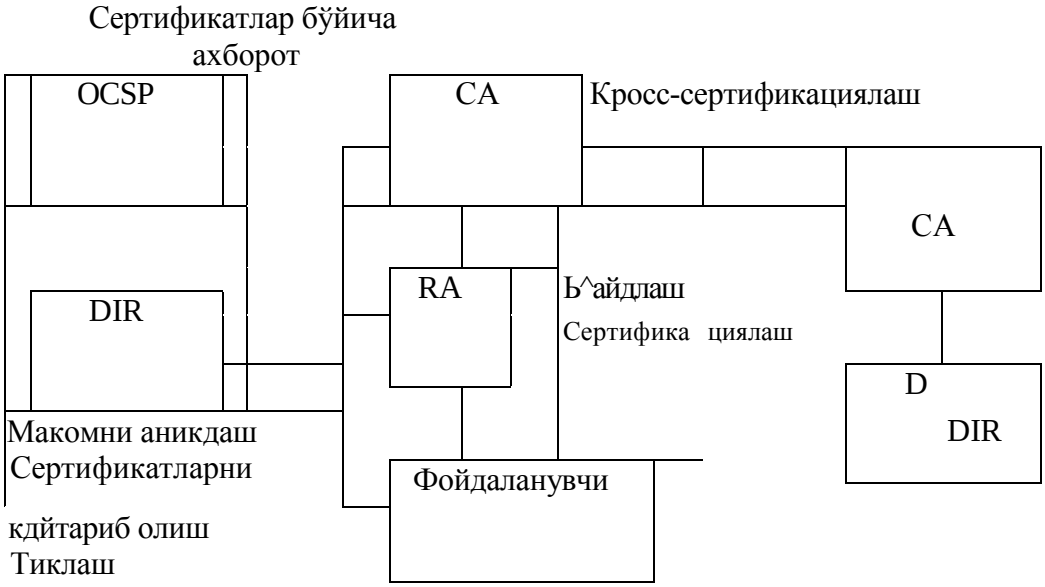
- фойдаланувчининг тизимдан фойдаланиш вактини имкони борича камайтирувчи идентификациялаш ва аутентификациялаш жараёнларини мададлаш:

- мавжуд иловалар ва хавфсизлик кием тизимининг барча компонент - ларини интеграциялаш механизмини (PKIra асосланган) амалга ошириш;

- барча фойдаланувчилар ва иловалар учун бир хил ва таркибида бар ча зарурий калит компонентлари ва сертификатлар булган хавфсизликнинг ягона токенидан фойдаланиш имкониятини такдим этиш.

Хавфсизлик токени - фойдаланувчининг тизимдаги барча хукуклари ва куршовини аникдовчи хавфсизликнинг шахсий воситаси, масалан смарт-карта.

9.7-расмда очик, калитларни бошкариш инфратузилмасининг мантикий тузилмаси ва асосий компонентлари келтирилган.



9.7-расм. PKIнинг мантщий тузилмаси ва асосий компоненталари

Расмда куйидаги белгилашлар к,абул к,илинган:

- С А сертификациялаш маркази;

- RA - кайдлаш маркази;

- OCSP - жорий сертификат макрмининг протоколи (Online Certifi cate Status Protocol);

- DIR - X.511, X.519, DAP, LDAP фойдаланиш протоколлари буйича диркетория хизмати.

Кдйдлаш маркази RA - PKI элементи, кайдлашни амалга оширувчи вакил, яъни фойдаланувчига сертификатни химояланган хрлда бериш имкониятини таъминлаш максадида фойдаланувчиларни аутентификациялашни ва уларни кайдлашни амалга оширади. Кдйдлаш марказининг хусусияти шундай иборатки, у функционал нуктаи назаридан сертификация марказига Караганда фойдаланувчига якинрок,. Ундан ташкари айнан кайдлаш маркази РК1нинг узаро алокага лаёкатлигини таъминловчи самарали интерфейс хисобланади.

Сертификация маркази СА - РКЬшнг элементи (сертификатларнинг ишончли манбаи, нотариус), унга сертификатларни яратиш ва/ёки тасдиклаш ишониб топширилган. Сертификация марказининг ишлаш схемаси куйидагича:

- СА шахсий калитларини генерациялайди ва фойдаланувчилар сертификатларини текширишга аталган С А сертификатларини шакллантиради;
- фойдаланувчилар сертифкациялашга суровларни шакллантирадилар ва уларни у ёки бу усул буйича САга етказади;
- СА фойдаланувчилар суровлари асосида уларнинг сертификатлари ни шакллантиради;
- СА бекор килинган сертификатлар руйхатларини (CRL) шакллан тиради ва вакти-вакти билан янгилайди;
- фойдаланувчи сертификатлари, СА сертификатлари ва бекор килинганлар руйхати CRL сертификатлар маркази томонидан чоп этилади (фойдаланувчиларга таркатилади ёки умумфойдаланувчи маълумотномага жойлаштирилади).

PKI бажарадиган функцияларни шартли равишда бир неча гурухларга ажратиш мумкин:

- сертификаталарни бошк,ариш функциялари;
- калитларни бошк,ариш функциялари;
- кушимча функциялар (хизматлар).

Сертификаталарни бошк,ариш функцияларига к,уйидагилар киради:

- *цайдлаш.* Нафакат функцияларнинг бир кисми, балки РК1нинг хавфсизлиги хам тугри кайдлашга ва идентифкациялашга асосланган. Фойдаланувчилар сифатида физик фойдаланувчилар, татбикий дастур, тармок, курилмаси ва х,. иштирок этиши мумкин. Идентификациялашда ишлатиладиган усулларни сертифкациялаш сиёсати белгилайди. Шундай килиб, фойдаланувчиларни идентификациялаш ва кайдлаш **PKI** тизимининг минимал тулик, компонентлари хисобланади;

- *очщ калитларни сертификациялаш.* Сертификациялаш жараёнига сертифкациялаш маркази СА жавоб беради. Мохиятан, сертификациялаш жараёни фойдаланувчи исмини очик, калит билан боглашдан иборат.

СА куйидаги харакатларни бажарган хрлда фойдаланувчи ва пастрок, сатхдаги С А сертификатларини имзолайди:

- фойдаланувчиларнинг хакикийлигини текшириш;
- сертифкатга идентификатор бериш;
- маълумотларни сертифкатга киритиш;
- харакат вактини (бошланиш-нихряси) урнатиш;
- сертификатни имзолаш;
- сертифкатни сертификатларнинг очик, серверида чоп этиш.

САнинг махфий калитини сацлаш. Бу тизимнинг энг нозик нуктаси. СА махфий калитини *обрусизлантирилиши* унинг ихтиёридаги бутун тизимни бузади. САнинг махфий калиги жойлашган компьютер ишончли курикланиши л озим;

- *сертификатлар базасини сацлаш ва сертифкатларни тацсимлаш.* Тизим ишлашининг кулайлигини таъминлаш максадида фойдаланувчилар нинг ва оралик, САларнинг (энг юкрри сатх, САсидан булак) барча сертифкатлари сертификатлар сервери деб аталувчи умумфойдаланувчи серверга олиб куйилади. Бу х,олда фойдаланувчилар абонентнинг сертификатини, хатто у тармокда вактинча булмаган х,олда х,ам, олишлари мумкин;

- ***сертификатни янгилаш.*** Ушбу жараён сертификат таъсири муддати утган хрлда фаоллашади ва фойдаланувчи очик, калиги учун янги серти фикатни беришдан иборат булади. Агар калитлар жуфти обрусизлантирилган булса ёки янги сертификат сиёсат, кенгайиш ёки хусу-

снят атамаларида олдингисидан фаркланса бу усул ишлатилмайди. Ярокчилик муддати даврида сертификатнинг исми ва мансублиги (фойдаланувчининг бошка булимга утиши) каби жиддий булмаган хусусиятларининг узгариши хам сертификатни олдинги очик, калит билан янгилашни (регенерациялашни) талаб этишга олиб келиши мумкин.

- ***калитларни янгилаш.*** Фойдаланувчилар ёки учинчи томон калитларнинг янги жуфтини генерациялаганларида янги очик, калитга мое келувчи сертификатни яратиш зарур. Бу усулдан сертификатни янгилаш мумкин булган хрлларида хам фойдаланилади;

- ***сертификатни кайтариб олиш макомини аниклаш.*** Ушбу жараён фойдаланувчига сертификатининг кайтариб олинган эмаслигини текширишга имкон беради. Бу жараён сертификатнинг очик, калитлар каталоги РКБда (Public Key Directory) ва сертификатларни кайтариб олиш руйхати СЯЬда (Certificate Revocation List) борлигини текшириш оркали ёки бу масалани ечишга ваколати булган учинчи томонга суров ёрдамида ташкил этилиши мумкин.

- ***сертификатни кайтариб олиш.*** Бу жараён турли хрлатлар натижасида хавфеизликнинг муайян сиёсатига боглик, х,олда (масалан, калитларнинг обрусизлантирилиши, исмларнинг узгариши, фойдаланишнинг тухташи ва х,.) булиши мумкин.

- ***калитларни бошкариш функцияси*** — калитларни генерациялаш ва таксимлаш асосий к,исм гурухдарига булинади.

Калитларни тацеимлаш функциялари уз навбатида очик, калитларни так,симлаш ва токенларни персоналлаштиришга булинади.

Токенларни персоналлаштиришда физик к,урилмалар - токенлардан фойдаланиб махфий калитларни ва к,ушимча маълумотларни саклаш ташкил этилади; токенларнинг персонализацияси С А, RA ва фойдаланувчи томонидан мададланиши лозим. Масалан, смарт-картанинг персонализацияси урнатиш (файл тизимини яратиш) муолажасини, тасодифий PIN-кодни ёки паролни танлаш, бу смарт-картага тегишли барча маълумотларни етказиш ва саклашни уз ичига олиши мумкин.

Кушимча функциялар (хизматлар) гурухи таркибига куйидагилар киради:

- узаро сертификациялаш (турли САларда кросс-сертификациялаш);

- очик, калитни унинг унга куйиладиган арифметик талабларга мое келишини, яъни очик, калит хакикий эканлигини текшириш;

- сертификатни текшириш; агар фойдаланувчи бошка фойдаланувчининг ракамли имзосига ишонишни хрхдаса ва мое сертификатни текшираолмаса, текширишни ишончли учинчи томондан илтимос килиши мумкин;

- архивлаш хизматлари ва х,.

Очик, калитлар инфратузилмаси PKI куйидаги катор иловалар ва стандартларни мададлайди:

- очик, калит сертификатларини мададловчи воситалар урнатилган Li nux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris operацион тизимлари;

- очик, калит сертификатлари асосида фойдаланувчиларни аутентификациялаш механизмини мададловчи маълумотлар базасини бошкариш ти зимлари, хусусан Oracle, DB2, Informix, Sybase;

- IP протоколи асосида амалга оширилувчи виртуал химояланган тармокдарни (VPN) ташкил этиш воситалари, хусусан Cisco Systems, Nortel Network компанияларининг телекоммуникация асбоб-ускуналари, хамда ихтисослаштирилган дастурий таъминот.

- электрон хужжат айланиши тизимлари, масалан Lotus Notes, Micro soft Exchange, хамда химояланган почта алмашиш стандарти S/MIMEнн мададловчи почта тизимлари;

- Microsoft Active Directory, Novell NDS, Netscape iPlanet каталогларининг хизмати;

- SSL стандарти асосида амалга оширилувчи Web-ресурслардан фойдаланиш тизимлари.

- фойдаланувчиларни аутентификациялаш тизимлари, хусусан RSA компаниясининг SecurlD ва х,.

Уз навбатида, очик, калитлар инфратузилмаси санаб утилган функционал сох,аларни интеграциялаши мумкин. Натижада, очик, калитлар ин-

фратузилмаларини компания ахборот тизимига интеграциялаш ва умумий стандартлар ва очик, калит сертификатларидан фойдаланиш йули билан ахборот хавфсизлигининг комплекс тизимини яратиш мумкин.

Юкррида келтирилганлар очик, калитлар инфратузилмасини яратиш ва мададлаш хизматлари ахамиятини ошишига олиб келади.

X боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СУК.ИЛИБ КИРИШЛАРНИ АНИКЛАШ

10.1. Хавфсизликни адаптив боищариш концепцияси

Ташкилотларда химоялаш билан боглик, булган муаммоларни ечиш учун аксарият хрлларда кисман ёндашишлардан фойдаланишади. Бу ёндашишлар, одатда, аввало фойдалана олувчи ресурсларнинг жорий даражаси оркали аникданади. Ундан ташкари, хавфсизлик маъмурлари купинча узларига тушунарли булган хавфсизлик хавф-хатарларига реакция курсатишади. Аслида хавф-хатарлар жуда куп булиши мумкин. Корпоратив ахборот тизимини факат катъий жорий назорати ва хавфсизликнинг умумий сиёсатини таъминловчи комплекс ёндашиш хавфсизлик хавф-хатарларини анчагина камайтириши мумкин.

Охирги вактда турли компаниялар томонидан катор ёндашишлар ишлаб чикилдики, бу ёндашишлар нафак,ат мавжуд заифликларни аникдашга, балки узгарган эски ёки пайдо булган янги заифликларни аникдашга ва уларга мое химоялаш воситаларини к,арши к,уйишга имкон беради. Хусусан, ISS(Internet Security Systems) компанияси томонидан *хавфсизликни адаптив бошкариш модели* ANS (Adaptive Network Security) ишлаб чикилди.

Хавфсизликка адаптив ёндашиш, тугри лойих,аланган ва яхши бошкарилувчи жараён ва воситалар ёрдамида хавфсизлик хавф-хатарларини реал вакт режимида назоратлаш, аникдаш ва уларга реакция курсатишга имкон беради.

Тармокнинг адаптив хавфеизлиги к,уйидаги асосий учта элемент орк,али таъминланади:

- хавф-хатарларни бахрлаш;
- химояланишни тахдиллаш;
- хужумларни аникдаш.

Хавф-хатарларни бахолаш. Хавф-хатарларни (келтирадиган зарарнинг жиддийлик даражаси буйича), тармок, к,исм тизимларини (жиддийлик даражаси буйича), тахдиддарни (уларнинг амалга оширилиши эх,тимоллиги

буйича) аниклаш ва рутбалашдан иборат. Тармок, конфигурацияси муттасил узгариши сабабли, хавф-хатарларни бахрлаш жараёни хам узлуксиз утказилиши лозим. Корпоратив ахборот тизимининг химоялаш тизимини куриш хавф-хатарларни бахрлашдан бошланиши лозим.

Химояланишни тахлиллаш - тармокнинг заиф жойларини кидириш. Тармок, уланишлардан, узеллардан, хостлардан, ишчи станциялардан, иловалардан ва маълумот базаларидан таркиб топган. Буларнинг барчаси химояланишлар самарадорлигининг хамда ноъмалум заифликларининг аникланишига мухтож. Химояланишни тахлиллаш технологияси тармокни тадкиклаш, нозик жойларини топиш, бу маълумотларни умумлаштириш ва улар буйича хисобот бериш имкониятига эга. Агар бу технологияни амалга оширувчи тизим адаптив компонентга хам эга булса, аникланган заифликларни автоматик тарзда бартараф этиш мумкин. Химояланишни тахлиллаш технологияси тармок, хавфсизлиги сиёсатини, уни ташкилот ташкарисидан ёки ичкарисидан бузишга уринишлардан олдин, амалга оширишга имкон берувчи таъсирчан усул хисобланади.

Химояланишни тахлиллаш технологияси томонидан идентификацияланувчи муаммоларнинг баъзилари куйидагилар:

- тизимлардаги "тешиклар" (back door) ва троян оти хилидаги дастур;
- кучсиз пароллар;
- химояланмаган тизимдан сук,илиб киришга ва "хизмат к,илишдан воз кечиш" хилидаги хужумларга таъсирчанлик;
- операцион тизимлардаги зарурий янгиланишларнинг йукдиги;
- тармоклараро экранларнинг, Web-серверларнинг ва маълумотлар базасининг нотугри созланиши ва х,.

Хужумларни аницлаш - корпоратив тармокдаги шубх,али харакатларни бахрлаш жараёни. Хужумларни аниклаш операцион тизим ва иловаларни к,айдлаш журналларини ёки реал вактдаги трафикни тахлиллаш орк,али амалга оширилади. Тармок, узеллари ёки сегментларида жойлаштирилган хужумларни аниклаш компонентлари турли ходисаларни, хусусан, маълум заифликлардан фойдаланувчи х,аракатларни х,ам бахрлайди (10.1-раем).

10.1-расм. Химояланганликни тахлиллаш ва хужумларни аниклаш тизимларининг ўзаро алокаси

Хавфсизликни адаптив бошкариш модели ANSHUHZ адаптив компоненты, янги заифликлар хусусидаги энг охирги ахборотни такдим килган хрлда, химояланишни тахлиллаш жараёнини модификациялашга жавоб беради. У хужумларни аниклаш компонентини хам, уни хужумлар хусусидаги охирги ахборот билан тулдириш орк,али, модификациялайди. Адаптив компонентнинг мисоли сифатида янги вирусларни аникдаш учун вирусга кдрши дастурнинг маълумотлар базасини янгилаш механизмини курсатиш мумкин.

Хавфсизликни адаптив бошкариш моделидан (10.2-расм) фойдаланиш

10.2-расм. Хавфсизликни бошкариш адаптив (мослашувчан) модели

барча тахдидларни назоратлаш ва уларга уз вактида самарали реакция курсатиш имконини беради. Бу эса уз навбатида, нафакат тахдидларнинг амалга оширилишига сабаб булувчи заифликларни бартараф килишга, балки заифликлар пайдо булиш шароитларини тахдиллашга имкон беради.

Тармок, хавфсизлигини адаптив бошкариш модели тармокда суиистеъмол килишни камайтиришга, тармокдаги ходисалардан фойдаланувчилар, маъмурлар ва компания рахбариятининг хабардорлик даражасини ошишига хам имкон беради. Таъкидлаш лозимки, ушбу модель олдин ишлатилувчи химоялаш механизмларидан (фойдаланишни чегаралаш, аутентификациялаш ва х,.) воз кечмайди. Уларнинг функционаллигини янги технология эвазига кенгайтиради. Узларининг ахборот хавфсизлигини таъминлаш тизимларини замонавий талабларга мое келишини хохловчи ташкилотлар мавжуд ечимларни учта янги компонент-химояланишни тахлиллаш, хужумларни аниклаш ва хавф-хатарни бахрлаш билан тулдириши лозим.

10.2. Хдмояланишни тахлиллаш

Химояланишни тахлиллаш воситалари заифликларни топиб ва уз вактида йук, килиб хужумни амалга ошириш имкониятини бартараф килади. Натижада, х,имоялаш воситаларини ишлатилишига буладиган барча сарф-х,аражатлар камаяди.

Химояланишни тахлиллаш воситалари тармок, сатх,ида, операцион тизим сатх,ида ва иловалар сатх,ида ишлаши мумкин. Улар текширишлар сонини бора-бора купайтириш, ахборот тизимига "ичкарилаб бориш" ва унинг барча сатхдарини тадк,икдаш орк,али заифликларни кидириши мумкин.

Тармоц протоколлари ва сервислари щмояланишини тахлиллаш воситалари. Хдр кандай тармокда абонентларнинг узаро алок,аси иккита ва ундан куп узеллар орасида ахборот алмашиниш муолажаларини белгиловчи тармок, протоколлари ва сервисларидан фойдаланишга асосланган. Тармок, протоколлари ва сервисларини ишлаб чикишда уларга ишланувчи ахборот хавфсизлигини таъминлаш буйича талаблар (одатда шубхасиз етарли

булмаган) куйилган. Шу сабабли, тармок, протоколларида аникданган заифликлар хусусида ахборотлар пайдо булмокда. Натижада, корпоратив тармокда фойдаланадиган барча протокол ва сервисларни доимо текшириш зарурияти тугилади.

Хдмояланишни тахлиллаш тизими заифликларни аникдаш буйича тестлар сериясини бажаради. Бу тестлар нияти бузук, одамларнинг корпоратив тармокларга хужумларида кулланиладиганига ухшаш.

Заифликларни аникдаш максадида сканерлаш текширувчи тизим хусусидаги дастлабки ахборотни, хусусан, рухсат этилган протоколлар ва очик, портлар, операцион тизимнниг ишлатилувчи версиялари ва х,. хусусидаги ахборотни олиш билан бошланади. Сканерлаш кенг тарк,алган хужумлар, масалан, тулик, саралаш усули буйича паролларни танлашдан фойдаланиб, сукилиб киришни имитациялашга уриниш билан тугайди.

Химояланишни тахлиллаш воситалари ёрдамида тармок, сатхдда нафакат InternetHHHr корпоратив тармокдан рухсатсиз фойдаланиши имкониятини тестлаш, балки ташкилот ички тармогида текширишни амалга ошириш мумкин. Тармок, сатхида х,имояланишни тахлиллаш тизими ташкилот хавфсизлик даражасини бахрлашга хамда тармок, дастурий ва аппарат таъминотини созлаш самарадорлигини назоратлашга хизмат килади.

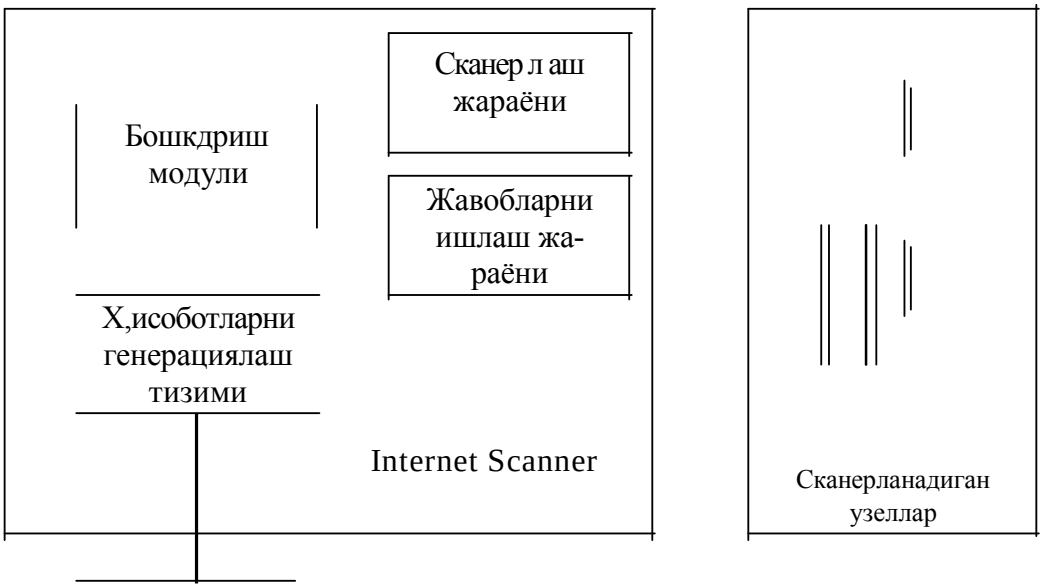
Химояланишни тахлиллашни амалга оширувчи (Internet Scanner тизими мисолида) намунавий схема 10.3-расмда келтирилган.

Химояланишни тахлиллаш воситаларининг бу синфи нафакат тармок, протоколлари ва сервислари, балки тармок, билан ишлашга жавобгар тизимли ва татбикий дастурий таъминоти заификларини х,ам тахлиллайди. Бундай таъминот к,аторига Web-, FTP-, ва почта серверларини, тармоклараро экранларни, браузерларни ва х,. киритиш мумкин.

Баъзи воситалар дастурий таъминотни тахлиллаш билан бир каторда аппарат воситаларини сканерлайди. Бундай воситаларга коммутацияловчи ва маршрутловчи асбоб-ускуналар киради.

Операцион тизим щмояланишини тахлиллаш воситалари. Воситаларнинг бу синфи операцион тизим химояланишига таъсир этувчи унинг

созланишларини текширишга аталган. Бундай созлашлар куйидагиларни аниклайди:



10.3-расм. Internet Scanner тизими мисолида химояланганликни тщлиллаш схемаси.

- фойдаланувчиларнинг хдсоб ёзуви, масалан, парол узунлиги ва унинг таъсир муддати;

- фойдаланувчиларнинг жиддий тизимли файллардан фойдаланиш хукуклари;

- заиф тизимли файллар;

- урнатилган патчлар ва х,.

Операцион тизим сатхидаги хдмояланишни тахлиллаш тизимлари операцион тизимлар конфигурациясини назоратлашда хам ишлатилиши мумкин.

Тармок, сатхи химояланишни тахлиллаш воситаларидан фаркли равишда, ушбу тизимлар тахлилланувчи тизимни ташк,аридан эмас, балки ичкаридан сканерлайди, яъни улар ташкаридаги нияти бузук, одамлар хужумларини имитацияламайди. Операцион тизим сатх,ида химояланишни тахлиллаш тизимларининг баъзилари (масалан, Internet Security Systems компаниясининг System Scanner тизими) заифликларни аниклаш имконияти-

дан ташкари, аникланган муаммоларнинг бир кисмини автоматик тарзда бартараф килишта ёки ташкилотда кабул килинган хавфсизлик сиёсатини крниктирмайдиган тизим параметрларига тузатиш киритишга имкон беради.

Танланувчи химоялашни тахлиллаш воситаларига цуйиладиган у мумий талаблар. Танланувчи тизимга куйиладиган мажбурий талаб-корхона тармок, инфратузилмасини узгартириш заруриятининг йуклиги. Акс хрлда бундай кайтадан ташкил этишга килинадиган харажат химояланишни тахдиллаш тизими нархидан ошиб кетиши мумкин. Хрзирда бу талабга факат Internet Security Systems компаниясининг Security Systems тизими жавоб беради.

Химояланишни тахлиллаш воситаларини нотугри ишлатиш улардан нияти бузук, одамларнинг корпоратив тармоккд сукилиб кириш учун фойдаланишларига имкон яратади. Шу сабабли, химояланишни тахлиллаш воситалари узларининг компонентларидан ва йигилган маълумотлардан фойдаланишни чегараловчи механизмлар билан таъминланиши лозим. Бундай механизмларга к,уйидагилар киради:

- факат маъмур хук,ук,ига эга булган фойдаланувчи томонидан ушбу воситаларни ишга тушириш;
- сканерлаш маълумотлари архивини шифрлаш;
- масофадан бошкаришда уланишни аутентификациялаш;
- каталоглар билан ишлаш учун махсус хукукларни аникдаш ва х,.

Заифликларни аникдаш жараёнининг куйидаги имкониятларига эътиборни к,аратиш лозим:

- бир неча курилма ёки сервисларни параллел ишлаш эвазига сканер лаш тезлигини ошириш;
- тизимдан рухсатсиз фойдаланишни олдини олиш учун хар бир сканерланувчи узелга билдириш к,огозини юбориш;
- ёлгон ишлашларни минималлаштириш учун тармок,ни эксплуатация талабларига тугрилаш.

Корпоратив тармок, холатининг доимо узгариб туриши, унинг химояланишига таъсир курсатади. Шу сабабли, химояланишни тахлиллашнинг яхши тизими жадвал буйича ишлаш режимига эга булиб, маъмур уни эслагунича узи тармок, узеллари заифликларини текшириши ва пайдо

булган муаммолар хусусида нафакат маъмурни огохдантириши, балки аникданган заифликларни йукртиш усулларини тавсия этиши л озим.

Эътибор бериш зарур булган характеристикалардан бири- хисоботларни генерациялаш тизимининг мавжудлиги. Бу тизим фойдаланувчиларнинг турли категорияларлари - техник мутахассислардан тортиб то ташкилотлар рахбарлари учун тафсилоти турли даражада булган хужжатларни яратишга имкон бериши лозим.

Хужжатларда маълумотларни ифодалаш шакли хам мухим хисобланади. Факат матнли ахборот билан тулдирилган хужжатларнинг фойдаси булмайди. Графиклардан фойдаланиш эса маъмурга ташкилот тармогидаги барча муаммоларни якдол намойиш этишга имкон беради. Хисоботларда аникданган муаммоларни йукртиш буйича тавсияларнинг мавжудлиги химояланишни тахлиллаш воситаларини танлашдаги мажбурий шарт хисобланади.

Доимо янги заифликларнинг аникданиши химояланишни тахлиллаш тизимининг заифликлар маълумотлари базасини тулдира олиши имкониятига эга булишини такрзо этади. Бу заифликларни тавсифловчи махсус тил ёрдамида ёки тизим ишлаб чикарувчилари томонидан заифликларни вактивакти билан тулдириш йули билан амалга оширилади. Корпоратив тармок, узелларининг химояланиш даражасининг узгаришини тахлиллаш учун танланувчи восита утказилган сканерлаш сеанслари хусусидаги ахборотни тупланишига имкон бериши лозим.

10.3. Хужумларни аниклаш

Тармоц ахборотини тахлиллаш усуллари. Мох,ияти буйича, хужумларни аникдаш жараёни корпоратив тармокда булаётган шубх,али харакатларни бах,олаш жараёнидир. Бошк,ача айтганда хужумларни аникдаш- хисоблаш ёки тармок, ресурсларига йуналтирилган шубх,али х,аракатларни идентификациялаш ва уларга реакция курсатиш жараёни. Хрзирда хужумларни аникдаш тизимида к,уйидаги усуллар ишлатилади:

- статистик усул;

- эксперт тизимлари;
- нейрон тармокдари.

Статистик усул. Статистик ёндашишнинг асосий афзаллиги - аллакачон ишлаб чикилган ва узини танитган математик статистика аппаратини ишлатиш ва субъект характерига мослаш.

Аввал тахдилланувчи тизимнинг барча субъектлари учун профиллар аникланади. Ишлатиладиган профилларнинг эталондан хар кандай четланиши рухсат этилмаган фойдаланиш хисобланади. Статистик усуллар универсал хисобланади, чунки мумкин булган хужумларни ва улар фойдаланадиган заифликларни билиш талаб этилмайди. Аммо бу усуллардан фойдаланишда бир канча муаммолар пайдо булади:

1. Статистик тизимлар ходисалар келиши тартибига сезувчанмаслар; баъзи холларда бир ходисанинг узи, келиши тарти бига кура аномал ёки нормал фаолиятни характерлаши мум кин.
2. Аномал фаолиятни адекват идентификациялаш максадида хужумларни аниклаш тизими томонидан кузатилувчи характеристикалар учун чегаравий (бусагавий) кийматларни бериш жуда кийин.
3. Статистик усуллар вакт утиши билан бузгунчилар томонидан шундай "урнатилиши" мумкинки, хужум харакатлари нормал каби к,абул к,илинади.

Эксперт тизимлари. Эксперт тизими одам-эксперт билимларини камраб олувчи к,оидалар тупламидан ташкил топган. Эксперт тизимидан фойдаланиш хужумларни аниклашнинг кенг тарк,алган усули булиб, хужумлар хусусидаги ахборот кридалар куринишида ифодаланади. Бу к,оидалар харакатлар кетма-кетлиги ёки сигнатуралар куринишида ёзилиши мумкин. Бу кридаларнинг х,ар бирининг бажарилишида рухсатсиз фаолият мавжудлиги хусусида к,арор к,абул к,илинади. Бундай ёндашишнинг мух,им афзаллиги - ёлгон тревоганинг умуман булмаслиги.

Эксперт тизимининг маълумотлари базасида х,озирда маълум булган аксарият хужумлар сценарияси булиши лозим. Эксперт тизимлари, дол-

зарбликни сакдаш максадида, маълумотлар базасини муттасил янгилашни талаб этади. Гарчи эксперт тизимлари кайддаш журналларидаги маълумотларни куздан кечиришга яхши имкониятни тавсия килсада, суралган янгиланиш эътиборсиз крлдирилиши ёки маъмур томонидан кулда амалга оширилиши мумкин. Бу энг камида, эксперт тизими имкониятларининг бушашига олиб келади.

Эксперт тизимларининг камчиликлари ичида энг асосийси - номаълум хужумларни акслантира олмаслиги. Бунда олдиндан маълум хужумнинг хатто озгина узгариши хужумларни аниклаш тизимининг ишлашига жиддий тусик, булиши мумкин.

Нейрон тармоцлари. Хужумларни аниклаш усулларининг аксарияти кридалар ёки статистик ёндашиш асосида назоратланувчи мухитни тахдиллаш шаклларидан фойдаланади. Назоратланувчи мухит сифатида кайддаш журналлари ёки тармок, трафиги курилиши мумкин. Бундай тахлиллаш маъмур ёки хужумларни яникдаш тизими томонидан яратилган, олдиндан аникланган кридалар тупламига таянади.

Хужумни вакт буйича ёки бир неча нияти бузук, одамлар уртасида х,ар кандай булиниши эксперт тизимлар ёрдамида аниклашга к,ийинчилик тугдиради. Хужумлар ва улар усулларининг турли-туманлиги туфайли, эксперт тизимлари кридаларининг маълумотлар базасининг хатто доимий янгиланиши х,ам хужумлар диапазонини аник, идентификациялашни кафолатламайди.

Нейрон тармокдаридан фойдаланиш эксперт тизимларининг юкррида келтирилган муаммоларни бартараф этишнинг бир усули хисобланади. Эксперт тизимлари фойдаланувчига курилаётган характеристикалар к,оидалар маълумотлари базасидагига мое келиши ёки мое келмаслиги хусусида аник, жавоб бераолса, нейротармок, ахборотни тахлиллайди ва маълумотларни аникдашга урганган характеристикаларига мое келишини бах,олаш имкониятини такдим этади. Нейротармокди ифодалашнинг мослик даражаси 100%га етиши мумкин, аммо танлаш хак,ик,ийлиги тамоман к,уйилган масала мисолларини тахлиллаш сифатига боглик,.

Аввал предмет сохдсининг олдиндан танлаб олинган мисолида нейротармокни тугри идентификациялашга "ургатишади". Нейротармок, реакцияси тахлилланади, крникарли натижаларга эришиш максадида тизим созланади. Нейротармок, хам вакт утиши билан, предмет сохаси билан боглик, маълумотларни тахлиллашни утказишига караб "тажриба орттиради".

Нейротармокларнинг суиистеъмол килинишни аниклашдаги мухим афзаллиги, уларнинг атайин килинадиган хужумлар характеристикаларини "ургапиш" ва тармокда олдин кузатилганига ухшамаган элементларни идентификациялаш крбилиятидир.

Юкррида тавсифланган хужумларни аникдаш усулларининг х,ар бири афзалликларга ва камчиликларга эга. Шу сабабли, хрзирда тавсифланган усулларнинг факдт биттасидан фойдаланувчи тизимни учратиш к,ийин. Одатда, бу усуллар биргаликда ишлатилади.

Хужумларни анщлаш тизимларининг туркумланиши. Хужумларни аниклаш тизимлари IDS (Intrusion Detection System)fla ишлатилувчи хужумларни аникдовчи механизмлар бир неча умумий усулларга асосланган. Таъкидлаш лозимки, бу усуллар бир-бирини инкор этмайди. Аксарият тизимларда бир неча усулларнинг комбинациясидан фойдаланилади.

Хужумларни аникдаш тизимлари к,уйидаги аломатлари буйича туркумланиши мумкин:

- реакция курсатиш усули буйича;
- хужумларни фош этиш усули буйича;
- хужум хусусидаги ахборотни йигиш усули буйича.

Реакция курсатиш усули буйича пассив ва актив ГОБлар фаркланади. Пассив IDS лар хужум фактларини кайдлайди, маълумотларни журнал файлига ёзади ва огохдантиришлар беради. Актив ГОБлар, масалан, тармокдараро экранни кайта конфигурациялаш ёки маршрутизатордан фойдаланиш руйхатини генерациялаш билан хужумга карши х,аракат к,илишга уринади.

Хужумларни фош этиш усули буйича ШБларни куйидаги иккита категорияга ажратиш кабул килинган:

- аномал хдтти-хдракатни аникдаш (anomaly-based);

- суиистеъмолликларни аникдаш (misuse detection ёки signature-based).

Аномал хдтти-хдракатни аниклаш нули билан хужумларни аникдаш технологияси куйидаги гипотезага асосланган. Фойдаланувчининг аномал хдтти-хдракати (яъни хужуми ёки кдндайдир гаразли хдракати) - нормал хдтти-хдракатдан четлашиш. Аномал хдтти-хдракатга мисол тарикдсида кискд вакт оралигида уланишларнинг катта сонини, марказий процессорнинг юкрри юкланишини ва х,. курсатиш мумкин.

Агар фойдаланувчининг нормал хдтти-хдракати профилини бир маънода тавсифлаш мумкин булганида, хдр кдндай ундан четланишларни аномал хдтти-хдракат сифатида идентифкациялаш мумкин булар эди. Аммо, аномал хдтти-хдракат хдр доим хдм хужум булавермайди. Масалан, тармок, маъмури томонидан юборилган куп сонли суровларни хужумларни аникдаш тизими "хизмат курсатишдан воз кечиш" хилидаги хужум сифатида идентификациялаши мумкин.

Ушбу технология асосидаги тизимдан фойдаланилганда иккита кескин х,олат юз бериши мумкин:

- хужум булмаган аномал хдтти-хдракатни аникдаш ва уни хужумлар синфига киритиш;

- аномал хдтти-хдракат таърифига мое келмайдиган хужумларни утказиб юбориш. Бу х,олат хужум булмаган аномал хдтти х,аракатни хужум лар синфига киритишга нисбатан хавфлирок, хдеобланади.

Бу категория тизимларини созлашда ва экегшуатациясида маъмур к,уйидаги к,ийинчиликларга дуч келади:

- фойдаланувчи профилини куриш сермех,нат масала булиб, маъмурдан катта дастлабки ишларни талаб этади.

- юкррида келтирилган иккита кескин хдракатлардан бирининг пайдо булиши эхтимоллигини пасайтириш учун фойдаланувчи х,атти-х,аракатининг чегаравий кийматларини аникдаш зарур.

Аномал хатти-харакатларни аниклаш технологияси хужумларнинг янги хилини аникдашга мулжалланган. Унинг кимчилиги - доимо "урганиш" зарурияти.

Суиистеъмолликларни аникдаш йули билан хужумларни аниклаш технологиясининг мохияти хужумларни сигнатура куринишида тавсифлаш ва ушбу сигнатурани назоратланувчи маконда (тармок, трафигида ёки кдйдлаш журналида) кдциришдан иборат. Хужум сигнатураси сифатида аномал фаолиятни характерловчи харакатлар шаблони ёки символлар сатри ишлатилиши мумкин. Бу сигнатуралар вирусга кдрши тизимларда ишлатилувчи маълумотлар базасига ухшаш маълумотлар базасида сакданади. Таъкидлаш лозимки, вирусга кдрши резидент мониторлар хужумларни аниклаш тизимларининг хусусий холи хисобланади. Аммо бу йуналишлар бошидан параллел ривожланганлари сабабли, уларни ажратиш кдбул кхшинган. Ушбу хил тизимлар барча маълум хужумларни аникласада, янги, х,али маълум булмаган хужумларни аниклай олмайди.

Бу тизимларни эксплуатациясида х,ам маъмурларга муаммоларни дуч келади. Биринчи муаммо - сигнатураларни тавсифлаш механизмларини, яъни хужумларни тавсифловчи тилларни яратиш. Иккинчи муаммо, биринчи муаммо билан боглик, булиб, хужумларни шундай тавсифлаш лозимки, унинг барча модификацияларини к,айдлаш имкони тугилсин.

Хужум хусусидаги ахборотни йигиш усули буйича туркумлаш энг оммавий хисобланади:

- тармок, сатх,ида хужумларни аниклаш (network-based);
- хост сатхида хужумларни аниклаш (host-based);
- илова сатхида хужумларни аникдаш (application-based).

Тармок, сатх,ида хужумларни аникдаш тизимида тармокдаги трафикни эшитиш орк,али нияти бузук, одамларнинг мумкин булган х,аракатлари аникданади. Хужумни к,идириш "хостдан-хостгача" принципи буйича амалга оширилади. Ушбу хилга тааллукди тизимлар, одатда хужумлар сигнатурасидан ва "бир зумда" тахлиллашдан фойдаланиб, тармок, трафигини тахлиллайди. "Бир зумда" тахлиллаш усулига биноан тармок, трафиги реал ёки унга якхшрок, вак,тда мониторингланади ва мое аникдаш алгоритмларидан

фойдаланилади. Купинча рухсатсиз фойдаланиш фаолиятини характерловчи трафикдаги маълум сатрларни кидириш механизмларидан фойдаланилади.

Хост сатхида хужумларни аниклаш тизими маълум хостда нияти бузук, одамларни мониторинглаш, детектирлаш ва харакатларига реакция курсатишта аталган. Тизим химояланган хостда жойлашиб, унга карши йуналтирилган харакатларни текширади ва ошкор килади. Бу тизимлар операцион тизим ёки иловаларнинг кайдлаш журналларини тахлиллайди. Кдйдлаш журналларини тахлиллаш усулини амалга ошириш осон булсада, у куйидаги камчиликларга эга:

- журналда кайд этилувчи маълумотлар хажмининг катталиги назоратланувчи тизим ишлаши тезлигига салбий таъсир курсатади;

- кайдлаш журналини тахлиллашни мутахассислар ёрдамисиз амалга ошириб булмайди;

- хрзиргача журналларни сакдашнинг унификацияланган формати мавжуд эмас;

- кайдлаш журналларидаги ёзувни тахлиллаш реал вактда амалга оширилмайди.

ШБнинг учинчи хили маълум иловадаги муаммоларни к,идиришга асосланган.

Хужумларни аницлаш тизимининг компонентлари еа архитектураси. Мавжуд ечимларнинг тахлили хужумларни аниклашнинг намунавий тизими компонентларининг руйхатини келтиришга имкон беради.

Кузатиш модули назоратланувчи макондан (к,айдлаш журнали ёки тармок, трафиги) маълумотларни йигишни таъминлайди. Унинг к,уйидаги номлари хам учрайди: сенсор (sensor), монитор (monitor), зонд(ргоЬе) ва х,. Хужумларни аниклаш тизими архитектурасининг курилишига боглик, хрлда кузатиш модули бошк,а компонентлардан алох,ида, бошк,а компьютерда жойлашиши мумкин.

Хужумларни аницлаш цисм тизими асосий модул булиб, кузатиш модулидан олинадиган ахборотни тахлиллайди. Ушбу тахлиллаш натижаси буйича кием тизим хужумларни идентификациялаш, реакция курсатиш ва-

риантлари буйича тухтамга келиши, маълумотлар омборида хужумлар хусусидаги ахборотни сакдаши мумкин ва х,.

Билимлар базасида, хужумларни аникдаш тизимларида ишлатиладиган усулларга боглик, хрлда, фойдаланувчилар ва хисоблаш тизим профиллари, рухсатсиз фойдаланишларни характерловчи хужум сигнатуралари ёки шубхали сатрлар сакданиши мумкин. Билимлар базаси хужумларни аникдаш тизимларини ишлаб чикарувчилари, тизимдан фойдаланувчилар ёки учинчи томон, масалан бу тизимни мададловчи аутсорсинг компанияси томонидан тулдирилиши мумкин.

Маълумотлар омбори хужумларни аниклаш тизими ишлаши жараёнида йигилган маълумотларнинг сакданишини таъминлайди.

График интерфейс тизимнинг нихрятда зарурий компоненти булиб, хужумларни аниклаш тизими ишлашини бошкарувчи операцион тизимга боглик, хрлда де-факто Windows ва Unix стандартларига мое келиши лозим.

Реакция курсатиш кием тизими аникланган хужумлар ва бошка назоратланувчи ходисаларга реакция курсатишни амалга оширади. Мавжуд тизимларда ишлатиладиган реакция курсатиш усулларини к,уйидаги учта категорияга ажратиш мумкин:

- билдириш;
- сакдаш;
- фаол реакция курсатиш.

Билдириш усули буйича хужум хусусидаги ахборот хавфеизлик маъмурига тизимнинг консолига ёки электрон почта буйича, пейджерга факс ёки телефон оркали жунатилиши мумкин.

Сакдаш усулига реакция курсатишнинг куйидаги вариантлари тааллукди:

- ходисаларни маълумотлар базасида к,айддаш;
- хужумларни реал вакт масштабида тиклаш.

Биринчи вариант х,имоялашнинг бошк,а тизимларида хам кенг кулланилади. Иккинчи вариантни амалга ошириш учун хужум килувчини компания тармогига утказиб юбориш ва унинг барча харакатларини к,айддаш лозим. Бу хавфеизлик маъмурига кейин вактнинг реал масштабида

(ёки берилган тезликда) хужум килувчи томонидан килинган барча харакатларни тиклашга, муваффакиятли тахлиллашга ва уларни кейинчалик бартараф этишга хамда мухркама к,илиш жараёнида йигилган ахборотдан фойдаланишга имкон беради.

Фаол реакция курсатиш категориясига куйидаги вариантлар тааллукди:

- хужум килувчи ишини блокировка килиш;
- хужум килунувчи узел бил аи сеансни тугаллаш;
- тармок, асбоб-ускуналари ва химоя воситаларини бошкариш.

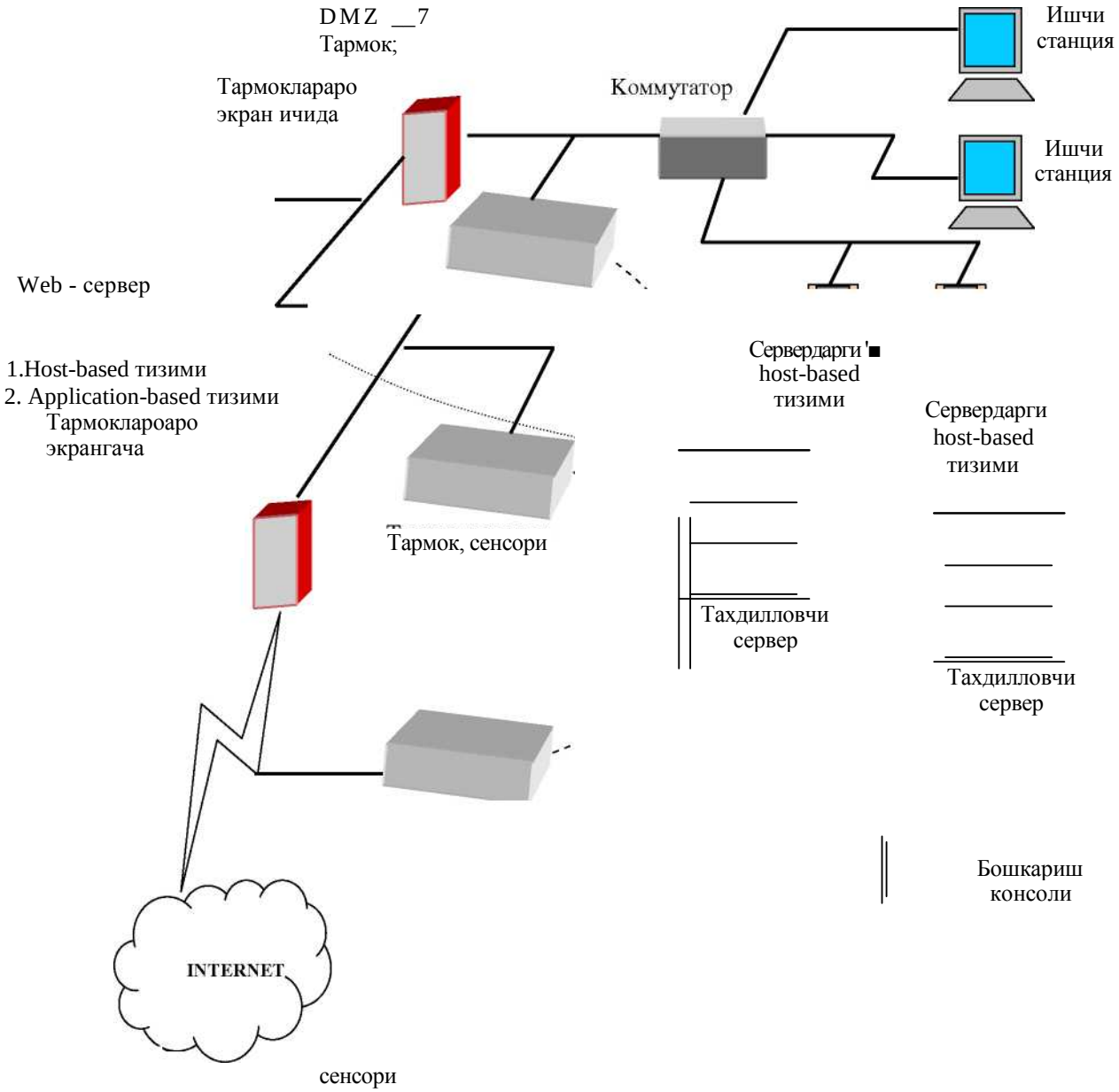
Реакция курсатиш механизмларининг ушбу категорияси бир томондан етарлича самарали булса, иккинчи томондан улардан жуда эхтиётлик билан фойдаланиш зарур, чунки уларни нотугри ишлатиш бутун корпоратив ахборот тизими ишга лаёкатлигининг бузилишига олиб келиши мумкин.

Компонентларни бошцариш цисм тизими хужумларни аниклаш тизимининг турли компонентларини бошкаришга аталган. "Бошкариш" атамаси оркали хужумларни аникдаш тизимининг турли компонентлари (масалан кузатиш модуллари) учун хавфсизлик сиёсатини узгартириш, х,амда ушбу компонентлардан ахборотни (масалан, кайдланган хужум хусусидаги) олиш тушунилади. Бошк,ариш ички протоколлар ва интерфейслар ва ишлаб чикилган стандартлар (масалан, SNMP) ёрдамида амалга оширилиши мумкин.

Хужумларни аникдаш тизимлари иккита архитектура - "автоном агент" ва "агент-менеджер" архитектуралари асосида к,урилади. Биринчи х,олда тармок,нинг хар бир х,имояланувчи узел ва сегментларига тизим агентлари урнатилиб, бу агентлар узаро ахборот алмаша олмайдилар, хамда уларни ягона консол орк,али марказлаштирилган х,олда бошк,ариб булмайди. "Агент-менеджер" архитектураси бу камчиликлардан холи. Бу хрлда катта тармокнинг турли кисмларида жойлашган купгина ШБдан иборат хужумларни аниклашнинг так,симланган тизими dIDS (distributed IDS)fla маълумотларни йигиш серверлари ва марказий тахлилловчи сервер кайдланувчи маълумотларни марказлаштирилган йигишни ва тахлиллашни амалга оширади. dIDS модулларини бошкариш бошк,аришнинг марказий консоли

оркали амалга оширади. Филиаллари турли худудлар, хатто шахарлар буйича тарк,алган йирик ташкилотлар учун бундай архитектуранинг ишлатилиши жиддий ахамиятга эга.

dIDS ишлашининг умумий схемаси 10.4-расмда келтирилган.



10.4-расм. Тщсимланган IDS ишлашининг умумип схемаси

Бундай тизим турли ШБлардан хужумлар хусусидаги ахборотларни марказлаштирилиши эвазига корпоратив к,исм тармок, х,имояланишини кучайтиришга имкон беради. Хужумларни аникловчи так,симланган тизим dIDS к,уйидаги к,исм тизимлардан ташкил топган: бошкариш консоли, тахлилловчи серверлар, тармок, агентлари, хужум хусусидаги ахборотни йигувчи сервер. Марказий тахдилловчи сервер одатда маълумотлар базаси

ва Web-сервердан ташкил топган булиб, хужумлар хусусидаги ахборотни саклашга ва кулай Web-интерфейс ёрдамида маълумотларни манипуляция-лашга имкон беради. Тармок, агенти сИББнинг энг мухим компонентларидан бири хисобланиб, максади марказий тахлилловчи серверга хужум хусусида хабар бериш булган кичкина дастурдир. Хужум хусусидаги ахборотни йигувчи сервер марказий тахлилловчи серверга мантикий таянган ва тармок, агентларидан олинган маълумотларни гурухдашда фойдаланиладиган пара-метрларни белгилайди.

Маълумотларни гурухлашни куйидаги параметрлар буйича амалга ошириш мумкин:

- хужум килувчининг 1Р-адреси;
- кабул килувчининг порти;
- агент номери;
- сана, вакт;
- протокол;
- хужум хиллари ва х,.

ГОБдан фойдаланиш самарадорлигига кандайдир шубхалар булишига карамай, фойдаланувчилар ШБнинг очик, тарк,атилувчи ва тижорат воситаларидан кенг фойдаланадилар.

10.4. Компьютер вируслари ва виру сдан ^имояланиш муаммолари

Компьютер вирусининг куп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: "Компьютер вируси - бошка дастурларни, уларга узини ёки узгартирилган нусхасини киритиш орк,али, уларни модификациялаш билан зах,арловчи дастур. Бунда киритилган дастур кейинги купайиш крбилиятини сакдайди". Вируснинг уз-узидан купайиши ва хисоблаш жараёнини модификациялаш к,обилияти бу таърифдаги таянч тушунчалар хисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ухшаш.

Хозирда компьютер вируси деганда к,уйидаги хусусиятларга эга булган дастурий код тушунилади:

- аслига мое келиши шарт булмаган, аммо аслининг хусусиятларига (уз-узини тиклаш) эга булган нусхаларни яратиш крбилияти;

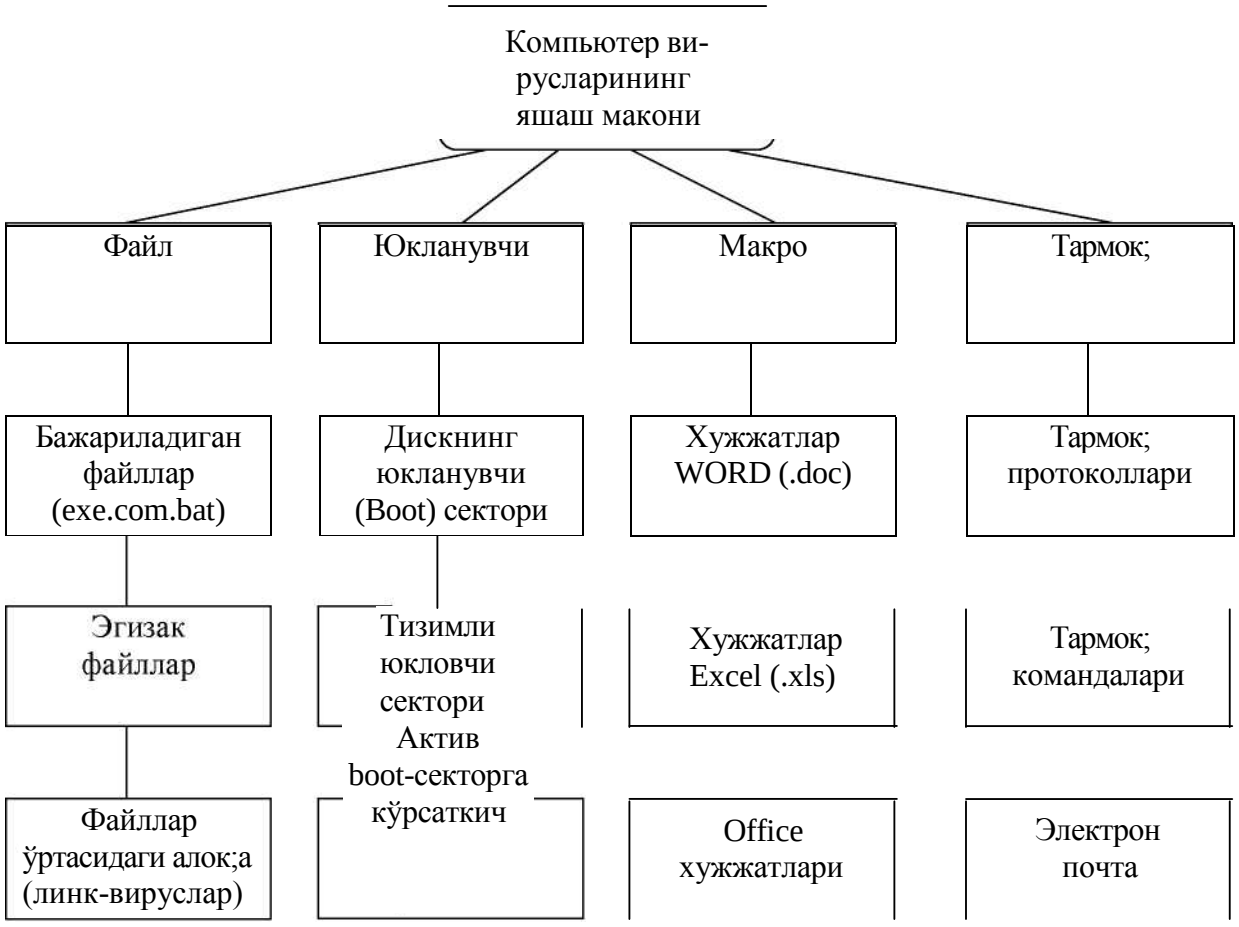
- хисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш л озимки, бу хусусиятлар зарурий, аммо етарли эмас. Курсатилган хусусиятларни хисоблаш мухитидаги зарар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тулдириш л озим.

Вирусларни куйидаги асосий аломатлари буйича туркумлаш мумкин:

- яшаш макони;
- операцион тизим;
- ишлаш алгоритми хусусияти;
- деструктив имкониятлари.

Компьютер вирусларини яшаш макони, бошкача айтганда вируслар киритилувчи компьютер тизими объектларининг хили буйича туркумлаш асосий ва кенг таркалган туркумлаш хисобланади (10.5-расм).



10.5-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Файл вируслари бажарилувчи файлларга турли усуллар билан киритилади (энг куп тар калган вируслар хили), ёки файл-йулдошларни (компаньон вируслар) яратади ёки файлли тизимларни (link-вируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар узини дискнинг юклама секторига (boot - секторига) ёки винчестернинг тизимли юкловчиси (Master Boot Record) булган секторга ёзади. Юклама вируслар тизим юкланишида бошкаришни олувчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан MicroSoft Word, MicroSoft Excel ва х,. каби оммавий мухаррирларнинг файл-хужжатларини ва электрон жадвалларини захарлайди.

Тармоц вируслари узини таркатишда компьютер тармоклари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзида тармок, вирусларини "курт" хилидаги дастурлар деб юритишади. Тармок, вируслари Internet-куртларга (Internet буйича таркалади), IRC-куртларга (чатлар, Internet Relay Chat) булинади.

Компьютер вирусларининг купгина комбинацияланган хиллари хам мавжуд, масалан - тармокди макровирус тахрирланувчи хужжатларни захарлайди, хамда узининг нусхаларини электрон почта оркали тарк,атади. Бошк,а бир мисол сифатида файл-юклама вирусларини курсатиш мумкинки, улар файлларни х,амда дискларнинг юкланадиган секторини захарлайди.

Вирусларнинг щёт даври. Хдр к,андай дастурдагидек компьютер вируслари хаёт даврининг иккита асосий боскичини сакданиш ва бажарилиш боск,ичларини ажратиш мумкин.

Сацланиш босцичи вируснинг дискда у киритилган объект билан биргаликда шундайгина сакданиш даврига тугри келади. Бу боск,ичда вирус вирусга к,арши дастур таъминотига заиф булади, чунки у фаол эмас ва химояланиш учун операцион тизимни назорат кила олмайди.

Компьютер вирусларининг *бажарилиш даври,* одатда, бешта боскични уз ичига олади:

1. Вирусни хотирага юклаш.

2. Курбонни кддириш.
3. Топилган курбонни захарлаш.
4. Деструктив функцияларни бажариш.
5. Бошкаришни вирус дастур-элтувчисига утказиш.

Вирусни хотирага юклаш. Вирусни хотирага юклаш операцион тизим ёрдамида вирус киритилган бажарилувчи объект билан бир вактда амалга оширилади. Масалан, агар фойдаланувчи вирус булган дастурий файлни ишга туширса, равшанки, вирус коди ушбу файл кисми сифатида хотирага юкланади. Оддий хрлда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш булиб, сунгра бошкариш вирус бадани кодига узатилади. Бу харакатлар операцион тизим томонидан бажарилади, вируснинг узи пассив хрлатда булади. Мураккаброк, вазифаларда вирус бошкаришни олганидан сунг узининг ишлаши учун кушимча харакатлар бажариши мумкин. Бу билан боглик, иккита жихат курилади.

Биринчиси вирусларни аникдаш муолажасининг максимал мураккаблашиши билан боглик,. Сакланиш боск,ичида баъзи вируслар х,имояланишни таъминлаш максадида етарлича мураккаб алгоритмдан фойдаланади. Бундай мураккаблашишга вирус асосий баданини шифрлашни киритиш мумкин. Аммо факат шифрлашни ишлатиш чала чора хисобланади, чунки юкланиш боскичида расшифровкани таъминловчи вирус к,исми очик, куринишда сакланиши лозим. Бундай х,олатдан к,утилиш учун вирусларни ишлаб чикувчилар расшифровка килувчи кодини "мутациялаш" механизмидан фойдаланади. Бу усулнинг мох,ияти шундан иборатки, объектга вирус нусхаси киритилишида унинг расшифровка килувчига тааллукди к,исми шундай модификацияланадики, оригинал билан матнли фаркланиш пайдо булади, аммо иш натижаси узгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф вируслар* номини олган. Полифморф вируслар (ро1утогрЫс)-кийин аникланадиган вируслар булиб, сигнатураларга эга эмас, яъни таркибида бирорта хам кодининг доимий кисми йук,. Полиморфизм файлли, юкламали ва макровирусларда учрайди.

Стеле-алгоритмлардан фойдаланилганда вируслар узларини тизимда тула ёки кисман беркитишлари мумкин. стеле-алгоритмларидан фойдаланадиган вируслар - *стелс-вируслар* (Stealth) деб юритилади. Стеле вируслар операцион тизимнинг шикастланган файлларга мурожаатини ушлаб крлиш йули билан узини яшаш маконидалигини яширади ва операцион тизимни ахборотни шикастланмаган кисмига йуналтиради.

Иккинчи жихат *резидент вируслар* деб аталувчи вируслар билан боглик,. Вирус ва у киритилган объект операцион тизим учун бир бутун булганлиги сабабли, юкланишдан сунг улар, табиий, ягона адрес маконида жойлашади. Объект иши тугаганидан сунг у оператив хотирадан бушалади. Бунда бир вактнинг узида вирус хам бушалиб сакланишнинг пассив боскичига утади. Аммо баъзи вируслар хили хотирада сакданиш ва вирус элтувчи иши тугашидан сунг фаол крлиш крбилиятига эга. Бундай вируслар резидент номини олган. Резидент вируслар, одатда, факат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш маконини захарлайди ва маълум шароитларда зараркунандалик вазифасини бажаради. Резидент вируслар хотирада жойлашади ва компьютер учирилишигача ёки операцион тизим кайта юкланишигача фаол хрлда булади.

Резидент булмаган вируслар фак,ат фаоллашган вактларида хотирага тушиб зах,арлаш ва заракунандалик вазифаларини бажаради. Кейин бу вируслар хотирани бутунлай тарк этиб яшаш маконида крлади.

Таъкидлаш лозимки, вирусларни резидент ва резидент булмаганларга ажратиш фак,ат файл вирусларига тааллукли. Юкланучи ва макровируслар-резидент вирусларга тегишли.

Курбонни цидириш. Курбонни к,идириш усули буйича вируслар иккита синфга булинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол кидиришни амалга оширувчи вируслар киради. Иккинчи синфга кидиришнинг пассив механизмларини амалга оширувчи, яъни дастурий файлларга тузок, к,уювчи вируслар тааллукли.

Топилган цурбонни зщарлаш. Оддий хрлда зах,арлаш деганда к,урбон сифатида танланган объектда вирус кодининг уз-узини нусхалаши тушунилади.

Аввал файл вирусларининг захдрлаш хусусиятларини курайлик. Бунда иккита синф вируслари фаркланади. Биринчи синф вируслари узининг кодини дастурий файлга бевосита киритмайди, балки файл номини узгартириб, вирус бадани булган янги файлни яратади. Иккинчи синфга курбон файлларига бевосита кирувчи вируслар тааллукли. Бу вируслар киритилиш жойлари билан характерланади. Куйидаги вариантлар булиши мумкин:

1. ***Файл бошига киритиш.*** Ушбу усул MS-DOSНННТ *com*-файллари учуй энг кулай хисобланади, чунки ушбу форматда хизматчяи сарлавх,алар кузда тутилган.
2. ***Файл охирига киритиш.*** Бу усул энг куп таркалган булиб, вируслар кодига бошкаришни узатиш дастурнинг биринчи командаси *(com)* ёки файл сарлавхасини *(exe)* модификациялаш оркали таъминланади.
3. ***Файл уртасига киритиш.*** Одатда бу усулдан вируслар тузилмаси олдиндан маълум файлларга (масалан, *Command.com* файли) ёки таркибида бир хил кийматли байтлар кетма-кетлиги булган, узунлиги вирус жойлашишига етарли файл ларга татбикан фойдаланади.

Юклама вируслар учун зах,арлаш боск,ичининг хусусиятлари улар киритилувчи объектлар - кайишкрк, ва к,аттик, дискларнинг юкланиш секторларининг сифати ва к,аттик, дискнинг бош юклама ёзуви (MBR) оркали аникланади. Асосий муаммо-ушбу объект улчамларининг чегараланганлиги. Шу сабабли, вируслар узларининг к,урбон жойида сигмаган к,исмини дискда сакдаши, х,амда зах,арланган юкловчи оригинал кодини ташиши лозим.

Макровируслар учун захарлаш жараёни танланган хужжат-курбонда вирус кодини саклашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужжат файллари форматининг макропрограммаларни сакдаши кузда тутилмаган булиши мумкин.

Деструктив функцияларни бажариш. Деструктив имкониятлари буйича безиён, хавфсиз, хавфли ва жуда хавфли вируслар фаркланади.

Безиён вируслар - уз-узидан таркалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, факат дискдаги буш хотирани сарфлайди холос.

Хавфсиз вируслар - тизимда мавжудлиги турли таассурот (овоз, видео) билан богаик, вируслар, буш хотирани камайтирсада, дастур ва маълумотларга зиён етказмайди.

Хавфли вируслар - компьютер ишлашида жиддий нуксонларга сабаб булувчи вируслар. Натижада дастур ва маълумотлар бузилиши мумкин.

Жуда хавфли вируслар - дастур ва маълумотларни бузилишига хамда компьютер ишлашига зарур ахборотни учирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

Бопщаришни вирус дастур - элтувчисига утказиш. Таъкидлаш лозимки, вируслар бузувчилар ва бузмайдиганларга булинади.

Бузувчи вируслар дастурлар захарланганида уларнинг ишга лаёкатлигини сакдаш хусусида кайгурмайдилар, шу сабабли уларга ушбу боскичнинг маъноси йук,.

Бузмайдиган вируслар учун ушбу боскич хотирада дастурни коррект ишланиши шарт булган куринишда тиклаш ва бошкаришни вирус дастур-элтувчисига утказиш билан боглик,.

Зарар келтирувчи дастурларнинг боища хиллари. Вируслардан ташк,ари зарар келтирувчи дастурларнинг куйидаги хиллари мавжуд:

- троян дастурлари;
- мантикий бомбалар;
- масофадаги компьютерларни яширинча маъмурловчи хакер утилиталари;
- InternetflaH ва бошка конфиденциал ахборотдан фойдаланиш паролларини угирловчи дастурлар.

Улар орасида аник, чегара йук,: троян дастурлари таркибида вируслар булиши, вирусларга мантикий бомбалар жойлаштирилиши мумкин ва х,.

Троян дастурлар узлари купаймайди ва тарк,атилмайди. Ташк,аридан троян дастурлар мутлакр беозор куринади, хатто фойдали функцияларни тавсия этади. аммо фойдаланувчи бундай дастурни компьютерига юклаб,

ишга туширса, дастур билдирмай зарар келтирувчи функцияларни бажариши мумкин. Купинча троян дастурлар вирусларни дастлабки таркатишда, Internet оркали масофадаги компьютердан фойдаланишда, маълумотларни угирлашда ёки улар ни йук, килишда ишлатилади.

Мантщий бомба - маълум шароитларда зарар келтирувчи хдракатларни бажарувчи дастур ёки унинг алохдда модуллари. Мантикий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо булганида ёки йук, булганида ва х,. ишга тушиши мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши мумкин.

Вируслар еа зарар келтируечи дастурларни тарцатиш каналлари. Компьютерлар ва корпоратив тармокларни хдмояловчи самарадор тизимни яратиш учун каердан хавф тугилишини аник, тасаввур этиш лозим. Вируслар таркалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усулларга янгиси кушилади.

Таркатшмнинг классик (муттоз) усуллари. Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмашишда, тармок, катологларидан, Web- ёки FTP - серверлардан дастурлар юкланишида таркатилади. Юклама вируслар Компьютерра фойдаланувчи захдрланган дискетани дисководда крлдириб, сунгра операцион тизимни кайта юклашида тушиб крлади. Юклама вирус Компьютерра вирусларнинг бошка хили орк,али киритилиши мумкин. Макрокоманда вируслари MicroSoft Word, Excel, Access файллари каби офис хужжатларининг захарланган файллари алмашинишида таркалади.

Агар захдрланган компьютер локал тармок,к,а уланган булса вирус осонгина файл-сервер дискларига тушиб к,олиши, у ердан каталоглар орк,али тармок,нинг барча компьютерларига утиши мумкин. Шу тарика вирус эпидемияси бошланади. Вирус тармокда шу вирус тушиб колган компьютер фойдаланувчиси хук,укдари каби хук,ук,к,а эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга тушиб к,олиши мумкин. Агар вирус тармок, маъмури ишчи станциясига тушиб крлса ок,ибати жуда огир булиши мумкин.

Электрон почта.

Хрзирда Internet глобал тармоги вирусларнинг асосий манбаи хисобланади. Вируслар билан захарланишларнинг аксарияти MicroSoft Word форматида хатлар алмашишда содир булади. Электрон почта макрокоманда вирусларини таркатиш канали вазифасини утайди, чунки ахборотлар билан бир каторда купинча офис хужжатлари жунатилади.

Вируслар билан захарлаш билмасдан ва ёмон ниятда амалга оширилиши мумкин. Масалан, макровирус билан захарланган мухарриридан фойдаланувчи узи шубха килмаган хрлда, адресатларга захарланган хатларни жунатиши мумкин. Иккинчи тарафдан нияти бузук, одам атайин электрон почта оркали харкандай хавфли дастурий кодни жунатиши мумкин.

Троян Web-сайпглар. Фойдаланувчилар вирусни ёки троян дастурни Internet сайтларининг оддий кузатишда, троян Web-сайтни курганида олиши мумкин. Фойдаланувчи браузерларидаги хатоликлар купинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига за-рар келтирувчи дастурларни киритишига сабаб булади. Троян сайтни куришга таклифни фойдаланувчи оддий электрон хат орк,али олиши мумкин.

Локал тармоклар.

Локал тармоклар хам тезликда зах,арланиш воситаси хисобланади. Агар х,имоянинг зарурий чоралари курилмаса, зах,арланган ишчи станция локал тармоккд киришда сервердаги бир ёки бир неча хизматчи файлларни захарлайди. Бундай файллар сифатида Login.com хизматчи файлни, фирмада к,улланилувчи Excel-жадваллар ва стандарт хужжат-шаблонларни курсатиш мумкин. Фойдаланувчилар бу тармоккд киришида сервердан захарланган файлларни ишга туширади, натижада вирус фойдаланувчи компьютеридан фойдалана олади.

Зарар келтирувчи дастурларни таркатиигнинг бошка каналлари.

Вирусларни таркатиш каналларидан бири дастурий таъминотнинг карокчи нусхалари х,исобланади. Дискетлар ва CD-дисклардаги нокунуний нусхаларда купинча турли-туман вируслар билан захарланган файллар булади. Вирусларни таркатиш манбаларига электрон анжуманлар ва FTP ва BBS файл-серверлар х,ам тааллукли.

Укув юртларида ва Internet-марказларида урнатилган ва умумфойдаланиш режимида ишловчи компьютерлар хам осонгина вирусларни таркатиш манбаига айланиши мумкин. Агар бундай компьютерлардан бири навбатдаги фойдаланувчи дискетидан захдрланган булса, шу компьютерда ишловчи бошка фойдаланувчилар дискетлари хам захдрланади.

Компьютер технологиясининг ривожланиши билан компьютер вируслари хдм, узининг янги яшаш маконига мослашган хрлда, такомиллашади. Хдр кандай онда янги, олдин маълум булмаган ёки маълум булган, аммо янги компьютер асбоб-ускунасига мулжалланган компьютер вируслари, троян дастурлари ва куртлар пайдо булиши мумкин. Янги вируслар маълум булмаган ёки олдин мавжуд булмаган таркатиш каналларидан хдмда компьютер тизимларга татбик, этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан захарланиш хавфини йукртиш учун корпоратив тармокнинг тизим маъмури, нафакат вирусга карши усуллардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

10.5. Вирусга карши дастурлар

Компьютер вирусларини аниклаш ва улардан химояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чик,илган булиб, бу дастурлар компьютер вирусларини аниклаш ва йукотишга имкон беради. Бундай дастурлар вирусга карши дастурлар деб юритилади. Умуман, барча вирусга карши дастурлар захарланган дастурларнинг ва юклама секторларнинг автоматик тарзда тикланишини таъминлайди.

Вирусларга к,арши дастурлар фойдаланадиган вирусларни аниклашнинг асосий усуллари к,уйидагилар:

- эталон билан такдослаш усули;
- эвристик тахлил;
- вирусга карши мониторинг;
- узгаришларни аникдовчи усул;
- компьютернинг киритиш/чикариш базавий тизимига (BlOSra) вирус га к,арши воситаларни урнатиш ва х,.

Эталон билан тащослаш усули энг оддий усул булиб, маълум вирусларни кхгдиришда ник,облардан фойдаланади. Вируснинг ник,оби-мана шу муайян вирусга хос коднинг кдндайдир узгармас кетма-кетлигидир. Вирусга кдрши дастур маълум вирус ник,обларини кхгдиришда текширилувчи файлларни кетма-кет куриб чикдди (сканерлайди). Вирусга кдрши сканерлар факдт ник,об учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг сукхглиб киришидан химояламайди. Янги дастурни ёки юклама секторини захдрлашда кодини тула узгартира олувчи шифрланувчи ва полиморф вируслар учун ник,об ажратиш мумкин эмас. Шу сабабли сканер уларни аникдамайди.

Эвристик тщлил. Компьютер вируси купайиши учун хотирада нусхаланиш, секторга ёзилиш каби кдндайдир муайян харакатларни амалга ошириши лозим. Эвристик тахдиллагичда бундай хдракатларнинг руйхати мавжуд. Эвристик тахдиллагич дастурларни ва диск ва дискет юклама секторларини, уларда вирусга хос кодларни аникдашга уринган хрлда, текширади. Тахлиллагич зах,арланган файлни топиб, монитор экранига ахборот чикдради ва шахсий ёки тизимли журналга ёзади. Эвристик тахлил олдин маълум булмаган вирусларни аникдайди.

Вирусга карши мониторинг. Ушбу усулнинг мохияти шундан иборатки, компьютер хотирасида бошк,а дастурлар томонидан бажарилувчи шубх,али х,аракатларни мониторингловчи вирусга кдрши дастур доимо булади. Вирусга кдрши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сакданувчи хужжатларни, Internet орк,али олинган ёки дискетдан ёки хдр к,андай компакт-дискдан нусх,аланган дастур ва хужжатларнинг файлларини текширишга имкон беради. Агар кдндайдир дастур хавфли хдракатни кхшишта уринмок,чи булса, вирусга к,арши монитор фойдаланувчига хабар беради.

Узгаришларни анщлоечи усул. Дискни тафтиш кхглувчи деб аталувчи ушбу усулни амалга оширишда вирусга кдрши дастур дискнинг хужумга дучор булиши мумкин булган барча сох,аларини олдиндан хотирлайди, сунгра уларни вак,ти-вак,ти билан текширади. Вирус компьютерларни захдрлаганида к,аттик, диск таркибини узгартиради: масалан, дастур ёки

хужжат файлига узининг кодини кушиб куяди, Autoexec.bat файлига дас-тур-вирусни чакиришни кушали, юклама секторни узгартиради, файл-йулдош яратади. Диск сох,алари характеристикаларининг кийматлари со-лиштирилганида вирусга карши дастур маълум ва ноъмалум вируслар томо-нидан килинган узгаришларни аниклаши мумкин.

Компъютерларнинг киритиш/чщариш базавий тизимига (BlOSza) ви-русга царши воситаларни урнатиш. Компьютерларнинг тизимли платасига вируслардан химоялашнинг оддий воситалари урнатилади. Бу воситалар каттик, дискларнинг бош юклама ёзувига хамда дисклар ва дискетларнинг юклама секторларига барча мурожаатларни назоратлашга имкон беради. Агар кандайдир дастур юклама секторлар таркибини узгартиришга уринса, химоя ишга тушади ва фойдаланувчи огохдантирилади. Аммо бу х,имоя жу-да х,ам ишончли эмас.

Вирусга царши дастурларнинг хиллари. Вирусга карши дастурлар-нинг куйидаги хиллари фаркланади:

- дастур-фаглар (вирусга к,арши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка килувчилар;
- дастур-иммунизаторлар.

Дастур-фаглар энг оммавий ва самарали вирусга карши дастур хисобланади. Самарадорлиги ва оммавийлиги буйича иккинчи уринда дастур-тафтишчилар туради. Одатда, бу иккала дастур хиллари битта вирусга карши дастурга бирлаштирилади, натижада унинг к,уввати анчагина ошади. Турли хил блокировка килувчилар ва иммунизаторлар х,ам ишлатилади.

Дастур-фаглар (сканерлар) вирусларни аниклашда эталон билан так,к,ослаш усулидан, эвристик тахлиллашдан ва бошкалардан фойдаланади. Дастур-фаглар оператив хотира ва файлларни сканерлаш йули билан муай-ян вирусга характерли булган ник,обни к,идиради. Дастур-фаглар нафак,ат вируслар билан захарланган файлларни топади, балки уларни даволайди хам, яъни файлдан дастур-вирус баданини олиб ташлаб, файлни дастлабки холатига кайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниклайди ва уларни йук,отади, сунгра файлларни даволашга

киришади. Файллар ичида вирусларни катта сонини к,идиришга ва йук, килишга аталган дастур-фаглар, яъни полифаглар хам мавжуд.

Дастур-фаглар иккита категорияга булинади: универсал ва ихтисослаштирилган сканерлар. Универсал сканерлар сканер ишлаши мулжалланган операцион тизим хилига боглик, булмаган хрлда, вирусларнинг барча хилларини кидиришга ва зарарсизлантиришга мулжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни зарарсизлантиришга аталган. Факат макровирусларга мулжалланган ихтисослаштирилган сканерлар MS WORD ва Excel мухитларида хужжат алмашиниш тизимини химоялашда энг кулай ва ишончли ечим хисобланади.

Дастур-фаглар сканерлашни "бир зумда" бажарувчи мониторинглашнинг резидент воситаларига ва факат суров буйича тизимни текширишни таъмнловчи резидент булмаган сканерларга хам булинади. Мониторинглашнинг резидент воситалари тизимни ишончлирок, химоялашни таъминлайди, чунки улар вируслар пайдо булишига даров реакция курсатади, резидент булмаган сканер эса вирусни аниклаш крбилиятига факат навбатдаги ишга туширилишида эга булади.

Дастур-фагларнинг афзаллиги сифатида уларнинг универсаллигини курсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни кидириш тазлигининг нисбатан катта эмаслигини ва вирусга карши базаларнинг нисбатан катта улчамларини курсатиш мумкин. Ундан ташкари, янги вирусларнинг доим пайдо булиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

Дастур-тафтишчилар (CRC-сканерлар) вирусларни кидиришда узгаришларни аникдовчи усулдан фойдаланади. CRC-сканерлар дискдаги файллар/тизимли сектордагилар учун CRC-йигиндини (циклик назорат кодини) хисоблашга асосланган. Бу CRC-йигиндилар вирусга карши маълумотлар баъзасида файллар узунлиги, саналар ва охирги модификацияси ва бошк,а параметрлар хусусидаги кушимча ахборотлар билан бир к,аторда сакланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал х,исобланган кийматларни так,к,ослайди. Агар маълу-

мотлар базасидаги ёзилган файл хусусидаги ахборот реал кдшматларга мое келмаса, CRC-сканерлар файл узгартирилганлиги ёки вирус билан захдрланганлиги хусусида хабар беради. Одатда холатларни такдослаш операцион тизим юкланишдан сунг дархрл утказилади.

CRC-сканерларнинг камчилиги сифатида уларнинг янги файллардаги вирусларни аникдай олмаслигини курсатиш мумкин, чунки уларнинг маълумотлар базасида бу файллар хусусидаги ахборот мавжуд эмас.

Дастур-блокировка цилувчилар вирусга кдрши мониторинглаш усулини амалга оширади. Вирусга кдрши блокировка к,илувчилар резидент дастурлар булиб, вирус хавфи вазиятларини тухтатиб к,олиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг купайиши онларидаги характерли чак,ирикдар киради. Блокировка К11лувчиларнинг афзалликлари сифатида вируслар купайишининг илк боскхгчида уларни тухтатиб к,олишини курсатиш мумкин. Бу айник,са, купдан бери маълум вируснинг мунтазам пайдо булишида мухим х,исобланади. Аммо, улар файл ва дискларни даволамайди. Блокировка к,илувчиларнинг камчилиги сифатида улар химоясининг айланиб утиш йулларининг мавжудлигини ва уларнинг "хираликлигини" (масалан, улар бажарилувчи файлларнинг харкдндай нусхаланишига уриниш хусусида мунтазам огохдантиради) курсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга кдрши блокировка к,илувчилар мавжуд.

Дастур-иммунизаторлар — файллар захдрланишини олдини олувчи дастурлар икки хилга булинади: захдрланиш хусусида хабар берувчи ва вируснинг кдндайдир хили буйича зах,арланишни блокировка к,илувчи. Биринчи хил иммунизаторлар, одатда, файл охирига ёзилади ва файл ишга туширилганда хдр марта унинг узгаришини текширади. Бундай иммунизаторлар битта жиддий камчиликка эга. Улар стелс-вирус билан захарланишни аникдай олмайдилар. Шу сабабли бу хил иммунизаторлар хрзирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан захдрланишдан химоялайди. Бу иммунизатор дастур ёки дискни шундай мо-

дификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни захарланган деб кабул килади ва сукилиб кирмайди. Иммунизациялашнинг бу хили универсал булаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмалум вирусдан, у вирусга карши сканерлар томонидан аникданишига кадар, ишончли химоялаши мумкин.

Вирусга царши дастурнинг сифат мезонлари. Вирусга карши дастурни бир неча мезонлар буйича бахрлаш мумкин. Куйида бу мезонлар мухимлиги даражаси пасайиши тартибда келтирилган:

- ишончлилик ва ишлаш кулайлиги фойдаланувчилардан махсус харакатларни талаб этувчи техник муаммоларнинг йуклиги; вирусга карши дастурнинг ишончлилиги энг мухим мезон хисобланади, чунки хатто энг яхши вирусга карши дастур сканерлаш жараёнини охиригача олиб бора олмаса, у бефойда хисобланади;

- вирусларни барча тарк,алган хилларини аниклаш фазилати, ички файл-хужжатлар/жадвалларни (MS Office), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга карши дастурнинг асосий вазифаси-100% вирусларни аниклаш ва уларни даволаш;

- барча оммавий платформалар (DOS, Windows 95/NT, Novell Net Ware, OS/2, Alpha, Linux ва х,.) учун вирусга карши дастур версияларининг мавжудлиги; суров буйича сканерлаш ва "бир зумда" сканерлаш режимларининг борлиги, тармокни маъмурлаш имкониятли сервер версияларининг мавжудлиги. Вирусга карши дастурнинг куп платформалилиги мухим мезон хисобланади, чунки муайян операцион тизимга мулжалланган дастургина бу тизим функцияларидан тула фойдаланиш мумкин. Файлларни "бир зумда" текшириш имконияти хам вирусга карши дастурларнинг етарлича мухим мезони хисобланади. Компьютерга келувчи файлларни ва куйилувчи дискетларни бир лахзада ва мажбурий текшириш вирусдан захарланмасликка 100%-ли кафолат беради. Агар вирусга карши дастурнинг сервер вариантида тармокни маъмурлаш имконияти булса, унинг киймати янада ошади.

- ишлаш тезлиги. Вирусга кдрши дастурнинг ишлаш тезлиги хдм унинг мухдм мезони хисобланади. Турли вирусга кдрши дастурларда вирус -ни кддиришнинг хдр хил алгоритмларидан фойдаланилади. Вир алгоритм тезкор ва сифатли булса, иккинчиси сует ва сифати паст булиши мумкин.

Х,имоянинг профилактика чоралари. Хдр бир компьютерда вирус -лар билан захдрланган файллар ва дискларни уз вак,тида аникдаш, аникданган вирусларни тамомила йук,отиш вирус эпидемиясининг бошкд компьютерларга таркдлишининг олдини олади. Хдр кдндай вирусни аникдашни ва йук, к,илишни кафолатловчи мутлок, ишончли дастурлар мавжуд эмас. Компьютер вируслари билан курашишнинг мухим усули уз вак,тидаги профилактика хисобланади.

Вирусдан захдрланиш эхтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сакданишини таъминлаш учун к,уйидаги профилактика чораларини бажариш лозим:

- факдт к,онуний, расмий йул билан олинган дастурий таъминотдан фойдаланиш;

- компьютерни замонавий вирусга кдрши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошкд компьютерларда дискетда ёзилган ахборотни укдшгдан один бу дискетда вирус борлигини узининг компьютеридаги вирусга кдрши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элтувчиларини сакдашга ва ишчи ахборотни сакданишига эътибор бериш;

- компьютер тармокдаридан олинувчи барча бажарилувчи файлларни назоратлашда вирусга кдрши дастурдан фойдаланиш;

- компьютерни юклама вируслардан захдрланишига йул к,уймаслик учун, операцион тизим ишга туширилганида ёки кдйта юкланишида дисковод чунтагида дискетани к,олдирмаслик.

Вирусга к,арши дастурларнинг хдр бири узининг афзалликларига ва камчиликларига эга. Фак,ат вирусга кдрши дастурларнинг бир неча хилини комплекс ишлатилиши мак,бул натижага олиб келиши мумкин.

Куйида вирусдан захдрланиш профилактикасига, вирусларни аниклаш ва йукртишта мулжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) - Россиянинг вирусга карши пакети. Пакет таркибига куйидагилар киради:

Office Guard - блокировка килувчи, макровирусдан 100% хдмояланишни таъминлайди;

- Inspector - тафтишчи, компьютердаги барча узгаришларни кузатади, вирус фаоллиги аникланганида дискнинг асл нусхасини тиклашга ва зарар келтирувчи кодларни чикариб ташлашга имкон беради;

- Monitor - вирусларни ушлаб колувчи, компьютер хотирасида доимо хрзир булиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида улар ни вирусга карши текширади;

- Scanner - вирусга карши модул, локал ва тармок, дисклар таркибини кенг куламли текшириш имконини беради. Сканерни кул ёрдамида ёки берилган вактда автоматик тарзда ишга тушириш мумкин.

Пакет ёрдамида электрон постани вирусга карши фильтрлаш ва почта корреспонденциясини комплекс текшириш амалга оширилади. Вирусга карши базани янгилаш Internet оркали бажарилади.

Dr.Web - Россиянинг вирусга карши оммавий дастури, Windows 9x/NT/2000/XP учун мулжалланган булиб, файлли, юклама, ва файл-юклама вирусларни кидиради ва зарарсизлантиради. Дастур таркибида резидент крровул SpIDer Guard, Internet оркали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган.

Dr.Web да ишлатилувчи алгоритмлар хакида маълум булган барча вирус хилларини аниклашта имкон беради. Dr.Web дастурининг мухим хусусияти - оддий сигнатурли кидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниклаш имкониятидир.

Symantec Antivirus - Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга к,арши мах,сулоти туплами.

Symantec мах,сулотидан ишчи жойларининг умумий сони 100 ва ундан ортик, булганида ва булмаганда битта Windows NT/2000/NetWare серве-

ри мавжудлигида фойдаланиш максадга мувофик, хисобланади. Ушбу пакетнинг бапщалардан ажралиб турадиган хусусияти куйидагилар:

- бошкаришнинг иерархик модели;
- янги вирус пайдо булишига реакция килиш механизмининг мавжудлиги.

AntiVir Personal Edition - вирусга карши дастур AVP, Dr.Web ва х,.лар имкониятларидек имкониятларга эга. Дастур комплектига куйидагилар киради:

- дискларни сканерловчи;
- резидент крровул;
- бошкариш дастури;
- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet оркали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси хам мавжуд. Дастур хотирани, юкланиш секторини текширишда ва унда вируслар буйича кенг куламдаги маълумотнома мавжуд.

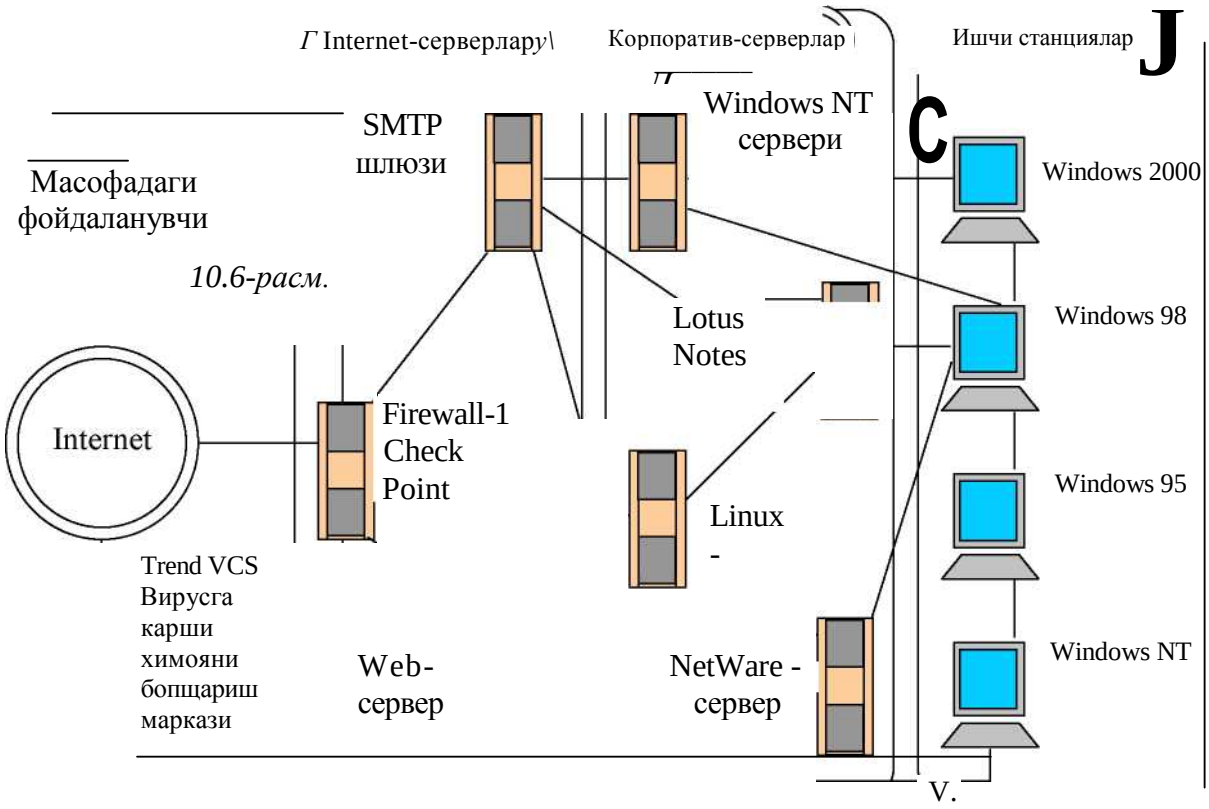
10.6. Вирусга карши з^имоя тизимини

Хрзирда уртача компаниянинг корпоратив компьютер тармоги таркибида унлаб ва юзлаб ишчи станциялари, унлаб серверлар, телекоммуникациянинг турли фаол ва пассив асбоб ускуналари мавжуд булган етарлича мураккаб тузилмага эга (10.6-расм).

Корпоратив тармокдан фойдаланувчилар тармокда вирусларнинг сук,илиб кириш файллари билан доимо тук,нашадилар. Internet/intranet корпоратив тизимларига вирус хужумлари мунтазам булиб туради, фойдаланувчи ишчи станциясининг зах,арланган ахборот элтувчиси томонидан захарланиши эса одат тусини олган.

Корпоратив тармок, вируслар ва бошка зарар келтирувчи дастурлар хужумларига дучор булганида тармок,нинг вирусга к,арши химояси купинча вирусга к,арши локал дастурий таъминот ёрдамида, сканерлаш ва катор ишчи станцияларни даволаш билан тугайди ва х,имоя таъминланади деб

хисобланади. Аслида муаммонинг бундай локализациялаш минимал чора хисобланади ва корпоратив тармокнинг кейинги баркарор ишлашини кафолатламайди. Бошкача айтганда, вирусга карши локал ечимларнинг ишлатилиши корхонани вирусдан самарали хдмоялаш учун зарурий, аммо етарли восита хдсобланмайди.



Корпоратив тармоц намунавий архитектураси

Вирусга карши х,имоянинг самарали корпоратив тизими-"мижоз-сервер" технологияси буйича амалга оширилган, тармокдаги х,ар к,андай шубх,али харакатни сезгирлик билан фах,млаб олувчи, тескари богланишли мосланувчан тизимдир. Бундай тизим корпоратив тармокнинг ички тузилмаси доирасида вирусларни ва бошк,а ганим дастурларнинг тарк,алишига йул к,уймайди. Вирусга карши химоянинг самарали корпоратив тизими турли вирус хужумларини-маълумларини, хам номаълумларини, улар намоён булишининг дастлабки боскичида, аникдайди ва бетарфлаштиради.

Албатта, турли вазиятлар булиши мумкин, масалан масофадан фойдаланувчининг зах,арланган компьютерини корпоратив серверга улаганда ёки макровируслар булган WORD ёки Excel файлли дискетлардан иш жойларида фойдаланишда тармок, зах,арланиши мумкин. Аммо, сифатли курилган

вирусга карши химоянинг корпоратив тизими учун бу жидций эмас, чунки, биринчидан, захдрланишнинг курсатилган хрлатлар камдан-кам учрайди, иккинчидан, вируслар вактида аникланади ва бетарафлаштирилади. Натижада уларнинг купайишига ва корпоратив тармок, доирасида таркалишига йул куйилмайди.

Уланадиган ишчи станциялари сони ошган сари корпоратив тармокнинг хизмат курсатиш нархи оша боради. Корпоратив тармокни вируслардан химоялаш харажатлари корхона умумий харажатлари руйхатида охирги бандини эгалламайди.

Ушбу харажатларни корпоратив тармокни вирусга карши химоялашни вактнинг реал масштабида марказлаштирилган бошкариш оркали оптималлаштириш ва камайтириш мумкин. Бундай ечим корхона тармоги маъмурларига вирусни барча сукилиб кириш нукталарини бошк,аришнинг ягона консоли орк,али кузатишга ва корпоратив тармокдаги барча вирусга карши воситаларни самарали бошк,аришга имкон беради. Вирусга карши химояни марказлаштирилган бошкариш максади жуда оддий - вирусларнинг барча сукилиб кириш нукталарини блокировка килиш. Куйидаги сук,илиб киришларни ва захарланишларни курсатиш мумкин:

- ташувчи манбалардан (флоппи-дисклар, компакт-дисклар, Zip, Jazz, Floptical ва х,.) охирги зах,арланган файллардан фойдаланишда ишчи станцияларга вирусларнинг сукилиб кириши;

- InternetflaH Web ёки FTP орк,али олинган локал ишчи станциясида сакданган зах,арланган текин дастурий таъминот ёрдамида зах,арланиш;

- масофадаги ёки мобил фойдаланувчиларнинг зах,арланган ишчи станциялари корпоратив тармоккд уланганида вирусларнинг сукилиб кири ши;

- корпоратив тармоккд уланган масофадаги сервердаги вируслар билан захарланиш.

- иловаларида макровируслар билан зах,арланган Excel ва Word файллар булган электрон почтанинг таркалиши.

Вируслардан ва бошка зарар келтирувчи дастурлардан х,имояловчи корпоратив тизимни куриш к,уйидаги боск,ичларни уз ичига олади.

Биринчи босқичда химояланувчи тармокнинг узига хос хусусиятлари аникланади ва бир неча вирусга карши химоя вариантлари танланади ва асосланади. Бу боскичда куйидагилар бажарилади:

- компьютер тизими ва вирусга карши химоя воситаларининг аудити;
- ахборот тизимини текшириш ва *картирлаш;*
- вирусларнинг сукилиб кириши билан боглик, тахдидларнинг амалга ошириш сценарийсини тахлиллаш.

Натижада вирусга карши химоянинг умумий хрлати бахрланади. *Иккинчи босқичда* вирусга карши хавфсизлик сиёсати ишлаб чикилади. Бу боскичда куйидагилар бажарилади:

- ахборот ресурсларини туркумлашнинг тури;
- вирусга карши хавфсизликни таъминловчи кучларни яратиш- вакалатларни таксимлаш;
- вирусга к,арши хавфсизликни ташкилий-хукукий мададлаш;
- вирусга карши хавфсизлик инструментларига талабларни аникдаш;
- вирусга карши хавфсизликни таъминлаш харажатларини хисоблаш.

Натижада корхонанинг вирусга карши хавфсизлик сиёсати ишлаб чикилади.

Учинчи босқичда дастурий воситалари, ахборот ресурсларини инвентаризациялаш ва мониторингини автоматлаштириш воситалари танланади. Вирусга карши хавфсизликни таъминлаш буйича ташкилий тадбирлар руйхати ишлаб чик,илади.

Натижада корхонанинг вирусга карши хавфсизлигини таъминловчи режа ишлаб чикилади.

Туртинчи боск,ичда вирусга карши танланган ва тасдикданган хавфсизлик режаси амалга оширилади. Бу боскичда вирусга карши воситалар етказиб берилади, жорий этилади ва мададланади.

Натижада корпоратив вирусга карши химоялашнинг самарали тизими яратилишига имкон тугилади.

XI боб. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОИВДА АХБОРОТНИ ХИМОЯЛАШ

11.1. Маълумотларни узатиш тармоцларида ахборот щшоясини таъминлаш

Маълумотларни узатиш тармокдарида ахборот химоясини таъминлаш масаласи маълумотлар узатиш тармогининг муайян архитектурасини амалга оширувчи ва унинг баркарор ишлашини таъминловчи аппарат-дастурий воситалари билан боглик, хрлда ечилиши лозим.

Маълумотларни узатиш тармокдарида ахборот хавфсизлигини таъминлашга куйидаги талаблар куйилади:

маълумотларни узатиш тармокдарида ахборот хавфсизлигига буладиган маълум тахдидлардан химоялаш хизмати ва механизмларини белгиловчи *функционал талаблар;*

- ахборот хавфсизлигига буладиган маълум тахдидлардан химоялаш механизмини маълумотларни узатиш тармоги архитектурасига кай тарзда жорий этилиши лозимлигини белгиловчи *архитектуравий талаблар;*

- бошкдришнинг к,андай функциялари ишлаб чик,илиши ва улар к,ай тарзда маълумотларни узатиш тармогига жорий этилишини белгиловчи *бошкариш (маъмурлаш) талаблари.*

Функционал талаблар. Маълумотларни узатиш тармоги компонентларига ва архитектурасига реал таъсир этувчи умумий функционал талаблар куйидагилар:

фойдаланувчини аутентификациялаш. Маълумотларни узатиш тармогида ахборот хавфсизлигини таъминловчи тизим ахборотни (маълумотларни) узатиш жараёнида иштирок этувчи компонентининг (объект, субъект ва фойдаланувчининг) хакикийлигини аникдаш имкониятини таъминлаши лозим;

- *назоратланувчи фойдаланиш.* Маълумотларни узатиш тармогида ах борот хавфсизлигини таъминловчи тизим тармок, субъектлари ва фойдала-

нувчиларининг рухсат этилмаган ахборот ресурсларидан фойдалана олмасликларини кафолатлаши л озим;

- *конфиденциалликни таъминлаш.* Конфиденциалликни таъминлаш хизмати асосан маълумотларни узатиш тармогини ахборот мухитини очиш, ахборотдан рухсатсиз фойдаланиш ва угирлаш имкониятларидан химоялаш учун зарур хисобланади;

- *маълумотлар яхлитлигини таъминлаш.* Маълумотларни узатиш тармогида ахборот хавфсизлигини таъминловчи тизим таркибида фойдаланувчи ва бошкариш ахбороти булган маълумотларнинг сакланиш ва узатилиш яхлитлигини кафолатлаши лозим. Маълумотларнинг бузилиши, сохталаштирилиши, кечиктирилиши, рухсатсиз кайталаниши ахборот узатилишининг блокировка килинишига олиб келиши мумкин;

- *цатьий хисоб-китоб.* Маълумотларни узатиш тармоги ресурсларидан фойдаланувчи хар кандай субъект бажарган хар кандай амаллари учун жавоб бериши лозим. Маълумотларни узатиш тармоги устида килинган барча харакатлар ва тармокда содир булган барча ходисалар хусусидаги ахборотнинг сакланиш имконияти таъминланиши лозим;

- *хавфни билдирувчи сигнални генерациялаш.* Маълумотларни узатиш тармоги тармок, ахборот хавфсизлиги объектлари томонидан хавфсизликнинг бузилиши хусусидаги сигнални генерациялаш имконини таъминлаши лозим;

- *аудит.* Аудит тизимни бошкаришнинг самарадорлигини бах,олаш х,амда ахборот хавфсизлигининг бузилишини аникдаш мак,садида тизимли ёзувларни ва амалларни мустак,ил тахлиллаш ва тадкиклаш сифатида курилиши лозим;

- *тиклаш.* Маълумотларни узатиш тармогида ахборот хавфсизлигини таъминлаш тизими хавфсизликнинг бузилишини тиклаш крбилиятига эга булиши лозим. Хар доим, качон ахборот хавфсизлигини бузишга уриниш содир булганида, тизим ушбу уриниш хусусидаги ахборотни шундай ишлаши лозимки, ушбу уриниш маълумотларни узатиш тармогининг утказиш крбилиятини ва фойдаланувчанлигини жиддий пасайишига олиб келмасин;

- *мосланувчанлик.* Маълумотларни узатиш тармогида ахборот хавфсизлигини таъминлаш тизимига куйиладиган мухим концептуал талаб-мосланувчанлик талаби, яъни алока тармогининг тузилмаси, технологияси ва ишлаш шароити узгарганида мослашув крбилияти талабидир.

Архитектураеий талаблар. Маълумотларни узатиш тармогида ахборот хавфсизлигини таъминлаш тизими ахборот хавфсизлигининг турли сиёсатини мададлаши, яъни мосланувчан булиши лозим. Тизимга кйидаги асосий хизматлар киритилиши мумкин:

- шифрлаш калитларини ва паролларни шакллантириш, саклаш ва таксимлаш хизмати;
- шифрлаш хизмати;
- фойдаланувчиларни ва хабарларни аутентификациялаш хизмати;
- фойдаланишни бошкариш хизмати;
- хабарлар яхлитлигини таъминлаш хизмати;
- фойдаланувчанликни таъминлаш хизмати;
- етказилганликни тасдиклаш хизмати;
- рад к,илмаслик хизмати;
- кушимча трафикни шакллантириш хизмати;
- маъмурлаш хизмати.

Бу хизматларнинг хар бири ахборот хавфсизлигини таъминлаш буйича масалаларни мустак,ил тарзда у ёки бу химоя механизмларидан фойдаланиб ечиши мумкин. Бунда химоянинг битта механизми ахборот хавфсизлигининг турли хизматларида кулланилиши мумкин.

Бошцариш (маъмурлаш) талаблари. Маълумотларни узатиш тармогида ахборот хавфсизлигини маъмурлаш хизмати химоянинг техник воситаларини тулдирувчи химоя чораларининг маълум комплексини уз ичига олади. Бу химоя чоралари бузгунчининг тармок, ахборот хавфсизлигига тах,дидни кучайтиришга к,аратилган у ёки бу таъсирни утказишини к,ийинлаштириш максадида мавжуд х,имоя тизимига оператив тарзда узгартиришлар киритишга имкон яратади.

Маъмурлаш хизматининг асосий вазифалари к,уйидагилар:

- химоя хизмати ва механизмига зарур ахборотни таркатиш;

- хдмоя хизмати ва механизмининг ишлаши хусусидаги ахборотни йигаш ва тахлиллаш;

- хдмояланувчи объектларни аниклаш;

- хизмат функцияларини самарали амалга ошириш максадида хдмоя механизмларини комбинациялаш;

- маълумотларни узатиш тармогининг ишончли ва баркарор ишлашини таъминлаш хизматларига жавобгар бошка маъмурлар билан узаро алока;

-маълумотларни узатувчи тармокнинг бузилган ишлаш жараёнини тиклаш.

Хавфсизлик маъмури маъмурлаш хизматининг мухим элементи хисобланади. Ахборот хавфсизлигининг хдр кандай воситаларидан фойдаланилмасин, маълумотларни узатиш тармогида ахборот хавфсизлигини таъминлаш сифати маъмурнинг крбилиятига, унинг тиришишига, техник жихозланганлигига богаик,.

Таъкидлаш лозимки, бирорта хам реал химояланган маълумотларни узатиш тармога мутлок, хдмояланган булмайди. Шунга карамасдан х,имоянинг адекват чоралари бузгунчи таъсири самарасини (зарар келтириш харажатининг кутилаётган зарар улчамига нисбатини) анчагина пасайтиради.

11.2. Ало^а каналларида маълумотларни з^имоялаш усуллари

Маълумотларни узатишни химоялаш масаласини ечиш усулларининг учта асосий гурухи мавжуд: каналга мулжалланган химоялаш усуллари, чеккалараро х,имоялаш усуллари ва уланишга мулжалланган химоялаш усуллари. Биринчиси х,ар бир канал учун мустакил равишда маълумотлар ок,имини х,имоялашни таъминласа, иккинчиси х,ар бир хабарни, уни манбадан адресатгача узатишда умумий х,имоялашни таъминлайди. Учинчи усул иккинчи усулнинг бир тури хисобланади.

Каналга мулжалланган усуллар манба ва адресатга богаик, булмаган хрлда, алох,ида узеллар орасидаги алох,ида алок,а канали буйича узатилаётган хабарлар ок,имини хдмоялашни таъминлайди. Бу хил х,имояни таъмин-

лашда бузгунчининг узелга (пакетни коммутацияловчи марказга) Караганда каналга таъсир этиш кулайлиги фараз килинади. Ундан ташкари, маълумотларни узатиш тармогидаги узелларни фойдаланувчи терминалларини химоялагандек химоялаш мумкин эмас ёки иктисод нуктаи назаридан фойдасиз. Ушбу гурух, усулларининг камчилиги-кисм тармок, узелларидан бирининг очилиши тармок, оркали утаётган хабарлар окимининг талайгина кисмини очилишига олиб келиши мумкин.

Терминаллар ва тармокдар уртасидаги алока каналларини каналга мулжалланган химоялаш харажатлари бевосита дахлдор тарафлар томонидан крплансада, маълумотларни узатиш кием тармога ичидаги каналга мулжалланган химоялаш усулларининг умумий нархи кием тармокдан фойдаланувчиларнинг барчаси уртасида хисоблаб чик,илиши мумкин.

Чеккалараро щмоялаш усуллари хабарларни манба узеллари ва кабул килувчи орасида узатиш жараёнида шундай х,имоялайдики, манба ва адресат орасидаги алок,а каналларидан биринг очилиши хабарлар окимининг очилишига олиб келмайди. Ушбу усулларнинг асосий афзаллиги - улардан фойдаланиш масаласи алох,ида фойдаланувчилар орасида, бошка фойдаланувчиларни жалб этмасдан, ечилиши мумкин.

Уланишга мулжалланган усуллар. Аксарият к,улланиш сох,аларида маълумотларни узатиш тармогини манбадан адресатгача уланишни ёки виртуал канални урнатиш учун фойдаланувчига такдим этилувчи мух,ит сифатида тасаввур этиш мумкин. Бундай тасаввур этишда х,имоя уланишга муллжалланиши фараз к,илинади, яъни, х,ар бир уланиш ёки виртуал канал алох,ида х,имояланади. Шундай к,илиб, уланишга мулжалланган усуллар чеккалар аро химоялаш усулларининг бир тури хисобланади. Уланишга мулжалланган усуллар турли шароитларда умумий химоянинг юкрри даражасини таъминлайди ва химояга к,уйиладиган талаблар хусусидаги фойдаланувчининг идрокига мое келади. Чунки, уланишга мулжалланган ахборот конфиденциаллигини химоялаш усуллари асбоб-ускунани химоялашни, масалан, фак,ат хабарлар манбаида ва кабул килувчида ахборотдан рухсатсиз фойдаланишдан х,имоялашни кузда тутади. Айни вактда х,имоялашнинг каналга мулжалланган усуллари рухсатсиз фойдаланишдан химоялашнинг

маълумотларни узатиш тармогидаги хар бир узели томонидан таъминланишини талаб этиши мумкин. аммо, баъзида иккала усулни куллаганда химоялашнинг тежамли даражасига эришилади.

Маълумотларни узатишни химоялашнинг у ёки бу усулидан фойдаланишдаги асосий вазифалар куйидагилар:

- хабарлар мазмунининг фош килинишини олдини олиш;
- хабарлар окимининг тахлилланишини олдини олиш;
- хабарлар окими хакикийлигини бузилганлигини аниклаш;
- ёлгон уланишни аниклаш.

Ахборот тизимлари ёки маълумотларни узатиш тармокларида ахборот хавфсизлигини таъминлаш максадида маълумотларни узатишни химоялаш усулларидан нафакат бузгунчи таъсири окибатларини аникдашни, балки, агар окибатлар вактинча характерга эга булганида, узилган (бузилган) узатиш жараёнини автоматик тарзда тиклашни талаб этиш керак.

Хрзирда юкррида келтирилган вазифаларнинг бажарилишини таъминловчи химоялашнинг стандартлаштирилган механизмлари мавжуд эмас. Хдр бир муайян х,олда маълумотларни узатиш хавфсизлиги масалалари ахборотларни криптографик узгартириш усуллари, ахборотларни х,алалларга бардош кодлаш усуллари, хабарларнинг хакикийлигини таъминловчи усуллар, тизимлар ишлашининг ишончлилигини, яшовчанлигини ва барк,арорлигини таъминловчи усулларга асосланган химоялашнинг турли механизмларини биргаликда ишлатиш орк,али х,ал этилади.

Хабарлар мазмунининг фош цилинишини олдини олишда химоялашнинг каналга мулжалланган х,амда уланишга мулжалланган усулларидан фойдаланиш мумкин.

Юкррида айтиб утилганидек, каналли шифрлаш алока тармогининг х,ар бир каналида мустак,ил тарзда бажарилиши мумкин. Каналли шифрлашда, одатда, ок,имли шифрлаш ишлатилади ва узеллар орасида шифрланган матн битларининг узлуксиз окими мададланади. Тармокдарда коммутациялаш (маршрутлаш) вазифалари фак,ат узелларда бажарилиши сабабли, алока каналида пакетнинг сарлавх,алари билан бирга ахборот к,исмини х,ам шифрлаш мумкин.

Аммо маълумотлар факат каналда (каналлар оркали уланган узелларда эмас) шифрланиши сабабли барча оралик, узеллар химояланиши лозим. Бунинг устига узелларни нафакат физик химояланиши, балки бу узелларнинг аппарат-дастурий воситалари томнидан узеллар оркали утувчи хар бир уланишдаги ахборотни яккалаши кафолатланиши зарур.

Чеккалар аро шифрлашда маршрутизаторда ишланувчи хар бир хабар (сарлавханинг баъзи маълумотлари бундан истисно) йул бошида шифрланади ва белгиланган жойга етмагунча расшифровка килинмайди. Хар бир уланиш учун узининг калити ишлатилиши мумкин.

Хабарлар оцимини тахлилланишидан химоялаш, одатда, турли синфларга мансуб хабарлар узунлиги ва частотасининг кийматларини, манба адресларини ва хабарлар окими адресларини беркитишга йуналтирилган. Агар каналли шифрлаш ишлатилса, узеллар орасида маълумотлар узатилганида шифрланган матн битларининг узлуксиз окими урнатилиши мумкин. Бу эса частота кийматларини ва уланишнинг давомлигини беркитишга имкон беради. Бундай ёндашишда тармокнинг самарали утказиш крбилияти пасаймайди, чунки хеч к,андай кушимча ахборот талаб этилмайди. Аммо, узел очилса бу узел орк,али утувчи хабарларнинг бутун окими тахлиллаш мавзуига айланади.

Химоялашнинг чеккалараро усулларидан фойдаланилганда узатилувчи хабарларнинг х,ак,ик,ий частотаси ва узунлигини беркитиш учун турли узунликдаги "буш" хабарлар генерацияланиши, хакикий хабар эса буш символлар билан тулдирилиши мумкин. К,абул килувчи бегона кенгайишларни ва "буш" хабарларни аниклашда хабардаги шифрланган х,ошиядан фойдаланиши мумкин.

Аксарият иловаларда окимни тахлиллаш орк,али ахборотни чик,ариб олиш иккинчи даражали хавф сифатида талкин килиниши ва махсус к,арши чоралар курилмаслиги мумкин.

Хабарлар сатхида хацщийликни тасдицлаш хабарларни кечиктириш, уларни йук, килиш, алмаштириб к,уйиш ёки кайталаш каби таъсирлардан х,имоялашни таъминламайди. Шунга карамасдан, бундай тахдидлардан х,имоялашнинг турли усуллари мавжуд:

- хабарларни номерлаш. Хдр бир хабарни номерлаб, номерни хабар таркибига киритиб, демак, шифрлаб узатиш оркали хабарнинг хакикийлигига ишонч хрсил килиш мумкин. Тармокнинг хар бир объекти у билан алокада булувчи объектларнинг хар бири учун алох,ида санагичларга (счетчикларга) эга булиши лозимлиги бу муолажанинг камчилиги хисобланади.

- вактни белгилаш. К,абул килувчи хар бир узатилган хабарнинг куни ва вактини билган хрлда унинг адекватлигини текшириши мумкин. Бундай белгилашнинг интервали ва аниклиги шундай танланиши лозимки, бир то-мондан хатоли хабарлар, иккинчи томондан узатиш каналига хос булган табиий кечикиш аникланиши мумкин булсин.

- тасодифий сонлардан фойдаланиш. Вактнинг реал масштабида икки томонлама алока ишлатилганида кабул килувчи жунатувчига хабар жунатилмасдан олдин тасодифий сон юборади. Жунатувчи бу сонни шифр-ланган хабарга шундай урнатадики, кабул к,илувчи уни текшириши мумкин булсин. Шу тарзда ёлгон хабарлар чикариб ташланиши мумкин.

- хар бир уланиш учун алох,ида калитдан фойдаланиш. Натижада олинган хабарда уланишнинг ошкор булмаган идентификацияланиши амал-га оширилади.

Хабарлар оцими узилишини аницлаш масаласини "суров-жавоб" про-токолидан фойдаланиб х,ал этиш мумкин. Бундай протоколнинг таркибида уланишнинг вактинчалик яхлитлигини ва мак,омини урнатувчи хабарлар жуфтини алмашиш муолажаси булади. Уланишнинг хар бир чеккасида "хабар-суров" узатишни вакти-вакти билан ишга туширувчи таймер ишлатила-ди ва "хабар-суров" узатишга уланишнинг бошка чеккасидан жавоб олина-ди. Хар бир "хабар-суров"да передатчик ахбороти мавжуд булиб, бу ахбо-рот уланишдаги хабар йукртилишини аникдашга имкон беради.

Ёлгон уланишни аницлаш учун хар бир чеккадаги "уланишга жавоб-гар"нинг х,ак,ик,ийлигини ва уланишнинг вактинчалик яхлитлигини текши-ришга ишончли асосни таъминловчи к,арши чоралар ишлаб чик,илган.

Уланиш бошланиши вактида хар бир чеккада уланишга жавобгарнинг хакикийлигини текшириш кейинги хабарлар окимининг хакикийлиги хусусида карор кабул килишга асос хисобланади.

Уланишнинг вактинчалик яхлитлигини текшириш бузгунчининг олдинги к,онуний уланиш ёзувидан фойдаланиб, фойдаланувчини хато фикрга солишидан ёки адаштиришидан, маълумотлар узатиш жараёнини бузишидан х,имоялайди.

XII боб. СИМСИЗ АЛОК.А ТИЗИМЛАРИДА АХБОРОТ ХИМОЯСИ

12.1. Симеиз тармок, концепцияси ва тузилмаси

Симеиз тармок, концепцияси. Симеиз тармоклар одамларга симли уланишеиз узаро богланишларига имкон беради. Бу силжиш эркинлигини ва уй, шахдр кисмларидаги ёки дунёнинг олис бурчакларидаги иловалардан фойдаланиш имконини таъминлайди. Симеиз тармоклар одамларга узларига кулай ва хохлаган жойларида электрон почтани олишларига ёки Web-сахифаларни куздан кечиришларига имкон беради.

Симеиз тармокларнинг турли хиллари мавжуд, аммо уларнинг энг мухим хусусияти богланишнинг компьютер курилмалари орасида амалга оширилишидир. Компьютер курилмаларига шахеий ракамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахеий компьютерлар, серверлар ва принтерлар тааллукли. Одатда уяли телефонларни компьютер курилмалари каторига киритишмайди, аммо энг янги телефонлар ва хатто наушниклар маълум хисоблаш имкониятларига ва тармок, адаптерларига эга. Якин орада электрон курилмаларнинг аксарияти симсиз тармокдарга уланиш имкониятини таъминлайди.

Богланиш таъминланадиган физик худуд улчамларига боглик, х,олда симсиз тармокларнинг куйидаги категориялари фаркданади:

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

12.1-жадвалда Ушбу тармокларнинг кискача тавсифи келтирилган.

Симсиз шахеий тармоцлари узатишнинг катта булмаган масофаси билан (17 метргача) ажралиб туради ва катта булмаган бинода ишлатилади. Бундай тармокларнинг характеристикалари уртача булиб, узатиш тезлиги одатда 2Мб/с дан ошмайди.

Бундай тармок,, масалан, фойдаланувчи PDA сида ва унинг шахеий компьютерида ёки ноутбукида маълумотларни симсиз синхронлашни

таъминлаши мумкин. Худди шу тарифа принтер билан симсиз уланиш таъминланади. Компьютерни ташки курилмалар билан уловчи симлар чигалликларининг йукрлиши етарлича жиддий афзаллик булиб, бунинг эвазига тапщи курилмаларнинг бошлангич урнатилиши ва кейинги, зарурият тугилганда, жойининг узгартирилиши анчагина осонлашади.

12.1-жадвал

Тармок хили	Таъсир доираси	Характеристикаси	Стандартлар	Кулланиш сохаси
Шахсий симсиз тармоклар	Фойдаланувчидан бевосита якинликда	уртача	Bluetooth, IEEE, 802.15, IRDA	Ташки курилмалар кабелларининг урнида
Локал симсиз тармоклар	Бинолар ва кампуслар доирасида	юкори	IEEE 802.15, Wi-Fi, Hiper-LAN	Симли тармокларни Мобил кенгайтириш
Регионал симсиз тармокдар	Шахар доирасида	Юкори	Патентли, IEEE 802.16, WIMAX	Бинолар ва корхоналар ва Internet орасида белгиланган симсиз богланиш
Глобал симсиз тармокдар	Бутун дунё буйича	Паст	CDPD ва 2, 2.5 ва 3-авлод уяли телефон оркали тизимлар	Бинодан ташкарида InternetflaH мобил фойдаланиш

Симсиз шахсий тармокдарнинг аксарият узатувчи-кдбул кдлувчиларнинг (transceiver) кам к,увват исътемол к,илиши ва ихчамлиги микропроцессорлар билан таъминланган, катта булмаган фойдаланувчи курилмаларини самарали мададлашга, х,амда компьютер курилмасини узок, вак,т мобайнида битта батареяда (ёки аккумуляторда) ишлашига имкон беради. Ундан ташк,ари, кам кувват истеъмол к,илиниши симсиз шахсий тармокларни уяли телефонларга, PDA ларга ва наушникларга татбик, этишга сабаб булди.

Симсиз шахсий тармокдар Internet га ва иловаларга уланишдан биргаликда фойдаланиш мак,садида ноутбуклар ва шахсий компьютерларнинг узаро алок,асини таъминлаши мумкин. Бу таъсир доираси битта хона билан чегараланган тармокдар га тугри келади.

Симеиз локал тармоқлар офисларнинг ичида ва ташкарисида, ишлаб чикариш биноларида узатишларнинг юкрри характеристикаларини таъминлайди. Бундай тармокдардан фойдаланувчилар одатда ноутбукларни, шахеий компьютерларни ва катта ресуреларни талаб этувчи иловаларни бажаришга крдир процессорли ва катта экранли *PDA* ларни ишлатишади. Хизматчи тармок, хизматларидан мажлислар залида ёки бинонинг бошка хоналарида була туриб фойдаланаши мумкин. Бу хизматчига уз вазифаларини самарали бажаришга имкон беради. Симеиз локал тармокдар узатишнинг 54Мбит/сгача тезлигида барча офис ёки маиший иловалар талабларини крндириш имконига эга. Характеристикалари, компонентлари, нархи ва бажарадиган амаллари буйича бундай тармокдар Ethernet хилидаги анъанавий симли локал тармокларига ухшаш.

Симеиз регионал тармоқлар юзаси буйича шахарга тенг булган худудга хизмат килади. Аксарият холларда иловаларни бажаришда белгиланган уланиш талаб этилади, баъзида эса мобиллик зарур булади. Масалан, касалхонада бундай тармок, асосий бино ва масофадаги клиникалар орасида маълумотларни узатишни таъминлайди. Ёки энергетик компания бундай тармокдан шахар масштабида фойдаланиб, турли туманлардан бериладиган иш нарядларидан фойдаланишини таъминлайди. Натижада, симсиз регионал тармокдар мавжуд тармок, инфратузилмаларини бир ерга туплайди ёки мобил фойдаланувчиларга мавжуд тармок, инфратузилмалари билан уланишни урнатишга имкон беради.

Симсиз Internet хизматлари билан таъминловчилар (Wireless Internet Service Provider, WISP) уйда фойдаланувчилар ва компаниялар учун доимий симсиз уланишларни таъминлаш мак,садида шахарларда ва кишлок, жойларда симсиз регионал тармокдарни мижозлар ихтиёрига такдим этади. Бундай тармокдар, купинча симли уланишларни ёткизиш билан боглик, чегараланишларга эга булган оддий симли уланишларга нисбатан самарали хисобланади.

Симсиз регионал тармокдарнинг характеристикалари турлича. Уланишларда инфракизил технологиянинг ишлатилиши маълумотларни узатиш тезлигининг 100 Гбит/с ва ундан катта булишини таъминлайди.

Симсиз глобал тармоқлар мобил иловаларнинг, улардан мамлакат ёки хатто континент масштабида фойдаланишни таъминлаш билан ишланишини таъминлайди. Ик,тисодий мулохазаларга таянган хрлда, телекоммуникация компаниялари купгина фойдаланувчилар учун узок, масофадан уланишни таъминловчи симсиз глобал тармокдшнг нисбатан кдммат инфратузилмасини яратадилар. Бундай ечимнинг харажати барча фойдаланувчилар уртасида так,симланади, натижада абонент тулови унчалик юк,ори булмайди.

Купгина телекоммуникация компанияларининг кооперацияси туфайли симсиз глобал тармокдарининг таъсир доираси чегараланмаган. Телекоммуникация хизматини таъмнловчиларнинг бирига тулаб, симсиз глобал тармок, оркдпи дунёнинг хар кдндай нук,тасидан кдтор Internet хизматидан фойдаланиш мумкин.

Симсиз глобал тармок, характеристикалари нисбатан юк,ори эмас, маълумотларни узатишнинг тезлиги 56 Кбит/с ни, баъзида 170 Кбит/с ни ташкил этади.

Симсиз глобал тармокдарга хос иловалар InternetflaH фойдаланишни, электрон почта хабарларини узатиш ва кдбул к,илишни, фойдаланувчи уйдан ёки офисдан ташкдрида булганида корпоратив иловалардан фойдаланишни таъминловчи иловалардир. Абонентлар, масалан, таксида кетаётганларида ёки шахар буйича сайр К11линаётганларида уланишни урнатишлари мумкин. Умуман, симсиз глобал тармокдан фойдаланувчилар худудий чегараланмаганлар.

Симсиз глобал тармокдар технологиясини татбик, этишдаги муаммолардан бири унинг бино ичидаги фойдаланувчилар учун богланишни таъминлай олмаслиги. Чунки бундай тармок, инфратузилмалари бино ташк,арисида жойлашган ва радиосигналлар бинода айтарлича сусаяди. симсиз глобал тармокдарни бино ичига урнатилиши эса к,имматга тушади ва техник нук,таи назаридан асосланмаган.

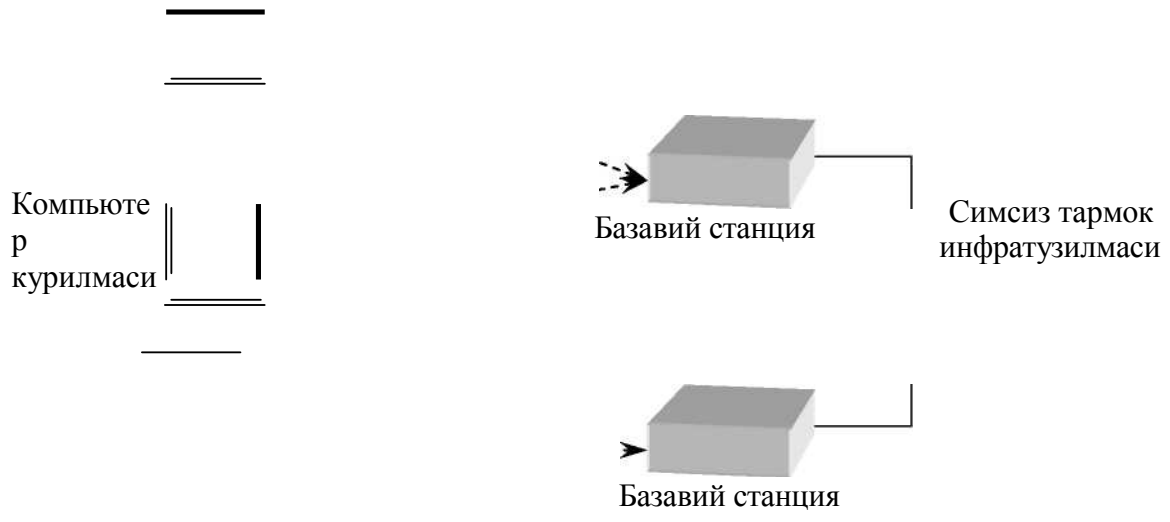
Симсиз шахсий, локал, регионал ва глобал тармокдар бир-бирини тулдирувчи булиб, турли талабларни к,ондиради. Аммо, баъзида бир тармокххи иккинчисидан фаркдаб булмайди. Масалан, бино ичидаги симсиз локал тармок, фойдаланувчи РБАси билан шахсий компьютерини симсиз

шахсий тармок, каби улашни таъминлаши мумкин. Турли симсиз тармокдар орасидаги фаркни аникдашда уларда ишлатиладиган технологиялар ва стандартлардан фойдаланишади (12.1-жадвалга каралсин).

Агар фойдаланувчи нуктаи назаридан истикбол хусусида суз юритилса, симсиз тармокдар орасида чегаранинг йукрлиши шарт. Турли хил симсиз тармок, ишини мададловчи компьютер курилмалари тармоги интерфейсининг платалари пайдо булмокда. Масалан, сайёхда ёки тижоратчида хам симсиз локал хам симсиз глобал тармок, билан узаро алока килувчи замонавий уяли телефон булиши мумкин.

Симсиз тармо^ тузилмаси. Симсиз тармокдарда симли тармокда ишлатиладиган компонентлар ишлатилади. Аммо, симсиз тармокдарда ахборот хаво мухити (medium) орк,али узатишга ярокди куринишга узгартирилиши лозим.

12.1-расмда симсиз тармокдарда ишлатиладиган компонентларнинг асосийлари курсатилган. Уларга фойдаланувчилар, компьютер курилмалари, базавий станциялар ва симсиз инфратузилма киради.



12.1-расм. Симсиз тармоцда ишлатиладиган асосий компонентлар

Фойдаланувчилар. Симсиз тармок, фойдаланувчига хизмат к,илишлиги сабабали, фойдаланувчига симсиз тармок,нинг мух,им кисми сифатида к,араш мумкин. Фойдаланувчи симсиз тармокдан фойдаланиш жараёнини бошлайди ва унинг узи тугаллайди. Шу сабабли унга "охирги фойдаланувчи" атамаси жоиз х,исобланади. Одатда, фойдаланувчи симсиз тармок, билан узаро алокани таъминлаш билан бир к,аторда, муайян иловалар билан боглик.

бошка вазифаларни бажарувчи *компьютер курилмалари (computer device)* билан иш куради.

Мобиллик - симсиз тармокнинг энг сезиларли афзалликларидан биридир. Масалан, мобиллик хусусиятидан кандайдир бино буйича харакатланувчи ва узининг РБАси ёрдамида электрон почтани олувчи ёки жунатувчи одам фойдаланади. Бу хрлда PDA симсиз тармок, инфратузилмасига узлуксиз ёки тез-тез тикланувчи уланишни таъминлаши лозим.

Баъзи фойдаланувчиларга факат компьютер курилмасининг портативлиги зарур, яъни улар вактнинг маълум оралигида симсиз тармок, билан ишлаганида бир жойда буладилар. Бундай фойдаланишга мисол тарикасида мажлислар залида симсиз тармоккд уланган ноутбукда ишловчи ходимни курсатиш мумкин.

Компьютер цурилмалари. Компьютер курилмаларининг (баъзида уларни мижозлар деб аташади) купгина хиллари симсиз тармок, билан ишлайолади. Баъзи компьютер к,урилмалари фойдаланувчилар учун атайин к,урилган булса, бошкалари охирги тизим х,исобланади. 12.2-расмда симсиз тармокларнинг компьютер к,урилмалари келтирилган.

Принтер

Мобил телефон

Ноутбук

Маълумотларни йиғувчи курилма

Шахсий комьютер

PDA

Оддий телефон

12.2-расм. Симсиз тармоцларнинг компьютер курилмалари.

Мобил иловалар ишини таъминлаш ва одамларга узлари билан узок, вак,т мобайнида олиб юришларида кулайлик тугдириш учун Компьютер курилмалари ихчам булиши лозим. Одатда, улар катта булмаган экранга, кам сонли тугмачаларга ва улчамлари кичик батареяга эга. Компьютер курилмалари мобилликка эга булга хрлда факдт баъзи иловаларни мадад-лайди. Нисбатан юк,ори характеристикаларни талаб этувчи иловаларни ба-жаришда катта экранга ва катта клавиатурага эга булган улчамлари катта компьютер курилмаларидан фойдаланилади. Аммо улар массасининг катта-лиги ва бир жойдан иккинчи жойга кучиришнинг нокулайлиги муаммо хисобланади. Симеиз тармокдарнинг компьютер курилмалари серверлар, маълумотлар базаси ва Web-узеллар каби охирги тизимларни хам уз ичига олади.

Фойдаланувчилар мавжуд компьютер курилмаларини симсиз тармокда ишлатиш учун (масалан, симсиз тармок, интерфейси платасини ноутбукка урнатиш орк,али) мослаштиришлари мумкин. *Тармоц интерфейси платаси* ёки *тармоц адаптери* (network interface card) компьютер курилмаси ва симсиз тармок, инфратузилмаси орасида интерфейсни таъминлайди. Бу плата компьютер курилмаси ичига урнатилади, баъзида ташк,и тармок, адаптери х,ам ишлатилади. Бундай адаптерлар, ишга туширилиши билан компьютер курилмаси ташк,арисида к,олади.

Компьютер к,урилмалари Windows-XP, Linux ёки MAC OS каби one-рацион тизимга хам эга булиб, бу операцион тизим симсиз тармок, илова-ларини амалга ошириш учун зарур булган дастурий таъминотни ишга ту-ширади.

Хаео муути. Хаво компьютер курилмалари ва симсиз инфратузил-мага орасида ахборот окдшини узатиш канали х,исобланади. Симсиз тармокдар орк,али алок,ани нутк, орк,али мулок,отга ухшатиш мумкин. Агар сух,батдошлар орасидаги масофа ошаверса, улар бир-бирларини ёмон эшита бошлайдилар.

Симсиз тармокдарнинг ахборот сигналлари х,ам хаво орк,али тарк,алади, аммо узининг хусусияти эвазига нутк, сигналарига Караганда ан-чагина катта масофага тарк,алиши мумкин. Бу сигналлар одамга эшитил-

майди, шу сабабли уларни, сузлашга халакит беришидан куркмай, янада юкрри сатхдаргача кучайтириш мумкин. Аммо алока сифати тусикдарнинг мавжудлигига боглик,. Тусиклар сигналлар тарк,алишига халакит килади ёки уларни сусайтиради, натижада сигналлар сатхи пасаяди, уларнинг таркалиш узокдиги камаяди.

Ёмгир, крр, туман, тутун (смог) симсиз тармокдарда ахборот сигналларини таркалишига таъсир этувчи оби-хаво шароитлари хисобланади. Масалан, кучли жала алока узунлигини икки мартага камайтириши мумкин. Бинолар ва дарахтлар каби бошка тусиклар таркалиш шароитларига ва симсиз тармок, характеристикаларига таъсир этиши мумкин. Симсиз регионал ва глобал тармокдарни жойлаштиришни режалаштиришда бу муаммоларнинг мух,имлиги ортади.

Симсиз тармоцлар инфратузилмаси. Симсиз тармок^ инфратузилмаси фойдаланувчилар ва охирги тизимларнинг узаро симсиз алок,аларини таъминлайди. Уни базавий станциялар, фойдаланиш контроллерлари, уланиш урнатилишини таъминловчи иловаларнинг дастурий таъминоти ва таксимловчи тизим ташкил этиши мумкин.

Базавий станция инфратузилманинг таркалган компоненти х,исобланади. У хаво мухити орк,али тарк,алувчи симсиз тармок, ахборот сигналларининг симли тармок,к,а узатилишини таъминлайди. Базавий станцияни баъзида *таксимловчи тизим* деб хам юритишади. Демак, базавий станция Web-сахифаларни куздан кечириш сервислари, электрон почта ва маълумотлар базаси каби тармок, хизмати йуналишидан фойдаланишни таъминлайди. Базавий станцияда купинча симсиз тармок, интерфейси платаси булиб, бу плата фойдаланувчи компьютеридаги симсиз тармок, интерфейси платасининг ишлаш принципидан фойдаланади. Базавий станция "нукта-нукта" ёки "нукта-бир неча нукта" каби уланишларни мададлаши мумкин (12.3-расм).

Нук;та-нук;та

Нук;та-бир неча нук;та

12.3-расм. Базавий станциянинг "нук;та-нук;та" ва "нук;та-бир неча нук;та" уланишларини мададлаши

"Нукта-нукта" тизими сигналлар окимини бир базавий станциядан иккинчисига ёки бир компьютердан иккинчисига узатиш имкониятига эга. "Нукта-бир неча нукта" конфигурацияси холида базавий станция биттадан ортик, компьютер курилмаси ёки бир неча базавий станциялар билан богланиши мумкин. Бундай хил богланишни, масалан, симсиз локал тармок, таркибидаги фойдаланиш нуктаси таъминлайди. Фойдаланиш нуктаси битта к,урилма булиб, купгина компьютер к,урилмалари бир-бирлари билан хамда симсиз тармок, инфратузилмасидаги тизимлар билан богланиш мак,садида у билан уланишни урнатади.

Фойдаланиш контроллеры. Фойдаланиш контроллерлари, одатда, тармок,нинг утказувчи к,исмида, фойдаланиш нуктаси ва тармокнинг х,имояланиш кисми орасида жойлашган аппарат узели хисобланади. Фойдаланиш контроллерлари очик, симсиз тармок, ва мухим ресурслар орасида трафикни тартибга солиш максадида фойдаланиш нукталарини марказлаштирилган назоратини таъминлайди. Баъзи холларда фойдаланишни бошк,ариш вазифасини фойдаланиш нуктаси бажаради.

Фойдаланиш контроллерлари кенг кулланилади. Умумфойдаланувчи симсиз локал тармокда, фойдаланиш контроллери фойдаланувчиларни ау-

тентификациялаш ва авторизациялаш билан InternetijaH фойдаланишни тартибга солади.

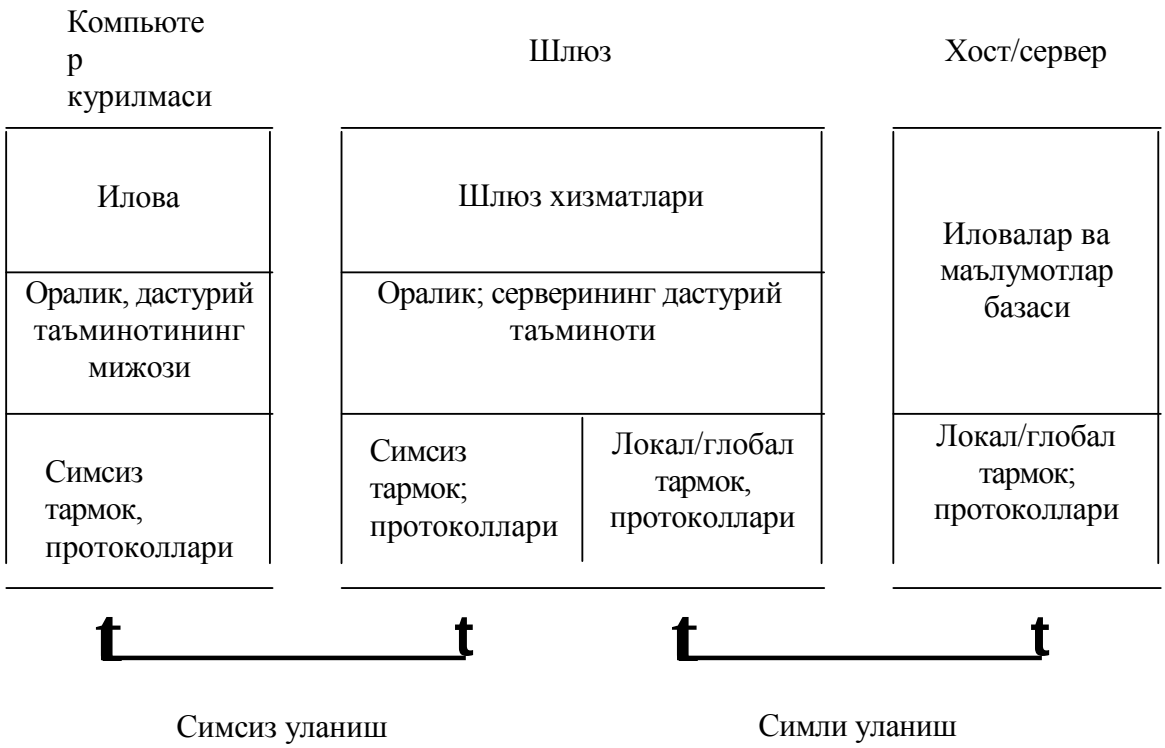
Уланиш урнатилишини таъминловчи иловаларнинг дастурий таъминоти. Internet дан ва электрон почтадан симсиз тармок, оркали, одатда, осон фойдаланилади. Бунинг учун *мижоз цурилмасида* браузер ва электрон почта дастури урнатилиши лозим. Фойдаланувчилар вакти-вакти билан симсиз уланишдан махрум булишлари мумкин, аммо нисбатан мураккаб булмаган иловаларни бажаришда ишлатилувчи протоколлар етарлича баркарор хдсобланади.

Аммо, бундай оддий иловалар билан бир каторда махсус, янада мураккаб иловалар ишлашини таъминловчи дастурий таъминот зарур. Куйида уланишни таъминловчи иловаларнинг асосийлари келтирилган.

Терминал эмуляторы (therminal emulation). Терминал эмуляторининг дастурий таъминоти компьютер курилмасида бажарилиб, уни фойдаланувчини нисбатан содда интерфейс билан таъминлашга имкон берувчи терминал каби ишлашга мажбур этади. Бу содда интерфейс фойдаланувчига бошка компьютерда бажарилувчи иловалар билан узаро алока килишта имкон беради.

Маълумотлар базаси билан тугридан-тугри уланиш (direct database connectivity). Маълумотлар базаси билан тугридан-тугри уланишда (баъзида мижоз-сервер технологияси деб аталади) илова фойдаланувчи компьютерида бажарилади. Бундай конфигурацияда охирги фойдаланувчи курилмасидаги дастурий таъминот иловага юкланган барча вазифаларни бажаради ва, одатда, марказий серверда жойлашган маълумотлар базаси билан узаро алокада булади.

Оралщ дастурий таъминот (Wireless middleware). Оралик, дастурий таъминот фойдаланувчининг компьютер к,урилмаси ва илова дастурий таъминоти ёки сервердаги маълумотлар базаси орасида оралик, уланишни амалга оширади (12.4-расм).



12.4-расм. Оралиц дастурий таъминоти.

Оралик, дастур симли тармокда уланган кушимча компьютерда (оралик, шлюзида) бажарилади. У фойдаланувчининг компьютер курилмаси ва серверлар орасида айланувчи пакетларни ишлайди. Бу дастурий таъминот симсиз тармокда самарали ва ишончли богаанишни яратишга имкон беради, чунки маълумотлар базасига уланиш ва иловаларнинг дастурий таъминоти билан узаро алокд янада ишончли симли тармок, орк,али амалга оширилади. Баъзида бу технологияни чидамли богланиш (session persistence) деб аташади.

Тщсимланган тизим. Симсиз тармок, камдан-кам тула маънода симсиз ишлатилади. Таркибида купинча симли уланишлар булган так,симловчи тизим одатда фойдаланиш нук,таларини, фойдаланиш контроллерларини ва серверларни бир бутунга бирлаштириш учун зарур булади. Аксарият хрлларда так,симловчи вазифасини оддий Internet тармоги бажаради.

12.2. Симсиз тармо^лар хавфеизлигига таадидлар

Симсиз технологиядан фойдаланилиб жуда катта афзалликларга эришиш мумкин. Бу технология фойдаланувчиларга алок,ани йук,отмасдан бемалол х,аракатланиш хиссиётини берса, тармок, яратувчиларига

богаанишларни ташкил этиш учун катта имкониятларни яратади. Ундан ташкари тармокдан фойдаланиш учун купгина янги курилмаларни пайдо булишига имкон беради. Аммо симсиз технология оддий симли тармокларга Караганда узида купрок, тахдидларни элтади. Хавфсиз симсиз иловани яратиш учун симсиз "хужумлар" утувчи булиши мумкин булган барча йуналишларни аниклаш лозим. Афсуски, иловалар хеч качон бутунлай хавфсиз булмайди, аммо симсиз технологиялардаги хавф-хатарни синчиклаб урганиш хар холда химояланиш даражасини ошишига ёрдам беради. Демак, мумкин булган тахдидларни тахлиллаб, тармокни шундай куриш лозимки, хужумлар га халакит бериш ва нестандарт "хужумлар "дан химояланишга тайёр туриш имкони булсин.

Назоратланмайдиган худуд. Симли ва симсиз тармоклар орасидаги асосий фарк, тармок, четки нукталари орасидаги мутлакр назоратланмайдиган зона билан боглик,. Уяли тармокдарнинг етарлича кенг маконида симсиз мух,ит асло назоратланмайди. Замонавий симсиз технологиялар тармок, маконини бошк,ариш воситаларининг чегараланган тупламини такдим этади. Бу симсиз тузилмаларнинг як,инидаги хужум к,илувчиларга симли дунёда мумкин булмаган хужумларни амалга оширишга имкон беради.

Яширинча эшитиш. Симсиз тармоклар каби очик, ва бошкарилмайдиган мухитда энг тарк,алган муаммо - аноним хужумларнинг мумкинлиги. Аноним зараркунандалар 12.5-расмда курсатилганидек радиосигналларни ушлаб крлиб, узатилувчи маълумотларни расшифровка килиши мумкин.

Узатишни ушлаб к,олиш учун нияти бузук, одам узатгич (передатчик) олдида булиши лозим. Ушлаб крлишнинг бундай турларини умуман к,айдлаш мумкин эмас ва уларга халакит бериш ундан хам кийин. Антенналар ва кучайтиргичлардан фойдаланиш, ушлаб крлиш жараёнида нияти бузук, одамларга нишондан айтарлича узок, масофада булишларига имкон беради.

Яширинча эшитишнинг яна бир усули - симсиз тармоккд уланиш. Локал симсиз тармокда яширинча фаол эшитиш одатда *Adress Resolution Protocol* (ARP) протоколидан нотугри фойдаланишга асосланган. Бошида

бу технология тармокни "эшитиш" максадида яратилган эди. Аслида, биз маълумотлар богланиши сатх,ида "man in the middle" (MITM - "уртада одам", пастроккд каралсин) хилидаги хужум билан иш курамиз. Хужум килувчи локал симсиз тармокнинг нишон станциясига суралмаган ARP-жавобларни юборади, нишон станцияси эса хужум килувчига узидан утаётган барча трафикни жунатади. Сунгра нияти бузук, одам пакетларни курсатилган адресатларга йуллайди. Шундай килиб, симсиз станция бошка симсиз мижознинг (ёки локал тармокдаги симли мижознинг) трафигини

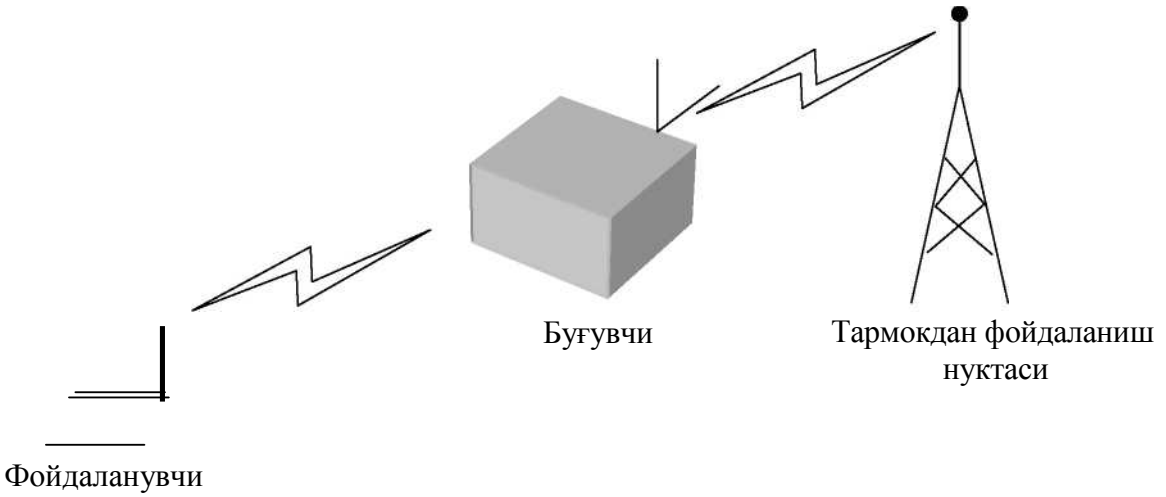
ушлаб крлиши мумкин.

12.5-расм. Симсиз коммуникацияларда яширинча эшитиш

Бугиш. Тармокларда бугиш атайин ёки атайин булмаган интерференциянинг алока каналидаги жунатувчи ва кабул килувчи имкониятидан ошганида содир булади. Натижада бу канал ишдан чикарилади. Хужум килувчи бугишнинг турли усулларидан фойдаланиши мумкин.

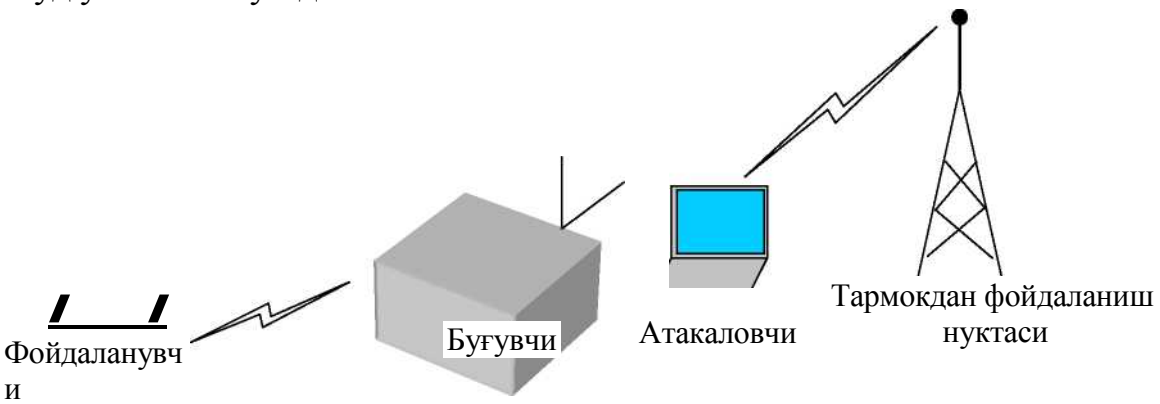
Хизмат курсатишдан воз кечиш. DoS (Denial of Service - хизмат курсатишдан воз кечиш) хилидаги хужум тармокни бутунлай ишдан чикариши мумкин. Бутун тармокда, жумладан базавий станцияларда ва мижоз терминалларида, шундай кучли интерференция пайдо буладики, станциялар бир-бирлари билан боглана олмайдилар (12.6-расм). Бу хужум маълум доирадаги барча коммуникацияни учиради. Симсиз тармок,к,а буладиган DoS хужумни олдини олиш ёки тухтатиш кийин. Симсиз тармок.

технологияларининг аксарияти лицензияланмаган частоталардан фойдаланади, демак, бир канча электрон курилмалардан интерференция булиши мумкин.



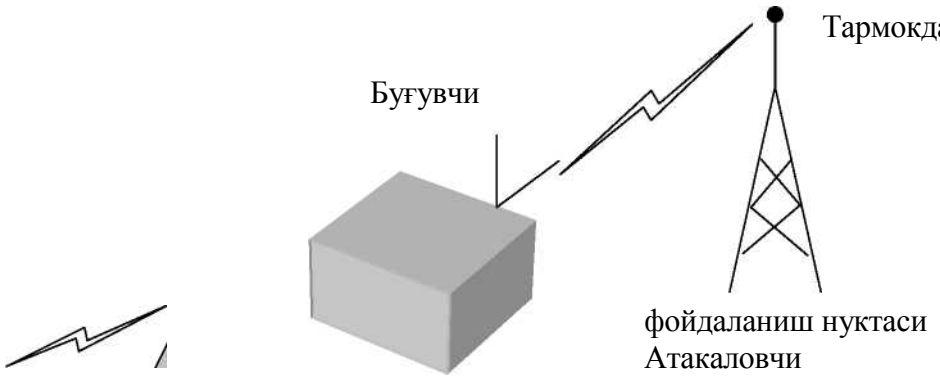
12.6-расм. Симсиз коммуникацияларда буғиш атакалари

Мижозларни бугиш. Мижоз станциясини бугиш фирибгарга узини бугилган мижоз урнига куйишига имкон беради (12.7-расм). Мижоз уланишни амалга ошира олмасин деган максадда унга хизмат курсатишдан воз кечиш учун хам бугишдан фойдаланилади. Жуда мох,ирлик билан килинган хужумлар нияти бузук, одам станциясини базавий станцияга улаш мак,садида мавжуд уланишни узади.



12.7-расм. Уланишни ушлаб цолиш мацеадида мижозни бўғиш атакаси

Базавий станцияни бугиш. Базавий станцияни бугиш уни хужум килувчи станция билан алмаштиришга имкон беради (12.8-расм).



Фойдаланувчи *12.8-расм. Уланишни ушлаб қолиш мақсадида базавий станцияни бўғиш атакаси*

Бундай бугиш фойдаланувчиларни хизматлардан фойдаланишдан, телекоммуникация компанияларини эса фойдадан махрум килади.

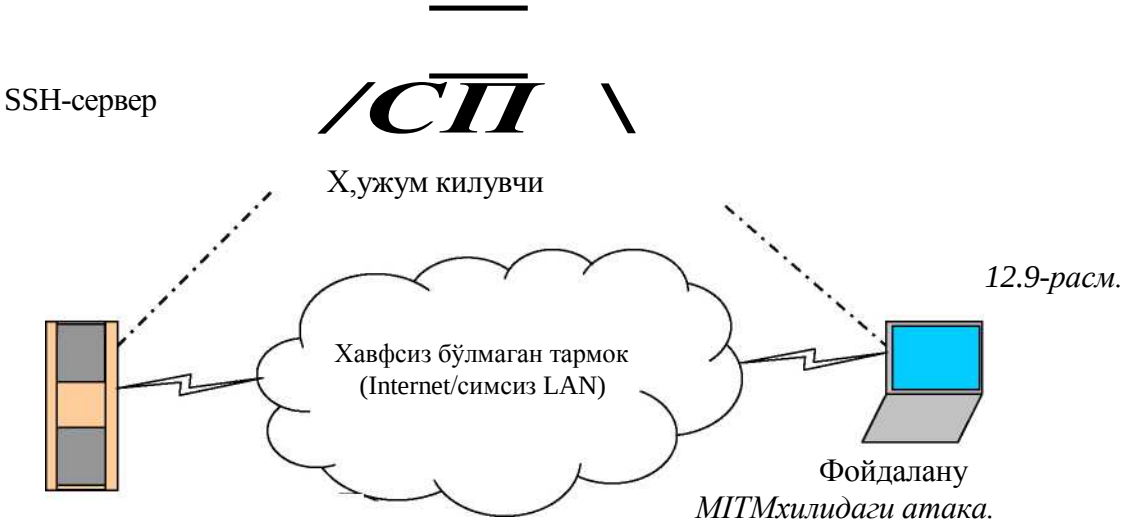
Юкррида кайд этилганидек, аксарият симсиз технологиялар лицензияланмаган частоталардан фойдаланади. Шу сабабли купгина курилмалар - радиотелефонлар, кузатиш тизимлари ва микротулкинли учоклар - симсиз тармок, ишига таъсир этиши ва симсиз уланишни бугиши мумкин. Бундай атайин булмаган бугиш холларини олдини олиш учун, кимматбахр симсиз асбоб-ускунани сотиб олишдан аввал у урнатиладиган жойни синчиклаб тахлиллаш л озим. Бундай тахлил коммуникацияларга бегона курилмаларнинг таъсир этмаслигига ишонч хрсил килишга имкон беради ва маъносиз харажатлардан асрайди.

Бостириб кириш ва маълумотларни модификация.! аш. Нияти бузук, одам уланишни ушлаб колиш, маълумотларни ёки командаларни узатиш максадида маълумотларнинг мавжуд окимига ахборотни к,ушганида бостириб кириш содир булади. Хужум к,илувчи пакетларни базавий станцияга юбориб бошк,ариш командалари ва ахборот окимлари устида манипуляцияни амалга ошириши мумкин. Бошкариш командаларини керакли бошк,ариш каналига юбориш оркали фойдаланувчини тармокдан узишга эришиш мумкин.

Бостириб кириш хизмат курсатишдан воз кечиш учун ишлатилиши мумкин. Хужум к,илувчи тармокдан фойдаланиш нукталарини уланиш командалари билан тулиб-тоштиради. Натижада бошк,а фойдаланувчиларга тармокдан фойдаланишга рухсат берилмайди.

MITM(man in the middle) хужуми. MITM хужуми юкорида тавсифланган бостириб киришларга ухшаш. Улар турли шаклларни олишлари мумкин ва алока сеансининг конфиденциаллигини ва яхлитлигини бузиш учун ишлатилади. MITM хужумлар анчагина мураккаб, чунки уларни амалга ошириш учун тармок, хусусида батафсил ахборот талаб этилади. Нияти бузук, одам, одатда, тармок, ресурсларидан бирининг идентификациясини бажаради. Хужум курбони уланишни бошлаганида, фирибгар уни ушлаб крлади ва исталган ресурс билан уланишни тугаллайди, сунгра ушбу ресурс билан барча уланишларни узининг станцияси оркали утказади (12.9-расм). Бунда хужум килувчи ахборотни жунатиши, жунатилганини узгартириши ёки барча музокараларни яширинча эшитиши ва сунгра расшифровка килиши мумкин.

Абонент-фирибгар. Тармок, абонентининг ишини синчиклаб урганиб чиккдн хужум килувчи узини "тармок, абоненти" к,илиб курсатиб, тармок, ва унинг хизматларидан фойдаланишга уринади. Ундан ташкари фойдаланишда к,улланиладиган к,урилманинг угирланиши тармок,к,а киришга етарли булади. Барча симсиз курилмаларнинг хавфсизлигини таъминлаш осон иш эмас, чунки улар фойдаланувчиларнинг харакатланишида к,улайлик тугдириш мак,садида атайин кичкина килиб яратилади.

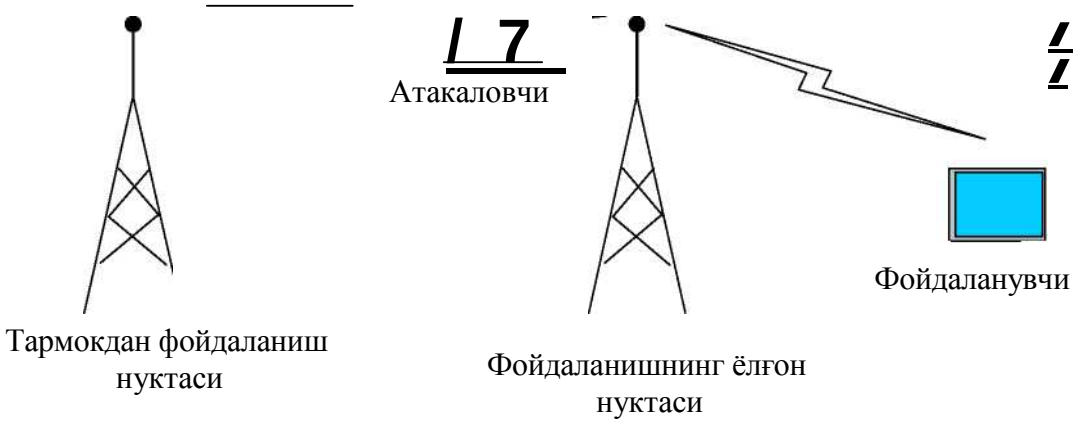


12.9-расм.

MITMхилидаги атака.

Тармовдан фойдаланишнинг ёлгон ну^талари. Тажрибали хужум килувчи тармок, ресурсларини имитация килиш билан фойдаланишнинг

ёлгон нукталарини ташкил этиши мумкин. Абонентлар, хеч шубх,аланмасдан фойдаланишнинг ушбу ёлгон нуктасига мурожаат этадилар ва уни узининг мухим реквизитларидан, масалан, аутентификация ахборотидан хабардор киладилар. Хужумнинг бу хили тармокдан фойдаланишнинг хакикий нуктасини "бугиш" максадида баъзида тугридан-тугри бугиш билан биргаликда амалга оширилади (12.10-расм).



12.10-расм. Фойдаланишнинг ёлғон нуцтаси

Симли тармокдан фойдаланувчилар хам, билмасдан тармокни хужумга очиб бериб фойдаланишнинг ёлгон нукталарининг урнатилишига сабабчи булишлари мумкин. Баъзида фойдаланувчи, кулайликка интилиб, симсиз алок,а такдим этувчи фойдаланишнинг симсиз нукталарини урнатади, аммо хавфсизлик муаммосини уйламайди. Бу нукталар симли тармок,к,а кириш учун "орк,а эшик" вазифасини бажариши мумкин, чунки улар турли хужумларга дучор буладиган конфигурацияда урнатилади.

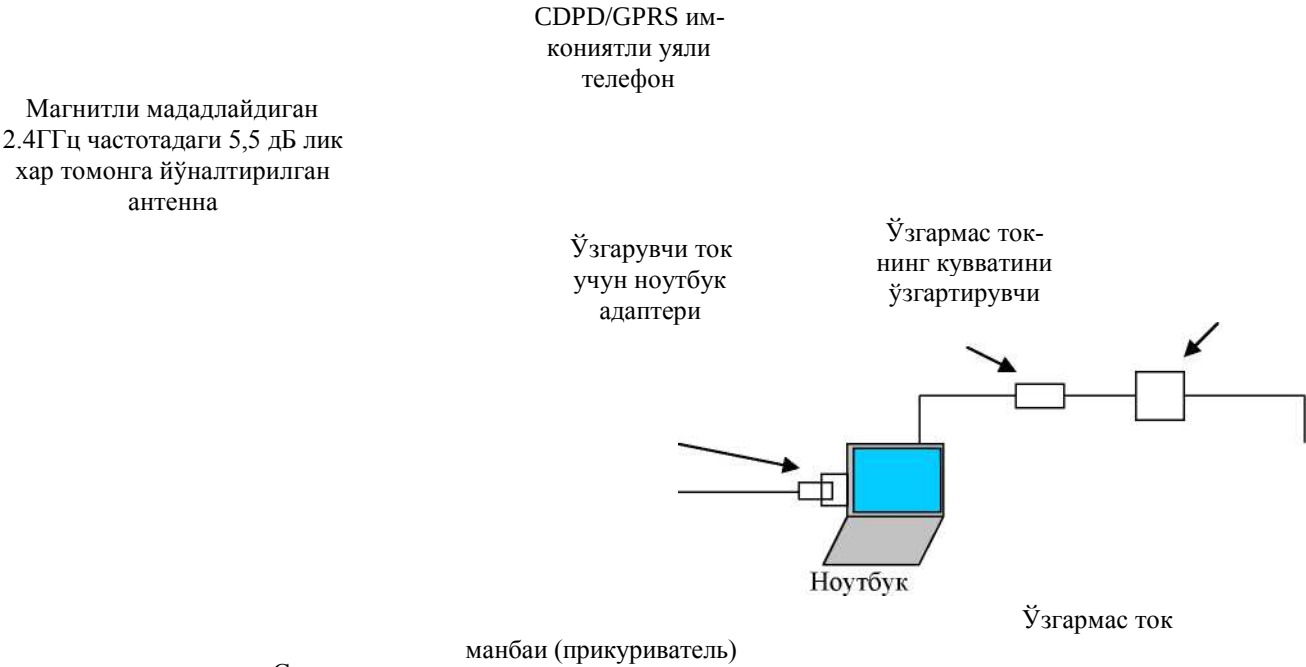
Хужумларнинг анонимлиги. Симсиз фойдаланиш хужумнинг тулик, анонимлигини таъминлайди. Урнатилган жойни аникловчи мое тармок, асбоб-ускунаси булмаса, хужум к,илувчи анонимликни осонгина саклаши ва симсиз тармок, таъсири худудидаги х,ар к,андай жойда беркиниши мумкин. Бундай х,олда нияти бузук, одамни тутиш кийин, ишни судга ошириш эса ундан х,ам к,ийин.

Таъкидлаш лозимки, аксарият фирибгарлар тармок,ни, уларнинг ички ресуреларига хужум килиш учун эмас, балки InternetflaH текин аноним фойдаланиш учун урганадилар ва Internet химоясида бошк,а тармокдарни хужумлайдилар.

"Мижоз-мижоз" хилидаги хужумлар. Тармокнинг барча абонентлари хужумланиши мумкин. Биринчи муваффакиятдан сунг хужум к,илувчи корпоратив ёки телекоммуникацион тармокдан фойдаланиш хукукига эга булади. Аксарият тармок, маъмурлари хавфсизлик режимига талабни оширишга ёки шахсий тармокдараро экранларни (брандмауэрларни) урнатишга етарлича эътибор бермайдилар. Шу сабабли, симсиз тармок, мижозларига муваффакиятли хужумлар нияти бузук, одамларга фойдаланувчиларнинг исмини ва паролини очиш, демак, бошка тармок, ресурсларидан фойдаланиш имконини бериши мумкин.

Тармок асбоб-ускуналарига хужумлар. Нотугри конфигурацияланган асбоб-ускуналар хужум килувчилар учун биринчи "хурак" хисобланади ва тармоккд кейинги сукилиб киришга йул очади. Хужумларнинг асосий объектлари - маршрутизаторлар, узиб-улагичлар, архивларни сакдовчи серверлар ва фойдаланиш серверлари.

Махфий симсиз каналлар. Симсиз тармок, фойдаланувчилари тармок, ни яратиш ёки бахрлаш жараёнида яна бир омилни хисобга олишлари зарур. Симсиз фойдаланиш нуктасининг нархи паст хамда дастурий таъминот, стандарт ноутбук ва NIC-карталар асосида фойдаланиш нуктасини яратиш етарлича осон булганлиги сабабли, нокоррект конфигурацияланган ёки симли тармокда уйламасдан жойлаштирилган симсиз асбоб-ускунани зийраклик билан кузатиш талаб этилади. Бу асбоб-ускуна (12.11-раем) симли

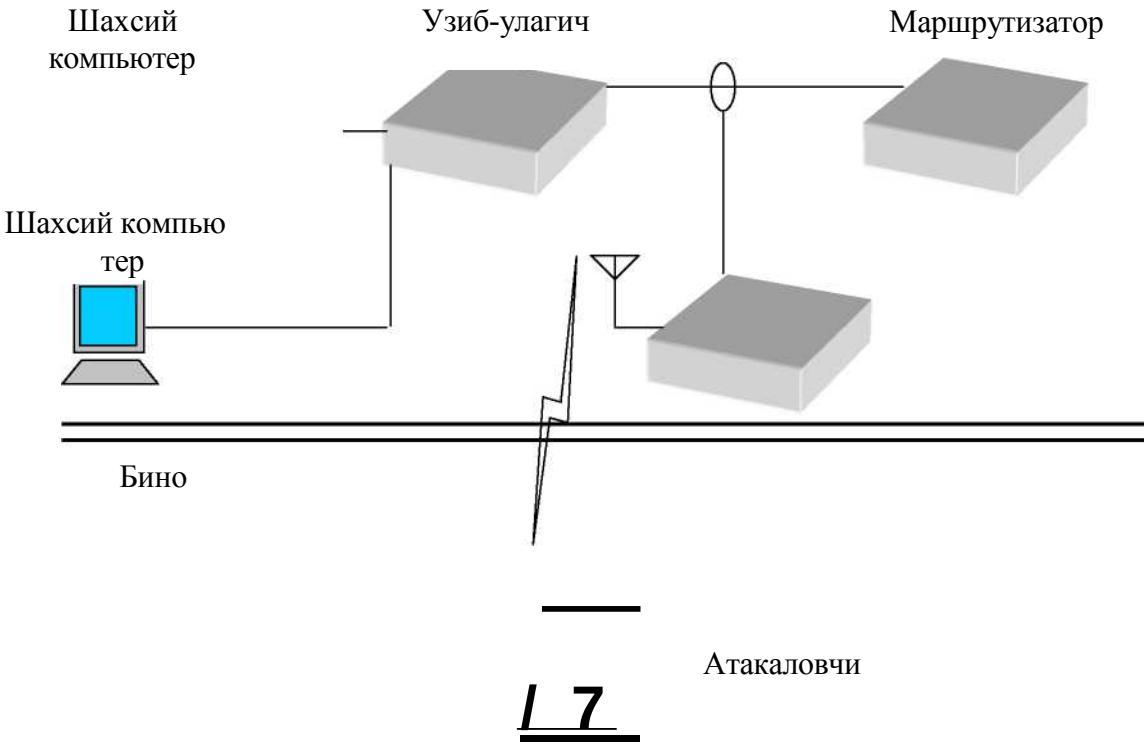


ч

12.11-расм. "Симсизурушни" олиб бориш асбоб-ускунаси.

инфратузилмада жуда сезиларли "рахналар" хрсил килиши мумкинки, улар тармокдан бир неча километр узокдаги хужум килувчилар диккдтини тортиши мумкин.

Худди шунга ухшаш конструкция ёрдамида узига хос "симсиз куприк," утказиш ва фойдаланиш нукталарининг бутун занжирини ташкил килган хрлда тармокдан маълумотларни химояланган бино ташкарисида чикариб олиш мумкин (12.12-расм)



12.12-расм. "Орца эшик" кўринишидаги тармоцдан фойдаланиш нуцтаси

Роуминг муаммоси. Симсиз тармокнинг симли тармокдан яна бир мухим фарки фойдаланувчининг тармок, билан алок,ани узмасдан жойини узгартириш крбилиятидир. Роуминг концепцияси турли симсиз алока стандартлари CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) ва симсиз Ethernet учун бир хил. ТСРЯРнинг купгина тармок, иловалари сервер ва мижоз 1Р-адресларининг узгармаслигини талаб этади, аммо тармокдаги роуминг жараёнида абонент албатта унинг бир жойини тарк этиб, бошка жойига кушилади. Симсиз тармокдарда мобил IP-адресларнинг ва бошк,а роуминг механизмларининг ишлатилиши ушбу талабга асосланган.

Мобил IP-алокднинг асосий гояси - фойдаланувчининг турган жойини кдйдлаш ва трафикни кдйта йуналтириш. Абонент турган жойига боглик, булмаган адрес TCP/IP - уланишни мададлайди, фойдаланувчи турган жойига боглик, булган вак,тинча адрес эса локал тармок, ресурслари билан уланишни таъминлайди. IP мобил тизими учун учта тартибга солувчи талаблар мавжуд: мобил узели (фойдаланувчининг симсиз курилмаси), уй агенти (уй тармогида жойлашган сервер) ва ажнабий агент (роуминг узатилувчи тармокда жойлашган сервер). Мобил узели янги тармокда утганида, у турган жойига боглик, булган вак,тинча IP-адресни олади ва ажнабий агентда кдйдланади. Сунгра ажнабий агент уй агенти билан богланиб мобил агентнинг узига богланганлигини хабар к,илади. Шу ондан бошлаб барча пакетлар ажнабий агент-роуминг оркдпи уй агентига йуналтирилади.

Криптоз^имоялаш таадидлари. CDMA, GSM уяли тармокдарда ва симсиз Ethernet-тармокда ахборотнинг конфиденциаллигини ва яхлитлигини таъминлаш мак,садида криптографик воситалар ишлатилади. Аммо хатоликларга йул к,уйиш коммуникациянинг бузилишига ва ахборотнинг ёмон ниятда ишлатилишига олиб келади.

WEP(Wired Equivalent Privacy - симсиз тармок, даражасидаги махфийлик) - 802.11 хилидаги тармок, хавфсизлигини таъминлаш учун яратилган криптографик механизм. WEPнн татбик, этишдаги хатоликлар ва бошк,ариш муаммолари уни бефойда к,илиб к,уйди. Ушбу механизм барча фойдаланувчилар ишлатадиган ягона статик калитга эга. Internet тармокда нияти бузук, одамга бир неча соат мобайнида калитни тиклашга имкон берувчи воситалар мавжуд. Шу сабабли, WEPra аутентификация ва конфиденциаллик воситаси сифатида ишониш мумкин эмас. Тавсифланган криптографик усулларни ишлатилгани, умуман ишлатилмаганига Караганда яхширок,, аммо юк,орида келтирилган хужумлардан химоялашнинг бошк,а усуллари зарур.

12.3. Симеиз тармоклар хавфеизлиги протоколлари

SSL/TLS протоколлари. Ххшояланган уланишлар протоколи - Secure Sockets Layer (SSL) Internet браузерларининг хавфеизлиги муаммосини ечиш учун яратилган. SSL таклиф этган биринчи браузер - Netscape Navigator тижорат транзакциялари учун Internet тармогини хавфеиз килди, натижада маълумотларни узатиш учун хавфеиз канал пайдо булди. SSL протоколи шаффоф, яъни маълумотлар тайинланган жойга шифрлаш ва расшифровка килиш жараёнида узгармасдан келади. Шу сабабли, SSL купгина иловалар учун ишлатилиши мумкин.

SSL узидан кейинги TLS (Transport Layer Security - транспорт сатхи химояси протоколи) билан Internets кенг таркалган хавфеизлик протоколидир. Netscape компанияси томонидан 1994 йили татбик, этилган SSL/TLS хрзирда хар бир браузерга ва электрон почтанинг купгина дастурларига урнатилади. SSL/TLS хавфеизликнинг бошка протоколлари, масалан, Private Communication Technology (PCT - хусусий коммуникация технологияси), Secure Transport Layer Protocol (STLP-хавфсиз сатхнинг транспорт протоколи) ва Wireless Transport Layer Security (WTLS - симсиз мухитда транспорт сатхини химоялаш протоколи) учун асос вазифасини утади.

SSL/TLSHHHr асосий вазифаси тармок, трафигини ёки гиперматнни узатиш протоколи HTTPни химоялашдир. SSL/TLS ал ока жараёнининг асосида ётади. Оддий HTTP-коммуникациялар да TCP-уланиш урнатилади, хужжат хусусида суров юборилади, сунгра хужжатнинг узи юборилади.

SSL/TLS уланишларни аутентификациялаш ва шифрлаш учун ишлатилади. Бу жараёнларда симметрик ва асимметрик алгоритмларга асосланган турли технологиялар комбинациялари иштирок этади. SSL/TLSfla мижозни ва серверни идентификациялаш мавжуд, аммо аксарият х,олларда сервер аутентификацияланади.

SSL/TLS турли тармок, коммуникациялар хавфсизлигини таъминлаши мумкин. Протоколнинг жуда кенг таркалиши электрон почта, янгиликлар, Telnet ва FTP (File Transfer Protocol - файлларни узатиш протоколи) каби

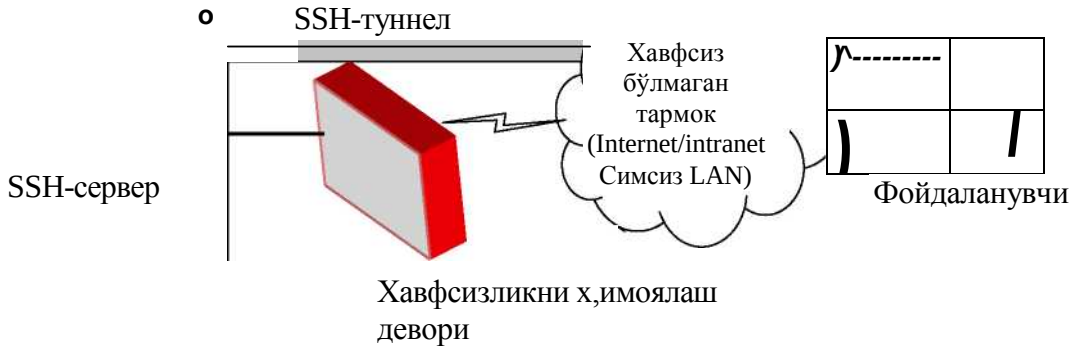
машхур TCP-коммуникациялар билан боглик,. Аксарият хрлларда SSL/TLS ёрдамида коммуникация учуй алохдда портлар ипшатилади.

SSH протоколи. Secure Shell протоколи, SSL/TLSKa6n коммуникацияларни химоялаш учун 1995 йили яратилган. Узининг мосланувчанлиги ва ишлатилишининг соддалиги туфайли SSH оммавий хавфсизлик протоколига айланди ва хрзирда аксарият операцион тизимларда стандарт илова хисобланади.

SSHfla ал ока сеанси жараёнида маълумотларни узатиш учун симметрик калитдан фойдаланилади. Серверни, хам мижозни аутентификациялаш учун SSHнн осонгина кайта конфигурациялаш мумкин.

Купинча SSH тармок, хостларини бошкаришда ишлатиладиган, куп тармк,алган илова - telnet ни алмаштириш учун ишлатилади.

Баъзида ишлаб чикарувчилар SSHнн telnet ёки FTPнн алмаштирувчи сифатида мададламайдилар. Бундай хрлларда SSHнн telnet, FTP, POP (Post Office Protocol - почта хабарлари протоколи) ёки хатто HTTP каби хавфсиз булмаган иловалар хавфсизлигини таъминлаш учун ишлатиш мумкин. 12.13-расмда трафикни хавфсиз булмаган тармокдан SSH серверга утказиш учун конфигурацияланган брандмауэр келтирилган.



Электрон почта
сервери

12.13-расм. SSH-туннел.

Хавфсиз булмаган тармокдан SSH серверга ва аксинча хеч кандай трафик утказилмайди. SSH-сервернинг SSH дан терминал фойдаланишидан ташкари, портнинг кайта йуналтирилиши электрон почта трафигини SSH-серверга хавфсиз тармок, буйича узатилишини таъминлаши мумкин. Сунгра SSH-сервер пакетларни электрон почта серверига кайта йуналтиради. Электрон почта серверига трафик SSH-сервердан келганидек туюлади ва пакетлар SSH-серверга, фойдаланувчига туннеллаш учун юборилади.

WLTS протоколи. SSL/TLSra асосланган WLTS протоколи WAP (Wireless Application Protocol - симсиз иловалар протоколи) курилмаларида, масалан, уяли телефонларда ва чунтак компьютерларида ишлатилади. SSL ва WLTS бир-биридан транспорт сатхи билан фаркданади. SSL йукрлган пакетларни кайта узатишда ёки нестандарт пакетларни узатишда TCP ишига ишонади. WLTS дан фойдаланувчи WAP курилмалари уз функцияларини бажаришида TCPни куллай олмайдилар, чунки факат UDP (user Datagram Protocol) буйича ишлайдилар. UDP протоколи эса уланишга мулжалланмаган, шу сабабли бу функциялар WLTS га киритилиши л озим.

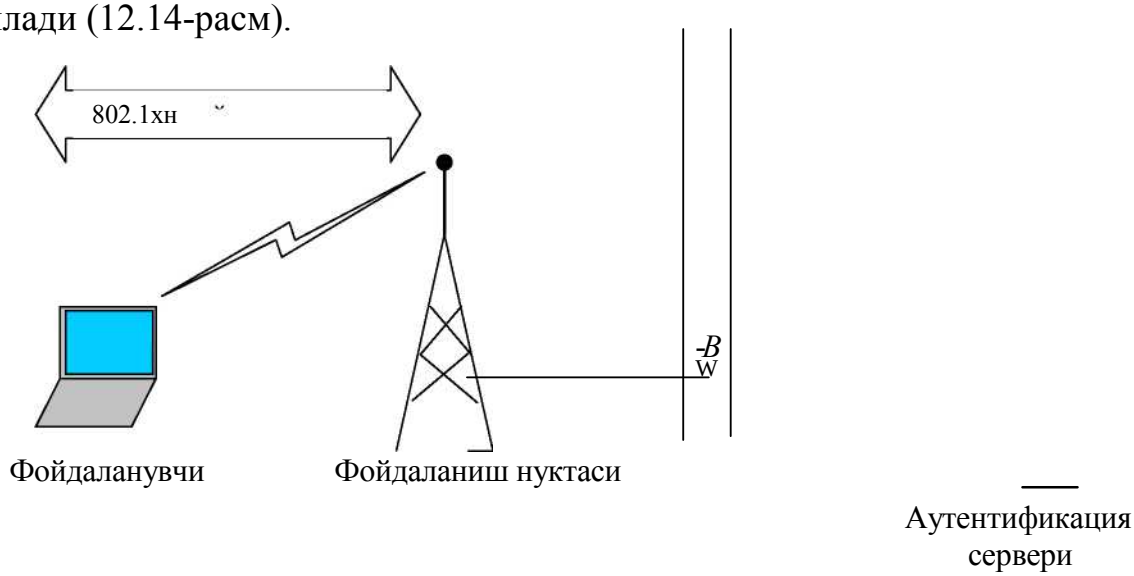
"Кул бериб куришиш" жараёнида куйидаги учта синф фаоллашиши мумкин:

- WLTS - 1-синф. Сертификатсиз;
- WLTS - 2-синф. Сертифкатлар серверда;
- WLTS - 3-синф. Сертифкатлар серверда ва мижозда.

1-синфда аутентификациялаш бажарилмайди, протокол эса шифрланган канални ташкил этишда ишлатилади. 2-синфда мижоз (одатда фойдаланувчи терминал) серверни аутентификациялайди, аксарият хрлларда сертификатлар терминалнинг дастурий таъминотига киритилади. 3-синфда мижоз ва сервер аутентификацияланади.

802.1x протоколи. Бу протоколнинг асосий вазифаси - аутентификациялашдир; баъзи хрлларда протоколдан шифрловчи калитларни урнатишда фойдаланиш мумкин. Уланиш урнатилганидан сунг ундан факат 802.1x. трафиги утади, яъни DHCP (Dynamic Host Configuration Protocol - хостларни динамик конфигурациялаш протоколи), IP ва х,. каби протоколларга

рухсат берилмайди. Extensible Authentification Protocol (EAP) (RFC 2284) фойдаланувчиларни аутентификациялашда ишлатилади. Бошланишида EAP "нукта-нукта" (PPP, Point-to-Point Protocol) пртоколи ёрдамида аутентификациялашнинг баъзи муаммоларини х,ал этиш учун ишлаб чик,илган эди, аммо унинг асосий вазифаси симсиз алока муаммоларини х,ал этишга каратилиши лозим. EAPнинг аутентифкациялаш пакетлари фойдаланувчи маълумотларини киритган фойдаланиш нуктасига юборилади; аксарият хрлларда бу маълумотлар фойдаланувчи исми (login) ва паролдан иборат булади. Фойдаланиш нуктаси тармок, яратувчиси танлаган воситаларнинг бири билан фойдаланувчини идентификациялаши мумкин. Фойдаланувчи идентификацияланганидан ва шифрлаш учун канал урнатилганидан сунг алока мумкин булади ва DHCP каби протоколларнинг утишига рухсат берилади (12.14-расм).

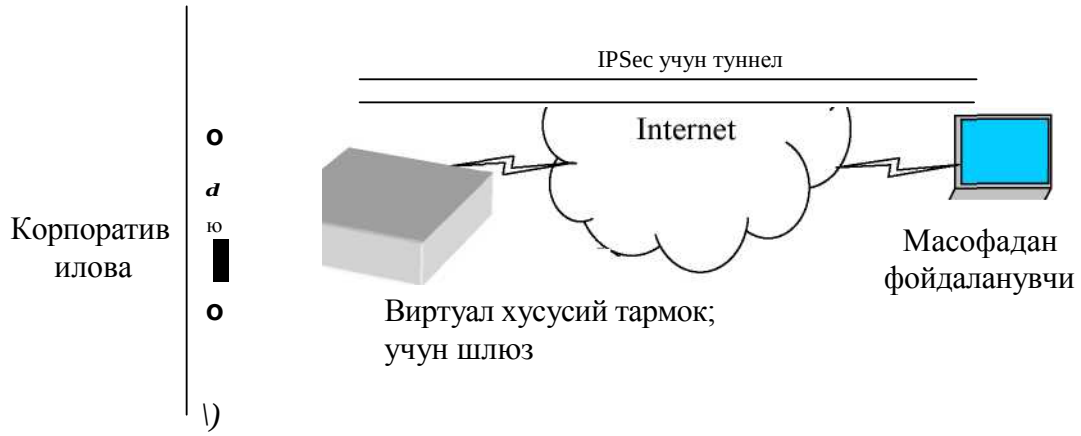


12.14-расм. 802.1х протоколининг кўриниши

IPSec протоколи. Протоколлар стекида IPSec протоколи SSL/TLS, SSH ёки WLTS протоколларидан пастда жойлашган. Хавфсизликни таъминлаш 1P-сатх,ида ва Internet-моделда амалга оширилади. IPSec ни татбик, килиш усулларидан куп тарк,алгани туннеллаш булиб, у битта сессияда IP-трафикни шифрлаш ва аутентификациялаш имконини беради. IP-Sec хрзирда Internets ишлатилувчи аксарият виртуал хусусий

тармокдардаги (VPN-Virtual Private Network) асосий технология хисобланади. IPSecHHHr мослашувчанлиги ва иловалар танланишининг кенглиги сабабли, купчилик айнан бу схемадан симсиз иловалар хавфсизлигини таъминлашда фойдаланади.

IPSecHH иловаларга асосланган кулланишининг жуда куп имкониятлари мавжуд. Хавфсиз коммуникациялар учун IPSecHHHr кулланиши купинча Internet оркали масофадан фойдаланиш виртуал хусусий тармоги VPN билан боглик. Кдчонки умумфойдаланувчи тармок хусусий тармок функцияларини амалга ошириш учун ишлатилса, уни VPN деб аташ мумкин. Бундай таърифга ATM (Asynchronous Transfer Mode - узатишнинг асинхрон усули), Frame Relay ва X.25 каби тармок технологиялари хам тушади, аммо аксарият одамлар Internet буйича шифрланган канални ташкил этиш хусусида ran кетганида VPNaTaMacHHH ишлатишади. Корпоратив тармок, периметри буйича 12.15-расмда курсатилганидек шлюзлар урнатилади ва IPSec-туннел оркали шлюздан масофадан фойдаланиш амалга оширилади.



12.15-расм. IPSec VPN-туннел.

12.4. Симеиз курилмалар хавфеизлиги муаммолари

Симеиз курилмаларни туртта категорияга ажратиш мумкин: ноутбуклар, чунтак компьютерлари (PDA), симсиз инфратузилма (куприклар, фойдаланиш нукталари ва х,.) ва уяли телефонлар.

Ноутбуклар — корпоратив симсиз тармокдарда ва SOHO (Small Office Home Office - кичик ва уй офислари) тармокдарида кенг тарк,алган курилма.

Физик хавфеизлик ноутбуклар учуй жиддий муаммо хисобланади. Бундай компьютерларни харид к,илишдаги параметрлардан бири-унинг улчами. Ноутбук канчалик кичкина булса, у шунчалик киммат туради. Бошка тарафдан, ноутбук канчалик кичкина булса, уни угирлаш шунчалик осонлашади. Шифрлаш калитларининг, масалан, WEP-калитлар (Wired Equivalent Privacy), дастурий калитлар, пароллар ёки шахеий калитларнинг (PGP, Pretty Good Privace кабилар) йукртилиши катта муаммо хисобланади ва уни иловалар яратилиши боскичидаёк, хисобга олиш зарур. Нияти бузук, одам ноутбукни уз ихтиёрига олганидан сунг аксарият хавфеизлик механизмлари бузилиши мумкин.

Ноутбукларнинг мобиллилиги уларнинг корпоратив тармоклараро экранлар (брандмауэрлар) билан химояланмаган бошк,а тармокдар билан уланиш эхтимоллигини оширади. Бу Internet-уланишлар, фойдаланувчи тармокдар, асбоб-ускуна ишлаб чикарувчиларининг тармоги ёки рак,иблар хам жойланувчи мехмонхона ёки кургазмалардаги умумфойдаланувчи тармокдар булиши мумкин. Бундай холларда мобил компьютерларнинг ахборот хавфеизлиги хусусида жиддий уйланиш лозим.

Ноутбукларнинг физик сакданишларини таъминлаш усулларидан бири-хавфеизлик кабелидан фойдаланиш. Ушбу кабел ноутбукни столга ёки бошка йирик предметга "бойлаб" к,уйишга мулжалланган. Албатта, бу юз фоизлик кафолатни бермайди, аммо хар холда угрининг анчагина куч сарф килишига тугри келади.

Ноутбукларнинг тез-тез угирланиши сабабли, ахборотни архивлашнинг хавфеизликни таъминлашга нисбатан мухимлиги кам эмас. Шифрлаш

дастурлари файллар хавфсизлигини таъминлашда ёки каттик, дискларда шифрланган маълумотлар хажмини яратишда ишлатилади. Бу маълумотларни расшифровка килиш учун, одатда, паролни киритиш ёки шахсий калитларни ишлатиш талаб этилади. Барча ахборотларни шифрланган файлларда ёки архивларда сакданиши керакли файллар тупламини архив учун нусхалашни енгиллаштиради, чунки улар энди маълум жойда жойлашган булади.

Угрилар учун ноутбуклар "биринчи номерли нишон" эканлигини фойдаланувчилар тушуниб етишлари ва уларни каровсиз крлдирмасликлари зарур. Хдтто офисларда ноутбукни кечага крлдириш мумкин эмас, чунки офисга куп кишилар (компания ходимлари, фаррошлар, мижозлар) ташриф буюрадилар.

Ахборотнинг чикиб кетиши ноутбук эгасининг куп одамлар тупланган жойларда хам содир булиши мумкин. Самолет - компания менеджерлари фойдаланадиган одатдаги транспорт воситасидир. Самолетда кушни креслодаги йуловчи ноутбук эгасининг елкаси устидан мухим ахборотни укиб олиши мумкин. Хдтто "уй шароитидаги" ноутбуклар хам химояланиши зарур. Бу хрлда компьютернинг химояси сервер химоясидан фаркданмайди. Жуда хам зарур булмаган сервисларнинг учирилиши к,урилма ишлашини яхшилайди.

Узининг дастурий таъминотини ноутбукка урнатган нияти бузук, одам хавфсизликнинг барча механизмларини четлаб утиш имкониятига эга булади. Компьютерни уз ихтиёрига олган угри унга узининг дастурини урнатганида уни тухтатиб булмайди. ВЮБда (Basic Input/Output System-киритиш/чик,аришнинг базавий тизими) ва каттик, дискда урнатилган пароллар угриланган ноутбукдан фойдаланишга тускинлик к,илиши мумкин.

Ушбу барча воситалар, афсуски, тажрибали хакер учун тусик, булаолмайди.

Чунтак компьютерлари. PDA(Personal Digital Assistans - "шахсий ракамли ёрдамчилар")нинг купгина хилларидан симсиз иловалар билан ишлашда фойдаланилади. Махсус курилган РБАларда тиббиёт, саноат ёки авиация иловалари ишга туширилади. Чунтак компьютерлари хам мавжуд булиб, уларда симсиз алока учун урнатилган карточка, штрих кодларнинг

сканери, хизмат мудцати узок, булган батареялар ёки магнит хршияли карталарни укувчи курилма каби к,ушимча курилмалар билан биргаликда **Palm OS** ёки Windows SE операцион тизим урнатилган. Бундай компьютерлардан фойдаланиш учуй махсус техник тайёргарлик талаб этилмайди. Шунга ухшаш курилмаларни ёки иловаларни химоялаш айник,са мураккаб масала хисобланади.

РБАдан фойдаланишга хохиш билдирган хужум к,илувчи учун ундаги ахборот киритиш механизмларининг барчаси нишон хисобланади. Ундан ташкдри, аксарият чунтак компьютерлари шундай ишлаб чик,илганки, уларни ишлаб чик,увчилари учун иловалардаги хатоликларни осонгина аникдаш йуллари таъминланган. Хатоликларни аникдашда ишлатилувчи интерфейслар нияти бузук, одамлар учун х,ак,ик,ий "тешик" хизматини уташи мумкин.

Чунтак компьютери ишлайдиган ахборотни х,имоялаш учун ахборотни чунтак компьютерида эмас, балки маълумотларнинг хавфсиз резерв базасида сакдаш лозим. Яна бир вариант - **JAVA** тили иловасидан ёки фойдаланувчи учун махсус яратилган иловалардан фойдаланиш. Бу хрлда ахборот курилмада сакданмайди, аммо, РБАнинг дисплейида акслантирилади. Бошкдча айтганда, симсиз иловалардан фак,ат симсиз тармокдан фойдаланиш мавжуд булган жойларда фойдаланиш мумкин.

Аксарият РБАларда парол ёрдамида блокировка ва разблокировка к,илиш имконияти мавжуд. Бу усулларга бутунлай ишонмаслик лозим, аммо улар нияти бузук, одамларни вак,тинча тухтатиб туриши мумкин. Ундан ташкдри PDAнн блокировка к,илиш тизими к,урилмадаги иловалардан ёки ахборотдан нияти бузук, одамларнинг фойдаланишни к,ийинлаштиради. РБАнинг зарур булмаган барча функцияларини учириб к,уйиш лозим, чунки хар бир учирилган киритиш механизми булиши мумкин булган хужумлар сонини камайтиради.

Чунтак компьютерида мухим ахборотни сакдаш учун шифрлашни к,уллаш ва унга к,ушимча сифатида манбани улаш ва экранни блокировка к,илиш учун пароллар урнатиш тавсия этилади.

Симсиз инфратузилма. Симсиз инфратузилма курилмалари одатда одамлар йигилган ерда жойлаштирилади. Уларга кафелар, аэропортлар,

корпоратив тадбирларни утказиш жойлари ва х,. киради. Турли хил одамлар EAP(Extensible Authentification Protocol - аутентифкациялашнинг кенгайтирилувчи протоколи) ёки WEP каби хавфсизлик воситаларини ишдан чикариш ёки тармоккд сукилиб кириш учуй тармок, конфигурацияси хусусидаги ахборотни кулга киритиш максадида ушбу компонентлардан фойдаланишни хохлапшари мумкин.

Симеиз инфратузилма курилмаларида тармокни бошкариш функцияларининг хавфеизлигини таъминлаш учуй улардан фойдаланишда SSH, SSL (Secure Sockets Layer) ёки SNMP3 (Simple Network Management Protocol 3 - тармокни оддий бошкариш протоколи, 3-версия) каби хавфеиз протоколлардан фойдаланиш л озим. Ундан ташкари telnet, HTTP даги тугри матн, ва SNMP (биринчи версия) каби хавфсизлик етарли даражасини мададламайдиган протоколлар учирилиши лозим. Хавфеиз бошкаришни таъминлаш иложи булмаса, фойдаланишнинг баъзи бир нукталарини кетма-кет портлар оркали бошкариш мантик,ан тугри хдеобланади. Фойдаланиш нукталарини юк,орига к,ул етмайдиган жойга мах,камлаб к,уйиш х,ам уларни угарланишдан сакдайди.

Уяли телефонлар. Уяли телефонлар учун хавфсизлик мулохазалари ноутбук ва РБАларга нисбатан келтирилган мулохдзаларга ухшаш. К,урилмаларнинг узи ва мое дастурий таъминот учун хавфсизлик муаммоси хдм х,еч нимаси билан фарк, к,илмайди.

Уяли телефонлар х,ам бошка симсиз к,урилмаларга буладиган хужумларга дучор буладилар. Одатда буфернинг тулиб-тошиши, к,атор форматига хужумлаш, грамматик хатоликлар ишлатилади, натижада хужум к,илувчи угирланган к,урилмада узининг дастурини ишга туширишга эришади. Мисол сифатида SMSHmrr киска хабарларини курсатиш мумкин. Узининг телефони орк,али SMS жунатган фойдаланувчига хужумга дучор булиши хавфи тугилади. Бу хужум натижасида хизмат к,илиш тухтатилади ёки фойдаланувчи терминалида бегонанинг командалари бажарилади.

Ундан ташкари SIM-карталарни (Subscriber Idenity Module - абонент идентифкацияси модули) ишлаб чикарувчилари к,урилмаларига уяли телефонга симсиз интерфейс орк,али юкланилиши рухсат этиладиган кушимча

функцияларни кирита бошладилар. Мисол тарикасида Sim Toolkit ва МЕХЕни курсатиш мумкин. Зарарли иловаларни бошка фойдаланувчига узатишни олдини олувчи усуллар ташки хужумларга дучор булади. Бундай иловаларнинг мох,ияти шундаки у нияти бузук, одамга фойданувчининг адрес китобини ёки телефондаги бутун SMS руйхатини узатиши мумкин. Баъзи ечимлар DES стандарта асосида ишлайди, аммо худди шундай DES-калитлар хар бир SIM-карталар учун ишлатилади.

Терминаллар учун парол ёки PIN-кодларни ишлатиш тавсия этилади. GSM(Global System for Mobile Communications - мобил коммуникацияларнинг глобал тизими) тармокдарида ишловчи телефонлар хавфсизлигини таъминлашда SIM PIN керак булади. Бу функциядан максимал фойдаланиш учун барча булиши мумкин булган РЕЧлардан фойдаланиш хамда IMEI (International Mobile Equipment Identity - мобил курилманинг харкаро номери)нинг ишончли жойда ёзилиши тавсия этилади.

Мухим ахборотни узатиш учун терминалдан фойдаланишида ахборотни албатта шифрлаш зарур. Кредит карточкалар номерларини ёки бошка шахсий ахборотни узатиш учун албатта SSL-химояли WTLS-уланиш хизматидан фойдаланиш зарур. Ундан ташк,ари GSM ичидаги алгоритмларга буладиган аксарият хужумлар нияти бузук, одамга фойдаланувчининг телефон номерини уйлаб чик,аришга (клонировка) имкон беради. Бу хужумлар одатда телефон мавжудлигини талаб к,илади, шу сабабли телефонии хавфсиз жойда саклаш, йук,отилган ёки угирланган х,олда тезлик билан операторга хабар бериш лозим.

XIII боб. ХАВФСИЗЛИКНИ БО11ЩАРИШ ВА ХИМОЯ ТИЗИМИНИ К.УРИШ

13.1. Бошкаришнинг функционал масалалари

Замонавий ахборот технологияларидан муваффакиятли фойдаланиш учун нафакат тармокларнинг узини, балки тармок, хавфсизлиги воситаларини хам ишончли ва самарали бошкариш зарур. Хрзирги вактда компаниянинг бутун инфратузилмасини камраб олувчи бошкаришнинг комплекс тизимини яратиш биринчи галдаги вазифа хисобланади. Бундай бошкариш тизими ахборот тизимининг мураккаблиги ва масштабидан катъий назар, к,уйидагиларга имкон яратади:

- бутун ахборот инфратузилмасига марказлаштирилган ва оператив бошк,ариш таъсирни курсатиш;
- оператив ечимларни кабул килиш учун ахборот хавфсизлиги хрлати хусусидаги объектив ахборотни берувчи мунтазам аудитни ва кенг куламдаги мониторинг утказиш;
- ахборот инфратузилмаси ривожини башоратлаш учун унинг ишлаши хусусидаги статистик маълумотларни туплаш.

Ахборот тизимларини бошкаришнинг ITIL методологияси ITIL (IT Infrasructure Library) методологиясига мувофик, ахборот тизими иккита йирик блокдан - ахборот инфратузилмаси ва ахборот сервис-ларидан иборат (13.1-раем).

13.1-расм. ITIL методологияси нуқтаи назаридан ахборот тизимининг кўриниши

Ахборот инфратузилмаси ахборот сервислари ишловчи моддий асос, мухит хисобланади. Ахборот сервисларига Internet-сервислар, иловалар сервиси, бошкариш, ечим кабул килиш сервислари ва х,. киради. Ахборот инфратузилмаси сер висл ар ишлашини таъминловчи техник воситалар, ал ока линиялари, муолажалар, меъёрий хужжатлар ва х,. мажмуидир. Ахборот сервисларининг сифати бевосита ахборот инфратузилмаси ва уни бошкариш сифатига богаик,.

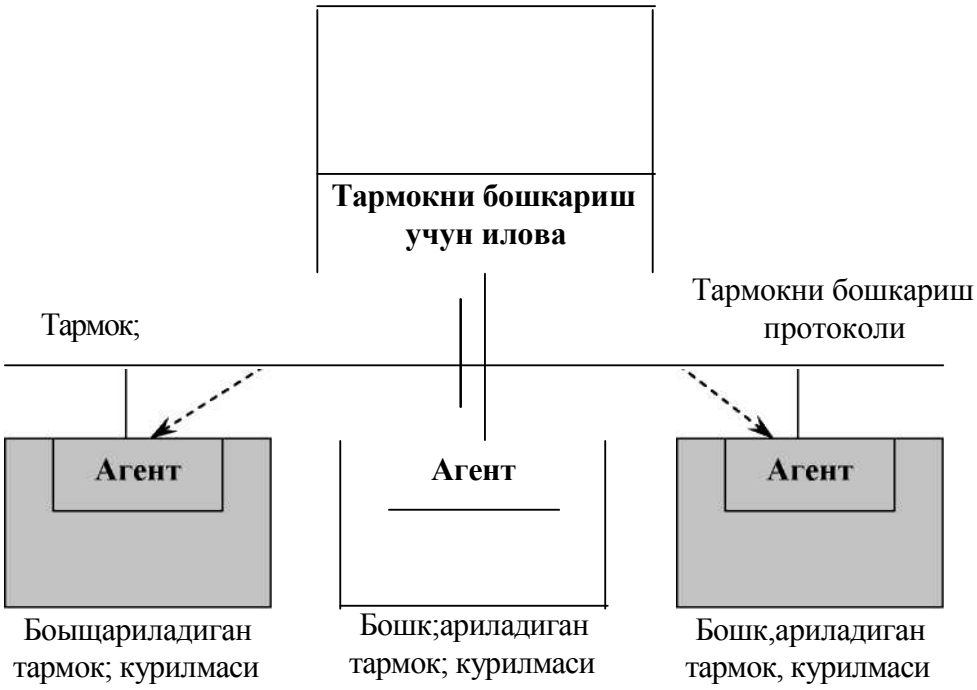
Ахборот инфратузилмасини асосида ахборот ресурслари (хисоблаш платформалари, серверлар, шахсий компьютерлар, маълумотларни узатиш тармокдари, алока линиялари) ётувчи пирамида сифатида тасаввур этиш мумкин (13.2-расм).

Бизнес	• Электрон бизнес • Бошкдрма тизимлар • Молиявий тизимлар
Иловалар	• Кафолатли етказиб бериш • Иловаларни бошкариш • Internet/intranet • Ишлаб чикдриш • Электрон почта • Маълумотлар базаси • Энг зарур тизимлар
Ресурслар	• Тармокдар • Мэйнфреймлар • Серверлар • Шахсий компьютерлар

13.2-расм. Ахборот инфратузилмасини ташкил этувчилари Пирамиданинг иккинчи сатхини турли иловалар ташкил этади. Бу иловалар биринчи сатх, ресурсларидан фойдаланиб татбикий дастур таъми-ноти, электрон почта, кафолатланган етказиш тизими, маълумотлар базаси, Web-серверлар ва х,. каби муайян иловалар ишлашини таъминлайди. В а нихрят, энг юкрри сатхда бизнес ва ишлаб-чикариш жараёнларининг утишини таъминловчи иловалар ишлайди. Иккала пастки сатхдан фойдала-нувчи бу иловалар ишлаб-чикаришни бошк,ариш, буюртмачилар ва таъмин-

ловчи билан узаро алока, молиявий хисоб ва ечимни кабул килишни мададлаш каби бизнес масалаларни ечишга йуналтирилган.

Умумий хрлда, тармокни бошкариш тизимининг архитектураси 13.3-расмда келтирилган куриништа эга. Тармокни бошкариш иловаси тармок, маъмурининг иш жойида ёки бошка компьютерда бажарилиши мумкин. Унинг вазифаси бошкарилувчи курилмаларда бажариладиган *агент* - иловалардан ёки операцион тизим сервисларидан келувчи бошкарилувчи объект хусусидаги ахборотни йигаш.



13.3-расм. Тармоцни бощцариш тизимининг умумлаштирилган архитектураси

Бундай иловаларни агентлар билан узаро алокаси учун одатда SNMP (Simple Network Management Protocol) ёки CMIP (Common Management Information Protocol) протоколларидан фойдаланилади. Биринчиси, одатда, локал тармокда ишлатилса, иккинчиси телекоммуникациядан фойдаланувчи таксимланган тармокдарда ишлатилади. Аммо дастур таъминотини баъзи ишлаб чикарувчилари тармок,ни бошкаришда хусусий тармок, протоколларидан фойдаланишади.

Тармок,ни бошк,арувчи замонавий воситалар куйидаги вазифаларни бажара олади:

- бошкарилувчи компьютер ва курилмалардаги бузилишларни кузатиш, сабабларни аникдаш ва бартараф этиш (купинча автоматик тарзда), окибатларини тузатиш ва бузилишларни олдини олиш (масалан ташхислаш амалини бажариш оркали);

- компьютерларнинг ва тармок, курилмаларининг конфигурацияланишини бошкариш (хусусан, инициализациялаш, кайта конфигурациялаш ва тармок, курилмалари ва компьютерларни узиб куйиш);

-фойдаланувчилар ва фойдаланувчилар гурухи томонидан тармок, ресурсларидан фойдаланишни тартибга солиш (масалан, дискли ва бошка квоталарни тартибга солиш);

- тармок, курилмалари ва сервислар унумдорлигини бошкариш (тармок, курилмалари ишлатилиши жадаллиги статистикасини ва хатоликлар частотасини йигаш ва тахлиллаш хамда олинган маълумотлар асосида улар унумдорлигини сунъий тарзда урнатиш);

- олдиндан белгиланган хавфсизлик сиёсати асосида тармок, ресурсларидан фойдаланишни назоратлашдан фойдаланиб маълумотлар химоясини бошкариш ва уларни бузишга уринишлардан маъмурни хабардор этиш.

Корхона ахборот хавфсизлиги тизими корпоратив тармокни бошкариш тизимининг энг мухим компоненти хисобланади. Корхона масштабидаги так,симланган тармокда ахборотни х,имоялаш воситаларини бошк,арувчи тизим куйидаги вазифаларни бажариши лозим:

- корхона тармоги доирасида хавфсизлик сиёсатини бошкариш, алох,ида к,урилмалар хавфсизлигининг локал сиёсатини шакллантириш ва уни ахборотни химояловчи барча к,урилмаларга етказиш;

- фойдаланиш объектларини ва субъектларини конфигурациялашни бошк,ариш; х,имоя к,урилмалари ва дастурий таъминоти таркибини, версиясини, компонентларини бошкаришни уз ичига олади;

- таксимланган татбик,ий тизимларга х,имоя сервисларини такдим этиш, х,имояланган иловалар ва улар ресурсларини руйхатга олиш. Иловаларнинг бу гурухи, аввало, татбикий тизимлар томонидан х,имоя сервисларини бошкариш учун интерфейсни таъминлаш лозим;

- криптовоситаларни бошкариш, хусусан калитли бошкариш (калитли инфратсруктура). Калитли инфратузилма инфратузилма хизмати таркибида ишлаши л озим;

- ходисавий протоколлаш; турли курилмаларга *логларни* беришни созлашни, логларни деталлаштириш сатхини бошкаришни, протокол олиб борилувчи ходисаларни таркибини бошкаришни уз ичига олади;

- ахборот тизими хавфсизлигини аудитлаш; ахборот тизимлари химояланишининг жорий хрлати хусусидаги объектив маълумотларни бахрлашни таъминлайди;

- тизим хавфсизлигини мониторинглаш; курилмалар ва курилмаларда кечувчи ходисалар (химоялаш контексти буйича) хрлати, фаоллиги хусусида, масалан, булиши мумкин булган хужумлар хусусида реал вактда ахбо рот олинишини таъминлайди;

- махсус химояланган иловалар, масалан амаллар устидан нотариал назорат ишини таъминлаш хамда регламентда кузда тутилган тадбирларни (калитларни, паролларни, химоя курилмаларини алмаштириш, смарт-карталарни ишлаб чикариш ва х,.) мададлаш;

- иловаларнинг лойиха-инвентаризациялаш гурух,и ишини таъминлаш. Иловаларнинг бу гурухи корхона тармогига х,имоя воситаларини урнатишни, к,улланиладиган х,имоя воситаларини хисобга олишни, х,имоя воситаларининг модул таркибини назоратлашни, химоя воситалари х,олатини назоратлашни ва х,. бажаради.

Тармокдарни анъанавий бошкариш тизими ва тармокдаги ахборотни химоялаш воситаларини бошк,ариш тизими орасида узаро алок,ани комплекслаш ва ташкил этиш муаммоси мавжуд.

13.2. Хавфсизлик воситаларини бошкариш архитектураси

Компаниянинг так,симланган ахборот тизимида узининг хавфсизлик сиёсатини муваффакиятли амалга ошириши учун хавфсизликни бошк,ариш марказлиштирилган булиши ва ишлатиладиган операцион тизимга ва татбикий тизимларга боглик, булмаслиги лозим. Ундан ташк,ари, корпора-

тив ахборот тизимида кечувчи жараёнларни (рухсатсиз фойдаланиш, фойдаланувчилар имтиёзини узгариши ва х,.) руйхатга олиш тизими ягона булиши ва маъмурга корпоратив ахборот тизимидаги барча узгаришларнинг тулик, куринишини тасаввур этишига имкон бериши лозим.

Корпоратив ахборот тизими хавфсизлигини марказлаштирилган бошкариш асосида глобал бошкариш концепцияси GSM (Global Security Management) ётади. Ушбу концепция корхона ахборот ресурсларини куйидаги хусусиятларга эга булган комплекс бошкариш тизимини куришта имкон беради:

- корхонанинг барча ресурслари (хавфсизлик сиёсати объектлари) учун химоялашнинг яхлитлигини, зиддиятлик эмаслигини ва кридалар тупламининг тулалигини таъминловчи, барча мавжуд химоя воситаларини корхона хавфсизлиги сиёсати асосида бошкариш;

- ресурсларни тавсифловчи шахсий воситалар хамда корхонанинг бошка каталоглари билан алокаси буйича фаоллашувчи корхона мухитининг ягона (таксимланган) каталоги оркали корхонанинг барча ре сурсларини аниклаш;

- хавфсизлик сиёсатига асосланиб, ахборотни химоялашнинг локал воситаларини марказлаштирилган бошкариш;

- корхона мухитида сиёсат объектларини токенлар ва очик, калитлар инфратузилмасидан фойдаланиб к,атъий аутентификациялаш;

- каталогда белгиланган корхона ресурсларидан ёки бутун каталог к,исмларидан фойдаланишни маъмурлашнинг кенгайтирилган имкониятлари;

- х,исоб-китобликни (корпоратив тармок, масштабида тизимнинг так,симланган объектларининг узаро алок,асидаги барча амалларини руйхат га олиш) ва аудитни, хавфсизлик мониторингини, хавотирли сигнализация-ни таъминлаш;

- умумий бошк,ариш тизимлари ва хавфсизликнинг инфратузилма тизимлари билан интеграцияланиши;

Ушбу концепция доирасида "хавфсизлик сиёсатига асосланган PBM (Policy Based Management) бошкариш" деганда корхона бизнес-объекти учун таърифланган кридалар туплами тушунилади. Бу кридалар туплами

объектларнинг бизнес-сохдни тулик, камраб олишини ва ишлатилувчи бошкариш кридаларининг зиддиятлик эмаслигини кафолатлайди.

РВМ принципларига асосланган, корхона хавфсизлигини бошкаришга мулжалланган GSM бошкариш тизими куйидаги талабларга жавоб беради:

- корхона хавфсизлиги сиёсати мантикий ва семантик богланган, шаклланувчи, тахрирланувчи ва тахлилланувчи маълумотларнинг бир бутун тузилмасидан иборат;

- корхона хавфсизлиги сиёсати ягона контекстда химоянинг барча сатхдари учун химоянинг тармок, сиёсати ва корхона ахборот ресурслари хавфсизлик сиёсатининг бир бутуни сифатида белгиланади;

- корхона ресурсларини ва хавфсизлик сиёсатини маъмурлашни енгиллаштириш максадида сиёсат параметрлари сони минималлаштирилади.

GSM бошкариш тизими хавфсизлик сиёсатининг корхона хавфсизлиги концепцияси моделига мослигини текширувчи куп мезонли воситалар эвазига хавфсизлик сиёсатини тахдиллашнинг турли-туман механизмларини таъминлайди.

Хавфсизликнинг глобал ва локал сиёсатлари

Корхона хавфсизлигининг глобал сиёсати ахборот хавфсизлиги контекстида корпоратив тармок, объектлари узаро алокасининг параметрларини тавсифловчи хавфсизлик кридаларининг чекли тупламидир.

Бунда хавфсизликнинг глобал сиёсати объекти сифатида алохдда ишчи станциялари ва кием тармокдар хамда уз ичига компаниянинг бутун тузилмавий булимларини олувчи (масалан, маркетинг булими ёки молиявий департамент) объектлар гурухи ёки х,атто алох,ида компания курилиши мумкин.

Хавфсизликнинг глобал сиёсати тармокдаги узаро алок,ага, х,амда тизимнинг назоратлаш ва бошкариш функцияларига тааллукли булиши мумкин. Бажарадиган функциялари буйича хавфсизликнинг глобал сиёсати куйидаги гурухдарга булинади:

- *VPN цоидалари.* Кридаларнинг бу гурух,и IPSec протоколлари ёрдамида амалга оширилади;

- *пакетли филътрлаш қоидалари*. Бу кридалар Stateful ва Stattles хилидаги пакетли фильтрлашни таъминлайди.

- *proxy-қоидалар.* Бу кридалар берилган татбикий протокллар бошкарувида узатилувчи трафикни фильтрлашга жавоб беради;

- *аутентификацияланган/авторизацияланган фойдаланиш қоидалари;*

сигнализацияга ва ходисавий протоколлашга жавоб берувчи қоидалар.

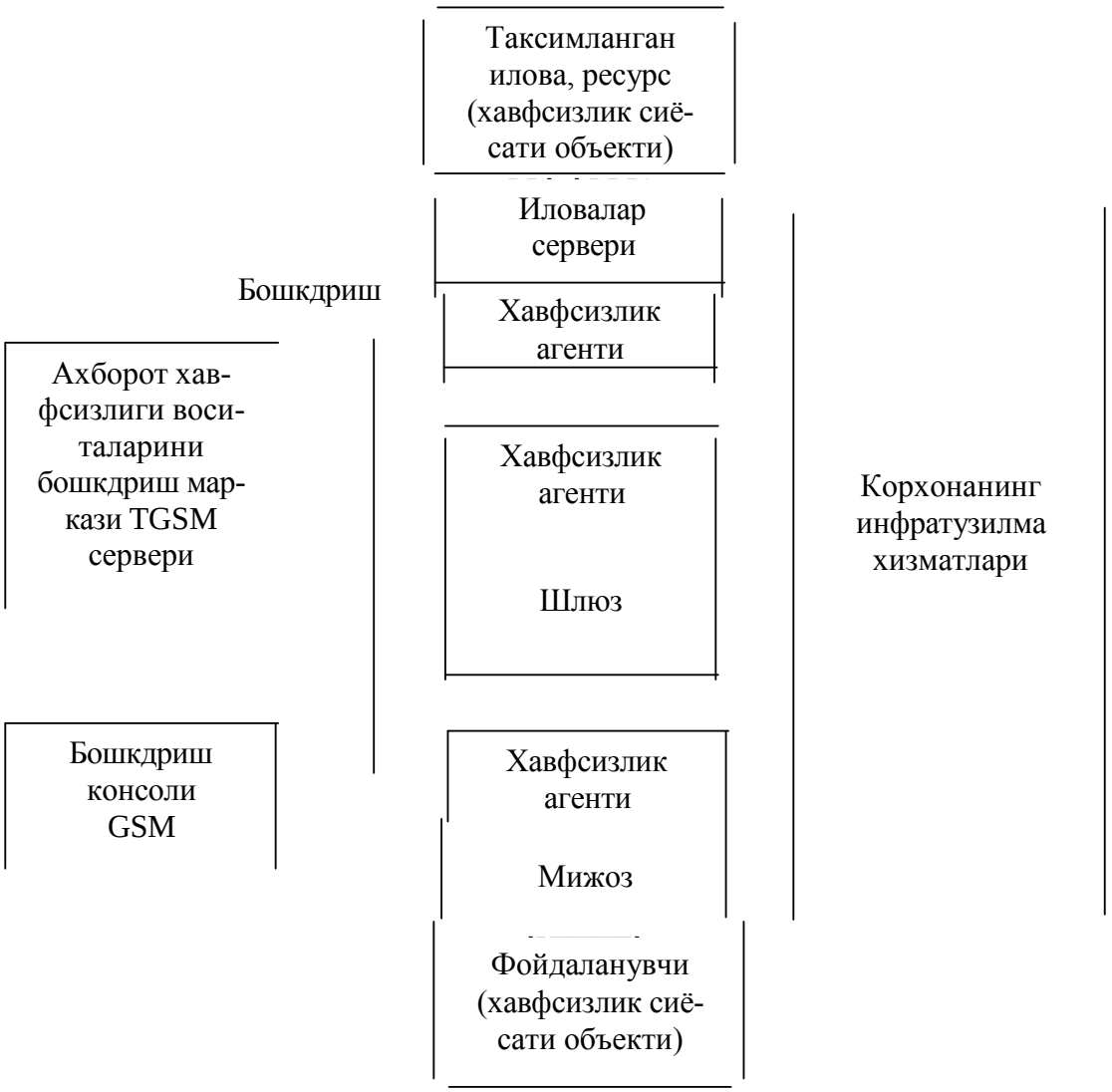
Хавфсизликнинг глобал сиёсати тармок, сатх,ида хавфсизлик сиёсатининг мантикий яхлит ва семантик тулик, тавсифи булиб, унинг асосида алохида курилмалар хавфсизлигининг локал сиёсати курилиши мумкин.

Хавфсизликнинг локал сиёсати ахборот хавфсизлигининг кандайдир сервисини амалга оширувчи хар кандай химоялаш воситасига зарур хисобланади. Анъанавий ёндашишда маъмурга хар бир химоя воситасини алохида созлашга ёки энг оддий созлашни узелларнинг катта сонига кайтаришга (регшикациялашга) тугри келар эди. Равшанки, бу маъмурлашнинг катта сонли хатолигига олиб келар ва натижада корпоратив тармокнинг х,имояланиш даражаси жиддий пасаяр эди.

Маъмур томонидан хавфсизликнинг глобал сиёсати шакллантирилганидан сунг бошк,ариш маркази унинг асосида хар бир химоя воситаси учун автоматик тарзда химоялашнинг алох,ида локал сиёсатини хисоблайди ва мое химоя воситасининг бошкариш модулига зарурий созлашларни автоматик тарзда юклайди.

Тармокда хавфсизликнинг глобал сиёсатини ва муайян к,урилмада хавфсизликнинг локал сиёсатини амалга ошириш кридаларининг бир-биридан фарк,и шундаки, хавфсизликнинг глобал сиёсатидаги кридаларда фойдаланиш объектлари ва субъектлари тармок, чегарасида ихтиёрий равишда таксимланиши мумкин, хавфсизликнинг локал сиёсатидаги кридалардан эса фак,ат тармок, курилмаларидан бирининг мух,ити чегарасида фойдаланиш мумкин.

Ахборот хавфсизлиги воситаларини бошкариш тизимининг умумий тузилма схемаси 13.4-расмда келтирилган. Асосий хавфсизлик воситаларининг вазифалари куйидагича. Мижоз шахсий компьютерида урнатилган *хавфсизлик агенти* одатда "мижоз-сервер" иловаларида мижоз сифатида



13.4-расм. Ахборот хавфсизлиги воситаларини бошцариш тизимининг умумий тузилма схемаси

катнашувчи алохида фойдаланувчини химоялашга мулжалланган.

Иловалар серверига урнатилган *хавфсизлик агенти* таксимланган иловаларнинг сервер компоненти хавфсизлигини таъминлашга мулжалланган. Шлюз компьютерига урнатилган *хавфсизлик агенти* турли тармок, хавфсизлиги сиёсатини мувофиклаштириш масаласини ечган хрлда, корхона ичида ёки корхоналар орасида тармок, агентларини ажратилишини таъминлайди.

Бошцариш маркази тармок, масштабида хавфсизликнинг глобал сиёсатини тавсифлашни, глобал сиёсатни химоялаш курилмаси хавфсизлигининг

локал сиёсатига трансляциялашни, химоялаш курилмасини юклашни ва тизимнинг барча агентлари хрлатини назоратлашни таъминлайди.

Вошкариш консоли маъмур (маъмурлар) иш жойини ташкил этишга мулжалланган. GSMнннғ хар бир сервери учун бир неча консоллар урнатилиши мумкин.

Хавфсизликнинг локал агенты охирги курилмада (мижозда, серверда, шлюзда) жойлаштирилувчи дастур булиб, куйидаги функцияларни бажаради:

- хавфсизлик сиёсати объектларини аутентификациялаш, жумладан аутентификациялашнинг турли сервисларини интеграциялаш;
- тизимдаги фойдаланувчини ва у билан боглик, ходисаларни аниклаш;
- хавфсизлик воситаларини марказлаштирилган бошкаришни ва фойдаланиш назоратини таъминлаш;
- иловалар манфаати учун ресурсларни бошкариш, татбикий сатх, ресурсларидан фойдаланишни бошк,аришни мададлаш;
- трафикни химоялаш ва аутентификациялаш;
- трафикни фильтрлаш;
- ходисавий протоколлаш, мониторинг, хавотирли сигнализация.

Локал агентнинг марказий элементи - хавфсизликнинг локал сиёсатининг процессори (LSP processor) хавфсизликнинг локал сиёсатини изохдайди ва бошка компонентлар орасида чакиришларни таксимлайди.

13.3. Ахборот тизимларининг аудити ва мониторинги

Ахборот хавфсизлиги тизими амалга оширилганида тармок, инфратузилмасини мураккаблиги, маълумотлар ва иловаларнинг турли-туманлиги сабабли купгина тахдидлар хавфсизлик маъмурининг эътиборидан четга к,олиши мумкин. Шунинг учун ахборот тизимларининг мунтазам аудити ва доимий мониторинги амалга оширилиши зарур.

Ахборот тизимлари хаефсизлигининг аудити. Аудит-корхонанинг алохида сох,аларини мустакил экспертизаси. Корхона аудитининг ташкил этувчиларидан бири унинг ахборот тизими аудити хисобланади. Ахборот тизимларининг аудити - ахборот тизимининг химояланишининг жорий хрлати, ундаги харакатлар ва ходисалар хусусидаги объектив маълумотларни олиш ва бахрлаш, улар сатхининг белгиланган мезонга мослигини аникдовчи тизимли жараёндир. Аудит утказилиши ахборот тизимининг жорий хавфсизлигини бахрлашга, хавф-хатарни бахрлашга, уларнинг ташкилот бизнес-жараёнларига таъсирини башоратлашга ва бошкаришга, ташкилот ахборот ресурслари хавфсизлигини таъминлаш масаласига асосли ёндашишга имкон беради.

Ахборот тизимлари хавфсизлигининг аудити куйидаги боскичларни уз ичига олади:

- аудит муолажасининг бошланиши;
- аудит ахборотини йигиш;
- аудит маълумотларини тахлиллаш;
- тавсиялар ишлаб чикиш;
- хисобот тайёрлаш.

Аудит боскичларининг бажарилиш кетма-кетлиги 13.5-расмда келитирилган.

Аудит муолажасининг бошланиши. Аудит, бу масалада манфаатдор хисобланувчи, компания рахбарияти ташаббуси билан утказилади. Аудит тадбирларнинг комплекси булиб, унда аудитор билан бирга компаниянинг аксарият тузилмавий булинмаларининг вакиллари катнашади. Бу жараёнда иштирок этувчиларининг харакатлари аник, мувофиклаштирилиши шарт. Шу сабабли, аудит муолажасининг бошланиши боскичида аудит утказиш режасини тайёрлаш ва тасдиклаш, аудитор хукуки ва мажбуриятини белгилаш билан боглик, ташкилий масалалар ечилиши лозим.

Аудит муолажасининг бошланиши боскичида текшириш доираси аникланиши лозим. Компаниянинг ахборот кисми тизимининг бирини конфиденциаллик нуктаи назаридан аудитга тортиб булмаса, иккинчисини,

етарлича жидций булмаганлиги сабабли, аудит доирасидан чикдриш мумкин.

13.5-расм. Аудит босцичларининг бажарилиш кетма-кетлиги.

Аудит ахборотини йигиш. Бу боскдга энг мураккаб ва узок, давом этади. Бунга сабаб, ахборот тизимга керакли хужжатларнинг йукдиги ва аудиторнинг ташкилотнинг купгина лавозимли шахслари билан бевосита узаро мулок,отда булиши зарурияти. Аудитор ташкилот, ахборот тизимининг ишлаши ва жорий х,олати хусусидаги ахборотни компаниянинг жавобгар шахслари билан махсус ташкил этилган сухбат оркдпи, техникавий ва ташкилий-бошк,ариш хужжатларни урганиш йули билан, х,амда ихтисослаштирилган дастурий воситалар ёрдамида ахборот тизимини таддиклаш орк,али олади.

Аудит маълумотларини тахлиллаш. Тахлиллаш ахборот тизимларининг аудитида энг маъсулиятли боск,ич х,исобланади. Тахлиллашда ноаник,, эскирган маълумотлардан фойдаланиш ножоиздир, шу сабабли маълумотларга аникдик киритилиши ва ахборотлар жиддий йигилиши мумкин. Аудит маълумотларини тахлиллашда куйидаги учта ёндашишдан фойдаланилади.

Биринчи ёндашиш хавф-хатарларни тахлиллашга асосланади. Хавф-хатарларни тахлиллашдан мак,сад мавжуд хавф-хатарларни аникдаш ва улар катталигини бахрлаш (уларга сифатий ва микдорий бахр бериш). Ушбу ёндашиш жуда мураккаб булиб, куп мехнат сарф этилади ва аудиторнинг энг юк,ори малакасини талаб к,илади.

Иккинчи ёндашиш ахборот хавфсизлиги стандартларидан фойдаланишга асосланган. Стандартлар ахборот тизимларининг кенг синфи учун дунё амалиётини умумлаштириш натижасида шаклланган хавфсизлик талабларининг базавий тупламини белгилайди. Бу хрлда аудитордан, берилган ахборо тизими учун стандарт талаблари тупламини тугри танлаш талаб этилади. Соддалиги ва ишончлилиги туфайли бу ёндашиш амалда кенг к,улланилади. У ресурсларнинг минимал сарфида ахборот тизими хусусида асосланган хулосалар к,илишга имкон беради.

Учинчи ёндашиш олдинги икала ёндашишни комбинациялашни кузда тутади. Ахборот тизимига куйиладиган хавфсизликнинг базавий талаблари стандарт оркдпи аникданса, берилган ахборот тизими ишлашининг хусусиятларини хисобга олувчи к,ушимча талаблар хавф-хатарларни тахлиллаш асосида шакллантирилади.

Тавсиялар ишлаб чщиш. Тахлиллаш натижалари тавсиялар ишлаб чик,иш учун асос булади. Аудитор тавсиялари муайян ва берилган ахборот тизимига к,улланиладиган, ик,тисодий асосланган, исботланган (тахлиллаш натижалари билан кувватланган), ва мухимлик даражаси буйича рутбаланган булиши шарт. Аудитнинг мунтазам утказилиши ахборот тизимининг барк,арор ишлашини кафолатлайди. Шунинг учун профессионал аудит натижаларидан бири кейинги текширишларин утказиш режа-графигини шакллантиришдан иборат.

Хисобопг тайёрлаш. Аудитор хисоботи аудит утказишнинг асосий хужжати х,исобланади ва унинг сифати аудитор ишининг сифатини характерлайди.

Хисобот таркибида аудит утказиш мак,садининг тавсифи, текширилувчи ахборот тизимининг характеристикаси, аудит утказиш доираси ва ишлатилувчи усуллар буйича курсатма, аудит-маълумотлари тахлилининг

натижаси, бу натижаларни умумлаштирувчи ва ахборот тизими хдмояланиш сатхининг стандарт талабларга жавоб бериши буйича хулосалар ва албатта, мавжуд камчиликларни бартараф этиш ва химоя тизимини такомиллаштириш буйича тавсиялар булиши лозим.

Ахборот тизимлари хавфсизлигининг мониторинги Хрзирда тармокдараро экран, виртуал хусусий тармок,, рухсатсиз фойдаланишдан химоялаш воситалари каби химоянинг анъанавий воситала-ри ишончли ва самарали ахборот хавфсизлиги тизимини куришга зарур булсада, етарли эмас. Чунки бу анъанавий воситалар факат хужумни блокировка килишга крдир, аммо хужумларни олдини олиш ва окибатларини аникдаш имконияти уларда мавжуд эмас.

Ушбу муаммонинг ечими асосланган ёндашиш фаол аудит технологияси ёки хавфсизликни фаол (адаптив) бошкариш технологияси номини олган. Хавфсизликни фаол бошкариш технологияси куйидаги компонентларни уз ичига олади:

- ишчи станциялари, серверлар, маълумотлар базасини бошкарувчи тизимлар, тармок, уланишлари ва Internet ва бошка глобал тармокдарга уланиш нукталари каби ахборот тизими объектлари химояланишини тахлилловчи ва заифликларини кидирувчи воситалар;
- хужумларни аникдаш ва тахлиллаш воситалари;
- инфратузилма узгаришида ёки хужумларда х,имоялаш воситаларини вактнинг реал режимида созлашларни мослаштириш ва бошкариш восита лари.

Ахборот хавфсизлиги тизими мониторинги вазифаларини химояланишни тахлиллаш ва хужумларни аникдаш воситалари бажаради. Химояланишни тахлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим х,имояси элементларининг созланишини тадк,икдайди. Улар тармок, топологиясини тадк,икдайди, х,имояланмаган ёки нотугри тармок, уланишларини кидиради, тармокдараро экранлар созланишини тахлиллайди. Химояланишни тахлиллаш воситаларини, уларнинг ишлаши буйича хавфсизлик сканерлари деб хам юритишади. Тахлиллаш натижасида сканер маъмурга юборилувчи, таркибида

аникданган заифликлар ва уларни йукртиш коидалари булган хисоботни шакллантиради. Агар сканер таркибида хавфсизлик воситалари созланишини бошкарувчи воситалар булса, у мустакил тарзда уларни кайта конфигурациялаши мумкин.

Ташкилотнинг замонавий инфратузилмасини хдсобга олган хрлда айтиш мумкинки, бундай сканерларнинг мавжудлиги ахборот тизимлари хавфсизлиги мониторингининг мухим элементи хисобланади. Таъкидлаш лозимки, бу воситалар химояни хужум содир булишидан аввал амалга оширади.

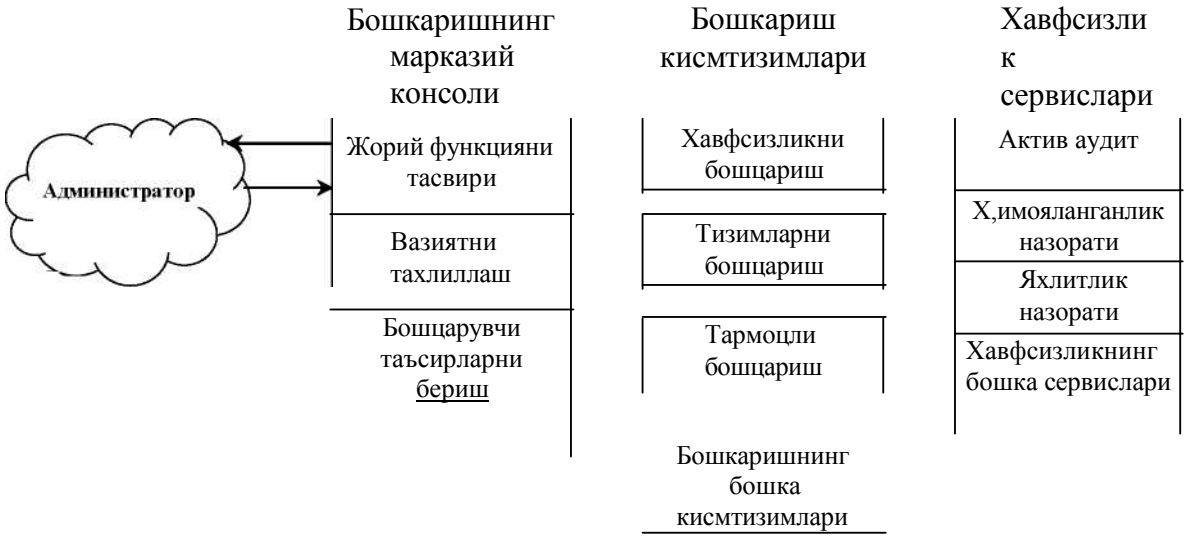
Ахборот тизими хавфсизлиги мониторингининг яна бир зарур элементи хужумларни аникдовчи воситалардир. Хужумларни аникдаш корпоратив тармокда кечувчи шубх,али харакатларни бахрлаш жараёнидир. Хужумларни аникдаш вактнинг реал режимида тармок, трафигини, хамда операцион тизим ва иловаларнинг руйхатга олиш журналларини тахлиллаш орк,али амалга оширилади. Хужумларни аникдаш тизимининг компонентлари агентлар деб аталади, ва ишчи станцияларда, серверларда жойлаштирилади ёки тармокнинг к,андайдир сегментини ёки бутун тармокни к,оплайди. Агентлар узларининг ишида сканерлар каби маълум заифликлар руйхатидан фойдаланиб, ходисаларни ушбу заифликлар билан такдослайди. К,андайдир узелда шубх,али фаолият аникданганида хужумларни аникдаш тизими ушбу фаолият фаоллиги хусусидаги огохдантиришни маъмурга жунатади. У огохдантиришни узелнинг узига жунатиши ёки узел ишини блокировка килиш мумкин. Ушбу тизимнинг фаркди хусусияти - унинг булиб утган хужумларни аникдаш учун ходисалар журналини тахлиллашидир.

Хавфсизлик воситаларини бошкариш шакли буйича пассив ва фаол (актив) булиши мумкин. Пассив бошкаришда тармок,ни бошк,ариш тизимига ёки маъмурга факат хабар берилса, фаол бошкаришда хужумловчи узел ёки фойдаланувчи билан мустакил тарзда сессия тугалланади.

Бундан ташк,ари, бу тизимнинг вазифасига тармокдаги, иловалардаги ёки ташкилот ахборот тизимининг бошка компонентларидаги заифликларни йукотиш буйича маъмурга тавсиялар ишлаб чикиш киради.

Фаол аудит тизими (мониторинга) ва умумий бошкариш уртасида узаро алокани ташкил этиш мухдм масалалардан хисобланади. Фаол аудит намунавий бошкариш функцияларини, яъни ахборот тизимдаги фаоллик хусусидаги маълумотларни тахлиллашни, жорий вазиятни акслантиришни, шубх,али фаолликка автоматик тарзда реакция курсатилишини бажаради. Тармокни бошкариш тизими худди шунга ухшаш ишлайди. Фаол аудит ва умумий бошкаришни умумий дастурий-техник ва ташкилий ечимлардан фойдаланиб интеграциялаш максадга мувофик, хисобланади. Бу интеграция-ланган тизимга яхлитликни назоратлаш, хамда ахборот тизими хатти-харакатларининг узига хос жихатларини кузатувчи бошка йуналишдаги агентлар хам киритилиши мумкин (13.6-расм).

Бошкаришнинг марказий консоли мавжуд булиб, унда фаол аудит (мониторинг) яхлитликни назоратлаш, бошка жих,атлар буйича тизим ва тармокларни назоратлаш тизимларидан маълумотлар тупланади. Бу консол-да жорий вазият акслантирилади, ундан автоматик тарзда ёки кулда бошк,ариш командалари берилади. Техник ёки ташкилий сабабларга кура бу консол бир неча ишчи жойи куринишида физик амалга оширилиши мумкин (хавфсизлик маъмурига жой ажратиш билан).



13.6-расм. Хавфсизлик сервислари ва бошкариш тизимининг интеграцияси.

Тармок, хавфсизлигини адаптив бошкариш моделидан фойдаланиш барча тахдидларни назоратлаш ва уларга уз вактида реакция курсатиш, нафак,ат тах,дидларни амалга оширишга шароит яратувчи заифликларни

йукртиш, балки заифликларни пайдо булиш шароитларини тахлиллаш имконини беради.

13.4. Хавф-хатарларни тахлиллаш ва бопщариш

Хавф-хатарларни тахлиллаш ва бошкариш ахборот тизимидаги тахдидлар, заифликлар ва хавф-хатарларни бахрлаш, хамда ушбу ахборот тизими хавфсизлигининг етарли даражасини таъминловчи карши чораларни аникдаш учуй ишлатилади.

Хавф-хатарларни тахлиллаш-тахдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига булиши мумкин булган зарарларни аникдаш жараёни. Хавф-хатарларни тахлиллашдан максад мавжуд хавф-хатарларни аникдаш ва улар меъёрини бахрлаш (уларга микдорий бахр бериш). Хавф-хатарларни тахлиллаш компьютер ахборот тизими хавфсизлигини текшириш буйича тадбирни уз ичига олади. Бу тадбирга биноан кайси ресурсларни кайси тахдидлардан химоялаш зарурлиги хамда у ёки бу ресурслар кандай даражада химояга мухтож эканлиги аникданади.

Хавф-хатарларни тахлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимига куйиладиган талаблар даражасига ва эътиборга олинувчи тахдидлар характерига (тахдидлар таъсири спектрига) боглик,. Талабларнинг иккита даражаси фаркланади:

- ахборот хавфсизлиги режимига минимал талаблар;
- ахборот хавфсизлиги режимига оширилган талаблар.

Ахборот хавфсизлиги режимига минимал талаблар *ахборот хавфсизлигининг базавий даражасига* мое келади. Бу даражадан, одатда, намунавий лойиха ечимларида фойдаланилади. Хавф-хатарларни тахлиллаш соддалаштирилган схема буйича утказилади: хавфеизликка тахдидлар нинг куп тарк,алган туплами уларнинг эх,тимоллигини бах,оламасдан курилади. Вируслар, асбоб-ускуналарнинг бузилиши, рухсатсиз фойдаланиш ва х,. каби эх,тимоллиги юкрри тахдидларнинг минимал туплами куриладиган катор стандартлар ва спецификациялар мавжуд. Бундай тахдидларни бетарафлаштириш учун уларнинг амалга оширилиши эх,тимоллиги ва, ресуреларнинг заифлигидан к,атъий назар, к,арши чоралар курилиши лозим, яъни базавий даражада тахдидлар характеристикаларини куриш шарт эмас.

Ахборот хавфсизлиги режимига оширилган талаблар, ахборот хавфсизлиги режимининг бузилиши огир окибатларга сабаб булганида ва ахборот хавфсизлиги режимига минимал талаблар етарли булмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учуй ресурслар ахамиятини аниклаш, тадкикланувчи ахборот тизими учуй долзарб булган тахдидлар руйхати билан стандарт тупламни тулдириш, тахдидлар эхтимоллигини бахрлаш ва ресурслар заифлигини аниклаш зарур-

Хавф-хатарни тахлиллаш жараёнини куйидаги боскичларга ажратиш мумкин:

- корпоратив ахборот тизимининг таянч ресурсларини идентификациялаш;
- у ёки бу ресурснинг мухимлигини аниклаш;
- тахдидларнинг амалга оширилишига имкон берувчи мавжуд хавфсизлик тахдидларни ва заифликларни идентификациялаш;
- хавфсизликка тахдидларни амалга оширилиши билан боглик, хавф-хатарларни хисоблаш.

Ресурслар учта категорияга - ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, куприкдар, маршрутизаторлар ва х,.) булинади. Хар бир категория ичида ресурсларни синфларга ва к,исм синфларга ажратиш мумкин. Факат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуктаи назаридан мухим булган ресурлар идентификацияланиши лозим.

Ресурснинг мухимлиги (нарх,и) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар микдори билан белгиланади. Ресурслар нархини бахрлашда ресурсларининг хар бир категорияси учун булиши мумкин булган зарар микдори белгиланади.

Намунавий хавфсизлик тахдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий офат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб булувчи

корпоратив ахборот тизим ишидаги бузилишлар тааллукли. Тахдид даражаси деганда унинг амалга оширилиши эхтимоллиги тушунилади.

Химоянинг бушлиги корпоратив ахборот тизимидаги заифликларга сабаб булади. Заифликларни бахрлаш хавфсизлик тахдидларининг муваффак,иятли амалга оширилиш эхтимоллигини аникдашни назарда тутади. Шундай килиб, зарар етказиш эхтимоллиги тахдидларнинг амалга оширилиши эхтимоллиги ва заифлик микдори оркали аникданади.

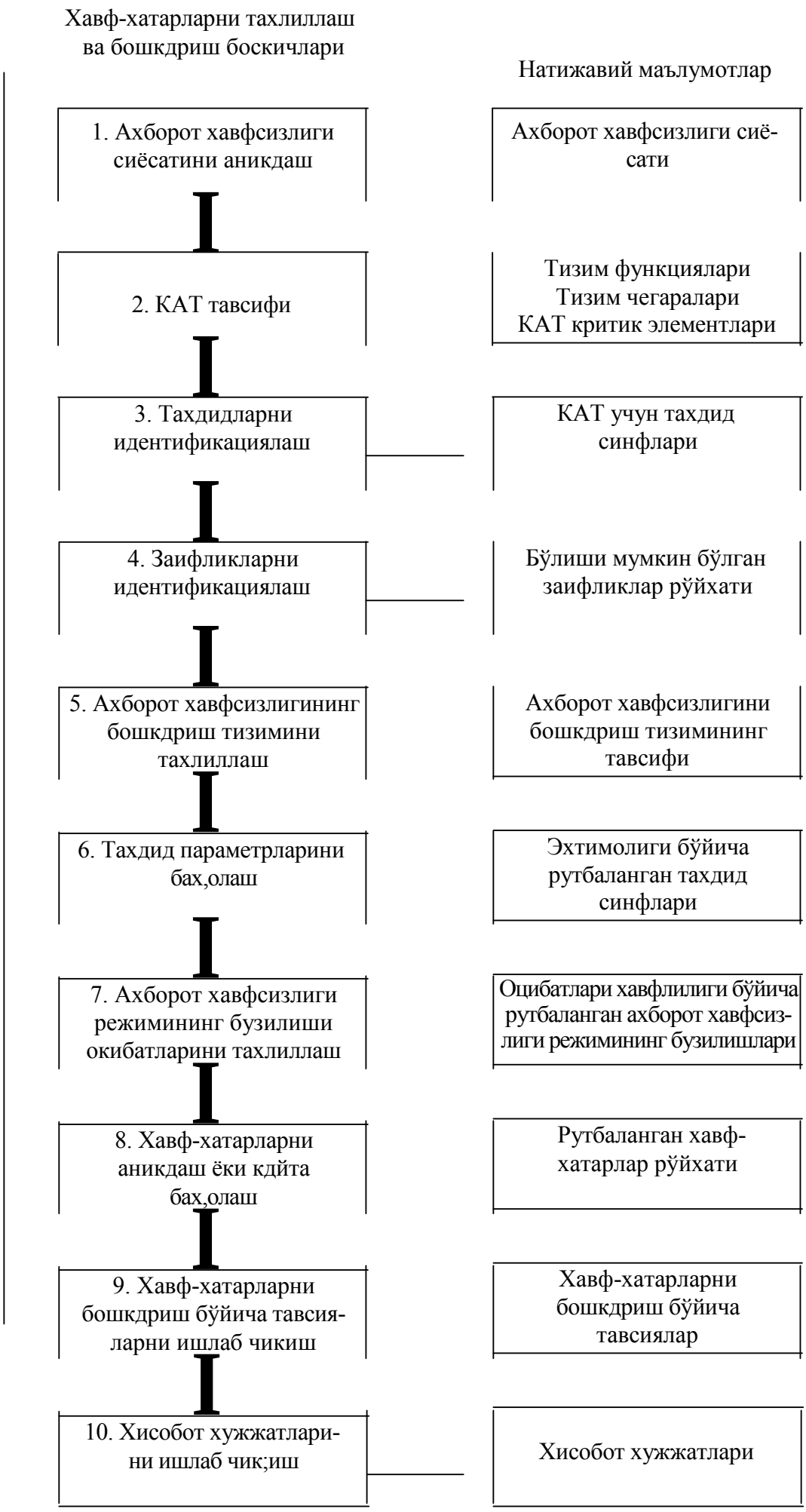
Хавф-хатар даражаси ресурс нархи, тахдид даражаси ва заифлик микдори асосида аникданади. Ресурс нархи, тахдид даражаси ва заифлик микдори ошиши билан хавф-хатар даражаси хам ошади. Хавф-хатарлар даражасини бахрлаш асосида хавфсизлик талаблари белгиланади.

Хавф-хатарларни бошкариш масаласи, хавф-хатар даражасини макбул микдоргача камайтиришга имкон берувчи карши чораларни асосли танлашни ва амалга ошириш нархини бахрлашни уз ичига олади. Табиийки, карши чораларни амалга ошириш нархи булиши мумкин булган зарар микдоридан кам булиши керак.

13.7-расмда хавф-хатарларни бошкариш технологиясининг боскичлари келтирилган.

Ахборот хавфсизлиги сиёсатини аницлаш. Бу боскичда ахборот хавфсизлиги сох,асидаги кулланма-хужжатлар, стандартлар, ахборот хавфсизлигининг асосий кридалари, хавф-хатарларни бошк,аришга ёндашишлар аникданади хамда к,арши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

Корпоратив ахборот тизимини (КАТ) тавсифлаш. Ушбу боскичда ахборот хавфсизлиги сохасидаги х,алкаро, давлат ва корпоратив стандартларга биноан корпоратив ахборот тизимнинг функционал вазифалари тавсифланади. Компаниянинг критик ахборот ресурслари, жараёнлари ва сервислари тавсифланади; корпоратив ахборот тизимининг чегаралари хамда бошкариш ва маълумотлар буйича энг мухим компонентларининг таркиби ва богланишлари аникданади.



13.7-расм. Хавф-хатарларни бошцариш технологиясининг варианти.

Тахдидларни идентификациялаш. Ушбу боскичда тахдидлар руйхати тузилади ва уларнинг даражаси бах,оланади. Бунда турли ташкилотларнинг тахдидлар синфлари руйхатидан хдм берилган тахдидни амалга ошириш эх,тимоллигининг рейтинги ёки уртача кийматидан фойдаланиш мумкин.

Заифликларни идентификациялаш. Ушбу боскичда берилган корпоратив ахборот тизимининг заифликлари руйхати, уларнинг амалга оширилишидаги жоиз натижалар курсатилган х,олда тузилади. Мавжуд корпоратив ахборот тизими учун руйхатлар катор манбалардан фойдаланилиб тузилади. Бу манбаларга заифликларни тармок, сканерлари, турли ташкилотларнинг заифликлар каталоги, хавф-хатарларни тахлилловчи ихтисослаштирилган усуллар киради.

Корпоратив ахборот тизимининг бошкариш тизимини тахлиллаш. Ушбу боскичда бошкариш, тизими, аникланган тахдидларга ва заифликларга жоиз булган таъсир нуктаи назаридан тахлилланади.

Тахдидлар параметрларини бахолаш. Ушбу боскичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти бах,оланади. Бах,олашнинг намунавий шкаласи - бир неча рутбали (масалан, паст, урта, ва юкрри сатх,) сифатий (балли) шкаладир. Бундай бах,о эксперт томонидан мавжуд объектив факторларни хдсобга олган х,олда берилади.

Ахборот хавфсизлиги режимининг бузилиши окибатларини тахлиллаш. Ушбу боскичда ахборот хавфсизлиги режимининг бузилиши бах,оси аникланади. Бузилиш окибатлари молиявий йук,отишларга, обрусизланишга, расмий тузилмалар томонидан кунгилсизликларга ва х,. сабаб булиши мумкин. Бузилиш окибатларини бах,олаш учун мезонлар тизими танланади ва ок,ибатлар огирлигини бах,олаш учун интеграцияланган шкала белгиланади.

Хавф-хатарларни бахолаш. Ушбу боскичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси бах,оланади. Хавф-хатар даражаси киймати тахдидлар, заифликлар даражасига ва булиши мумкин булган окибатлар огирлигига боглик,. Хавф-хатарларни бах,олашда сифатий ва микдорий усуллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг булиши мумкин булган хавф-хатарлар хавфлилиги даражаси буйича рутбаланиши лозим. Микдорий усул ишлатилганда хавф-хатарлар микдорий шкалаларда бах,оланиши мумкин. Бу тавсия

этилаётган карши чораларнинг нархи/самарадорлигини тахлиллашни осонлаштиради. Аммо бу хрлда дастлабки маълумотларни улчаш шкалаларига ва ишлатилаётган моделнинг адекватлигига жуда юкрри талаблар куйилади. Оддий хрлда хавф-хатарни бахрлашда иккита омил-ходиса эхтимоллиги ва булиши мумкин булган окибатлар огирлиги ишлатилиши мумкин.

Хавф-хатарларни бошцариш буйича тавсияларни ишлаб чщиш. Ушбу боскичда турли сатхдар (ташкилий, дастурий-техник) ва хавфсизликнинг алохида жихатлари буйича структуризацияланган карши чораларнинг комплекси тавсия этилиши лозим. Таклиф этилувчи карши чоралар комплекси хавф-хатарларни бошкаришнинг танланган стратегиясига биноан курилади.

Хисобот хужжатларни ишлаб чщиш. Ушбу боскичда хавф-хатарларни тахлиллаш ва бошкаришнинг барча боскичлари буйича иш натижалари акслантирилган хисобот хужжатлари тайёрланади.

Таъкидлаш лозимки, хрзирда ахборот хавф-хатарларини бахрлашни автоматлаштириш максадида дастурий махсулотлар ишлаб чикилган.

13.5. Ахборот хавфсизлиги тизимини куриш методологияси

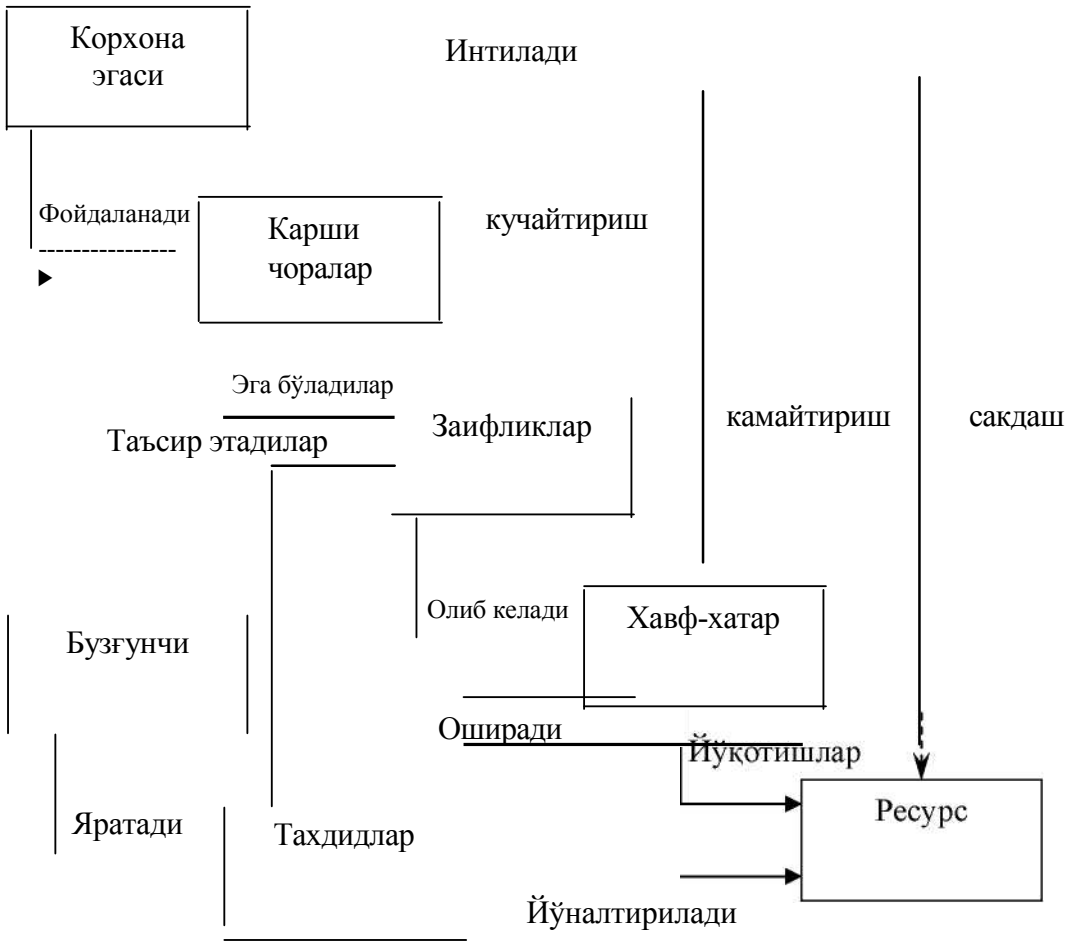
Ахборот хавфсизлиги моделини куриш. Корхонадаги ахборот хавфсизлиги буйича тадбирлар крнун чик,ариш, ташкилий ва дастурий-техник характерга эга булган катор жихатларни к,амраб олади. Уларнинг хар бирида корхона ахборот хавфсизлигини таъминлаш учун бажарилиши зарур булган катор масалалар таърифланади. Масалаларни х,ал этишда ахборот хавфсизлиги сох,асидаги халкаро стандартларга асосланган корхона ахборот хавфсизлигининг концептуал моделидан фойдаланиш мумкин.

Куйидаги халк,аро стандартлар корпоратив ахборот тизими химояланишини бах,олаш мезонини ва химоялаш механизмларига к,уйиладиган талабларни аникдовчи энг мухим меъёрий хужжатлар х,исобланади:

- ахборот технологиялари хавфсизлигини бах,олашнинг умумий мезонлари КОЯЕС 15408 (The Common Criteria For Information Technology Security Evalution);

- ахборот хавфсизлигини бошкаришнинг амалий кридалари IS O ЛЕС 17799 (Code of practice for Information Security Management).

Ушбу халкаро стандартларга тула мое равишда тузилган корхона ахборот хавфсизлигининг концептуал модели 13.8-расмда келтирилган.



13.8-расм. Корхона ахборот хавфсизлиги тизимининг концептуаль модели.

Корхона ахборот хавфсизлигининг концептуал моделида куйидаги омиллар хисобга олинган:

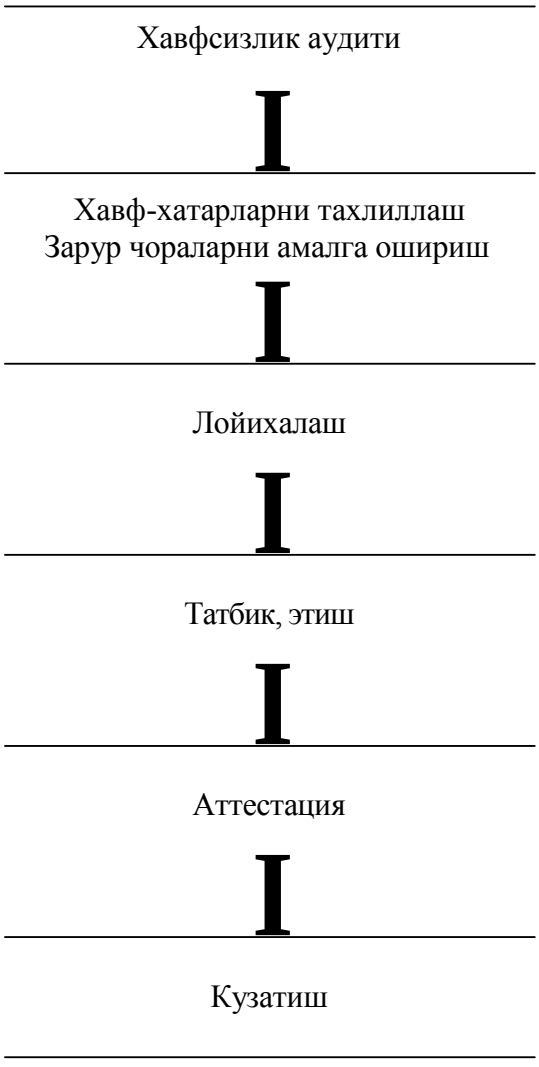
- пайдо булиш эхтимоллиги ва амалга оширилиш эхтимолиги билан характерланувчи ахборот хавфсизлиги *тщдидлари;*

- тахдидларнинг амалга оширилиши эхтимоллигига таъсир этувчи ах борот тизими ёки карши чора тизими (ахборот хавфсизлиги тизими) *заифликлари;*

- ахборот хавфсизлигига тахдидлар амалга оширилиши натижасида корхонага етказилувчи зарарни акслантирувчи *омил-хавф-хатар.*

Бу моделнинг харакатдаги субъектлари - Бузгунчи (тахдидлар манбаини ифодаловчи) ва Эга (корхона маъмури) объект-Ресурсга карама-карши максадларда таъсир киладилар. Ресурс-корхонанинг моддий ва ахборот ресурсларини ва ахборот хавфсизлиги хрлатини ифодалайди.

Ахборот хавфсизлиги тизимини куриш босцичлари. Ахборот хавфсизлиги тизимини куриш боскичларнинг куйидаги стандартлаштирилган кетма-кетлигида амалга оширилади: хавфсизлик аудити; хавф-хатарларни тахлиллаш, тизимни лойих,алаш, жорий этиш, аттестациялаш ва кузатиш (13.9-расм).



13.9-расм. Ахборот хавфсизлиги тизимини цуриш босцичлари Хавфсизлик аудити. Хрзирда "хавфсизлик аудити" тушунчаси етарлича кенг талкин этилади. Аудитнинг к,уйидаги куринишлари фаркданади.

- ахборот хавфсизлигини тестли бузиш;

- экспресс-текшириш;
- тизимни аттестациялаш;
- лойихдгача текшириш.

Ахборот хавфсизлиги тестли бузиш корпоратив ахборот тизимининг химояланиш даражасини аниклаш нуктаи назаридан самарали хисобланмайди. "Бузувчи"нинг асосий максади бир икки заифликларни топиб, уларни тизимдан фойдаланишда ишлатиш. Агар "тестли бузиш" муваффакиятли чикса, ушбу муайян " бузиш "нинг мумкин булган сценарийси ривожини олдини олиб, заифликларни кидиришда давом этиш керак. "Тестли бузиш"нинг муваффакиятсизлигини баббаравар тестланувчи тизимнинг химояланганлиги ва тестларнинг етишмаслиги каби талкин килиш мумкин.

Эксперсс-текшириш доирасида, одатда, куп вакт сарфини талаб этмайдиган, стандартизацияланган текширишлар асосида корпоратив ахборот тизими хавфсизлик воситаларининг умумий хрлати бахрланади. Экспресс-текшириш одатда ахборот ресурсларининг минимал химояланиш даражасини таъминловчи устивор йуналишларни аниклаш зарурияти тугилганда утказилади.

Тизимни аттестациялаш тизимнинг ахборот ресурсларининг химояланиш талабларига мослигини текшириш максадида амалга оширилида. Бунда хам ташкилий, хам техник жихатдан талаблар туплами расмий текширилади, хавфсизлик воситаларининг амалга оширилишининг туликлиги ва етарлилиги курилади.

Лойих,агача текшириш аудитнинг энг куп мехнат талаб к,иладиган варианти хисобланади. Бундай аудит ахборот ресурслари иловаларида корхона ташкилий тузилмасини ва ходимларнинг у ёки бу иловалардан фойдаланиш к,оидаларини тахлил этишни кузда тутади. Сунгра иловаларнинг узи тахлилланади. Ундан кейин бир сатхдан иккинчи сатх,нинг фойдаланишдаги муайян хизматлар хамда ахборот алмашишга зарур булган хизматлар тахлилланиши л озим. Сунгра хавфсизликнинг урнатилган воситаларини тахлиллаш билан тасаввур тулдирилади.

Хавф-хатарларни тахлиллаш 13.4-булимда батафсил курилган. Ахборот хавфсизлиги бузилганда лойихагача текшириш, хавф-хатарларни тахлиллаш билан биргаликда ахборот тизимидаги мавжуд хавф-хатарларни рутбалашга ва адэкват чораларни ишлаб чикишга имкон беради.

Тизимни лойихалаш. Ххшояни ташкил этиш стратегияси нуктаи назаридан ресурсли ва сервисли ёндашиш фаркланади. Ресурсли ёндашишда тизим ресурслар туплами сифатида курилади ва ахборот хавфсизлиги тизимининг компонентлари бу ресурсларга богланади. Ресурсли ёндашиш амалга оширилганида ахборотни химоялаш масаласи хизматлар тузилмасига кушимча чеклашларсиз ечилади. Бу эса бир жинсли булмаган тизим шароитида мумкин эмас. Сервисли ёндашишда тизим фойдаланувчиларга такдим этилувчи хизматлар туплами каби талкин к,илинади. Хрзирги вактда сервисли ёндашиш афзалрок, хисобланади, чунки у тизимда амалга оширилган хизматларга богланади ва "ортикча" хизматларни рад этиш хисобига к,атор тахдидларни истисно килинишига имкон беради. Бу эса тизимни янада мантикан асосланган тизимга айлантиради. Айнан сервис ёндашиш хавфсизликнинг замонавий стандартлари, хусусан ISO/IEC 15408 асосида ётади.

Ахборот хавфсизлиги тизимни куришнинг иккита асосий сценарийси мавжуд: махсулотли ва лойих,али. Мах,сулотли сценарий (ёндашиш) доирасида аввал химоя воситалари туплами танланади, уларнинг функциялари тахлилланади, сунгра функциялар тахлили асосида ахборот ресурсларидан фойдаланиш сиёсати белгиланади.

Лойихага харажатлар нук,таи назаридан махсулотли сценарий энг арзон хисобланади. Ундан ташк,ари, ечимларнинг танк,ислиги шароитида купинча мах,сулотли ёндашиш ягона хисобланади (масалан, криптографик х,имояда фак,ат шу ёндашиш кулланилади).

Лойих,али сценарийда аввал хавфсизлик сиёсати ишлаб чикилади, унинг асосида хавфсизлик сиёсатини амалга оширишда зарур булган функциялар аникланади, сунгра бу функциялар бажарилишини таъминловчи химоя воситалари танланади.

Лойих,али сценарий асосида курилган тизимлар яхширок, оптимизацияланган ва аттестациянинг юкрри натижаларини беради. Ушбу ёндашиш махсулотли ёндашишдан фаркли равишда бошидан у ёки бу платформа билан богаанмаганлиги туфайли, катта гетероген тизимларни куришда афзал хисобланади. Ундан ташкари, узок, муддатга мулжалланган ечимларни таъминлайди, чунки хавфсизлик сиёсатини узгартирмасдан ечимларни ва химоя воситаларини алмаштиришга имкон беради.

Ахборот хавфсизлиги тизими архитектурасини танлаш нуктаи назаридан объектли, татбикий ёки аралаш ёндашишдан фойдаланилади. Объектли ёндашиш ахборот хавфсизлигини у ёки бу объект (булинма, филиал, ташкилот) тузилмаси асосида яратади. Объектли ёндашишнинг кулланиши ташкилий чораларнинг бир жинсли тупламини мададловчи хавфсизлик механизмлари учун универсал ечимлар тупламидан фойдаланишни кузда тутади. Бундай ёндашишга мисол тарикасида ташки ахборот алмашиш, локал тармок,, телекоммуникация тизимларининг ва х,. химояланган инфратузилмаларини к,уришни курсатиш мумкин. Объектли ёндашишнинг камчилиги унинг универсал механизмларининг, айник,са, узаро мураккаб богланишли катта сонли иловаларга эга булган ташкилотлар учун тугал эмаслиги.

Татбик,ий ёндашиш хавфсизлик механизмини муайян иловага боглаб яратади. Татбик,ий ёндашишга мисол тарикасида автоматлаштиришнинг алох,ида масаласи (бухгалтерия, кадрлар ва х,.) учун к,исм тизимларнинг х,имоясини курсатиш мумкин. Ушбу ёндашишнинг камчилиги - маъмурлаш ва ишлатиш харажатларини минималлаштириш максадида хавфсизликнинг турли воситаларини уйгунлаштириш зарурияти.

Аралаш ёндашиш юкррида тавсифланган иккита ёндашишни комбинациялашни кузда тутади. Бундай ёндашиш лойих,алаш боск,ичида купрок, мех,нат талаб к,илсада, ахборот хавфсизлиги тизимини жорий этиш ва ишлатиш нархи буйича афзалликларни бериши мумкин.

Жорий этиш. Жорий этиш боскичи куйидаги кетма-кет утказилувчи тадбирларни уз ичига олади:

- химоя воситаларини урнатиш ва конфигурациялаш;
- ходимларни химоя воситалари билан ишлашга ургатиш;

- дастлабки синовии утказиш;

- тажрибавий ишлатишга топшириш.

Тажрибавий ишлатиш, ахборот хавфсизлиги тизимини ишчи режимига туширишдан аввал, унинг ишлашидаги мумкин булган камчиликларни аниклашга ва йукртишга имкон беради. Агар тажрибавий ишлатиш жараёнида компонентларнинг тугри ишламаслиги фактлари аникланса, химоя воситалари созланишига ва уларнинг ишлаш режимларига ва х,. тузатишлар киритилади.

Тизимни апипестациялаш. Ахборот хавфсизлиги тизимини ваколатли идора томонидан аттестациялаш унинг функционал туликлигини ва корпоратив ахборот тизими химоясининг талаб килинган даражаси таъминланганлигини тасдикдашга имкон беради. Тизимнинг аттестацияси хавфсизлик аудитининг бир куриниши хисобланади ва ишлатилувчи чоралар комплекси ва химоя воситаларининг хавфсизлик даражаси талабларига мослигини бахрлаш максадида химояланувчи корхонани ишлатишнинг реал шароитларида комплекс текширишни кузда тутади.

Аттестация натижасида хисобот хужжати тайёрланади ва мослик аттестати берилади. Бу аттестат конфиденциал ахборот билан аттестатда курсатилган вакт мобайнида ишлаш хукукини беради.

Кузатиш. Ахборот хавфсизлиги тизимининг ишга лаёкатлигини ва уз вазифаларини текис бажарилишини мададлаш учун хавфсизлик тизимининг дастурий ва аппарат таъминотини техник мададлаш ва кузатиш буйича тадбирлар комплекси кузда тутилиши лозим. Ахборот хавфсизлиги тизимини техник мададлаш ва кузатиш хизматчи ходимларнинг билими ва куникмаларини талаб этади ва химояланувчи тизим эгаси - ташкилот штатидаги ахборот хавфсизлигига жавоб берувчи ходимлар томонидан ёки ихтисослаштирилган ташкилот ходимлари томонидан амалга оширилиши мумкин.

Курилган методология к,оидаларидан фойдаланиш корпоратив ахборот тизимининг умумий ривожи билан бирга ривожлантирилиши ва модификацияланиши мумкин булган ахборот хавфсизлигининг самарали ва ишончли тизимини к,уришга имкон беради.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. С.С.Крсимов. Ахборот технологиялари. Укув кулланма. - Тошкент. "Алокдчи", 2006.
2. С.К.Ганиев, М.М. Каримов. Хисоблаш системалари ва тармокларида информация химояси. Олий укув юрт.талаб. учуй укув кулланма.- Тошкент Давлат техника университети, 2003.
3. В.И. Завгородний. Комплексная защита информации в компьютерных системах: Учебное пособие.-М: Логос; ПБОЮЛ Н.А.Егоров, 2001.
4. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия "Безопасность".- М.:СИНТЕГ, 2000.
5. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров.-Москва. 2004.
6. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.
7. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент.-2003.-№1,2.
8. А.В. Беляев. Методы и средства защиты информации // http://www.citforum.ru/internet/inf secure/its2000_01.shtml.
9. Вэк Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент.-2000.-№4-5.
10. А. Галатенко. Активный ayflHr//JetInfo.-1999.-№8.
11. А.В. Лукацкий. Адаптивная безопасность сети// Компьютер-Пресс. - 1999.-№8.
12. А.В. Лукацкий. Обнаружение атак. - СПб.: БХВ-Петербург, 2001.
13. Р.Норман. Выбираем протокол VPN//Windows2000Magazine.- 2001.№7.
14. В.Г. Олифер. Защита информации при работе в Интернет// Connect.- 2002. -№11.

15. Н.А. Олифер. Дифференцированная защита трафика средствами IP-Sec //LAN.-2001.-№04; http://www.osp.ru/lan/2001/04/024.htm.
16. Н.А. Олифер. Протоколы IPSec. //LAN.-2001.-№03; http://www.osp.ru/lan/2001/03/024.htm.
17. С.А. Петренко. Построение эффективной системы антивирусной за щиты // Конфидент.-2002.-№3.
18. С.А. Петренко. Централизованное управление антивирусной защитой корпоративных сетей Interne^ntranet // Конфидент.-2001.-№2.
19. А.А. Петров. Компьютерная безопасность. Криптографические мето ды защиты. -М.: ДМК Пресс, 2000.
20. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Уч.пособие для ВУЗов/ Авт.: П.Ю. Белкин и др. -М.:Радио и связь, 1999.
21. Н. Прокофьев. Антивирусная защита сети // Компьютер - Пресс.-2001. -№12.
22. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. - М.: Ра дио и связь, 2001.
23. СВ. Симонов. Анализ рисков в информационных системах. Практи ческие советы // Конфидент. -2001. -№2.
24. А.В. Соколов, В.Ф. Шаньгин. Защита информации в распределенных корпоративных сетях и системах. -М.: ДМК Пресс, 2002.
25. Типовые решения по применению средств VPN для защиты инфор мационных ресурсов / ООО "Конфидент". -СПб., 2001.
26. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов / ООО "Конфидент". -СПб., 2001.
27. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия/ ООО "Конфидент". -СПб., 2002.

28. "Ахборот технологияси. Ахборотларни криптографик мухофазаси. Маълумотларни шифрлаш алгоритми" Узбекистон Давлат стандарти. O'zDSt 1105:2006.
29. www.nasa.gov\statistics\
30. www.security.uz
31. www.cert.uz
32. www.uzinfocom.uz

Бошлангич ^арфлари билан уциладиган суз бирикмалари (дисцартирилган сузлар)

АСК	Acknowledgement - Тасдикдаш.
AES	Advanced Encryption Standard - Американинг янги шифрлаш стандарти.
АН	Authentication Header - Аутентификацияловчи сарлавха.
ANS	Adaptive Network Security - Хавфсизликни адаптив бошкдриш модели
ANSI	American National Standard Institute - АКД1нинг миллий стандартлаштириш институти.
AS	Authentication Server - Аутентифкациялаш сервери
ASA	Adaptive Security Algorithm - Хавфсизликнинг адаптив алгоритми
ASP	Applications Service Providing - Серверда исътемолчидан масофада жойлашган иловаларга Internet ёки хусусий тармок, оркали хизмат курсатиш.
B2B	Business to Business - «бизнес-бизнес» схемаси
B2C	Business to Consumer - «бизнес - истеъмолчи» схемаси
CA	Certification Authorities - Сертификациялаш маркази.
СЕК	Content Encryption Key - Маълумотларни шифрлаш калити.
CHAP	Challenge Handshake Authentication Protocol - «Кул узатиш» муолажаси асосида аутентифкациялаш протоколи
DDoS	Distributed Denial of Service - хизмат курсатишдан бош тортишга ундайдиган таксимланган хужум
DHCP	Dynamic Host Configuration Protocol - Хостларни динамик конфигурациялаш протоколи.
DNS	Domain Name Server - Доменли исмлар хизмати
e business	electronic business - Электрон бизнес. **e**
commerce	electronic commerce - Электрон тижорат.
ECP	Encryption Control Protocol - Шифрлашни бошкариш протоколи.
ESP	Encapsulated Security Payload - Киритилган узатиладиган химоялаган маълумотлар.
FTP	File Transfer Protocol - Файлларни узатиш протоколи.
GSM	Global System for Mobile Communications - Мобиль алоканинг глобал тизими.
GSP	Global Security Policy - VPN учун глобал хавфсизлик сиёсати.
HDLC	High level Data Link Control - Юкрри сатхдаги маълумотларни узатиш каналини бошкариш
HMAC	Hashing for Message Authentication - Калитларни хешлаш оркали хабарларни аутентифкациялаш.

HTML HyperText Markup Language - Web-сахифаларни гиперматнли белгиловчи тил

HTTP HyperText Transfer Protocol - Гиперматнли файлларни узатиш протоколи.

ICMP Internet Control Message Protocol - Internet тармощца хабарларни бошкдриш протоколи.

IETF Internet Engineering Task Force - InternetHH лойих.алаш муаммолари гурухи

IKE Internet Key Exchange - Internets калитларни алмашиш протоколи.

IP Internet Protocol - Тармоклараро маълумотларни алмашинишнинг Internet протоколи

IPSec Internet Security Protocol - Тармоклараро маълумотларни хавфсиз алмашиниш Internet протоколи

IRC Internet Relay Chat - Internet да чат-анжуманларни ташкил этиш хизмати

ISO International Standards Organization - Халкаро стандартлаштириш ташкил оти.

ISP Internet Service Provider - Internet хизматларини таъминотчиси

KDC Key Distrubution Center - калитларни таксимлаш маркази.

KEK Key Encryption Key - Калитларни шифрлаш учун калит

KS Kerberos Server - Kerberos тизими сервери.

L2F Layer2 Forwarding - Иккинчи (канал) сатхда маълумотларни узатиш протоколи.

L2TP Layer2 Tunneling Protocol - Канал сатхида маълумотларни туннеллаш протоколи.

LAC L2TP Access Concentrator - L2TP рухсатлар концентратори

LAN Local Access Network - мах.аллий тармок,.

LCP Link Control Protocol - Уланишларни бошкариш протоколи.

LDAP Lightweight Directory Access Protocol - Каталоглардан фойдаланишларни соддалаштирилган протоколи.

LNS L2TP Network Server - L2TP тармок, сервери.

LSP Local Security Policy - Max.аллий хавфсизлик сиёсати (мижоз учун)

MAC Message Authentication Code - Хабарларни аутентификациялаш коди.

MD Message Digest - Хабарлар дайджести

NAT Network Address Translation - Тармок, адресларини трансляциялаш.

NCP Network Control Protocol - Тармокни бошкариш протоколи.

NIST National Institute of Standards and Technology - АКШнинг стандартлар ва технологиялари миллий институти.

NNTP Network News Transfer Protocol - Тармок, янгиликларини узатиш протоколи

OSI	Open Systems Interconnection - Очик, тизимлар узаро богликлиги
OTK	One Time Key - Бир маротабалик калит.
P2P	Peer to Peer или Partner to Partner - Бизнес муносабатининг «тенг-тенг» схемаси.
PAP	Password Authentication Protocol - Парол буйича аутентифкациялаш протоколи.
PIN	Personal Identification Number - шахсий идентификация коди
PKD	Public Key Directory - Очик, калитлар каталоги.
PKI	Public Key Infrastructure - Очик, калитларни бошкариш инфратузилмаси.
PPP	Point to point Protocol - Икки нуктали богланиш протоколи.
PPTP	Point to Point Tunneling Protocol - Икки нуктали богланиш учун туннел-лаш протоколи.
POP	Post Office Protocol - фойдаланувчи узига келган электрон хабарлардан фойдаланишига имкон берувчи протокол
RADIUS	Remote Authentication Dial In User Service - Фойдаланувчиларни богланадиган линиялар буйича масофадан аутентифкациялаш тизими
RAS	Remote Access Service - Масофадан фойдаланаш хизмати
RFC	Request For Comments - Изохдарни сурови.
RMON	Remote MONitoring - Тармок, ускуналарини масофадан мониторинглаш-нинг стандарт спецификацияси.
RSA	Rivest, Shamir, Adleman - Райвест, Шамир, Адлеман. Асимметрик криптоалгоритм.
SHA	Secure Hash Algorithm - Х,имояланган хешлаш алгоритми
SKIP	Simple Key management for Internet Protocols - Internet протоколи учун калитларни оддий бошкариш.
SMTP	Simple Mail Transfer Protocol - Электрон почтанинг оддий протоколи
SNMP	Simple Network Management Protocol - Тармокни бошкаришнинг оддий про-токоли.
SPD	Security Policy Database - Хавфсизлик кридаларининг маълумотлар база-си.
TACACS	Terminal Access Controller Access Control System - Масофадан фойдала-нишни марказлаштирилган назоратлаш протоколи.
TCP	Transport Control Protocol - Узатишларни бошкариш протоколи.
TELNET	Виртуал терминал протоколи - масофадаги компьютерда дастурни бажа-ришга мулжалланган протокол
TFN	Trible Flood Net - DdoS хужумлар учун инструментал воситалардан бири
TGS	Ticket Granting Server - Мандатларни таркатиш сервери

TLS	Transport Layer Security - Транспорт сатхининг химояси.
UDP	User Data Protocol - Фойдаланувчининг маълумотларини узатиш про токол и.
VPN	Virtual Private Network - химояланган виртуал тармок,.
WAN	Wide Area Network - Глобал тармок,.
WWW	World Wide Web - InternetHHHr гиперматнли ахборотлар хизмати
XML	Extended Mark-up Language - белгилашнинг кенгайтирилган тили
МББТ	Маълумотлар базасини бошкдриш тизими