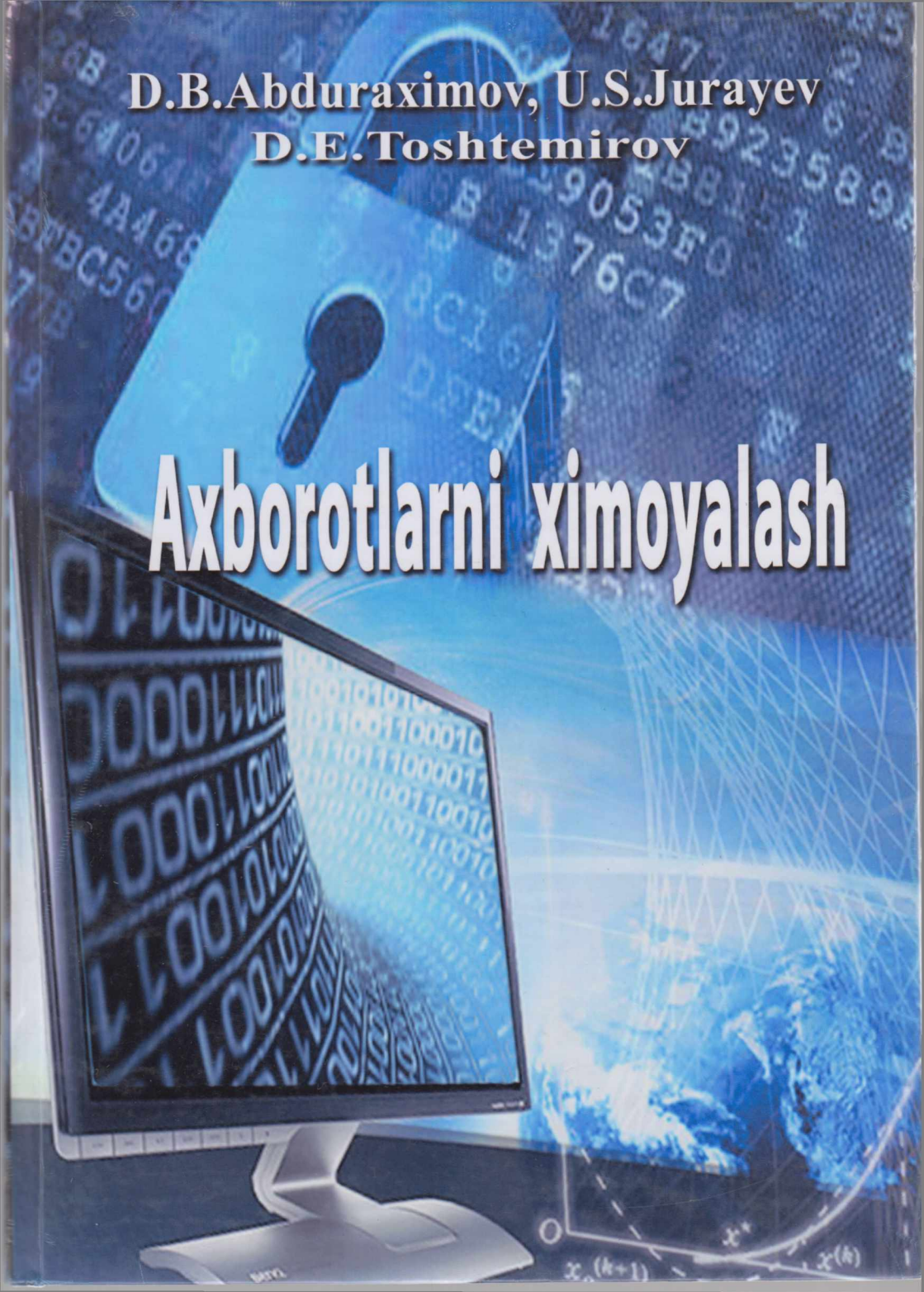
D.B.Abduraximov, U.S.Jurayev
D.E.Toshtemirov

Axborotlarni ximoyalash



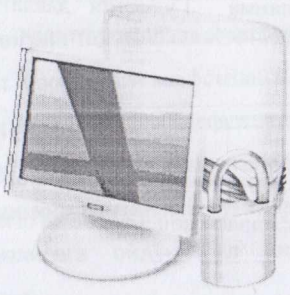
ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА
МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ГУЛИСТОН ДАВЛАТ УНИВЕРСИТЕТИ

Д.Б.Абдурахимов, У.С.Жўраев, Д.Э.Тоштемиров

АХБОРОТЛАРНИ ҲИМОЯЛАШ

Услубий қўлланма



ГУЛИСТОН – 2016

Д.Б.Абдураҳимов, У.С.Жўраев, Д.Э.Тоштемиров, Ахборотларни ҳимоялаш, услубий қўлланма 2016 й. 190 бет.

Услубий қўлланма Гулистон давлат университетида «Ахборотларни ҳимоялаш» (танлов фани) курси бўйича амалдаги ўқув дастурлари асосида яратилди. Услубий қўлланмада ахборот хавфсизлигининг асосий ташкил этувчилари, тушунчалари, ахборотга бўладиган таҳдидлар, ахборот хавфсизлигини таъминлашга оид ҳуқуқий-меъёрий ҳужжатлар, стандартлар, дастурий-техник воситалар, компьютер тармоқларида хавфсизликни таъминлаш масалалари ёритилган.

Услубий қўлланма 5110700 - Информатика ўқитиш методикаси йўналишидаги бакалавриат таълим босқичи талабалари ва шахсий компьютер фойдаланувчилари учун мўлжалланган.

Услубий қўлланма Гулистон давлат университети ўқув-методик Кенгаши томонидан (2016 йил 29 августдаги, № 1–сонли баённома) нашрга тавсия этилган.

Масъул мухаррир: С.Кулмаматов ГулДУ «Ахборот технологиялари» кафедраси доценти, педагогика фанлари номзоди.

Тақризчилар: Б.Ш.Раджабов, Ўзбекистон давлат санъат ва маданият институти, «Информатика ва табиий фанлар» кафедраси мудири, тех.ф.д, профессор.

С.П.Аллаёров, ГулДУ «Ахборот технологиялари» кафедраси доценти, техника фанлари номзоди, доцент.

МУНДАРИЖА

КИРИШ

XXI аср кишилик жамиятининг тараққиёти инсон фаолиятининг турли жабҳаларида бевосита ахборот ишлаб чиқариш, уни истеъмол қилиш ва жамлаш суръатларининг ўсиши билан бевосита боғлиқ. Сабаби, ахборот кишилик жамиятнининг муҳим ресурслари ҳисобланади. Ижтимоий тараққиётда ахборот стратегик муҳим аҳамиятга эга бўлган ҳом-ашё ва энергия билан тенглаштирилмоқда. Маълумки, дунё миқёсида миллий маҳсулотнинг 70% и ахборот тизимларида сақланаётган ахборот кўлами билан боғликдир. Кейинги ўн йил ичида биз ахборот технологияларининг шиддат билан ривожланиб, ҳаётнинг барча жабҳаларига, айникса, ишлаб чиқаришнинг турли соҳаларига жорий этилишининг гувоҳи бўлдик.

Ривожланган давлатларда кўпчилик фаолият кўрсатаётган ходимлар ишлаб чиқариш соҳасида эмас, балки у ёки бу даражада ахборотни қайта ишлаш билан банддирлар. Бугунги кунда ҳар бир ходим, мутахассис, талаба ўз фаолиятини ахборот технологияларисиз тасаввур қила олмайди. Улар ўзларининг қимматли вақтларини компьютер олдида ўтказиб, машаққатли меҳнат эвазига яратилган бебаҳо ахборотларини сақлашни «ақлли машиналарга» ишониб, уларнинг йўқ қилиниши, бузилиши ёки ўғирланиши ҳақида ўйламай, таваккалчиликка йўл қўядилар. Бундай қимматли ахборотларни сақлаш, уларнинг хавфсизлигини таъминлаш учун қоидалар, тамойиллар, воситалар, усулларни билиш ва усталик билан жорий этиш зарур бўлади. Нафақат қимматли ахборотлар хавфсизлигини таъминлаш, балки ахборот тизимлари ва уларнинг инфраструктураси хавфсизлигини таъминлаш ҳам муҳим аҳамият касб этмоқда.

Мамлакатимиз миллий иқтисодининг ҳеч бир тармоғи самарали ва мўтадил ташкил қилинган ахборот инфратузилмасисиз фаолият кўрсатиши мумкин эмас.

Ҳозирги кунда миллий ахборот ресурслари ҳар бир давлатнинг иқтисодий ва ҳарбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат

қилмоқда. Ушбу ресурсдан самарали фойдаланиш мамлакат хвфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот - коммуникациялар технологияларини қўллаш кенгаяди. Турли хилдаги ахборотлар худудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга INTERNET халқаро компьютер тармоғи орқали кириб келди. Ахборотлашган жамият шу компьютерлар тармоғи орқали тезлик билан шаклланиб бормоқда. Ахборотлар дунёсига саёҳат қилишда давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда, яъни давлат ахборотларнинг тарқалиши механизмини бошқара олмай қолади. Шунинг учун ҳам мавжуд ахборотларга ноконуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Буларнинг бири шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмоқда. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб. Ахборот ҳимояси эса давлатнинг бирламчи приоритет масалаларига айланмоқда.

Давлат органи ёки компания ходими ўз тасарруфидаги муҳим, қимматли ахборотни сақлашида, албатта, унинг хавфсизлигини таъминлашга эътибор қаратади. Бозор шароитидаги кескин рақобат, компанияга тегишли бўлган муҳим, оператив ва стратегик ахборотнинг ташқарига чиқиб кетишига йўл қўймайди. Агар ушбу вазиятларда эътиборсизликка йўл қўйилса, компания ноқулай ҳолатларга дуч келиши, ҳаттоки инқирозга юз тутиши турган гап. Шунинг учун ахборот хавфсизлигини таъминлаш кундан-кунга унинг қиммати билан тенглаштирилиб, долзарб масалага айланиб бормоқда.

Бугунги кунда ахборот хавфсизлиги жамиятдаги бош муаммолардан бири бўлиб қолмоқда. Бунга сабаб, кенг кўламда ахборотларни жамлаш, сақлаш, қайта ишлаш ва узатишнинг турли хил воситалари ва усулларидан фойдаланишдир.

Ўқув қўлланмада компьютер тизимлари ва тармоқларида ахборот хавфсизлиги масалалари, муаммолари, уларни ҳал этишда фойдаланиладиган дастурий-техник воситалар, усуллар ҳақида сўз юритилади.

Ўқув қўлланма 5110700-Информатика ўқитиш методикаси йўналишидаги бакалавриат таълим босқичи талабалари ва шахсий компьютер фойдаланувчилари учун мўлжалланган.

I боб. АХБОРОТ ХАВФСИЗЛИГИ ВА УНИ ТАЪМИНЛАШ БЎҒИНЛАРИ

1. 1. Ахборот хавфсизлиги тушунчаси

1.1.1. Жамиятнинг ахборот хавфсизлиги муаммоси

Бугунги кунда ахборотларни қайта ишлашнинг автоматлаштирилган тизимларидан оммавий равишда фойдаланиш жараёнларида жамият ахборот хавфсизлиги муаммосига дуч келмоқда. Ахборот технологияларининг, компьютер тизимларининг ҳаётнинг барча жабҳаларига оммавий равишда жорий этилиши натижасида электрон шаклдаги ахборот ҳажми бир неча минг маротаба ошди. Ҳозирда солиқ тўловчилар ёки маҳсулот ишлаб чиқариш режаси ҳақидаги муҳим бўлган маълумотларни сақловчи файлларни қисқа вақт ичида дискка ёки флэш-картали ташқи хотирага осонгина кўчириб олиш мумкин. Компьютер тармоқларида эса ахборот ресурсларига мурожаат қилишни назорат қилиш мураккаблиги туфайли тармоқда сақланаётган ахборотларнинг яхлит ҳолда сақланишига кафолат бериш мушкул. Демак, ахборот хавфсизлиги муаммоси жамиятдаги ахборотларнинг муҳим ва қимматлилигини эътироф этади.

1.1.2. Ахборот хавфсизлиги тушунчаси

Хавфсизлик деганда шахснинг, корхонанинг, давлатнинг муҳим ҳаётий манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати тушунилади.

Ҳозирги пайтда ахборот товар хусусиятига эга. Шунинг учун у ихтиёрий товар сингари товар айирбошлашда қатнашиши, ҳуқуқий объект сифатида ўзининг эгасига, ишлаб чиқарувчисига ва истеъмолчисига эга бўлиши мумкин. Истеъмолчи нуқтаи-назаридан фойдаланиладиган ахборотнинг сифати

қўшимча иқтисодий ва маънавий самарадорликка эришиш имконини яратади. Ахборот эгаси нуқтаи-назаридан муҳим тижорат ахборотини сир сақлаш бозорда рақобатбардош товар ишлаб чиқариш ёки хизмат кўрсатиш имконини яратади. Ишлаб чиқарувчи учун унинг шахсий ахборотлари маълум маънода қимматга эга. Чунки бундай ахборотларни яратиш ёки қўлга киритиш машаққатли меҳнат ёки маълум маблағ эвазига амалга оширилади. Албатта, ахборотнинг реал ёки потенциал қимматлилиги у келтираётган фойда билан аниқланади.

Бугунги кунга келиб махфий ахборотларни қўлга киритиш учун турли хил усул ва воситалардан фойдаланиш, замонавий ускуна ва қурилмалар ёрдамида ҳаттоки саноат жосуслиги авж олмоқда. Махфий сақланаётган ахборотларнинг тахминан 47% и саноат жосуслигида қўлланиладиган замонавий техник воситалар орқали қўлга киритилмоқда. Тижорат фирмалари махфий ахборотларининг 20% и рақобатчилар томонидан қўлга киритилиб ошкор қилиниши уларнинг 60% ининг банкрот ҳолатига тушиб қолишига олиб келган. Демак, хулоса шуки, ахборот муҳофазаси, унинг хавфсизлигини таъминлашга жиддий эътибор қаратиш керак.

«Ахборот хавфсизлиги» тушунчаси турли хил ҳужжатларда турлича талқин этилиши мумкин. Ривожланган давлатларнинг ахборот хавфсизлигига оид ҳужжатларида бу атама миллий манфаатлар хавфсизлиги, шахсга, жамиятга ва давлатга тегишли бўлган ахборот ресурслари хавфсизлиги маъносида фойдаланилади. Масалан, Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги Қонуни 3-моддасида **ахборот борасидаги хавфсизлик** тушунчасига «ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлик ҳолати», деб таъриф берилган. Шунга ўхшаш, «Ўзбекистон Республикаси ахборот ресурсларини тайёрлаш ва уларни маълумотларни узатиш тармоқларида, шу жумладан, Интернетда тарқатиш тартиби тўғрисида низом»нинг «Атамалар ва таърифлар» қисмида қуйидаги таъриф келтирилган: **Ахборот хавфсизлиги** - ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлиги ҳолати. Ушбу икки ҳужжатда

ахборот хавфсизлиги атамасига миллий микёсда ёраліб, унга кенг маънога эга бўлган таъриф берилган. Бошқа манбаларда ахборот хавфсизлиги деганда ахборотнинг муҳофазасини таъминлашга қаратилган, ахборотга рухсатсиз мурожаат қилиш, уни бузиш, ўзгартириш ва махфийлигини ошкор қилиш имкониятидан маҳрум қилишга қаратилган чоралар тушунилиши кўрсатиб ўтилган.

Россия Федерациясида қабул қилинган «Ҳалқаро ахборот айирбошлашда иштирок этиш тўғрисида»ги Қонунда ахборот хавфсизлиги жамиятнинг шаклланиши, ривожланиши ва фуқаролар, корхоналар, давлат манфаатлари учун фойдаланиладиган ахборот муҳити муҳофазасининг ҳолати сифатида аниқланган.

Ахборот хавфсизлиги деб ахборот тизимида тасодифий ёки ғаразли равишда ахборот эгасига ёки унинг фойдаланувчисига зарар етказувчи таҳдидлардан ҳимояланганликка айтилади.

Ахборотга ёки унинг инфраструктурасига нисбатан амалга ошириладиган ҳуружлар табиий ёки сунъий равишда бўлиб, улар ахборот орқали муносабатда бўлган субъектларга жуда катта зарар етказиши мумкин.

Ахборот хавфсизлигини таъминлашга қаратилган тадбирларнинг мажмуи *ахборот муҳофазаси* дейилади.

Ахборот хавфсизлиги муаммоларига тўғри ёндашиш учун дастлаб ахборот тизимларидан фойдаланувчи ахборот муносабатлари субъектлари ва уларнинг манфаатларини аниқлаб олиш керак. Ахборот хавфсизлигига бўладиган таҳдид -лар ахборот технологияларидан фойдаланишга тескари бўлган ҳаракатлардир. Бу фикрлар асосида қуйидаги икки хулосани келтириб чиқариш мумкин:

- ахборот хавфсизлиги муаммолари турли хил тоифадаги субъектлар томонидан турлича талқин қилиниши мумкин. Бунга мисол тариқасида давлат ташкилотлари билан Ўқув муассасаларини (коллежлар, институтлар ва университетлар) келтириш мумкин. Давлат ташкилотлари «Барча қурилмалар, тизимлар бузилса-бузилсин-у, лекин душман махфий бўлган бирорта бит маълумотни ҳам билолмасин!»

қабилида ёндашсалар, таълим муассасалари «Бизда ҳеч қандай сирнинг ўзи йўқ, асосан биз учун қурилма ва тизимлар ишласа бўлгани!» қабилида ёндашадилар.

- ахборот хавфсизлиги муаммоларини ҳал қилишда биргина ахборотга рухсатсиз мурожаат қилишдан ҳимояланиш билан чекланиб қолмай, қурилмалар ва тизимларнинг ишдан чиқиб носоз бўлиб қолишларига ҳам жиддий эътибор бериш керак.

Кўпинча «компьютер хавфсизлиги» атамасини ҳам ишлатишади. Бу тушунча тор маънодаги тушунча, чунки айрим олинган компьютер ахборот тизимлари таркибий қисмига киради. Ахборот хавфсизлиги фақатгина компьютер хавфсизлигига боғлиқ бўлмай, ахборот инфраструктурасига ҳам боғлиқ. Ахборот инфраструктурасига ахборот билан ишлашда зарур бўлган электр, иссиқлик, сув таъминоти, совутгичлар, коммуникация воситалари ва албатта, ахборот билан ишловчи ходимлар киради. Бу инфраструктура ўзига хос аҳамиятга эга. Ахборот хавфсизлигини таъминлашдан мақсад инсонлар саломатлигига, атроф муҳит ҳолатига жиддий зарар етказувчи таъсирларни ҳамда ахборотларга нисбатан амалга ошириладиган таҳдидлар натижасида келиб чиқадиган моддий зарар миқдорини камайтиришдир.

1.2. Ахборот хавфсизлигининг асосий ташкил этувчилари

Ахборот хавфсизлигини таъминлаш кўп қиррали фаолият билан боғлиқ жараён бўлиб, унда муваффақиятга эришиш учун тизимли ва комплекс ёндашиш талаб этилади. Ахборот тизимларидан фойдаланувчи субъектларнинг ахборот хавфсизлиги бўйича манфаатларини қуйидагилар ташкил қилади: ахборотга мурожаат қилиш имкониятини таъминлаш, ахборотнинг яхлитлигини таъминлаш, ахборотнинг махфийлигини таъминлаш. Гоҳида ахборот хавфсизлигининг бу асосий ташкил этувчиларига ахборотдан рухсатсиз нусха олишдан ҳимояланишни таъминлашни ҳам киритишади. Лекин бу тоифадаги ҳимояланиш ҳали-ҳануз ўз ечимини тўла-тўкис топмаган.

Маълумки, ахборот тизимлари керакли бўлган ахборотларга бўлган эҳтиёжни қондириш учун яратиладилар ёки жорий этиладилар. Агар маълум сабабларга кўра бу эҳтиёж қондирилмаса, албатта, бу ахборот муносабатларининг барча субъектларига зарар етказади. Шунинг учун ахборот тизимларини ахборот хавфсизлигининг асосий элементи деб қараш мумкин.

1.2.1. Ахборотга мурожаат қилиш имкониятини таъминлаш

Ахборотга мурожаат қилиш имкониятини таъминлаш белгиланган вақт оралиғида ваколатга эга бўлган ахборот фойдаланувчилари ва субъектлари учун ахборот ёки у билан боғлиқ сервисга мурожаат қилиб фойдаланиш имкониятини таъминлашни англатади.

Ахборотга мурожаат қилиш имкониятини таъминлаш турли соҳалардаги ахборот тизимларида, айниқса ишлаб чиқаришни Бошқариш, транспорт, банк ва шу каби соҳаларда муҳим аҳамиятга эга. Бу тизимлардан фойдаланишда тўхталишлар ёки носозликлар рўй берса, моддий ва маънавий зарар миқдори катта бўлиши билан бирга, кўпчилик ахборот фойдаланувчилари ўзларига зарур бўлган қимматли ахборотларни вақтида олиш имконидан маҳрум бўладилар. Мисол учун, темир йўл ва авиабилетларни сотиш, банкларда мижозларга хизмат кўрсатиш ва ҳ.к.

Ахборотга мурожаат қилиш имкониятидан маҳрум қилишга оид мисол. Россиянинг Қозон шаҳри Приволжск райони судида Қозон энергетика техникуми талабаси, 17 ёшли Илья И. жиноий иши кўриб чиқилиши бошланган. Гап шундаки, Илья И. «Татар-информ» информацион агентлиги серверига ҳужум уюштирганликда айбланган.

Суд текширувчилари маълумотларига қараганда Қозон энергетика техникуми талабаси Илья И. зарар етказувчи дастур коди орқали «Татар-информ» информациолн агентлигининг http://ch8.ru (ёшлар чати) ресурсига тақсимланган DoS ҳужумларини уюштирган. Бунинг натижасида сервер иши осилиб қолган ва Интернет фойдаланувчилари ёшлар чати хизматига мурожаат

қилиш имкониятига эга бўлмаганлар. Серверга юбориладиган битта файл бир варакай 130 компьютер орқали минутига 100 мингта сўров кўринишида фаол бўлиб жўнатилган. Агентлик 1,5 соат давомида хужум уюштираётган компьютерларнинг сўровини тўсиш имконига эга бўлган. Лекин шундай бўлсада, хужумлар 2007 йил 21 майнинг тушлигигача давом этган. Бошқа компьютерлар ҳаттоки 1 июнгача фаол бўлганлар. Ҳужумни бартараф этиш максадида агентлик Татаристон Республикаси ички ишлар вазирлиги тасарруфидаги «К» бўлимга мурожаат қилган. Бўлим ходимлари бузғунчининг координаталарини аниқлаб, уни ашёвий далиллар асосида қўлга олганлар. Хакернинг уйидан бир қанча ахборот ташувчи оптик воситаларни, зарар етказувчи дастурлар сақланаётган тизимли блокни, шу жумладан, тақсимланган хужум уюштиришда ишлатилган зарарли дастурни ҳам мусодара қилганлар. Бузғунчи кўнгилли равишда ўз қилмишлари ҳақида кўрсатмалар берган. Суд хакер-талабани Россия Федерациясини жиноят кодекси 272 модда 1-қисми бўйича (қўриқланаётган компьютер ахборотига рухсатсиз мурожаат қилиш) ва 273 модда, 1-қисми бўйича (ЭҲМ лар учун зарар етказувчи дастурларни яратиш ва тарқатиш) жавобгарликка тортди. Агар суд Илья И. ни айбдор деб топса, унга 200 минг рубль миқдорида жарима солинади («Компьютер-пресс» журнали 2008 йил №1 сони).

1.2.2. Ахборотнинг яхлитлигини таъминлаш

> *Ахборотнинг яхлитлигини таъминлаш* сақланаётган ахборот ваколатга эга бўлмаган субъектлар томонидан ўзгартирилишидан, яъни ахборот тузилиши ва маъноси қандай берилган бўлса, шундай сақлашни таъминлашни англатади.

Ахборот яхлитлиги икки турга бўлинади: статик ва динамик яхлитлик. Статик яхлитлик деганда белгиланган объект ҳақидаги маълумотлар ўзгармай сақланиши тушунилса, динамик яхлитликда ахборотларни қайта ишлаш жараёнида бир ахборотни қайта ишлаш натижасида тўғри натижавий ахборот

олиниб, ўзгартирилмаган ҳолда тегишли бўғинга етказилиши тушунилади. Ахборотнинг динамик яхлитлигини назорат қилувчи воситалар молиявий операцияларнинг тўғри бажарилишини аниқлашда, маълум бир қимматга эга бўлган ахборотларни тартиблашда, улардан нусха олиш жараёнларида ишлатиладилар.

Маълум бир амаллар ёки ҳаракатлар кетма-кетлигини бажариш кўрсатмаларига оид ахборотларда ахборотнинг яхлитлигини таъминлаш муҳим аҳамиятга эга. Мисол учун, дори-дармон тайёрлаш, тиббий муолажа амалиёти, маълум бир технологик жараёнлардаги операциялар кетма-кетлигига оид ахборотларда яхлитликнинг бузилиши жиддий зарарга, ҳаттоки фожиага олиб келиши мумкин. Интернетнинг давлатга тегишли айрим сайтларида ёки Web-серверларида расмий ахборот яхлитлиги бузилиши натижасида берилган маълумотларнинг нотўғри талқин қилиниши ноҳуш оқибатларни, ҳаттоки давлатлараро жиддий зиддиятларни келтириб чиқариши мумкин.

Ахборот яхлитлигини бузишга қаратилган ҳаракатлардан бири. Америкалик тизим маъмури компания раҳбариятидан ўч олиш максадида компаниянинг компьютер тармоғига атайлаб вирус жорий этади. Бу ҳолат далиллар асосида исботланиши натижасида Нью-Джерси округ суди тизим маъмури Юнг Сунн Линни 2.5 йил озодликдан маҳрум қилиш ва 81,23 минг доллар миқдорида жаримага тортиш ҳақида ҳукм қабул қилган. Юнг Сунн Лин «Medco Health Solutions» фармацевтика компаниясида ишлар эди. 2003 йилнинг кузида компания раҳбарияти томонидан штатлар қисқартирилиши ҳақида маълумотларни билиб олгач, у компания раҳбариятидан ўч олиш максадида тармоққа 2004 йилнинг 23 апрелидан (ўзининг туғилган кунида) бошлаб 70 та серверда компаниядан дори-дармон сотиб олувчи мижозларнинг тўлов ҳисоботлари ҳақидаги маълумотларни йўқ қилиш максадида фаоллашиши керак бўлган вирусни жорий этади. Вирус тармоқда сақланаётган компания мижозлари ҳақидаги маълумотларнинг яхлитлигини бузишга мўлжалланган эди. Компания раҳбарияти томонидан Лин штати қисқартирилмаслиги эълон қилингач, у ўз қилмишидан пушаймон бўлиб, жиноят изини йўқотиш

мақсадида тармоқдаги вирусни тозалашга киришади. Бироқ вирус фаоллашган ва шу билан бирга кўзланган мақсадга эришишнинг имкони бўлмаганди. Сабаби, вирус дастурининг кодида Лин томонидан йўл қўйилган хатолик ҳалакит берарди. Унинг ҳаракатлари кўзга ташланганида атайлаб ўз қилмишини давом эттираверган. 2005 йилнинг январида Лин ўрнига ишга олинган янги тизим маъмури унинг ҳаракатларини ўрганиб, тўплаган далилларни раҳбариятга маълум қилади. Фақатгина 2007 йилнинг январ ойида Лин ўз қилмишига иқрор бўлади.

Экспертлар фикрича, шу каби бузғунчилик ҳаракатлари кўплаб компанияларда ҳам амалга оширилиши мумкин. Антивирус дастури ишлаб чиқувчи Aviга компанияси (free-av.com ва free-av.de.) томонидан 2007 йилнинг кузида ўтказилган сўровда қатнашган 7297 компанияда фаолият кўрсатаётган ҳар уч ходимдан бири вируслар ёрдамида ўч олишлари мумкинлигини эътироф этган.

1.2.3. Ахборотнинг махфийлигини таъминлаш

Ахборотнинг махфийлигини таъминлаш ахборотга ваколати бўлмаган субъектлар томонидан мурожаат қилиб, ундан ошкор ҳолда фойдаланишдан ҳимоя қилишни англатади.

*Ахборотнинг махфийлиги*ни таъминлаш ҳозирги пайтда қатор давлатларда фаолият кўрсатаётган компания ва фирмалар учун жиддий муаммога айланмоқда. Сабаби, ахборот қайси канал орқали ташқарига чиқиб кетиши номаълум бўлиб, унинг олдини олиш таваккалчиликка олиб келмоқда. Шу билан бирга ахборотларни криптографик усуллар ёрдамида ҳимоялашда ҳали-ҳануз техник ва ҳуқуқий муаммолар мавжуд. Ахборот хавфсизлигини ташкил этувчилари орасида «ахборотга мурожаат қилиш имкониятини таъминлаш» биринчи ўринда туради. Чунки турли тоифадаги ахборот субъектлари биринчи навбатда фойдаланувчилар ўзларининг ваколати доирасида керакли бўлган ахборотга мурожаат қилишлари ва ундан

фойдаланишлари учун ахборотга мурожаат қилиш имкониятини таъминлаш кераклигини эътироф этадилар. Шунингдек, муҳимлиги жиҳатидан ахборотнинг яхлитлигини таъминлаш ҳам долзарблиги бўйича биринчи ташкил этувчидан ҳеч ҳам қолишмайди. Узатилаётган ахборот ўзгартирилган ҳолда фойдаланувчига келиб тушиши, албатта, нотўғри хулоса ва қарорлар ишлаб чиқишга олиб келиши муқаррар. Ва ниҳоят, ахборотнинг махфийлигини таъминлаш компания ва фирмалар, алоҳида олинган шахслар учун муҳим. Негаки, улардаги қимматли ахборотларининг ошкор қилиниши нохуш оқибатларга олиб келади.

Америкалик тадқиқотчилар 2007 йилда 2006 йилга нисбатан фуқароларга тегишли махфий ахборотларнинг ошкор бўлиш ва ўғирланиш ҳолатлари 4 баробар ошганлигини аниқлашган. Фуқароларга тегишли маълумотларнинг аксарият кўп қисми ижтимоий суғурта карта номерлари ва кредит карта кодлари бўлган.

Identity Theft Resource Center маълумотларига кўра АҚШ да 2007 йилда бундай шахсий маълумотларнинг йўқотилиши ва ошкор бўлишига оид 79 миллион ҳолат қайд қилинган. 2006 йилда бу кўрсаткич 20 миллионни ташкил этганди. Шуниси қизиқки, Identity Theft Resource Center ташкилотининг ўзи унинг муассиси Линда Фоли ўз шахсий маълумотларини ўғирлатганидан сўнг ташкил этилган.

Ахборот хавфсизлиги масалаларини ёритадиган www.attrition.org сайтида нафақат АҚШдаги вазиятлар, балки дунё миқёсидаги ҳолатлар ҳақида маълумотлар берилган. Унга кўра, 2007 йилда 162 миллион шахсий маълумотлар ўғирланиши ҳолатлари қайд қилинган. 2006 йилда бу кўрсаткич 49 миллионни ташкил этган («Компьютер-пресс» журнали, 2008 йил, №2)

1.3. Ахборот хавфсизлигини таъминлашнинг аҳамияти

Ахборот хавфсизлиги умуман хавфсизликнинг асосий йўналишларидан бири, деб ҳисобланади. У миллий, соҳа, корпоратив ёки шахсий хавфсизликда муҳим ўрин эгаллайди.

Бу фикрни асослаш мақсадида бир неча мисоллар келтириб ўтамиз.

Россия Федерациясининг ахборот хавфсизлиги доктринасида ахборотга ваколати бўлмаганлар томонидан рухсатсиз мурожаат қилишдан ҳимояланиш, ахборот ва телекоммуникацион тизимларнинг хавфсизлигини таъминлаш давлат миллий манфаатларининг муҳим таркибий қисмини эгаллайди.

АҚШ президенти Б.Клинтон кўрсатмасига биноан (15 июль 1996 йил, №13010) давлат микёсида муҳим инфраструктурани жисмоний ва информацион ҳужумлардан мухофаза қилиш бўйича комиссия ташкил этилган. 1997 йил октябрида мазкур комиссия бошлиғи Роберт Марш президент учун тайёрлаган ҳисоботида на давлат, на хусусий сектор коммуникацион тармоқ ва энерготаъминот тармокларига уюштириладиган компьютер ҳужумларини қайтарувчи воситаларга эга эмаслигини таъкидлаган.

«Йорктаун» номли АҚШ ракетали крейсери ўзига ўрнатилган Windows NT тизимида ишловчи дастурий таъминотдаги мавжуд муаммолар туфайли портга қайтиб келишга мажбур бўлган. Ҳарбий техникадан самарадорли фойдаланишга каратилган дастурий таъминотда заифликлар мавжудлиги аникланган (Government Computer News, июль 1998).

Россия ички ишлар вазирлиги иқтисодий жиноятлар бўйича Бошқарма бошлиғи ўринбосари 1994 -1996 йиллар оралиғида хакерлар Россия Марказий банкининг компьютер тармоғига 500 дан ортик рухсатсиз киришга уринганликлари ҳақида баёнот берган. 1995 йилда улар томонидан 250 миллиард рубль компьютер тармоғи орқали ўғирланган (ИТАР-ТАСС, АР, 17 сентябрь 1996 йил).

Ахборот хавфсизлигини таъминлашга оид воситалар яратишга ажратилган харажатларнинг ошиб боришига карамай, йирик компанияларнинг ахборот

тизимларига уюштирилган ҳужумлар натижасида кўраётган жиддий зарар миқдори тобора ўсиб бораётганлиги ҳақида Internet Week журналининг 1998 йил 23 мартдаги сонида маълумотлар келтирилган.

Ахборот хавфсизлиги бўйича тадқиқот институти ва Федерал Разведка бюроси ҳамкорликда олиб борган ишлари натижасида 1997 йилда компьютер жиноятлари содир этилиши натижасида 136 миллион доллар моддий зарар етказилганлиги аниқланган. Бу кўрсаткич 1996 йилга нисбатан 36% ўсганлиги ва ҳар бир жиноятдан кўрилган зарар ўртача 200 минг долларни ташкил этилиши маълум қилинган.

1996 йилнинг июл ойи ўрталарида General Motors корпорацияси ўзида ишлаб чиқилган ва сотилган Pontiac, Oldsmobile ва Buick русумли автомобиль эгаларига уларни зудлик билан корпорацияга қайтаришларини сўраган. Сабаби, автомобиль двигателини электрон Бошқариш учун мослаштирилган дастурий таъминотнинг нотўғри ишлаши ёнғин келтириб чиқариши мумкин эди.

2001 йилнинг февралида Commerce One компаниясининг икки собиқ ходими тармоқ администраторининг (маъмури) паролини билган ҳолда сервер компьютерда сақланаётган хорижий буюртмачига мўлжалланган бир неча миллион долларлик йирик лойиҳа файлларини ўчириб ташлаган. Ўчирилган файллар нусхаси мавжудлиги туфайли зарар миқдори рўй берган ҳодисани текширишга, келгусида бундай ҳолатнинг олдини олишга мўлжалланган воситаларга ва жиноятчиларни аниқлашга кетган харажатлар билан чекланган. Ётоқхонадаги дугонасига ўзиниг электрон почта қутисидан фойдаланишга рухсат берган Мичиган университетининг талабаси 18 минг доллар миқдоридаги стипендиясидан маҳрум бўлган. Чунки дугонаси ғаразли мақсадда унинг номидан стипендиядан воз кечиш ҳақида раҳбариятга ариза юборган.

Афсуски замонавий дастурлаш технологиялари хатосиз ишлайдиган дастурлар яратишнинг тўлиқ имкониятига эга эмас. Бу ҳолат эса ахборот хавфсизлигини таъминловчи пишиқ-пухта ишлайдиган дастурлар яратилишига тўсқинлик қилади. Лекин ахборот тизимлари маълум архитектура

тамойилларига ва ҳар томонлама назорат қилишга асосланган ҳолда лойиҳалаштирилиб яратилсалар, ишончли хавфсизликка эришиш мумкин.

Яна мисолларга мурожаат қилайлик. 1999 йилнинг март ойида «Компьютер жиноятлари ва хавфсизлик – 1999: муаммолар ва истиқболлар» мавзусида йиллик ҳисобот нашр этилди (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). Ҳисоботда компьютер жиноятлари туфайли ҳуқуқни муҳофаза қилиш органларига мурожаат қилганлар сони кескин ошганлиги (сўралганларнинг 32%) маълум қилинган. Сўралганларнинг 30% и ишлатаётган ахборот тизимларига ташқаридан туриб бузиб кириш ҳолатлари, 57% ига Internet тармоғи орқали ҳужумлар уюштирилганлиги ва 55% бузғунчиликлар корхона ёки компанияларнинг ўз ходимлари томонидан содир этилиши қайд қилинган. Бу кўрсаткичлар 2002 йилда ўзгаргани билан моддий зарар умумий миқдори 455 миллион долларни ташкил этган. Шундан 170 миллиони ўғрилик ва 115 миллиони фирибгарлик натижасида кўрилган.

Демак, ахборотга мурожаат қилиш имкониятини таъминлаш, унинг яхлитлигини ва махфийлигини таъминлаш масалалари муваффакиятли ечилса, ишончли ахборот хавфсизлигига эришилади.

1.3.1. Ахборот хавфсизлигини таъминлаш соҳасидаги давлат сиёсати

Ўзбекистон Республикасида ахборот хавфсизлигини таъминлаш соҳасидаги давлат сиёсати ахборот соҳасидаги ижтимоий муносабатларни тартибга солишга қаратилгандир. Унда шахс, жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлаш соҳасида давлат ҳокимияти ва бошқарув органларининг асосий вазифалари белгиланади. Шунингдек, ушбу сиёсат давлат ҳокимияти ва бошқарув органларининг фаолият йўналишларини, шунингдек фуқароларнинг ўзини ўзи бошқариш органлари, жамоат бирлашмалари ва бошқа нодавлат нотижорат ташкилотларининг, фуқароларнинг ўрни ва аҳамиятини белгилайди.

1.3.2. Шахснинг ахборот борасидаги хавфсизлиги

Шахснинг ахборот борасидаги хавфсизлиги унинг ахборотдан эркин фойдаланиши зарур шароитлари ва кафолатларини яратиш, шахсий ҳаётига тааллукли сирларини сақлаш, ахборот воситасида қонунга хилоф равишда рухий таъсир кўрсатилишидан ҳимоя қилиш йўли билан таъминланади.

Жисмоний шахсларга тааллукли шахсий маълумотлар махфий ахборот тоифасига киради.

Жисмоний шахснинг розилигисиз унинг шахсий ҳаётига тааллукли ахборотни, худди шунингдек шахсий ҳаётига тааллукли сирини, ёзишмалар, телефондаги сўзлашувлар, почта, телеграф ва бошқа мулоқот сирларини бузувчи ахборотни тўплашга, сақлашга, қайта ишлашга, тарқатишга ва ундан фойдаланишга йўл қўйилмайди, қонун ҳужжатларида белгиланган йўллар бундан мустасно.

Жисмоний шахслар тўғрисидаги ахборотдан уларга моддий зарар ва маънавий зиён етказиш, шунингдек уларнинг ҳуқуқлари, эркинликлари ва қонуний манфаатлари рўёбга чиқарилишига тўсқинлик қилиш мақсадида фойдаланиш тақиқланади.

Фуқаролар тўғрисида ахборот олувчи, бундай ахборотга эгалик қилувчи ҳамда ундан фойдаланувчи юридик ва жисмоний шахслар бу ахборотдан фойдаланиш тартибини бузганлик учун қонунда назарда тутилган тарзда жавобгар бўладилар.

Оммавий ахборот воситалари ахборот манбаини ёки тахаллусини қўйган муаллифни уларнинг розилигисиз ошкор этишга ҳақли эмас. Ахборот манбаи ёки муаллиф номи фақат суд қарори билан ошкор этилиши мумкин.

1.3.3. Жамиятнинг ахборот борасидаги хавфсизлиги

Жамиятнинг ахборот борасидаги хавфсизлигига қуйидаги йўллар билан эришилади:

- демократик фуқаролик жамияти асослари ривожлантирилишини, оммавий ахборот эркинлигини таъминлаш;
- қонунга хилоф равишда ижтимоий онгга ахборот воситасида руҳий таъсир кўрсатишга, уни чалғитишга йўл қўймаслик;
- жамиятнинг маънавий, маданий ва тарихий бойликларини, мамлакатнинг илмий ва илмий-техникавий салоҳиятини асраш ҳамда ривожлантириш;
- миллий ўзликни англашни издан чиқаришга, жамиятни тарихий ва миллий анъаналар ҳамда урф-одатлардан узоқлаштиришга, ижтимоий-сиёсий вазиятни бекарорлаштиришга, миллатлараро ва конфессияларо тотувликни бузишга қаратилган ахборот экспансиясига қарши ҳаракат тизимини барпо этиш.

1.3.4. Давлатнинг ахборот борасидаги хавфсизлиги

Давлатнинг ахборот борасидаги хавфсизлиги қуйидаги йўллар билан таъминланади:

- ахборот соҳасидаги хавфсизликка таҳдидларга қарши ҳаракатлар юзасидан иқтисодий, сиёсий, ташкилий ва бошқа турдаги чора-тадбирларни амалга ошириш;
- давлат сирларини сақлаш ва давлат ахборот ресурсларини улардан рухсатсиз тарзда фойдаланилишидан муҳофаза қилиш;
- Ўзбекистон Республикасининг жаҳон ахборот маконига ва замонавий телекоммуникациялар тизимларига интеграциялашуви;
- Ўзбекистон Республикасининг конституциявий тузумини зўрлик билан ўзгартиришга, ҳудудий яхлитлигини, суверенитетини бузишга;
- ҳокимиятни босиб олишга ёки қонуний равишда сайлаб қўйилган ёхуд тайинланган ҳокимият вакилларини ҳокимиятдан четлатишга ва давлат тузумига қарши бошқача тажовуз қилишга очиқдан-очиқ даъват этишни ўз ичига олган ахборот тарқатилишидан ҳимоя қилиш;

– урушни ва зўравонликни, шафқатсизликни тарғиб қилишни, ижтимоий, миллий, ирқий ва диний адоват уйғотишга қаратилган, терроризм ва диний экстремизм ғояларини ёйишни ўз ичига олган ахборот тарқатилишига қарши ҳаракатлар қилиш.

1.4. Ахборот хавфсизлигини таъминлаш бўғинлари

Ахборот хавфсизлигини таъминлашда комплекс ёндашувгина муваффақият келтириши мумкин. Ахборот муносабатлари субъектлари манфаатларини ҳимоя қилишда қуйидаги бўғинлар бўйича чора-тадбирлар ишлаб чиқилиши муваффақият келтиради:

- ҳуқуқий асослар (қонунлар ва меъёрий ҳужжатлар);
- маъмурий (ахборот тизимларида ахборот хавфсизлигини таъминлашга оид раҳбарият томонидан қабул қилинган буйруқлар, кўрсатмалар);
- техник (дастурий ва техник воситалардан фойдаланиш бўйича йўриқномалар).

Ҳуқуқий бўғин ахборот хавфсизлигини таъминлашда жуда катта аҳамият касб этади. Кўпчилик кишилар маълум соҳада билимга эга бўлмаганликлари учун эмас, балки ҳуқуқбузарлик содир этиш жамият томонидан ёки қонун асосида жазоланишга олиб келишини билганликлари учун қонунга зид иш тутмайдилар.

Ҳуқуқий бўғинда чора-тадбирларнинг қуйидаги икки гуруҳи мавжуд:

- ҳуқуқбузарлик ва ахборот хавфсизлиги бузғунчиларига нисбатан жамиятда салбий муносабат шаклланишига йўналтирилган чора-тадбирлар (шу жумладан жазолаш чораларини қўллаган ҳолда). Булар чекловчи чора-тадбирлар;
- жамиятда ахборот хавфсизлиги соҳаси бўйича саводхонликни ва маданиятни оширишга ва ахборот хавфсизлигини таъминлашга қаратилган воситаларни жорий этишга йўналтирилган мувофиқлаштирувчи чора-тадбирлар. Булар ижодий ёндашувни талаб этадиган чора-тадбирлар.

Амалда бу икки гуруҳ чора-тадбирлари тенг кучли аҳамиятга эга. Лекин ахборот хавфсизлигини таъминлашнинг ҳуқуқий меъёрлари ва қоидаларига онгли равишда риоя қилиш масалалари йўналиши ҳақида алоҳида тўхталиб ўтиш зарур. Чунки барча ахборот муносабатлари субъектлари томонидан хавфсизликни таъминлаш бу ҳуқуқни муҳофаза қилувчи ташкилотларнинг вазифаси, деб фикр юритилиши, албатта, нотўғри. Компьютер жиноятларини таҳлил қилишда, ахборот хавфсизлигига таҳдид солган бузғунчилар ишини исботлашда ва уларни жазолашда бу ҳуқуқий меъёрлар ва қонунларни билмаган ҳолда чоралар кўриш мумкин эмас.

Энг муҳими (ва энг мушкули) ҳуқуқий бўғинда ахборот технологиялари ҳолатига ва ривожланиб боришига хос бўлган қонунлар механизми ишлаб чиқилиши керакки, бу қонунлар реал шароитда ўз таъсир кучига эга бўлсин. Қонунлар ҳеч қачон ҳаётдан илгарилаб кетмайди, бироқ ҳаётдан ортда қолиб кетган қонунлар амалда ахборот хавфсизлигини таъминлашда салбий ҳолатларга олиб келади.

Ахборот хавфсизлигини таъминлашнинг маъмурий бўғинида ҳимоянинг амалий механизмларини жорий этишга йўналтирилган мувофиқлаштирилган тадбирлар, техник чоралардан иборат мажмуани ўз ичига олади. Ушбу бўғинда компанияда ахборот хавфсизлигини таъминлашга қаратилган ҳуқуқий ва меъёрий ҳужжатлар, талаблар, буйруқлар, кўрсатмалар ишлаб чиқилади. Шу билан бирга ходимларини ахборот хавфсизлиги чоралари ва концепцияси билан таништириш, уларни ахборот хавфсизлиги бўйича ўқитиш талабларини ишлаб чиқиш, қабул қилинган қарорлар ижросини ва қоидаларнинг бузилмаслигини назорат қилиш тизимини ишлаб чиқиш, масъул ходимларни аниқлаш, керакли дастурий-техник воситаларни ҳарид қилиш бўйича шартномалар тузиш ишлари амалга оширилади.

Ахборот хавфсизлигини таъминлашнинг дастурий-техник бўғини уч қисмдан иборат ҳимояни ташкил этади: жисмоний, техник (аппарат) ва дастурий. Ахборотнинг жисмоний ҳимояси ахборот ва ахборот тизимларига мурожаат қилишни жисмонан чеклаш масалаларини ҳал қилади. Унда

ахборотни сақлаш, қайта ишлаш, узатиш воситалари қўриқлаш тизимлари, кузатиш тизимлари, хоналарга киришни чекловчи қурилмалар ёрдамида муҳофаза қилинади.

Аппарат ва дастурий воситалар бевосита ахборотни қайта ишлаш жараёнларида ахборотнинг махфийлигини, яхлитлигини таъминлашда ишлатиладилар. Шу билан бирга улар ахборот тизимига рухсатсиз киришларнинг олдини олишда ишлатиладилар.

1.4.1. Ахборот хавфсизлигига оид қабул қилинган ҳуқуқий ва меъёрий ҳужжатлар

Ўзбекистон Республикасининг асосий Қонуни 1991 йил 8 декабрда қабул қилинган Конституциядир.

Конституциянинг 29-моддасида қуйидагилар келтирилган:

«Ҳар ким фикрлаш, сўз ва эътикод эркинлиги ҳуқуқига эга. Ҳар ким ўзи истаган ахборотни излаш, олиш ва уни тарқатиш ҳуқуқига эга, амалдаги конституциявий тузумга қарши қаратилган ахборот ва қонун билан белгиланган Бошқа чеклашлар бундан мустаснодир.

Фикр юритиш ва уни ифодалаш эркинлиги фақат давлат сири ва Бошқа сирларга тааллуқли бўлган тақдирдагина қонун билан чекланиши мумкин.»

Ўзбекистон Республикасида 1997 йил 24 апрелда қабул қилинган N 400-I сонли «**Ахборот олиш кафолатлари ва эркинлиги тўғрисида»** ги Қонуннинг 3-моддасида хар бир фуқаронинг ахборот олиш хуқуқи кафолатланиши, хар кимнинг ахборотни излаш, олиш, тадқиқ этиш, узатиш ва тарқатиш хуқуқи давлат томонидан химоя қилиниши ёзилган.

2003 йил 11 декабрда Ўзбекистон Республикасида қабул қилинган №560-II сонли «**Ахборотлаштириш тўғрисида»**ги Қонуннинг 4-моддасида ахборотлаштириш соҳасидаги давлат сиёсатининг асосий йўналишлари белгиланган.

Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон тамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратишга қаратилган.

Ахборотлаштириш соҳасидаги давлат сиёсатининг асосий йўналишлари қуйидагилардан иборат:

- ҳар кимнинг ахборотни эркин олиш ва тарқатишга доир конституциявий ҳуқуқларини амалга ошириш, ахборот ресурсларидан эркин фойдаланилишини таъминлаш;
- давлат органларининг ахборот тизимлари, тармоқ ва ҳудудий ахборот тизимлари, шунингдек юридик ҳамда жисмоний шахсларнинг ахборот тизимлари асосида Ўзбекистон Республикасининг ягона ахборот маконини яратиш;
- халқаро ахборот тармоқлари ва Интернет жаҳон ахборот тармоғидан эркин фойдаланиш учун шароит яратиш;
- давлат ахборот ресурсларини шакллантириш, ахборот тизимларини яратиш ҳамда ривожлантириш, уларнинг бир-бирига мослигини ва ўзаро алоқада ишлашини таъминлаш;
- ахборот технологияларининг замонавий воситалари ишлаб чиқарилишини ташкил этиш;
- ахборот ресурслари, хизматлари ва ахборот технологиялари бозорини шакллантиришга кўмаклашиш;
- дастурий маҳсулотлар ишлаб чиқариш ривожлантирилишини рағбатлантириш;
- тадбиркорликни қўллаб-қувватлаш ва рағбатлантириш, инвестицияларни жалб этиш учун қулай шароит яратиш;
- кадрлар тайёрлаш ва уларнинг малакасини ошириш, илмий тадқиқотларни рағбатлантириш.

Қонуннинг 6-моддасида Махсус ваколатли орган вазифалари белгилаб қўйилган:

- давлат ахборот ресурсларини шакллантириш ишларини ташкил этади ва мувофиқлаштиради;
- ахборотлаштириш ва ахборот технологияларини ривожлантириш давлат дастурларини ишлаб чиқади;
- давлат органларининг ахборот тизимлари, тармоқ ва ҳудудий ахборот тизимлари яратилишига кўмаклашади;
- ахборотлаштириш соҳасидаги стандартлар, нормалар ва қоидаларни ишлаб чиқади;
- ахборот тизимлари ва ахборот технологияларининг техника воситалари ҳамда хизматларини сертификатлаштириш ишларини ташкил этади;
- юридик ва жисмоний шахсларнинг ўз ахборот ресурслари ҳамда ахборот тизимлари муҳофаза этилишини таъминлаш борасидаги фаолиятини мувофиқлаштиради;
- ахборот ресурслари, хизматлари ва ахборот технологиялари бозорини ривожлантиришга кўмаклашади;
- ахборотлаштириш соҳасида маркетинг тадқиқотлари ва мониторингни ташкил этади;
- ахборот ресурсларидан фойдаланувчиларнинг ҳуқуқлари ва қонуний манфаатларини ҳимоя қилиш чораларини амалга оширади;
- Ўзбекистон Республикасининг мудофаа қобиляти ва хавфсизлиги манфаатларини кўзлаб ахборот хавфсизлигини ҳамда ахборот тизимларидан устувор фойдаланилишини таъминлайди;
- қонун ҳужжатларига мувофиқ Бошқа ваколатларни амалга оширади.

«**Ахборотлаштириш тўғрисида**»ги Қонуннинг «**Ахборот ресурслари ва ахборот тизимларини муҳофаза қилиш**» номли 19-моддасида ахборот ресурслари ва тизимларини муҳофаза қилишнинг асосий мақсадлари баён этилган:

– шахс, жамият ва давлатнинг ахборот хавфсизлигини таъминлаш;

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

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

– ахборот ресурсларидаги мавжуд давлат сирлари ва махфий ахборотни сақлаш.

«Ахборотлаштириш тўғрисида»ги қонуннинг «**Ахборот ресурслари ва ахборот тизимлари муҳофаза қилинишини ташкил этиш»** номли 20-моддасида ахборот ресурслари ва ахборот тизимлари муҳофаза қилинишини ташкил этиш масалалари ёритилган:

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

Давлат органлари, юридик ва жисмоний шахслар давлат сирлари ҳамда махфий сирлар тўғрисидаги ахборотни ўз ичига олган ахборот ресурслари ва ахборот тизимларининг муҳофаза қилинишини таъминлаши шарт.

Ахборот ресурслари ва ахборот тизимлари муҳофаза қилинишини ташкил этиш тартиби уларнинг мулкдорлари, эгалари томонидан мустақил белгиланади.

Давлат сирлари ҳамда махфий сирлар тўғрисидаги ахборотни ўз ичига олган ахборот ресурслари ва ахборот тизимларининг муҳофаза қилинишини ташкил этиш тартиби Ўзбекистон Республикаси Вазирлар Маҳкамаси томонидан белгиланади.

Республикамизда 1994 йил 6 майда қабул қилинган **«Электрон ҳисоблаш машиналари учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси тўғрисида»**ги Қонунида ЭҲМ учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси борасидаги муносабатлар ёритилган. Ушбу Қонун ЭҲМ учун яратилган дастурлар ва маълумотлар базаларини муаллифлик ҳуқуқи объектлари сирасига киритади. Қонунда вазифаси ва афзалликларидан қатъий назар, объектив шаклда ифодаланган, босиб чиқарилган ҳамда босиб чиқарилмаган, муаллиф (ҳаммуаллифлар) ижодий фаолиятининг натижаси бўлган, ЭҲМ учун яратилган ҳар қандай дастурлар ва маълумотлар базаларига нисбатан муаллифлик ҳуқуқи татбиқ этилиши белгилаб қўйилган.

Ўзбекистон Республикаси Олий Мажлисининг 29 август 1996 йилда қабул қилинган № 257 сонли қарорига биноан 1997 йил 1 мартдан бошлаб жорий этилган Ўзбекистон Республикаси Фуқаролик Кодексининг **«Хизмат ва тижорат сири»** номли 98-моддасида қуйидагилар баён этилган:

Фуқаролик қонун ҳужжатлари хизмат ёки тижорат сири бўлган ахборотни, башарти бу ахборот учинчи шахсларга номаълумлиги сабабли ҳақиқий ёки нисбий тижорат қимматига эга бўлган, қонун йўли билан ундан эркин баҳраманд бўлиш мумкин бўлмаган ҳамда ахборот эгаси унинг махфийлигини сақлашга доир чоралар кўрган ҳолларда ҳимоя этади.

Ахборотнинг махфийлигини таъминлаш борасида давлат манфаатлари 1993 йил 7 майда қабул қилинган № 848-XII сонли **«Давлат сирларини сақлаш тўғрисида»**ги Қонунда тўлиқ ўз аксини топган Унда Ўзбекистон Республикасининг давлат сирлари, деб давлат томонидан қўриқланадиган ва махсус рўйхатлар билан чегаралаб қўйиладиган алоҳида аҳамиятли, мутлақо махфий ва махфий ҳарбий, сиёсий, иқтисодий, илмий-техникавий ва ўзга хил маълумотлар ҳисобланиши таъкидланган. Шунингдек мазкур қонунда «Давлат сирларини сақлашнинг ҳуқуқий асоси», «Давлат сирларининг категориялари», «Ахборотларни давлат сирларига мансуб деб топиш», «Давлат сирларини сақлаш тизими», «Ахборотларни махфийлаштириш муддатлари», «Давлат

сирларини сақлаш борасидаги бурч, уларни ошкор этганлик ёки қонунга хилоф равишда махфийлаштирганлик учун жавобгарлик» номли моддалар алоҳида ёритилган.

Ўзбекистон Республикаси «Ахборотлаштириш тўғрисида»ги Қонунига мувофиқ равишда юридик ва жисмоний шахсларнинг информацион-коммуникацион технологиялари ва Интернет тармоғидан фойдаланишларида хавфсизликни таъминлаш, компьютер хавфсизлиги таҳдидларининг олдини олиш ва бартараф этишни янада такомиллаштириш максадида 2005 йил 5 сентябрдаги Ўзбекистон Республикаси Президентининг ПП-167-сонли Қарорига кўра компьютер ва ахборот технологияларини ривожлантириш ва жорий этиш маркази ҳузурида компьютер билан боғлиқ можароларига муносабат билдириш хизмати ташкил этилади. Ушбу хизматнинг асосий вазифалари:

- республикада компьютер ва ахборот технологияларидан фойдаланиш соҳасидаги қонунбузарликларнинг олдини олиш борасидаги саъй-ҳаракатларни мувофиқлаштириш;

- компьютер техникаси ва дастурий таъминотлардан фойдаланувчиларни компьютер хавфсизлиги таҳдидлар тўғрисида ахборотни, шунингдек компьютер билан боғлиқ можаролар, компьютер тизимларида қўлланиладиган дастурий-техникавий воситаларнинг самарадорлигига доир материалларни тўплаш, таҳлил қилиш ва тегишли маълумот базаларида жамғариб бориш;

- компьютер хавфсизлиги борасидаги илғор тажрибани ўрганиш ва жорий этиш, ахзборот тизимларига ноқонуний равишда кириш ҳолларининг олдини олишни таъминлаш учун тавсиялар ишлаб чиқиш;

- компьютер соҳасидаги жиноятлар ва ахборот хавфсизлигини ҳуқукий таъминлаш масалаларида ҳамкорлик қилиш.

Бугунги кунда компьютер билан боғлиқ можароларга муносабат билдириш хизмати ташкил этилган. Хизмат юзасидан фойдаланувчиларга ёрдам бериш максадида www.cert.uz сайти фаолият кўрсатмоқда.

2007 йил 27 сентябрда Олий Мажлис қонунчилик палатаси томонидан «Ахборотлаштириш ва маълумотларни узатиш соҳасида қонунга хилоф ҳаракатларни содир этганлик учун жавобгарлик кучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш тўғрисида»ги Ўзбекистон Республикасининг Қонуни қабул қилинди ҳамда 2007 йил 30 декабрда Олий Мажлис Сенатининг ўн иккинчи ялпи мажлисида маъқулланди.

Ушбу Қонуннинг 1-моддасига кўра, Жиноят Кодексининг «Ахборотлаштириш қоидаларини бузиш» номли 174-моддаси чиқариб ташланди ва унинг ўрнига «Ахборот технологияси соҳасидаги жиноятлар» номли 6 моддадан иборат янги боб киритилди. Бу бобда қуйидаги моддалар назарда тутилган:

- «Ахборотлаштириш қоидаларини бузиш» номли 278/ 1-модда;
- «Компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш» номли 278/ 2-модда;
- «Компьютер тизимидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадида кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш» номли 278/ 3-модда;
- «Компьютер ахборотини модификациялаштириш» номли 278/ 4-модда;
- «Компьютер саботажи» номли 278/ 5-модда;
- «Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш» номли 278/ 6-модда.

Ахборотлаштириш қоидаларини бузиш, яъни белгиланган ҳимоя чораларини кўрмаган ҳолда ахборот тизимлари, маълумотлар базалари ва банкларини, ахборотга ишлов бериш ҳамда уни узатиш тизимларини яратиш, жорий этиш ва улардан фойдаланиш ҳамда ахборот тизимларидан рухсат билан фойдаланиш фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлса (278/1-модда),

- энг кам ойлик иш ақининг эллик бараваригача миқдорда жарима ёки бир йилгача ахлоқ тузатиш ишлари билан жазоланади.

Ўша ҳаракатлар жуда кўп миқдорда зарар етказган ҳолда содир этилган бўлса,

- энг кам ойлик иш ҳақининг эллик бараваридан юз бараваригача миқдорда жарима ёки бир йилдан икки йилгача ахлоқ тузатиш ишлари ёхуд олти ойгача қамоқ билан жазоланади.

Компьютер ахборотидан, яъни ахборот- ҳисоблаш тизимлари, тармоқлари ва уларнинг таркибий қисмларидаги **ахборотлардан қонунга хилоф равишда (рухсатсиз) фойдаланиш**, агар ушбу ҳаракат ахборотнинг йўқ қилиб юборилиши, тўсиб қўйилиши, модификациялаштирилиши, ундан нусха кўчирилиши ёхуд унинг қўлга киритилишига, электрон ҳисоблаш машиналари, электрон ҳисоблаш машиналари тизими ёки уларнинг тармоқлари ишининг бузилишига сабаб бўлса (278/2-модда),

- энг кам ойлик иш ҳақининг юз бараваригача миқдорда жарима ёки уч йилгача муайян ҳуқуқдан маҳрум қилиш ёхуд бир йилгача ахлоқ тузатиш ишлари билан жазоланади.

Ўша харакат:

а) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

б) такроран ёки хавфли рецидивист томонидан;

в) хизмат мавқеидан фойдаланган ҳолда;

г) уюшган гуруҳ томонидан ёки унинг манфаатларини кўзлаб содир этилган бўлса,

- энг кам ойлик иш ҳақининг юз бараваридан уч юз бараваригача миқдорда жарима ёки бир йилдан икки йилгача ахлоқ тузатиш ишлари ёхуд уч йилгача озодликдан маҳрум қилиш билан жазоланади.

Ҳимояланган компьютер тизимидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус дастурий ёки аппарат воситаларини ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш (278/3-модда)

- энг кам ойлик иш ҳақининг икки юз бараваригача миқдорда жарима ёки бир йилгача ахлоқ тузатиш ишлари билан жазоланади.

Ўша харакатлар:

а) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

б) такроран ёки хавфли рецидивист томонидан;

в) хизмат мавкеидан фойдаланган ҳолда;

г) уюшган гуруҳ томонидан ёки унинг манфаатларини кўзлаб содир этилган бўлса,

- энг кам ойлик иш ҳақининг икки юз бараваридан уч юз бараваригача миқдорда жарима ёки бир йилдан уч йилгача ахлоқ тузатиш ишлари билан жазоланади.

Компьютер ахборотини модификациялаштириш, яъни компьютер тизимида сақланаётган ахборотни қонунга хилоф равишда ўзгартириш, унга шикаст етказиш, уни ўчириш, худди шунингдек била туриб унга ёлғон ахборотни киритиш фуқароларнинг ҳуқуқларига ёки қонун билан қўриқланадиган манфаатларига ёхуд давлат ёки жамоат манфаатларига кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлса (278/4-модда),

- энг кам ойлик иш ҳақининг юз бараваригача миқдорда жарима ёки бир йилгача ахлоқ тузатиш ишлари ёхуд икки йилгача озодликдан маҳрум қилиш билан жазоланади.

Ўша харакатлар:

а) жуда кўп миқдорда зарар етказган ҳолда;

б) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

в) такроран ёки хавфли рецидивист томонидан содир этилган бўлса,

- бир йилдан икки йилгача ахлоқ тузаташ ишлари ёки икки йилдан уч йилгача озодликдан маҳрум қилиш билан жазоланади.

Компьютер саботажи - ўзганинг компьютер ускунасини ёки хизматда фойдаланиладиган компьютер ускунасини қасддан ишдан чиқариш, худди шунингдек компьютер тизимини бузиш (278/5-модда)

- уч йилгача муайян ҳуқуқдан маҳрум қилиб, энг кам ойлик иш ҳақининг уч юз бараваридан тўрт юз бараваригача миқдорда жарима ёки икки йилгача озодликдан маҳрум қилиш билан жазоланади.

Ўша ҳаракатлар:

а) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

б) такроран ёки хавфли рецидивист томонидан содир этилган бўлса,

- икки йилдан уч йилгача аҳлоқ тузаташ ишлари ёхуд икки йилдан уч йилгача озодликдан маҳрум қилиш билан жазоланади.

Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш худди шунингдек махсус вирус дастурларини ишлаб чиқиш, улардан қасддан фойдаланиш ёки уларни қасддан тарқатиш (278/6-модда)

- энг кам ойлик иш ҳақининг юз бараваридан уч юз бараваригача миқдорда жарима ёки икки йилгача озод-ликдан маҳрум қилиш билан жазоланади.

Ўша ҳаракатлар:

а) жуда кўп миқдорда зарар етказган ҳолда;

б) бир гуруҳ шахслар томонидан олдиндан тил бириктириб;

в) такроран ёки хавфли рецидивист томонидан;

г) уюшган гуруҳ томонидан ёки унинг манфаатларини кўзлаб содир этилган бўлса,

- икки йилдан уч йилгача озодликдан маҳрум қилиш билан жазоланади.

Бундан ташқари, юқоридаги Қонун билан Ўзбекистон Республикасининг Маъмурий Жавобгарлик тўғрисидаги Кодекснинг XII бобига «Компьютер тизимида фойдаланиш қоидаларини бузиш» номли янги 155/1-модда киритилди. Ушбу моддага кўра, компьютер тизимидан фойдаланишга рухсати бўлган шахснинг ушбу тизимда фойдаланишнинг белгиланган қоидаларини бузиши компьютерда сақланаётган ахборотининг йўқ қилиб юборилишига, тўсиб қўйилишига, компьютер техникаси ишлашининг бузилишига сабаб бўлса, бундай шахслар маъмурий жавобгарликка тортилиши белгиланди.

2003 йилнинг 11 декабрида Ўзбекистон Республикаси Президенти томонидан юқорида келтирилган «**Ахборотлаштириш тўғрисида**»ги Қонунни такомиллаштириш ва конкретлаштириш мақсадида жуда ҳам муҳим роль ўйновчи N 562-II сонли «**Электрон рақамли имзо тўғрисида**»ги Қонун имзоланди.

Ушбу Қонуннинг мақсади электрон рақамли имзодан фойдаланиш соҳасидаги муносабатларни тартибга солишдан иборат.

Мазкур Қонунга фуқаролик-ҳуқуқий келишув ҳаракатларини юритиш жараёнида ва Ўзбекистон Республикаси Қонунлари доирасида Бошқа ҳолатлардаги муносабатларда амал қилинади. Ушбу Қонунда қуйидаги асосий тушунчалар қўлланилади:

электрон рақамли имзо - электрон ҳужжатдаги мазкур электрон ҳужжат ахборотини электрон рақамли имзонинг ёпиқ калитидан фойдаланган ҳолда махсус ўзгартириш натижасида ҳосил қилинган ҳамда электрон рақамли имзонинг очиқ калити ёрдамида электрон ҳужжатдаги ахборотда хатолик йўқлигини аниқлаш ва электрон рақамли имзо ёпиқ калитининг эгасини идентификация қилиш имкониятини берадиган имзо;

электрон рақамли имзонинг ёпиқ калити - электрон рақамли имзо воситаларидан фойдаланган ҳолда ҳосил қилинган, фақат имзо қўювчи шахснинг ўзига маълум бўлган ва электрон ҳужжатда электрон рақамли имзони яратиш учун мўлжалланган белгилар кетма-кетлиги;

электрон рақамли имзонинг очиқ калити - электрон рақамли имзо воситаларидан фойдаланган ҳолда ҳосил қилинган, электрон рақамли имзонинг ёпиқ калитига мос келувчи, ахборот тизимининг ҳар қандай фойдаланувчиси фойдалана оладиган ва электрон ҳужжатдаги электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш учун мўлжалланган белгилар кетма-кетлиги;

электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш - электрон рақамли имзонинг электрон рақамли имзо ёпиқ калитининг эгасига тегишлилиги ва электрон ҳужжатдаги ахборотда хатолик йўқлиги текширилгандаги ижобий натижа;

электрон ҳужжат - электрон шаклда қайд этилган, электрон рақамли имзо билан тасдиқланган ҳамда электрон ҳужжатнинг уни идентификация қилиш имконини берадиган бошка реквизитларига эга бўлган ахборот.

Қонунга кўра, электрон ҳужжатдаги электрон рақамли имзо айни бир вақтнинг ўзида қуйидаги шартларга риоя этилган тақдирда қоғоз ҳужжатга қўлда ўзи қўйган имзо билан бир хил аҳамиятга эгадир, агар:

- электрон рақамли имзонинг ҳақиқийлиги тасдиқланган бўлса;
- электрон рақамли имзонинг ҳақиқийлиги тасдиқланган пайтда ёки имзолаш пайтини белгиловчи далиллар бўлганда электрон ҳужжат имзоланаётган пайтда электрон рақамли имзо калитининг сертификати амал қилиб турган бўлса;
- электрон рақамли имзодан электрон рақамли имзо калитининг сертификатида кўрсатилган мақсадларда фойдаланилаётган бўлса.

Ахборот хавфсизлигини таъминлашга қаратилган, уларни амалда қўллаш имконини берувчи ҳуқуқий ва меъёрий база тобора мукаммаллаштирилиб, замон талабига жавоб берадиган даражада яратилмоқда.

Ҳозирги пайтда UZ домени доирасида ахборот хавфсизлиги масалаларини ёритиб борувчи www.security.uz сайти фойдаланувчилар эътиборига ҳавола этилмоқда.

1.4.2. Хорижий давлатларда ахборот хавфсизлигига оид қабул қилинган қонунлар таҳлили

Бу борада асосан ривожланган давлатларда (биринчи навбатда АҚШда) ахборот хавфсизлигига оид қабул қилинган қонунлар, уларнинг аҳамияти ва ўзига хос хусусиятлари билан танишиб чиқамиз. АҚШ нинг ўзида бундай қонун ҳужжатларидан 500 га яқини қабул қилинган.

АҚШ да қабул қилинган қонунлардан энг асосийси 1987 йилдан кучга кирган «Ахборот хавфсизлиги тўғрисида»ги қонундир (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Унинг асосий мақсади –

федерал компьютер тизимларида ахборот хавфсизлигини таъминлашга қаратилган етарли даражадаги амалларни қўллашдир.

Кириш қисмида қонуннинг муайян ижрочиси сифатида Стандартлар ва технологиялар Миллий институти (СТМИ) аниқланган. Мазкур институт ахборотларни ўчирилишидан ва уларга рухсатсиз мурожаат қилишдан, шунингдек компьютер ёрдамида амалга ошириладиган ўғрилик ва товламачиликдан ҳимоя қилишга йўналтирилган стандартлар ва қоидалар ишлаб чиқишга масъул бўлиб, унга бу борада етакчилик вазифасини бажариш юклатилган.

Мазкур қонунга кўра махфий ахборотларни қайта ишловчи федерал ахборот тизимлари операторлари ахборот хавфсизлигини таъминлашга қаратилган режаларини ишлаб чиқиб, унга амал қилган ҳолда иш юритишлари керак. Бундай ахборот тизимлари билан ишловчи ходимларни ахборот хавфсизлиги бўйича малака ва кўникмаларини ошириш ҳам қонунда мажбурий деб белгиланган. СТМИга, ўз навбатида, тизимлардаги заиф жойларнинг табиатини ва кўламини ўрганиш бўйича тадқиқот ишларини ўтказиб, хавфсизликни таъминлаш борасида самарали чораларни ишлаб чиқиш мажбурияти юкланган. Тадқиқот ишлари натижалари бўйича ишлаб чиқилган чоралар нафақат давлат федерал тизимларида, балки хусусий сектор тизимларида қўлланилиши кўзда тутилган.

Ахборот хавфсизлиги борасидаги чораларнинг уйғунлигини ва воситалар яратилишига оид тадқиқотлар такрорланмаслигини таъминлаш мақсадида қонунда СТМИ ўз фаолиятини бошқа вазирликлар ва маҳкамалар, жумладан Мудофаа вазирлиги, Энергетика вазирлиги, Миллий хавфсизлик агентлиги (МХА) билан келишган ҳолда олиб бориши белгиланган.

Бундан ташқари қонунда Савдо вазирлиги ҳузурида ахборот хавфсизлиги бўйича комиссия ташкил этилиши белгилаб қўйилган. Комиссиянинг асосий вазифалари:

• ахборот хавфсизлигини юқори савияда таъмиинлашга қаратилган бошқарув, техник, маъмурий ва жисмоний чораларини аниқлаш;

• СТМИ учун зарур тавсиялар бериш, ҳамда манфаатдор маҳкамаларга бундай чоралар бўйича етарли маълумотлар етказиш.

Ахборотларнинг йўқотилиши, улардан нотўғри фойдаланиш, ваколатсиз мурожаат қилиш ёки уларга рухсатсиз ўзгартириш киритиш каби ҳолатларнинг олдини олишга йўналтирилган хавфсизлик режасини (федерал ахборот тизимлари ва барча давлат маҳкамаларида) ишлаб чиқишни амалий жиҳатдан таъминланиши қонуннинг 6 бўлимида белгиланган. Ишлаб чиқилган ахборот хавфсизлиги режаларининг нусхалари СТМИ ва МХА ларга албатта жўнатилиши шарт.

1997 йилда юқорида келтирилган қонуннинг мантиқий давоми сифатида «Ахборот хавфсизлигини такомиллаштириш» номли қонун лойиҳаси (Computer Security Enhancement Act of 1997, H.R. 1903) ишлаб чиқилди. Бу лойиҳа СТМИ мавқеини оширишга ва криптографик воситалар бўйича операцияларини соддалаштиришга қаратилган

Қонун лойиҳасида хусусий секторда сақланаётган маълумотларнинг махфийлиги ва яхлитлигини таъминлашга қаратилган криптографик воситалар яратишга ва уларни фойдаланиш учун тақдим этишга тайёр эканликлари таъкидланган. Яъни бундай воситалар ҳукумат фармойиши асосида эмас, балки бозор иқтисодиёти сиёсатида талаб ва таклифдан келиб чиқиб яратилиши керак. Шу билан бирга Бошқа давлатларда рақобатбардош ва қулай криптографик технологиялар мавжудки, уларни АҚШ аппарат ва дастурий таъминот яратувчиларининг экспорт салоҳиятига таъсир этишини ҳисобга олиш керак.

Федерал ахборот тизимларида хавфсизликни таъминлаш учун хусусий секторда яратилган технологик янгиликларни кенг кўламда қўллаш тавсия этилиши билан бирга хорижий давлатларда жорий этилган илғор технологияларни таҳлил этиб, улардан фойдаланиш маъқулланган.

Лойиҳанинг 4 бўлимида ахборот хавфсизлиги соҳасида тизимда ёки дастурий таъминотдаги заиф жойларни баҳолаш воситалари ва усулларининг таҳлили зарурлиги алоҳида такидланган.

2001 йилда юқорида кўрилган қонун лойиҳасининг янги такомиллаштирилган варианти - Computer Security Enhancement Act of 2001 (H.R. 1259 RFS) Вакиллик Палатаси томонидан маъқулланиб, Сенатга топширилди.

1997-2001 йиллар оралиғида АҚШ ахборот хавфсизлиги ҳуқуқий бўғинида кўпгина муҳим ишлар амалга оширилди. Криптографик воситалар учун экспорт чекланишлар камайтирилди, кўпгина стандартлар яратилди.

Ахборот хавфсизлиги бўйича Германия Федератив Республикасида қабул қилинган қонунлар эътиборга лойиқдир. Республикада «Маълумотларни ҳимоя қилиш» (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)) номли қонун қабул қилинган бўлиб, у 44 бўлимдан иборат. Мазкур қонун шахсий маълумотлар хавфсизлигини таъминлашга қаратилган.

Бу қонунда давлат хавфсизлиги манфаатлари, албатта, хусусий махфий ахборотлардан устуворлиги таъкидланган. Шу билан бирга шахсга тегишли бўлган махфий ахборотлар ҳимоя қилиниши кафолатланади. Масалан, агар фирма ходими хусусий компания манфаатлари учун шахсга тегишли махфий ахборотларни қайта ишламоқчи бўлса, у махфий ахборотни ошкор қилмасликка тилхат бериши шарт.

Шахсий маълумотларни сақловчи ва қайта ишловчи давлат муассасалари шахсий ҳаётга оид махфий ахборотларни ошкор қилган ҳолларда қонунда белгиланган тартибда жавобгарликка тортилишлари кўрсатилган. Қонунбузарлик рўй берган тақдирда 250 минг немис маркасигача жарима солиниши кўзда тутилган.

Ахборот хавфсизлигига оид Буюк Британияда қабул қилинган қонунлардан эътиборга моликлари BS 7799 кўнгилли стандартларидир. Бу стандартлар ташкилот ва компанияларга хавфсизлик режаларини ишлаб чиқиб, улар бўйича ишлаш имкониятини яратишда хизмат қиладилар.

Россия Федерациясида қабул қилинган асосий қонунлардан бири «Ахборот, ахборотлаштириш ва ахборот ҳимояси» номли Қонун 1995 йил 20 февралда кучга кирган.

Қонунда ахборот хавфсизлигига оид қуйидагилар мақсадлар белгиланган:

- ахборотнинг ташқарига чиқиб кетиши, ўғирланиши, йўқолиши (ўчирилиши), қалбакилаштирилишининг олдини олиш;
- шахсга, жамиятга, давлатга бўладиган таҳдидларнинг олдини олиш;
- рухсатсиз ахборот манбаларига кириб, улардан фойдаланиш, ўчириш, бузиш, кўчириш, мурожаат қилиш имкониятидан маҳрум қилишнинг олдини олиш;
- ахборот ресурслари ва тизимларидаги ахборотларга ноқонуний тарзда кириш, ҳужжатлаштирилган ахборотнинг мулк сифатида яратилишини ҳуқуқий асосда таъминлаш;
- ахборот тизимларидаги фуқароларнинг шахсий сирлари ва махфий ахборотларини сақланишини таъминлаб, уларнинг конституцион ҳуқуқларини ҳимоя қилиш;
- қонун доирасида Давлат сирларини ҳимоялаш, ҳужжатлаштирилган ахборотларнинг махфийлигини таъминлаш.

Қонунда махфий ахборотларни ҳимоялашга алоҳида эътибор қаратилган.

Россия Федерациясининг Жиноят Кодекси (2002 йил 14 март таҳриридаги) 28 – боби «Компьютер ахборотларига оид жиноятлар» номли бўлиб, унда 3 та модда мавжуд:

• 272-модда. Компьютер ахборотларига ноқонуний тарзда мурожаат қилиб, кириш. Жазо чораси - икки юз минг рубль ёки 18 ойлик иш ҳақи ёки 6 ойдан 1 йилгача аҳлоқ тузатиш ишлари ёки икки йилгача озодликдан маҳрум қилиш. Қайта такрорланса, юз мингдан уч юз минг рублгача жарима ёки бир йилдан икки йилгача аҳлоқ тузатиш ишлари ёки 5 йилгача озодликдан маҳрум қилиш чоралари белгиланган;

• 273-модда. Зарарли ЭҲМ дастурларни яратиш, фойдаланиш ва тарқатиш. Жазо чораси - 18 ойлик иш ҳақи миқдорида жарима ёки уч йилгача озодликдан

маҳрум қилиш. Қайта такрорланса, уч йилдан саккиз йилгача озодликдан маҳрум килиш;

• 274-модда. ЭҲМ ишлатиш, ЭҲМ тизимларидан ва тармоқларидан фойдаланиш, қоидаларини бузиш. Жазо чораси – 5 йилгача муайян ҳуқуқдан маҳрум қилиш ёки 180 соатдан 240 соатгача мажбурий меҳнат ёки икки йилгача озодликдан маҳрум қилиш.

Глобал тармоқларга оид ахборот хавфсизлиги қонунлари халқаро амалиёт тажрибасидан келиб чиққан ҳолда ишлаб чиқилиши керак. Аргентинада рўй берган воқеа бундай қонунлар яратилишида ўгит бўлиши керак. Сабаби, 1996 йил охирида Аргентинада 21 ёшли Буэнос-Айрес фукароси «Крик» электрон-эълонлар хизмати тизими оператори Хулио Цезар Ардита (лақаби «El Griton»)ваколатли орган томонидан ҳибсга олинади. Унга АҚШ Харбий-денгиз флоти, НАСА, йирик Америка университетлари, шунингдек Бразилия, Чили, Корея, Мексика ва Тайвань компьютер тизимларига кўплаб рухсатсиз кирганлик ва бузғунчилик уюштириш айби қўйилган. Бирок, Аргентина ва АҚШ тегишли ҳуқуқ органларининг ҳамжиҳатлик билан ишлашларига карамай, Ардита расмий айблов эълон қилинмасдан озодликка чиқарилиб юборилди. Сабаби, Аргентина қонунчилигига биноан компьютер тизимларига рухсатсиз кириш жиноят ҳисобланмаган.

Хулоса қилиб айтганда, ахборот хавфсизлигининг ҳуқуқий бўғинида қуйидаги йўналишлар устувор йўналишлардир:

• ахборот муносабатлари барча субъектлари манфаатларини ҳисобга олган ҳолда янги қонунлар яратиш;

• ижодий ва чекловчи (биринчи навбатда ҳуқуқбузарларга нисбатан белгиланган жазо чораларини қўллаш мақсадида) қонунларнинг балансини таъминлаш;

• умумжаҳон ҳуқуқий фазоси билан интеграциялашуви;

• ҳозирги замон ахборот технологиялари ҳолатини ҳисобга олган ҳолда ҳуқуқий меъёрлар ва қонунларни яратиш.

1.4.3. Тарқатиш шартларига кўра дастурий таъминот турлари

Тарқатиш шартларига кўра дастурларни тўрт турга ажратиш мумкин:

- лицензияланган дастурлар;
- шартли равишда бепул тарқатиладиган дастурлар (shareware, trial, намойиш кўринишидаги);
- умуман бепул тарқатиладиган дастурлар (freeware);
- ўзининг очик коди билан биргаликда эркин равишда тарқатиладиган дастурлар (free software).

Лицензияланган дастурларнинг дистрибутивлари (дастурнинг ташки хотира воситасидан фойдаланувчи компьютерига ўрнатиладиган оригинал нусхаси) дастурни яратган фирма ёки сотувчи-фирма томонидан фойдаланувчи билан тузилган шартномада белгиланган тўлов асосида тарқатилади. Лицензион шартномага кўра дастурни сотувчи фирма ва дастурни яратган фирма фойдаланувчи учун дастурнинг нормал ҳолда ишлашига кафолат беради ва улар бунга тўлиқ жавобгардирлар.

Баъзи дастур яратувчи фирмалар реклама мақсадида шартли равишда бепул тарқатиладиган дастурларни (shareware) таклиф этадилар. Бунда фойдаланувчига чекланган муддат давомида ишлайдиган (trial) дастур лаҳжаси бепул берилади. Бу дастур маълум муддат ишлагач ёки маълум сондаги ишга тушириш буйруқлари берилганидан сўнг ундан фойдаланиш имконияти тўхтатилади. Сабаби, фойдаланувчи дастур билан танишиб чиққач, ундан кейинчалик фойдаланишни афзал кўрса, шартнома асосида пул ўтказиш йўли билан дастурнинг тўлиқ версиясини сотиб олиши мумкин. Баъзи дастур яратувчи фирмалар ўзлари яратган дастурни реклама қилиш ёки фойдаланувчиларни қизиқтириш мақсадида дастурнинг чекли функционал имкониятларини намойиш этувчи версиясини бепул тарқатадилар.

Дастурий таъминот яратувчи фирмалар шунингдек кенг кўламда бепул тарқатиладиган дастурларни (freeware) ҳавола этадилар. Сабаби, фирмалар ўзлари яратган дастурлар билан ўз имиджларини, рейтингларини оширишга

ҳаракат қилиб бундай дастурларни бепул тарқатишдан манфаатдор бўладилар. Бундай дастурларга қуйидагилар киради:

- янги, ҳали тўлиқ ишланмаган (ёки текширилиши керак бўлган) дастурларнинг версиялари;
- принципиал жиҳатдан янги технологияларни қамраб олган дастурлар (бундай дастурларни тарқатиш, фирма учун маркетинг тадқиқотларини ўтказиш имконини беради);
- аввал яратилган дастурларнинг янги, имкониятлари оширилган (ёки хатоликлардан бартараф этилган) вариантлари;
- эскирган дастурлар лаҳжалари;
- янги қурилмалар учун яратилган драйвер дастурлари.

Дастурий таъминотнинг яна битта тури – очиқ код билан (free software), яъни дастурлаш тили буйруқларининг тўлиқ матни ва изоҳлари билан тарқатиладиган дастурлардир. Бундай дастурлар муаллиф рухсати билан эркин равишда бепул ёки маълум миқдордаги пул эвазига тарқатилиши, улардан нусха кўчирилиши, фойдаланилиши, шунингдек фойдаланувчи томонидан ҳаттоки такомиллаштирилиши ҳам мумкин. Очиқ кодли дастурдан фойдаланиб бошқа дастур яратувчилар ёки фойдаланувчилар мураккаб, пишиқ-пухта ишлайдиган бошқа дастур яратишлари мумкин.

Эркин равишда тарқатиладиган дастурларда фойдаланувчилар қуйидаги тўрт турдаги эркинликларга эга бўлишлари керак:

- турли мақсадда дастурни ишга тушириш эркинлиги;
- дастурни ўз эҳтиёжи ёки манфаати йўлида ўрганиш ёки ундан фойдаланиш учун ўз компьютерига мослаштириш эркинлиги (бунинг зарурий шарти дастурнинг очиқ матнидан фойдаланиш имкониятининг мавжудлиги);
- нусха кўчириш ва тарқатиш эркинлиги;
- дастурни такомиллаштириш, такомиллашган дастур натижаларини матбуотда эълон қилиш эркинлиги.

Бирок, ягона чеклов мавжудки, у ҳам бўлса, дастурга ўзгартиришлар киритиб, у ҳар қанча такомиллаштирилса ҳам, муаллифлик ҳуқуқи дастлабки дастур яратувчисида сақланиб қолинади.

1.4.4. Дастур учун муаллифлик ҳуқуқи

Лицензион дастурлар учун ҳақ тўлаш керакми? Бу саволга қатъий равишда «Ҳа!», деб жавоб бериш мумкин. Шартли бепул дастурлар (shareware) ҳам, агар Сиз улардан кейинчалик ўз фаолиятингизда фойдаланмоқчи бўлсангиз, тўлов амалга оширилишини талаб этадилар. Баъзи очиқ кодли дастурлар учун ҳам улардан фойдаланганлик учун ҳақ тўланади. Бу ҳақ дастур учун бўладиган хизматлар, уни созлаш ва бошқа эксплуатацион харажатлар учун олинади. Фақат эркин равишда бепул тарқатиладиган дастурлар учун ҳақ олинмайди.

Дастурга муаллифлик ҳуқуқи Ўзбекистон Республикаси Қонуни томонидан ҳимояланади. «**Муаллифлик ҳуқуқи ва турдош ҳуқуқлар тўғрисида**»ги (20.07.2006 йил) Қонуннинг «Муаллифлик ҳуқуқи объектларининг турлари» номли 6-моддасида муаллифлик ҳуқуқи объектлари жумласига барча турдаги электрон-ҳисоблаш машиналари (ЭҲМ) учун дастурлар, шу жумладан амалий дастурлар ва операция тизимлари кириши белгиланган.

Мазкур қонуннинг «Муаллифлик ҳуқуқининг амал қилиш муддати» номли 35-моддасида муаллифлик ҳуқуқи муаллифнинг бутун ҳаёти давомида ва вафотидан кейин у вафот этган йилдан кейинги йилнинг биринчи январидан эътиборан эллик йил давомида амал қилиши, муаллифлик, муаллифнинг исм-шарифи ва асарнинг даҳлсизлиги муддатсиз ҳимоя қилиниши кўрсатилган.

1.4.5. Компьютер қароқчиларига қарши кураш

Амалдаги тажриба шуни кўрсатмоқдаки, фақат қонун асосида дастурий таъминотни ҳимоялаш ва бу қонунларга қатъий равишда риоя қилиш компьютер қароқчилигига жиддий тўсқинлик қила олади. Бунинг учун жамият аъзоларини бу қонунлардан хабардор қилиш, давлат томонидан фаол чоралар кўрилиши зарур.

Компьютер қароқчиларига қарши курашишда кишилар онгида дастурий таъминот муаллифлари ҳуқуқини ҳимоя қилиш муаммоларига янгича ёндашиш кўникмаларини шакллантириш муҳим аҳамият касб этади. Бу борада давлат органлари амалда фойдаланилаётган дастурларни қонуний равишда олинишини, муаллифлик ҳуқуқлари бузилиши фактларини аниқлаш мақсадида ички назоратни оқилона амалга оширишлари керак.

Компьютер қароқчилиги олдини олишда интеллектуал меҳнатга нисбатан инсонларда ҳурматнинг шаклланишида маърифат муҳим роль ўйнайди. Қароқчиликни камайтиришда давлат ўз фуқароларини муаллифлик ҳуқуқлари борасидаги мавжуд бўлган қонун ҳужжатлари билан таништириши, легал (лицензион) дастурлардан фойдаланишни қўллаб-қувватлаши ва қароқчилик йўли билан фойдаланилаётган дастурлар учун жавобгарлик масъулиятини шакллантириши керак.

Мисол тариқасида Россия ҳуқуқни муҳофаза қилиш органларида қайд қилинган компьютер қароқчилигига оид реал воқеаларни келтирамиз:

- 2004 йилнинг 5 февралида Москва шаҳрида Двинская кўчасида жойлашган омбордан 1 миллионга яқин қароқчилик йўли билан тайёрланган ва сотувга чиқарилиш учун мўлжалланган компакт-дисклар мусодара қилинди;
- 2004 йилнинг 10 февралида Москва вилояти иқтисодий жиноятлар бўйича хавфсизлик Бошқармаси оператив ходимлари томонидан Москва - Ростов-Дон трассасида катта партиядаги қароқчилик йўли билан тайёрланган DVD-дискларни мусодара этишди;

- 2004 йилнинг 2 апрелида Москва шаҳар ички ишлар бош Бошқармаси иқтисодий жиноятлар бўйича хавфсизлик Бошқармаси ходимлари томонидан Стаханов кўчасидаги омбордан 1С, Microsoft, АВВУУ, Symantec ва бошқа шу каби машҳур компания ва фирмаларга тегишли 800 минг нусхадаги қароқчилик йўли билан тайёрланган компакт-дискларнинг хуфиёна тарқатилиши олдини олиб қолдилар.

Келтирилган статистик маълумотлар қайси давлатда дастурий таъминот яратувчиларнинг муаллифлик ҳуқуқлари ҳимояси ва чоралари учун фаол ишлар амалга оширилса, ўша давлатларда бу соҳада ривожланиш ва ўсиш кузатилиши мукаррарлигини кўрсатади.

Компьютер қароқчилигига қарши курашиш учун давлат томонидан қатъий қонунлар ва уларнинг ижроси амалда натижа бера оладиган даражада тегишли механизм ва чора-тадбирлар ишлаб чиқилиши керак. Ҳар бир давлат Ҳалқаро савдо ташкилоти битимидаги интеллектуал мулк ҳуқуқини ҳимоя қилиш йўналиши бўйича ўз мажбуриятларини бажариши керак. Шунингдек Интернет тармоғидан қароқчилик йўли билан қўлга киритилган дастурларни тарқатиш бўйича хизмат кўрсатишни тавсия этувчи Web-узеллар фаолиятига чек қуйишнинг ҳуқуқий чоралари ва дастурларни хуфиёна кўпайтиришга мўлжалланган ускуна ва технологияларни тақиқлаш чораларини ишлаб чиқиш зарур. Булардан ташқари компакт-дискларни (CD и DVD) ишлаб чиқариш устидан, улардан нусха кўчиришда махсус ҳимоя воситаларидан, маркерлардан фойдаланиш талаблари бажарилишини қаттиқ назоратга олиш керак.

Қароқчилик йўли билан тайёрланган дискларни сотишдан келадиган фойда миқдорининг жуда катталиги туфайли ноқонуний бизнес уюшган жиноятчилар назорати остида кенгайиб бормоқда. Бу ҳолат эса қароқчиларга қарши курашни янада мушкуллаштирмоқда. Уюшган жиноятчиларига қарши самарали курашиш учун энг биринчи навбатда бундай жиноятларни фош этишга эришиш, оператив ходимларнинг, терговчиларнинг,

прокурорларнинг бу борадаги махсус билимларини оширишга эътиборни қаратиш керак.

1.5. Ахборот хавфсизлигига оид стандартлар ва хусусиятлар

Ахборот хавфсизлигига оид стандартлар ва хусусиятларнинг икки тури билан танишиб чиқамиз:

- хавфсизлик талаблари бўйича ахборот тизимларини ва хавфсизлик воситаларини синфларга ажратиш бўйича баҳолаш стандартлари;
- хавфсизлик воситаларини жорий этиш бўйича ўзига хос техник хусусиятлар.

Турли давлатларнинг ахборот хавфсизлиги бўйича стандартлаш базаларининг шаклланишига дунёда биринчи бўлиб АҚШ Мудофаа Вазирлиги кўрсатмасига биноан яратилган ва кенг кўламда фойдаланилган «Ишончли компьютер тизимларини баҳолаш мезонлари» номли стандарти асос бўлди.

Бу стандарт 1983 йилнинг августида чоп этилиб, ўзининг китоб шаклидаги муқоваси зарғалдоқ рангда бўлгани учун уни «Оранжевая книга» деб номлай бошладилар.

«Оранжевая книга»да хавфсизлик тизими тушунчаси тавсифланган. Унга кўра хавфсизлик тизими ахборотга мурожаат қилишда фақат ваколатга эга бўлган шахслар фойдаланишларини ва ахборотларни қайта ишлаш, уларни ўқиш, таҳрирлаш ёки ўчиришни тегишли воситалар ёрдамида бошқарилиши таъкидланган.

«Оранжевая книга»да ишончли тизим сифатида етарли даражада хавфсизлик талабларига риоя қилинган ҳолда керакли аппарат ва дастурий воситалардан фойдаланиб турли хил махфий бўлган ахборотларни бир гуруҳ фойдаланувчилар томонидан мурожаат қилиш ҳуқуқлари бузилмасдан қайта ишловчи тизим аниқланган.

Мазкур қўлланмада ***хавфсизлик*** ва ***ишончлилик*** ахборотга мурожаат қилишни бошқариш нуқтаи-назаридан инобатга олинган бўлиши билан бирга,

ахборотнинг махфийлигини ва яхлитлигини таъминлашда ҳам муҳим бўлиши ёритилган.

Ишончлилик даражаси қуйидаги икки асосий мезон бўйича баҳоланади:

Хавфсизлик сиёсати – ахборотни тўплаш, қайта ишлаш ва тарқатишни ташкил этишга қаратилган қонунлар, қоидалар ва меъёрий ҳужжатлар тўплами.

Хусусан, қоидалар ваколатга эга бўлган фойдаланувчи кайси ҳолларда муайян маълумотлар тўплами устида амал бажариш кераклигини белгилайди. Тизимга бўлган ишончлилик даражаси қанчалик юқори бўлса, хавфсизлик сиёсати ҳам шунчалик талабчан ва кўп қиррали бўлади. Ишлаб чиқилган хавфсизлик сиёсатига қараб хавфсизликни таъминловчи муайян механизмларни танлаш мумкин. Хавфсизлик сиёсати бўлиши мумкин бўлган таҳдидларни таҳлил қилиш ва уларга қарши кураш чораларини ишлаб чиқишни белгиловчи фаол ҳимоя йўналишидир.

Кафолатланганлик даражаси – ахборот тизими архитектураси ва жорий этилишида унга бўлган ишончлилик мезони бўйича бериладиган баҳо.

Хавфсизликнинг ишончлилиги тизимни назорат қилиш, тизимни бутунлай ва ташкил этувчи компонентларини алоҳида-алоҳида текшириш натижасида шаклланади. Кафолатланганлик даражаси хавфсизлик сиёсати механизмларининг қанчалик талаб даражасида танланиб ишлаётганлигини кўрсатади.

Хавфсизликни таъминлашнинг яна бир муҳим воситаларидан бири баённомалар (протоколлаштириш) юритиш механизмидир. Ишончли тизимда хавфсизликка оид ҳар бир ҳодиса, жараён қайд қилиниб борилиши керак. Баённомалар юритилиши аудит-текширувлари ёрдамида таҳлил этилиши ва назорат килиниб борилиши керак.

Баённомалар юритишдан мақсад – ҳар бир дақиқада тизим билан ким ишлаганини ва нима қилганлигини керак бўлган вақтда аниқлаб олиш. Баённомалар юритиш воситалари уч тоифага бўлинади:

- идентификация ва аутентификация;

- ахборотга бўлган ишончли йўлни ҳавола қилиш;
- қайд қилинган маълумотларни таҳлил этиш.

Идентификация – бир томоннинг (фойдаланувчи, дастур, техник қурилма) бошқа бир томонга (масалан, бошқа бир дастурга) ўзининг такрорланмайдиган, уникал номини маълум қилиш жараёнидир. Такрорланмайдиган ном идентификатор деб аталади.

Бундай идентификатор мос равишда объектни (фойдаланувчини, дастурни, техник қурилмани) характерлаши керак. Яъни шундай кафолат бўлиши керакки, икки турли объектлар бир хилдаги идентификаторга эга бўлишлари мумкин эмас.

Идентификация фақатгина ҳисоблаш техникасидагина эмас, балки турли соҳаларда қўлланилади.

Масалан, талабанинг идентификатори сифатида унинг рейтинг дафтарчасидаги номер ишлатилиши мумкин. Сабаби, бундай номер ҳар бир талаба учун такрорланмас хусусиятга эга. Солиқ тизимида солиқ тўловчининг идентификатори сифатида солиқ тўловчининг тартиб рақами (СТИР) ишлатилади. СТИР ҳар бир солиқ тўловчи учун уникал, такрорланмас кўринишда берилади.

Демак, идентификация – ўзининг такрорланмайдиган, уникал номини маълум қилишдир.

Маълум қилинган ном ҳақиқатан ҳам ҳақиқий ном эканлигига кафолат берилиши керак. Яъни, ўз номини маълум қилган объект, ҳақиқатан ҳам ўша объект эканлиги исботланиши керак. Бунинг учун *аутентификациядан* фойдаланилади.

Аутентификация – ўз идентификаторини маълум қилган субъект, ҳақиқатан ҳам ўзини маълум қилаётган, айнан ўша субъектлигига ишонч ҳосил қилиш жараёнидир.

Аутентификация сўзининг синоними сифатида кўпинча «ҳақиқийлигини текшириш» ибораси ишлатилади. Ўзининг ҳақиқийлигини тасдиқлаш учун кандайдир *аутентификатор* зарур бўлади.

Аутентификатор сифатида қуйидагилар ишлатилиши мумкин:

- қандайдир махфий ахборот (пароль, шахсий идентификацион номер, криптографик калит ва шу кабилар)
- қандайдир жисмоний объект, техник қурилма (электрон калит, шахсий карта, махсус плата)
- инсонни аутентификация қилиш учун унинг биометрик хусусиятларидан фойдаланиш мумкин (товуш, бармоқ излари, кўз қорачиғи тасвири ва шу кабилар).

Идентификациянинг энг оддий усули – фойдаланувчининг тизимга кириш учун паролини киритишдир. Фойдаланувчининг ҳақиқатан ҳам ваколатга эга эканлигини текшириш воситаси эса паролнинг тўғри ёки нотўғрилигини текшириш механизмидир.

Ишончли йўл фойдаланувчини хавфли компоненталарни хатлаб ўтиб, бевосита ишончли тизим базаси билан боғлайди. Ишончли йўл берилишидан максад – фойдаланувчига хизмат кўрсатувчи тизимнинг оригинал эканлигига ишонч ҳосил қилиш.

Қайд қилинган маълумотларни таҳлил этиш (аудит) тизимнинг хавфсизлигига қарши қаратилган ҳаракатлар ёки ҳодисаларни аниқлашда муҳим роль ўйнайди.

1.5.1. Хавфсизлик синфлари

АҚШ Мудофаа Вазирлигининг «Ишончли компьютер тизимларини баҳолаш мезонлари» ахборот тизимларининг хавфсизлик бўйича ишончлилик даражасини аниқлаш учун йўл очиб берди.

«Оранжевая книга»да ишончлиликнинг 4 поғонаси - D, C, B ва A белгиланган. D поғонаси ишончлилик даражаси паст ва талабга жавоб бермайдиган тизимлар учун мўлжалланган. Ишончлилкнинг C поғонасидан A поғонасига борган сари ахборот тизимларига бўлган талаблар ошиб бораверади. C ва B поғоналар мос равишда C1, C2, B1, B2, B3 синфларга

ажраладилар ва уларда ҳам ишончлилик даражасига бўлган талаблар ошиб бораверади.

Жами хавфсизликнинг 6 та синфи - C1, C2, B1, B2, B3, A1 мавжуд. Ахборот тизимининг хавфсизлик сиёсати ва кафолатланганлик даражаси қайси синфга қўйилган талаблар билан мос келса, уни ўша синфга тегишлилиги ҳақида сертификат берилади. Ҳар бир синф учун қандай талаблар қўйилади? Мисол тариқасида C1 синфига қўйиладиган талабларни кўриб чиқайлик.

C1 синфи: ишончли ҳисоблаш базаси ваколатга эга бўлган муайян фойдаланувчиларга муайян объектларга мурожаат қилиш имкониятини беришни Бошқариши зарур.

Ҳар бир фойдаланувчи ишончли ҳисоблаш базаси томонидан бошқариладиган тизимда бирор амални бажаришдан олдин ўзи кимлигини тизимга маълум қилиши керак. Фойдаланувчиларнинг кимлигини назорат қилиш учун қандайдир ҳимоя механизми, масалан, пароль билан ишлаш механизми ишлатилиши керак. Назорат қилишда ишлатиладиган ахборотлар ваколатга эга бўлмаган фойдаланувчилардан ҳимоя қилиниши керак.

Ишончли ҳисоблаш базаси ташқи таъсирлардан ҳимояланган ўз соҳасини қўллаб-қувватлаши лозим (хусусан, тизимдаги буйруқларни, унга тегишли маълумотларни ўзгартиришдан ҳимоялаш) ва тизимдаги иш жараёнини ваколатга эга бўлмаганлар томонидан кузатишдан ҳимояланган бўлиши зарур.

Ишончли ҳисоблаш тизимининг ташкил этувчи аппарат ва микродастурлардан иборат компонентларининг вақти-вақти билан тўғри ишлашини назорат қилувчи аппарат ёки дастурий таъминот мавжуд бўлиши керак.

Ҳимоя механизмлари тизим бўйича ишлаш ҳужжатларида белгиланган талаблар даражасида ишлаши назорат қилиниши зарур.

Назорат ваколатга эга бўлмаган фойдаланувчи учун бошқа усулларни қўллаб тизимга кириш имконияти йўқлигини тасдиқлаши керак.

Ҳимоя механизмларини ишлаб чиқувчи томонидан ишончли ҳисоблаш базасидан фойдаланиш ҳақида тафсилотлар хужжат кўринишида тайёрланган бўлиши керак.

А1 синфи (В3 синфидан юқори поғонадаги синф): назорат натижасида ишончли ҳисоблаш базаси юқори поғонадаги формал хусусиятларга мос келганлигини намойиш этиши керак.

Ҳужжатларда юқори поғонадаги формал хусусиятлар ҳам ёритилган бўлиши керак.

Формал хусусиятларнинг ва тизимни ўзини-ўзи текширишнинг замонавий методларидан фойдаланиш керак.

Хавфсизликни таъминлашда тизимнинг барча компоненталари ва унинг хаётий цикли учун конфигурацион бошқариш механизмидан фойдаланиш зарур.

Тизимдаги дастурлар матни билан формал хусусиятлар мослиги баён этилиши керак.

«Оранжевая книга»да берилган ахборот тизимларини ишончлилик даражаси бўйича синфларга ажратиш мезонлари ана шулардан иборат. Хулоса ўрнида уларни қуйидагича талқин этиш мумкин:

- С поғонаси – ахборотга мурожаат қилишни ихтиёрий равишда бошқариш;
- В поғонаси – ахборотга мурожаат қилишни мажбуран бошқариш;
- А поғонаси – ўзини-ўзи текширадиган ва хавфсизлик таъминланган ахборот тизими.

Албатта, «Ишончли компьютер тизимларини баҳолаш мезонлари»га нисбатан бир неча жиддий эътирозлар ҳам билдирилиши мумкин. Масалан, таксимланган тизимларда хавфсизлик муаммолари юзага келиши унда ҳисобга олинмаган. Шундай бўлса-да, «Оранжевая книга»нинг эълон қилиниши ахборот хавфсизлиги масалаларини ҳал этишда муҳим роль ўйновчи воқеа бўлди.

1.6. Ахборот хавфсизлигини таъминлашнинг маъмурий бўғини

1.6.1. Маъмурий бўғин мақсади, вазифалари ва мазмуни

Маъмурий бўғин ҳуқуқий ва дастурий-техник бўғинлар орасидаги оралиқ бўғиндир. Ҳуқуқий бўғинда қабул қилинган қонунлар, меъёрий ҳужжатлар, стандартлар маъмурий бўғинда ахборот хавфсизлигини таъминлашнинг комплекс тизимини амалда яратиш учун асос бўлиб хизмат қиладилар. Маъмурий бўғиннинг вазифаси ҳимояланадиган ахборот тизимлари хусусиятларини ҳисобга олган ҳолда ахборот хавфсизлигини таъминлашга қаратилган амалий чора-тадбирларни ишлаб чиқиш ва жорий этишдан иборатдир. Айнан маъмурий бўғинда хавфсизлик механизмлари ишлаб чиқилади ва бу механизмлар асосида дастурий-техник бўғин таркиб ташкил этилади.

Маъмурий бўғиннинг мақсади ахборот хавфсизлигини таъминлаш ишлари дастурини ишлаб чиқиш ва ахборот тизимидан фойдаланишнинг муайян ҳолатларида бу дастурнинг бажарилишини назорат қилишдир. Маъмурий бўғин мазмуни қуйидаги чора-тадбирлар ташкил этади:

1) хавфсизлик сиёсатини ишлаб чиқиш;
2) ахборот тизими ва унинг инфраструктурасига бўладиган таҳдидлар таҳлилини ўтказиш ва ҳалтисликларни аниқлаш;
3) ахборот хавфсизлигини таъминлаш механизмлари ва воситаларини танлаш.

1.6.2. Хавфсизлик сиёсатини ишлаб чиқиш

Хавфсизлик сиёсати – ахборотни тўплаш, қайта ишлаш ва тарқатишни ташкил этишга қаратилган қонунлар, қоидалар ва меъёрий ҳужжатлар асосида корхонанинг ахборот хавфсизлигини таъминлаш бўйича ишлаб чиқилган чора-тадбирлари мажмуидир.

Хавфсизлик сиёсатини ишлаб чиқиш ва шакллантириш ахборот хавфсизлигини таъминлаш режасини тузиб чиқиш демакдир. Бундай мақсадга эришиш учун корхонага хос бўлган ахборотлар, дастурий ва техник таъминот хусусиятларини ҳисобга олиш зарур.

Хавфсизлик сиёсатининг муҳим жиҳатларидан бири ҳар бир фойдаланувчининг хавфсизликни таъминлаш борасида ўз масъулиятини билишидир.

Хавфсизлик сиёсатини ишлаб чиқишнинг дастлабки босқичида хавф туғдирувчи, бўлиши мумкин таҳдидлар, уларнинг ўзаро боғлиқликлари, таҳдидлар натижасида кўриладиган зарар миқдори таҳлил қилиниши керак. Корхона ахборот тизимини қўллаб-қувватлашда ишлатиладиган барча объектлар, уларга бўлган талаблар аниқланиши керак. Бундай объектларга:

- компьютер техникаси қурилмалари, коммуникация воситалари;
- дастурий таъминот, операцион тизим, хизмат кўрсатувчи сервис дастурлар;
- тизимда киритиладиган ва қайта ишланадиган ахборотлар, маълумотлар базалари;
- тизим билан ишловчи фойдаланувчилар, персонал;
- техник воситалар ва тизим билан ишлашда фойдаланиладиган йўриқномалар, ҳужжатлар;
- тизим иши учун зарур бўлган материаллар – қоғоз, принтер картриджи, бўёғи, магнит дисклари ва шу кабилар киради.

Хавфсизлик сиёсатида қуйидаги таҳдидлар ҳисобга олиниши муҳим:

- ахборотга ёки тизимга рухсатсиз мурожаат қилиш;
- тизимга оид ҳужжатлар билан рухсатсиз танишиш;
- ахборот ва тизим компонеталари яхлитлиги бузилиши;
- хизмат кўрсатишдан воз кечиш.

Хавфсизлик сиёсатини ишлаб чиқишда ресурслардан фойдаланиш қоидалари, фойдаланувчининг ҳуқуқ ва мажбуриятлари, махфий ахборотлар билан ишлаш тартиблари эътиборга олиниши керак.

Хавфсизлик сиёсатини ишлаб чиқишнинг яна бир муҳим боскичларидан бири компьютер тизими ва ундаги сервисдан кимлар фойдаланишлари мумкинлигини аниқлаб олишдир. Ресурслардан фойдаланиш қоидалари барча фойдаланувчилар учун аниқланган бўлиши керак.

Хавфсизлик сиёсатини ишлаб чиқишда тармоқ доирасида хавфсизликни таъминлашда қўлланиладиган қуйидаги механизмлар алоҳида ҳисобга олиниши керак:

- шифрлаш механизмлари;
- ахборотларнинг криптографик ҳимояси;
- электрон рақамли имзодан фойдаланиш;
- мурожаатларни назорат қилиш;
- узатилаётган ахборотларнинг яхлитлигини таъминлаш;
- тармоқ объектларини аутентификациялаш;

Хавфсизлик сиёсатида дастурий таъминот учун муаллифлик ҳуқуқларига ва лицензион дастурларга бўлган муносабатлар ҳам тўлиқ ифодаланиши керак. Бундай дастурлардан тўғри фойдаланишни ташкил этиш, ноқонуний тарзда улардан нусха кўчириш, фойдаланувчилар томонидан ўзгартириш, модификация қилиш ман этилиши белгиланиши керак.

Хавфсизлик сиёсатида белгиланган тартиб-қоидалар бузилган ҳолда унга қарши қўлланиладиган чора-тадбирлар режаси асосида иш кўриш хавфсизликни самарали таъминлаш имконини яратади.

Бузилиш ҳолатлари юзага келганда қуйидагиларни ҳисобга олиш тавсия этилади:

- бузилган маълумотларни тиклаш ва сақлаш;
- тизим учун хизмат кўрсатувчи сервисни тиклаш ва йўлга қўйиш;
- нима учун бузилиш ҳолати юзага келгани сабабини таҳлил қилиш;

- бузғунчилик ҳаракатларини чеклаш ва келгусида уларнинг такрорланмаслиги учун чоралар қўллаш;
- бундай ҳолатларни кенг фойдаланувчилар ва ташқи ҳамкорлар учун ошкор қилмаслик;
- жавобгарларни аниқлаш;
- бузғунчиларни белгиланган тартибда жазолаш.

Шу тариқа ишлаб чиқилган хавфсизлик сиёсатига амал қилиниши учун бузғунчилик содир этилишига қарши амалда қўлланиладиган дастурий-техник воситалар кўлами, улардан фойдаланиш кўрсатмалари ишлаб чиқилиши керак. Таҳдидларни олдиндан аниқлаш, улар ҳақида ўз вақтида огоҳлантириш ва бартараф этишга мўлжалланган дастурий-техник воситалар таъминоти хавфсизлик сиёсатига амал қилишда муҳим роль ўйнайди. Шу билан бирга дастурий-техник воситалардан усталик билан фойдаланишда ҳар бир фойдаланувчи етарли кўникма ва малакаларга эга бўлиши ахборот хавфсизлигини ишончли таъминлаш имконини янада оширади.

Ишлаб чиқилган хавфсизлик сиёсатини амалда самарали жорий этилиши унинг соддалиги ва тушунарлилиги билан боғлиқдир. Шу билан бирга уни вақти-вақти билан қайта кўриб, такомиллаштириш мақсадида таҳрирлаб чиқиш керак бўлади.

1.7. Ахборотга бўладиган таҳдидларнинг кенг тарқалган турлари

1.7.1. Асосий тушунчалар

Таҳдид деганда кимларнингдир манфаатларига зиён етказувчи рўй бериши мумкин бўлган воқеа, таъсир, жараён тушунилади. Ахборотга ёки ахборот тизимига салбий таъсир этувчи потенциал рўй бериши мумкин бўлган воқеа ёки жараён *ахборот муносабатлари субъектлари манфаатларига қаратилган таҳдид* деб аталади.

Таҳдидни амалга оширишга қаратилган ҳаракат *ҳужум* деб аталади. Ҳужум уюштирувчи эса *бузғунчи* деб аталади. Потенциал бузғунчилар *таҳдид манбаи* деб аталади.

Ахборот тизимларидаги заифликларнинг мавжудлиги турли хил таҳдидларни келтириб чиқаради (масалан, муҳим бўлган қурилмалардан бегона, ваколати бўлмаган шахсларнинг фойдаланиши ёки дастурий таъминотдаги хатоликлар).

Заифликлар маълум бўлган вақтдан то уларни бартараф этилгунга қадар бўлган вақт оралиғи *хавфли дарча* дейилади. Хавфли дарча мавжуд экан, ахборот тизимига бўлган таҳдид муваффақиятли амалга оширилиши турган гап.

Агар гап дастурий таъминот ҳақида борса, у ҳолда хавфли дарча хатоликлардан фойдаланиш воситалари ёрдамида очилиб, камчиликлар ва хатоликлар бартараф этилганидан сўнггина ёпилади.

Ахборот тизимларидаги кўпгина заифликлар учун хавфли дарча давомийлиги узоқ вақтга чўзилади (бир неча кун, баъзида бир неча ҳафта). Сабаби бу вақт оралиғида қуйидаги ҳодисалар рўй бериши муқаррар:

- ахборот тизими хавфсизлигидаги заифликлардан ва бўшлиқлардан фойдалана оладиган воситаларнинг маълум бўлиши;
- бу воситалардан фойдаланишга тўсқинлик қилувчи ва заифликларни бартараф этувчи восита ва ишланмаларнинг яратилиши;
- восита ва ишланмаларнинг ҳимояга муҳтож бўлган ахборот тизимига жорий этилиши.

Ахборот тизимидаги заифликлар ва бу заифликлардан фойдаланувчи воситалар доимий равишда намоён бўладилар. Демак, хавфли дарча ҳар доим мавжуд ва уни ёпиш тезлик билан фавқулодда чоралар ишлаб чиқилишини тақозо этади.

Шуни айтиб ўтиш керакки, баъзи таҳдидлар тизимдаги хатолик ёки нотўғри ташкил этилган фаолият оқибатида эмас, балки табиий, объектив тарзда келиб чиқадилар. Масалан, электр таъминоти узилиши ёки кучланишнинг пасайиши ёки чегарадан ошиб кетиши билан боғлиқ таҳдидлар

ахборот тизимининг бевосита аппарат қурилмалари ишига боғлиқлигидан келиб чиқадилар.

1.7.2. Таҳдидларни синфларга ажратиш мезонлари

Ҳозирги замон ахборот тизимларига хавф туғдирувчи кенг тарқалган таҳдидлар билан танишиб чиқайлик. Таҳдидларнинг келиб чиқиши, уларнинг сабаби, ахборот тизимидаги заифликлар ҳақида тасаввурга эга бўлиш кам чиқимли ахборот хавфсизлигини таъминловчи воситалар билан қуролланиш имконини беради. Ахборот технологиялари соҳасида таҳдидлар, ҳужумларга оид нохуш маълумотлар кўплаб мавжуд. Уларнинг келиб чиқиш сабаблари ва хусусиятларини билмаслик таҳдидлардан ҳимояланиш чораларини ишлаб чиқишда ортиқча харажатлар сарфланишига олиб келиши мумкин.

Умуман «таҳдид» тушунчаси турли ҳолатларда турлича талқин этилиши мумкин. Масалан, очиқ кўринишда фаолият кўрсатувчи корхона учун ахборотнинг махфийлигини ошкор қилишга қаратилган таҳдид муаммоси умуман бўлмаслиги мумкин. Чунки бундай корхонада ахборотларга барча фойдаланувчилар мурожаат қилишлари мумкин. Лекин баъзи ваколати бўлмаган шахсларнинг корхона ахборотларидан фойдаланишлари жиддий хавф келтириб чиқариши мумкин. Бошқача қилиб айтганда, таҳдид ахборот муносабатлари субъектларининг манфаатларидан келиб чиққан ҳолда вужудга келади ва улар билан боғлиқ бўлади.

Таҳдидларни қуйидаги мезонлар асосида синфларга ажратиш мумкин:

- ахборот хавфсизлигининг асосий ташкил этувчиларига нисбатан бўладиган таҳдидлар (ахборотга мурожаат қилиш имкониятига қарши, ахборотнинг яхлитлигини бузишга қаратилган, ахборотнинг махфийлигини ошкор қилишга қаратилган таҳдидлар);

- ахборот тизимининг ташкил этувчиларига нисбатан бўладиган таҳдидлар (берилган малумотлар, дастурлар, аппарат қурилмалари ва тизимни қўллаб-қувватловчи инфраструктура);
- таҳдидни амалга ошириш усули бўйича (табиий, техноген, тасодифий, ғаразли максадда);
- таҳдид манбаининг ахборот тизимига нисбатан жойлашган ўрни бўйича (ички ёки ташқи).

1.7.3. Таҳдидларнинг кенг тарқалган турлари

Келтирадиган зарар миқдори нуқтаи-назаридан энг хавфли ва тез-тез бўладиган таҳдидлар ахборот тизимига хизмат кўрсатувчи корхона ходимлари (оператор, мухандис, тизим маъмури ва бошқалар) томонидан йўл қўйилган хатоликлар натижасида келиб чиқадиган таҳдидлардир.

Баъзида бундай хатоликлар бевосита таҳдидни келтириб чиқаради (нотўғри киритилган маълумот, дастурдаги хатолик, тизимдаги хатолик) ва гоҳида улар тизимдаги заифликларни келтириб чиқарадилар. Баъзи маълумотларга кўра кўрилган зарарларнинг 65% и мана шундай хатоликлар туфайли келиб чиққан.

Ёнғинлар ва сув тошқинлари туфайли ахборот тизимларига етказилган зарар миқдори саводсизлик ва масъулиятни ҳис этмаслик туфайли кўрилган зарар миқдоридан кам бўлса-бўладики, лекин ортиқ эмас.

Тасодифий ёки кўр-кўрона хатоликлар олдини олишнинг энг қатъий усули – ишни максимал даражада автоматлаштириш ва қатъий назорат. Бошқа кенг тарқалган таҳдидлар қуйидагилар натижасида келиб чиқадилар:

- фойдаланувчиларнинг воз кечишлари;
- ахборот тизимининг ички носозлиги;
- ахборот муносабатларини қўллаб-қувватловчи инфраструктуранинг рад этиши.

Фойдаланувчиларнинг воз кечишлари натижасида келиб чиқадиган таҳдидлар қуйидаги ҳолатларда намоён бўлиши мумкин:

- ахборот тизими билан ишлаш ҳохишининг йўқлиги (кўпинча янги турдаги тизим жорий этилганида, янги техникага мослаштирилган технологияларнинг жорий этилиши натижасида ёки фойдаланувчи сўрови бўйича керакли маълумотлар олишнинг иложи йўқлиги);
- тизим билан ишлаш учун касбий тайёргарлик савияси пастлиги (компьютер саводининг етарли даражада эмаслиги, критик ҳолатлардан чиқиб кета билмаслик, тизимга оид ҳужжатлар билан ишлаш кўникмасининг йўқлиги ва ҳ.к.);
- тизим билан ишлаш учун нормал шароитнинг йўқлиги (техник ҳужжатларнинг етарли эмаслиги, тизимда ишлатиладиган ахборотлар структураси ва уларни қайта ишлаш технологияси босқичларининг мукаммал ёритилмаганлиги).

Ахборот тизимидаги ички носозликларнинг асосий сабаблари:

- белгиланган тартиб ва қоидаларга риоя қилмасдан (тасодифий ёки ғаразли) ишлаш;
- фойдаланувчиларнинг ёки персоналнинг атайлаб ёки тасодифан ҳаракатлари туфайли тизимнинг ишдан чиқиши (бир вақтнинг ўзида кўплаб сўровлар берилиши, қайта ишланадиган маълумотлар ҳажмининг меъёридан ортиқлиги ва ҳ.к.);
- тизим параметрларини белгилашда ёки қайта ўзгартиришда рўй берадиган хатоликлар ва носозликлар;
- дастурий ва техник таъминотдаги узилиш ва носозликлар;
- ташқи хотирада сақланаётган маълумотларнинг бузилиши;
- аппаратура қурилмаларининг бузилиши ёки носозлиги.

Ахборот муносабатларини қўллаб-қувватловчи инфраструктуранинг рад этиши қуйидаги ҳолатларда вужудга келиши мумкин:

- алоқа, электр таъминоти, сув ва иссиқлик таъминоти, совутиш тизимларидаги носозликлар (тасодифий ёки атайлаб ташкил этилган);

- хоналар ва улардаги жиҳозларнинг бузилиши, авария ҳолатига келиши;
- хизмат кўрсатувчи персоналнинг нормал шароитда ишлаши учун шароитнинг йўқлиги ёки уларнинг ўз вазифаларидан воз кечиши (фукаролик тартибсизликлари, транспортдаги авария ҳолатлари, террористик ҳаракатлар ёки иш ташлашлар ва ҳ.к.).

Корхонадан «хафа» бўлган ходимлар (фаолият кўрсатаётган ва собиқ) айниқса, жуда катта хавф туғдирадилар. Улар одатда ўзларини хафа қилган корхонадан ўч олиш мақсадида зарар етказишга ҳаракат қиладилар. Масалан:

- қурилмалар ишини бузадилар;
- дастурий таъминотдаги айрим дастурларга атайлаб шундай буйруқлар кетма-кетлигини киритадиларки (маълум вақтдан кейин портлайдиган дастурий «бомба»), натижада кейинчалик, бу кетма-кетлик ишга тушиб тизимни ёки маълумотлар базасини ишдан чиқаради;
- ташқи хотирада сақланаётган ахборотларни атайлаб ўчириб юборадилар.

«Хафа» бўлган ходимлар ички тартиб-қоидалар билан таниш бўлган ҳолда катта зарар етказишлари мумкин. Айниқса, бундай ходимлар ишдан бўшаётганларида уларга берилган тизимга кириш ваколати (пароль, тизимдаги дастурлар ёки маълумотлардан фойдаланиш ҳуқуқи) бекор қилиниши устидан назорат олиб бориш керак.

Табиий офатлар, албатта, таҳдидлар келтириб чиқарадилар. Статистик маълумотларга кўра сув тошқини, ёнғин, зилзила ва кучли бўрон каби табиий офатлар натижасида ахборот тизимларида кўрилган моддий зарар улуши барча зарарларнинг 13% ини ташкил этар экан.

1.7.4. Ахборотга мурожаат қилиш имкониятига қарши қаратилган таҳдидлар

Ахборотга мурожаат қилиш имкониятига қарши қаратилган таҳдидлар аппарат қурилмаларининг носозлиги ёки кўпинча уларнинг бузилиши натижасида вужудга келадилар. Бундай носозликлар табиий равишда (кўпинча

кучли момақалдироқ туфайли) намоён бўладилар. Афсуски, ҳозирги замон кучланишни узлуксиз етказиб берувчи электр манбалари ҳам бундай ҳолатларда панд бермоқдалар. Қудратли қисқа тўлқинли импульслар таъсирида қимматбаҳо аппаратуранинг ишдан чиқиш ҳоллари кўплаб рўй берган.

Сув қувурлари ва иситиш тармоқлари носозлиги туфайли сув тошиши ҳолатлари таҳдидларга сабаб бўладилар. Ҳозирги пайтда кўпгина ташкилот ёки фирмалар жой масаласида иқтисод қилиш мақсадида ижарага эски бино ва хоналарни олиб фаолият кўрсатмоқдалар. Улар номигагина жойларни таъмирлаб, чириган қувурларга эътибор бермайдилар. Бирдан иссиқ сув қувури ёрилиб, ундан жуда катта босим остида сув оқаётганидагина ёқа ушлаб қоладилар.

Кун қизиган ёз паллаларида совутиш тизимида кондиционерларнинг ишдан чиқиши корхона учун қимматга тушиши турган гап. Бундай ҳолатларда сақланаётган маълумотларнинг нусхасини бошқа ташқи хотира воситасига кўчириб ёзиб қўйиш яхши самара беради. Лекин заҳира нусхалар сақланиши тартиби кўпол равишда бузилиши жиддий оқибатларга олиб келади.

Тизимни ишлаб турган ҳолатида ишдан чиқарувчи восита сифатида ресурслардан агрессив равишда истеъмол қилишни талаб этувчи сўровлар ишлатилиши мумкин. Бундай сўровлар кетма-кет берилиши натижасида тармоқда сигналларни ўтказиш имконияти сустлашади ёки процессор қурилмасида бирданига бажариладиган масалалар рўйхати кўпайиб кетади. Таҳдид манбаи жойлашишига қараб бундай сўровлар маҳаллий ва масофадан узатиладиган турларга ажралади. Маҳаллий сўров бажарилиши натижасида процессор бу сўров масаласини ечиш билан банд бўлиб, бошқа керакли дастур ишини бажарилишини секинлаштиради.

Масофадан узатиладиган сўровга, масалан, «SYN- тошқини» номли ҳужумни келтириш мумкин. Бундай сўров берилиши натижасида сервер компьютердаги TCP-уланишлар учун мўлжалланган жадвал тўлиб кетиб, бошқа абонентлар серверга мурожаат қилиш имконидан маҳрум бўлганлар.

«Papa Smurf» номли ҳужумда эса тармоқнинг заиф жойидан кетма-кет ping-пакетлар кенг кўламдаги адреслардан келиб тушиб, уларга бирданига жавоб йўллаш эса, бошқа пакетлар ишига тўсқинлик қилган.

Кейинги пайтларда масофадан узатиладиган сўровлар уюшган ҳолда бирданига бир неча адреслардан юборилиши ҳолатлари кузатилмоқда. Бунинг натижасида йирик-йирик электрон тижорат тизими серверлари иши «осилиб» қолиб, бошқа абонентлар учун ахборотга мурожаат қилиш имконияти йўққа чиқарилмоқда.

Компьютер аппарат қурилмаларидаги ва дастурий таъминотдаги хатоликлардан фойдаланиб, ваколати бўлмаган фойдаланувчи маълум буйруқлар асосида процессор ишини тўхтатиб қўйиши мумкинки, уни давом эттириш учун RESET тугмаси босилишидан бошқа чора йўқ.

1.7.5. Ахборотнинг яхлитлигини бузишга қаратилган таҳдидлар

Ахборотга бўладиган таҳдидларнинг кенг тарқалганлари орасида тасодифий хатоликлар ва заифликлардан келиб чиқадиган таҳдидлардан сўнг иккинчи ўринда ўғирлик ва товламачилик асосида бўладиган таҳдидлар туради. 2006 йилда шахсий компьютердан фойдаланиб бундай ноконуний ҳаракатлар натижасида дунё миқёсида компаниялар 8,5 миллиард доллар зарар кўрганлар. Реал зарар миқдори, албатта, бундан кўп бўлган. Кўпгина компаниялар ўзлари томонидан кўрилган зарар миқдорини камайтириб кўрсатишгани тушунарли ҳол.

Кўпгина ҳолларда компаниянинг ўз ходимлари томонидан бундай ҳаракатлар амалга оширилган. Демак, ички таҳдид нақадар хавфли эканлигига ишонч ҳосил қилиш мумкин.

Ахборотнинг статик яхлитлигини бузиш мақсадида бузғунчи қуйидаги ҳаракатларни амалга ошириши мумкин:

- нотўғри маълумотлар киритиши;
- маълумотларга ўзгартиришлар киритиши.

Баъзида бундай ҳаракатлар натижасида маълумотларнинг маъноси тубдан ўзгартирилса, баъзида расмий ҳужжат кўринишидаги маълумотлар атайлаб бўрттирилган ёки бузилган ҳолда киритилиб, сақланади. Ахборотнинг статик яхлитлигига оид мисол тариқасида Oracle корпорациясида бўлган воқеани келтириш мумкин. Корпорация вице-президентининг котибаси судга ўзининг ноҳақ равишда ишдан бўшатилганини даъво қилиб мурожаат қилган. Унинг айтишича, у корпорация президенти билан яқин муносабатда бўлишдан бош тортганлиги учун турли баҳоналар билан ишдан бўшатилган. Исбот тариқасида вице-президент номидан президентга йўлланган электрон хатни тақдим этган. Хатни маъноси қандай бўлишидан қатъий назар суд унинг йўлланган вақтини таҳлил қилиб, ўрганиб чиққан. Вице-президент судда хат жўнатилган вақтда ўз иш жойида бўлмаганлигини маълум қилган ва буни тасдиқлаш мақсадида уяли алоқа компаниясининг қайд қилинган файлини тақдим этади. Бу файлда ҳақиқатан ҳам вице-президент электрон хат жўнатилган вақтда ўз иш жойидан узоқда мобиль телефони орқали сўзлашганлиги қайд қилинган. Котиба вице-президент электрон почта кутисига кириш паролини билганлиги ва электрон хат қалбакилаштирилганлигини аниқлаб, суд унинг даъво аризасини бекор қилади.

Юқоридаги мисолдан келиб чиққан ҳолда, ахборот яхлитлигини бузишга қаратилган таҳдид билан бирга компьютер маълумотларига кўр-кўрона ишониш ҳам нақадар хавфли эканлигини хулоса қилиб айтиш мумкин. Электрон хатдаги сарлавҳа ўзгартирилиши, хатнинг ўзи эса жўнатувчининг паролини билган бузғунчи томонидан қалбакилаштирилиши мумкин.

Нафақат хатларни ўзгартириш ва қалбакилаштириш, балки амалга оширилган ҳаракатни инкор этиш ҳам ахборот яхлитлигини бузишга қаратилган таҳдид бўлади. Агар аниқ далиллар бўлмаса, компьютер маълумотлари исботловчи ашё сифатида ишлатилиши мумкин эмас.

Фақатгина маълумотлар яхлитлигини эмас, балки дастурларнинг ҳам яхлитлигини бузишга қаратилган таҳдидлар ҳам бўлиши мумкин.

Динамик яхлитликни бузишга қаратилган таҳдидлар натижасида электрон тижоратдаги олди-сотди билан боғлиқ бўлган ахборотлар бузилиши, қайта тартибланиши, ўғирланиши ва нусхаси кўпайтирилиши, қўшимча маълумотлар билан тўлдирилиши ҳолатлари вужудга келиши мумкин. Бунда бузғунчилар тармоқ микёсида тармоқ пакетлари жўнатилишини кузатиб, жосусларга хос ҳаракат қиладилар.

1.7.6. Ахборотнинг махфийлигини ошкор қилишга қаратилган таҳдидлар

Махфий ахборотларни маълум соҳага оид ва хизмат доирасига оид турларга ажратиш мумкин. Хизмат доирасига оид (масалан, фойдаланувчилар пароли) ахборот муайян соҳага тегишли бўлмаган маълумот бўлиб, ахборот тизимида техник роль ўйнайди, бироқ бундай маълумотни ошкор қилиш жуда ҳам катта хавф туғдиради. Сабаби, ундан фойдаланиб тизимдаги маълумотларга мурожаат қилиш ва соҳага оид бўлган махфий ахборотларга ҳам эга бўлиш имкони яратилади.

Компьютер хотирасида сақланаётган ахборот фақат компьютер соҳасига тегишли бўлса ҳам, унинг махфийлигини ошкор қилишга қаратилган таҳдидлар хусусияти умуман бошқача бўлиши мумкин.

Кўпгина фойдаланувчилар ўз фаолиятларида бир неча дастурий тизимлар билан ишлайдилар. Ҳар бир тизимга кириш учун эса пароль тизими ишлаб чиқилган бўладики, фойдаланувчи ҳар бир паролни эсга олиб, тўғри киритиши талаб этилади. Эсдан чиқариб қўймаслик учун эса кўпинча ён дафтарчага ёки оддий қоғоз саҳифасига парольларни ёзиб сақлаб қўядилар. Лекин бундай ҳолатларда бепарволикка берилиб, пароль маълумотлари бегоналарнинг қўлига тушиб қолиши ҳеч гап эмас. Пароль тизимидаги номларни тизим администратори томонидан тез-тез алмаштириб турилиши эса фойдаланувчиларни чалғитиши ва бундай ҳолат ҳаттоки тизимга мурожаат қилиш имкониятидан маҳрум бўлишларига олиб келади. Бундай заифликларни «махфий маълумотларни хавфсизлик таъминланмаган муҳитга жойлаштириб,

сақлаш», деб аташ мумкин. Қоғоздаги пароль ҳақидаги маълумотлардан ташқари муҳим махфий ахборотлар очиқ кўринишда (суҳбат, хат, тармоқ орқали) қизиқувчи шахсларга маълум бўлиб қолиши ҳам мумкин. Қизиқувчи шахслар бунда турли воситаларни (эшитиш тизими, видеоназорат, тармоқни кузатиш тизимлари ва ҳ.к.) ишга солишлари мумкин. Мақсад – махфий ахборотларни қўлга киритиб, ундан ғаразли мақсадларда фойдаланиш.

Маълумотларни эгаллаб олишга қаратилган таҳдид ахборот тизимларини ўрнатиб, уларнинг параметрларини созлаш жараёнидан, то уларни жорий этилгунга қадар вақт оралиғида солиниши мумкин. Хавфли таҳдидлардан яна бири расмий кўргазмадир. Чунки компания ўзининг тармоққа уланган компьютер жиҳозларини унда сақланаётган ахборотларига парво қилмай, ҳеч бир ўзгаришсиз кўргазмада намойиш қилиш учун юборадилар. Қизиқувчан кўргазма иштирокчилари эса вазиятдан фойдаланиб, керакли ахборотларни қўлга киритишга ҳаракат қиладилар.

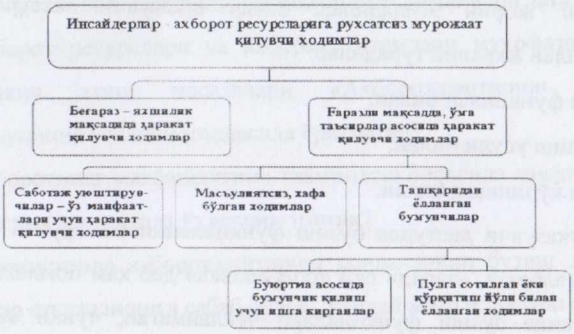
Яна бир хавф солувчи таҳдидлардан бири – маълумотларнинг заҳира нусхасини яратиб, унга бефарқ қарашдир. Шкаф ёки стол тортмасида қаровсиз қолдирилган бундай нусхани дарҳол қизиқувчилар илиб кетишлари мумкин.

Маълумотларни эгаллаб олиш – жиддий таҳдидлардан биридир. Агар махфий маълумотлар бир вақтнинг ўзида бир неча алоқа каналлари бўйича узатиладиган бўлса, уларнинг махфийлигини таъминлаш мураккаб ва катта харажатни талаб этади. Ҳозирги вақтда ахборотни эгаллаб олиш воситалари мукаммал ишланган, фойдаланишда қулай ва содда бўлганлиги билан хоҳлаган бузғунчи учун тармоққа суқилиб ўрнатиш имкониятини яратади. Бундай кўринишдаги ташқи таҳдидларга ҳам жиддий эътибор қаратиш керак.

1.7.7. Ички ва ташқи таҳдидлар

Барча таҳдидларни ички ва ташқи таҳдидларга ажратиш мумкин. Ички таҳдидларга ходимларнинг масъулиятсизликлари, саботаж ва молиявий товламачилик каби таҳдидлар, ташқи таҳдидларга эса вируслар, хакерлар, спам,

тармоқларга рухсатсиз кириш каби таҳдидлар кирадилар. Ички таҳдидлар асосан инсайдерлар - корхонада фаолият кўрсатаётган ходимлар ҳаракатлари туфайли юзага келадилар (1.1-расм).



1.1-расм. Инсайдерларнинг туркумланиши.

Ички ва ташқи таҳдидлар нисбати 2006 йилда ички таҳдидлар барча таҳдидларнинг 56,5% ини ташкил этган, ташқи таҳдидлар эса 43,5% ни ташкил этган (1.2-расм).

1.2-расм. Ички ва ташқи таҳдидлар фоизлардаги нисбати (Манба : InfoWatch, 2006).

1.7.8. Бошқа таҳдидлар

Хавфли ҳужум уюштириш мақсадида компьютер тизимига зарар етказувчи дастурларнинг жорий этиладилар. Зарар етказувчи дастурлар қуйидаги жиҳатлари билан ажралиб турадилар:

- бузиш функцияси билан;
- тарқалиш усули билан;
- ташқи кўриниши билан.

Зарар етказувчи дастурда бузиш функциясини бажарувчи қисм «бомба» деб аталади (албатта, «заряд» ёки «боеголовка» деб ҳам номлаш мумкин эди). Умуман олганда бузиш функциялари чекланмаган, чунки «бомба» бошқа дастурлар каби мантиқан мураккаб буйруқлар кетма-кетлигидан иборат бўлиб, унинг асосий вазифаси қуйидагилардан иборат бўлиши мумкин:

- Бошқа зарар етказувчи дастурни тизимга жорий этиш;
- ҳужум қилинаётган тизим устидан тўлиқ назорат қилишни ўз зиммасига олиш;
- ресурслардан агрессив тарзда фойдаланиш;
- ишлаб турган дастурларни ёки қайта ишланаётган маълумотларни бузиш.

Қурилмаларни ёки ташқи хотира воситаларини ўғирлаш ҳам ахборотга бўладиган таҳдидларга киради. Кўпгина ҳолларда дискларни, ҳаттоки портатив компьютерларни қаровсиз қолдирилиши ундаги маълумотларнинг йўқотилишга олиб келади.

Ўз ваколатини суистеъмол қилиш натижасида ҳам ахборотга таҳдид солиниши мумкин. Масалан, тизим администратори ўз ваколати доирасида бошқа фойдаланувчилар файлларига, почта қутисига кириш имконига эга бўлади. Бу эса, баъзи ҳолларда нохуш оқибатларга олиб келади.

Назорат учун саволлар :

1. Ахборот хавфсизлиги деб нимага айтилади?
2. Ахборот хавфсизлиги асосий ташкил этувчилари нималардан иборат?

3. Ахборотнинг статик яхлитлиги деганда нима тушунилади?
4. Ахборотнинг динамик яхлитлиги деганда нима тушунилади?
5. Ахборотнинг яхлитлигини таъминлаш нимани англатади?
6. Ахборотнинг махфийлигини таъминлаш нимани англатади?
7. Ахборот ресурслари ва ахборот тизимлари мухофаза қилинишини ташкил этиш масалалари «Ахборотлаштириш тўғрисида»ги Қонуннинг нечанчи моддасида ёритилган?
8. Ахборотнинг махфийлигини таъминлаш борасида давлат манфаатлари қайси ҳужжатларда ўз аксини топган?
9. Ўзбекистонда ахборотлаштириш қоидаларини бузиш анча миқдорда зарар етказилишига сабаб бўлса, қандай жазо чоралари кўрилади?
10. Ўзбекистонда тегишли рухсатсиз компьютер вируслари ёки унга хос дастурларни ишлаб чиқиш ва тарқатиш ҳолати қайд қилинса, қандай жазо чоралари кўрилади?
11. Ахборот хавфсизлигида «хавфсизлик сиёсати» деганда, нима тушунилади?
12. Ахборот хавфсизлигида кафолатланганлик даражаси деганда нима тушунилади?
13. Хавфсизликни таъминлашда баённомалар юритишдан мақсад нима?
14. «Оранжевая книга»да ишончлиликнинг қайси поғоналари келтирилган?
15. Аудентификация ёрдамида нималар амалга оширилади?
16. Ахборот хавфсизлигини таъминлашда қайси бўғиндаги чора-тадбирлар муваффақият келтиради?
17. Ахборот тизимларида ахборот хавфсизлигини таъминлашга оид раҳбарият томонидан қабул қилинган чора-тадбирлар қайси бўғинга тегишли?
18. Ҳуқуқий бўғиндаги чекловчи чора-тадбирларга қандай чора-тадбирлар киради?
19. Хавфсизлик сиёсатининг мазмунини нималар ташкил этади?

20. Ахборот муносабатлари субъектлари манфаатларига қаратилган таҳдид деб, нимага айтилади?
21. Ахборот хавфсизлигининг асосий ташкил этувчиларига нисбатан бўладиган таҳдидларни аниқланг.
22. Ахборот тизимининг ташкил этувчиларига нисбатан бўладиган таҳдидларни аниқланг.
23. Амалга ошириш усули бўйича бўладиган таҳдидларни аниқланг.
24. Энг хавфли ва тез-тез бўладиган таҳдидларни аниқланг.
25. Зарар етказувчи дастурлар қайси жиҳатлари билан ажралиб турадилар?

II боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ДАСТУРИЙ ВА ТЕХНИК ВОСИТАЛАРИ

2.1. Дастурий ва техник воситалардан фойдаланиш йўналишлари

Дастурий ва техник воситалар ахборот хавфсизлиги тизимининг техник асосини ташкил этади. Бундай воситаларни жорий этиш жойларда қабул қилинган ахборот хавфсизлиги сиёсатидан, меъёрий-услубий ҳужжатлардан келиб чиққан ҳолда мос ташкилий бўлимлар томонидан амалга оширилади.

Дастурий ва техник воситалар ахборот хавфсизлигини таъминлашда қуйидаги йўналишларда фойдаланилади:

- корпоратив тизимлар объектларини ҳимоя қилишда;
- ахборотни қайта ишлашда қўлланиладиган жараёнлар, дастурларни ҳимоя қилишда;
- алоқа каналларини ҳимоя қилишда;
- кераксиз ва халақит қилувчи электромагнит нурларини бартараф этишда;
- хавфсизлик тизимини бошқаришда.

Ҳимоя воситалари дастурий методлар ва воситалар, аппарат воситалари, ҳимоялашнинг алмаштириш усуллари, ҳамда ташкилий тадбирлар тўпламини ўз ичига олади.

Аппарат воситалари ва схемалар ёрдамида ҳимоя қилишнинг моҳияти шундан иборатки, махсус техник ишланмалар асосида ахборотни қайта ишловчи қурилмалар ва воситаларда ахборотни назорат қилиш ва ҳимоя қилишни таъминлаш амалга оширилади. Электромагнит нурларини бартараф этувчи қурилма ёки ахборот тизимидаги турли қурилмалар ўртасида ахборот алмашинувини назорат қилувчи схемалар буларга мисол бўла олади.

Дастурий воситалар – алгоритм ва дастурлар тўпламидан иборат бўлиб, ахборотга, тизимга рухсатсиз мурожаат қилишнинг олдини олиш, ахборот яхлитлиги ва махфийлигини таъминлашда ишлатиладилар.

Ҳимоялашнинг алмаштириш усуллари моҳияти шундаки, тизимда сақланаётган ахборот алоқа линиялари бўйича узатилишида маълум қоидага кўра кодлаштирилиб, ундан очиқ ҳолда бевосита фойдаланиш имконияти баратараф этилади.

Ташкилий тадбирлар ахборот тизимидаги жараёнларда ва дастурлардан фойдаланишда фаолият кўрсатувчи персонални танлаш ҳамда назорат қилиш, ахборотни қайта ишлаш жараёнларининг тартиб-қоидаларига қатъий риоя қилинишини таъминлаш каби тадбирларни ўз ичига олади.

Фақат ҳимоянинг турли воситалари ва чора-тадбириларидан комплекс фойдаланилгандагина ишончли ҳимояни таъминлаш мумкин. Негаки, ҳар бир восита ёки услуб ўзига хос ютуқ ва камчиликларига эга бўлиши мумкин.

2.2. Ахборот хавфсизлигини таъминлаш воситалари

Умуман ахборот хавфсизлигини таъминлашда қуйидаги воситалар ишлатилади:

- ахборотга рухсатсиз мурожаат қилишдан ҳимоя қилиш воситалари;
- ахборот оқимини таҳлил қилувчи ва моделлаштирувчи тизимлар (CASE-тизимлар);
- тармоқ мониторинги тизимлари;
- баённомаларни таҳлил этувчи анализаторлар;
- антивирус воситалари;
- тармоқлараро ҳимоя экранлари;
- криптографик воситалар;
- ахборотларнинг резерв нусхасини кўчириш тизимлари;
- узлуксиз кучланиш билан таъминловчи тизимлар;
- аутентификация тизимлари;
- аппаратура қурилмалари корпусларини ечиш ва бузишга қарши воситалар;
- хоналарга киришни назорат қилувчи воситалар;

• ҳимоя тизимини таҳлил этувчи ускунавий воситалар.

Бу воситалардан мос равишда фойдаланиш ахборот тизимларида ахборот хавфсизлигини таъминлашда муҳим роль ўйнайди. Булардан айримларини кўриб чиқайлик.

2.3. Криптографик усуллар ёрдамида ахборот хавфсизлигини таъминлаш

Махфий ахборотларнинг хавфсизлигини таъминлашда стеганографик ва криптографик усуллар қўлланилади. Стеганография сўзи грекча **steganos** (махфий, сир) ва **graphy** (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стеганографик усуллар ёрдамида ахборот мавжудлиги яширилади.

Компьютер стеганографияси ёрдамида ҳозирги вақтда дастурий таъминотни ниқоблаш, муаллифлик ҳуқуқларини ҳимоялаш ишлари амалга оширилмоқда. Масалан, график тасвирга шундай белги киритиладики, у кўздан яширилган ҳолда жойлаштирилади. Бу белги фақат махсус дастурий таъминот орқали аниқланиши мумкин. Стеганографиянинг ушбу йўналиши нафақат тасвирларни, балки аудио ва видеоахборотларни рухсатсиз нусхасини кўчиришдан ҳимоялашда қайта ишлашда қўлланилади.

Криптография сўзи грекча **kryptos** - сирли, **graphy** – ёзувни тасвирлаш сўзларидан келиб чиққан ва «яшириш, ёзувни беркитиб қўймоқ» маъносини билдиради. Криптографик усуллар ёрдамида махфий ахборот махсус алгоритм бўйича шифрланиб, унинг кўриниши ўзгартирилади ва шу тариқа бузғунчиларнинг ахборотга рухсатсиз мурожаат қилиш имкониятлари чекланади.

Одатда ахборотнинг маъносини яшириш учун ахборот маълум калит асосида шифрланади. Шифрлаш деганда бошланғич матнни маълум алгоритм асосида матн маъносини англаб бўлмайдиган кўринишдаги матнга алмаштириш тушунилади.

Матнни шифрлаш

Дешифрлаш шифрлаш жараёнига тескари бўлган жараён бўлиб, унда шифрланган матн калит ёрдамида бошланғич кўринишга ўтказилади.

Матнни дешифрлаш

Маълумотларни шифрлашда ушбу маълумотлар қайси алфавит асосида тузилганлиги муҳим. Алфавит – ахборотни ёзма ифодалашда зарур бўлган белгиларнинг чекли тўпламидир.

Масалан:

* Z_{33} алфавити – рус алфавитининг 32 ҳарфи ва бўшлиқ белгиси;
* Z_{256} алфавити – ASCII ва КОИ-8 стандарт кодлаштириш жадвали белгилари;
* Z_2 бинар алфавит – иккилик рақамлардан иборат {0,1};
* Саккизлик ёки ўн олтилик саноқ системаси рақамларидан иборат алфавит.

Демак, калит – матнни шифрлаш ва дешифрлаш учун ишлатиладиган муҳим ҳимоя объектидир.

Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қўйилади:

- етарли даражада криптомустаҳкамлик;
- шифрлаш ва қайтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;
- шифрлашдаги кичик хатоларга таъсирчан бўлмаслиги.

Ушбу талабларга қуйидаги криптографик тизимлар жавоб беради:

- ўринларини алмаштириш;
- алмаштириш;
- гаммалаштириш;
- аналитик ўзгартириш.

Ҳозирги кунда **криптографияда** икки усул қўлланилади:

- симметрияли бир калитли (махфий калитли);
- асимметрияли икки калитли (очиқ ва ёпиқ калитли).

Симметрияли усулда қуйидаги иккита муаммо мавжуд:

1)Ахборот алмашувида иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2)Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Асимметрияли усулда иккита калит қўлланилади. Биридан иккинчисини ҳисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул қилувчи томонидан ахборотни тиклашда қўлланилади ва биринчи калит сир сақланиши лозим.

Ўринларини алмаштириш шифрлаш усули бўйичи бошланғич матн белгиларининг матннинг маълум бир қисми доирасида махсус қоидалар ёрдамида ўринлари алмаштирилади.

Алмаштириш шифрлаш усули бўйича бошланғич матн белгилари фойдаланилаётган ёки бошқа бир алфавит белгиларига алмаштирилади.

Гаммалаштириш усули бўйича бошланғич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилади.

Таҳлилий ўзгартириш усули бўйича бошланғич матн белгилари аналитик формулалар ёрдамида ўзгартирилади, масалан, векторни матрицага кўпайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги бўлса, матрица эса калит сифатида хизмат қилади.

2.3.1. Ўринларни алмаштириш усуллари

Ушбу усул энг оддий ва энг қадимий усулдир. Ўринларни алмаштириш усулларига мисол сифатида қуйидагиларни келтириш мумкин:

- шифрловчи жадвал;
- мўъжизали квадрат.

Шифрловчи жадвал усулида калит сифатида қуйидагилар қўлланилади:

- жадвал ўлчовлари;
- сўз ёки сўзлар кетма-кетлиги;
- жадвал таркиби хусусиятлари.

1-мисол. Шаҳоб ал-Кошканди (араб, 1412 йил) алгоритми бўйича шифрлаш. Бошланғич матн: АХБОРОТ ХАВФСИЗЛИГИ УСУЛ ВА ВОСИТАЛАРИ

Шифр-матн: АОФИУОЛХТСГЛСАБХИИВИРОАЗУАТИРВЛСВА

Калит: Устунлар сони – 7, сатрлар сони – 5 бўлган 1-жадвал

Ушбу алгоритмда бошланғич матн жадвалга устунлар бўйича ёзилиб, тўлдирилади. Шифрланган матн эса сатрлар бўйича жойлашган белгилар кетма-кетлигидан иборат бўлади.

1-жадвал

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

2-мисол. 1-мисолда берилган бошланғич матнни шифрланишини янада мураккаблаштириш максадида ПЕНТИУМ таянч сўзи киритилса, қуйидаги шифр матн ҳосил бўлади :

ОУЛФАИОТЛАСЧГСХВРИБИИААИЗОУТВВ ЛРСА

Бунда ПЕНТИУМ калит сўзи жадвалнинг бошланғич сатрига жойлаштирилади ва ушбу сўздаги ҳар бир ҳарфнинг алфавитда жойлашган ўрни бўйича тартиб рақами иккинчи сатрга жойлаштирилади.

2-жадвал

П	Е	Н	Т	И	У	М
5	1	4	6	2	7	3
А	О	Ф	И	У	О	Л
Х	Т	С	Г	Л	С	А
Б	Х	И	И	В	И	Р
О	А	З	У	А	Т	И
Р	В	Л	С	В	А	

Ҳосил бўлган 2-жадвал иккинчи сатридаги 1 рақами ёзилган устун 3-жадвалнинг биринчи устунига, 2 рақами ёзилган устун иккинчи устунига ва шу каби қолган устунлар ҳам ўз тартиб рақамлари бўйича 3-жадвалга жойлаштирилиб, натижавий шифр матн ҳосил қилинади.

3-жадвал

1	2	3	4	5	6	7
О	У	Л	Ф	А	И	О
Т	Л	А	С	Х	Г	С
Х	В	Р	И	Б	И	И
А	А	И	З	О	У	Т
В	В		Л	Р	С	А

3-мисол. Мўъжизали квадрат матрица усулида шифрлаш.

Мўъжизали квадрат деб, ҳар бир катакчасига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал бўйича сонлар йиғиндиси битта сонга тенг бўлган квадрат шаклидаги жадвалга айтилади. Ўлчами 4х4 га тенг бўлган мўъжизали квадратлар сони 880 тага тенг. Масалан, ушбу мўъжизали квадрат берилган бўлсин:

13	8	12	1
2	11	7	14
3	10	6	15
16	5	9	4

Бошланғич матн - **ОЛТИНЧИДА КЕЛАМАН** бўлса, уни мўъжизали квадрат катакчаларига мос сон бўйича жойлаштирамиз:

А	Д	Л	О
Л	Е	И	М
Т	К	Ч	А
Н	Н	А	И

Шифрланган жадвалдан АДЛО ЛЕИМ ТКЧА ННАИ шифрланган матн ҳосил бўлади.

Лекин шифрлашнинг бу усули мўъжизали квадратлар сони чекли бўлгани учун мустаҳкамлиги бўйича суст роқ.

2.3.2. Алмаштириш усуллари

Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин:

—Цезарь усули;

—Аффин тизимидаги Цезарь усули;

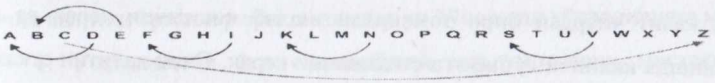
—Таянч сўзли Цезарь усули ва бошқалар.

1-мисол: Гай Юлий Цезарь (102-44 э.а.) алгоритми

бошланғич матн: VENI VIDI VICI (Келди Кўрди Ғолиб чиқди)

Шифр-матн: SBKF SFAF SFZF

Калит: Биринчи ҳарф ўрнига ўзидан олдинги келадиган 3-чи ҳарфни қўйиб ўқинг.



Цезарь усулининг камчилиги ҳарфларнинг алфавит бўйича жойлашган ўрни бўйича мос тартибда симметрик алмаштирилишидир.

Таянч сўзли Цезарь усулида силжитиш билан биргаликда таянч сўз қўлланилади. Таянч сўзни қўллашдан мақсад ҳосил қилинадиган алфавитда ҳарфлар кетма-кетлигини ўзгартиришдир.

Мисол. к=5 ва KOMPYUTER таянч сўзини оламиз ва бу сўз к — ўриндан ёзилади:

0	1	2	3	4	5	6	7	8	9	1	1	1	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N
					K	O	M	P	Y	U	T	E	R

1	15	16	1	1	1	2	2	2	2	2	2
O	P	Q	R	S	T	U	V	W	X	Y	Z

Ушбу таянч сўз алифбодаги кўрсатилган жойда жойлаштирилади, ундаги ҳарфлар инобатга олинмасдан, қолган ҳарфлар алфавитдаги тартиб бўйича таянч сўздан кейин кетма-кет ёзилади ва натижада, қуйидаги кўриниш ҳосил қилинади:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
S	V	W	X	Z	K	O	M	P	Y	U	T	E	R

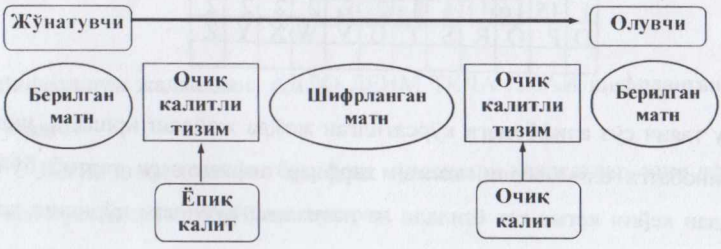
14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	F	G	H	I	J	L	N	Q

Юқорида кўриб чиқилган AXBOROT XAVFSIZLIGI сўзи эса мазкур усул ёрдамида SLVADAG LSIKFPQTPOP га ўтказилади.

2.3.3. Икки калитли ассимметрик алгоритмлар

Очиқ калитли криптографик тизимлардаги асосий муаммо калитларни тақсимлашдир. Икки субъект ўртасида махфий ахборотни ишончли узатиш учун очиқ калит улардан бири томонидан ишлаб чиқилиши керак ва яна махфий равишда иккинчи субъектга етказилиши керак. Очиқ калитни етказиш учун ҳам кандайдир криптографик тизим ишлатилиши керак. Очиқ калитли криптографик тизимнинг моҳияти шундан иборатки, ахборот тизими ҳар бир субъекти томонидан икки бир-бири билан маълум қоидага кўра боғланган калит ишлаб чиқилади. Калитлардан бири очиқ, иккинчиси эса ёпиқ деб эълон қилинади. Очиқ калит ахборот тизими субъекти билан ахборот алмашишни истаган барча фойдаланувчиларга ҳавола этилади. Ёпиқ калит эса махфий равишда сақланиб, сир тутилади.

Жўнатувчи томонидан юбориладиган бошланғич матн ёпиқ калит ёрдамида шифрланиб олувчига жўнатилади. Олувчи томонидан қабул қилинган шифрланган матн очиқ калит билан дешифрланади.



Очиқ калитли криптографик тизимлар тескари функциясига эга бўлмаган бир томонлама функцияга асосланадилар. Бундай функциялар қуйидаги

хоссага эгадирлар: берилган ихтиёрий x нинг қиймати учун $f(x)$ функция қийматини ҳисоблаш мумкин, лекин агар $y=f(x)$ бўлса, y орқали x нинг қийматини аниқлаш мумкин эмас.

Умуман ҳозирги пайтда очиқ калитли криптотизимларда мураккаб алгоритмлар ишлатилади. Уларда асосан тескари алмаштиришлар ўтказиш мумкин бўлмаган қуйидаги амаллардан бири бажарилади:

1. Катта сонларни оддий кўпайтувчиларга ажратиш.
2. Чекли майдонда логарифм қийматини ҳисоблаш.
3. Алгебраик тенгламалар илдизларини ҳисоблаш.

Очиқ калитли криптографик тизимлар уч йўналиши қўлланилиши мумкин:

1. Узатилаётган ёки сақланаётган маълумотларни мустақил равишда ҳимоялаш воситаси сифатида.

2. Калитларни тақсимлаш воситаси сифатида. Сабаби, очиқ калитли криптотизим алгоритмлари симметрияли криптотизимларга нисбатан мураккаб. Шунинг учун одатда бундай тизимлар ёрдамида сиғими унчалик катта бўлмаган калитларни тақсимлаб, улар асосида катта сиғимдаги ахборотларни узатиш мумкин.

3. Фойдаланувчиларни аутентификация қилиш воситаси сифатида.

Очиқ калитли криптографик тизимлар орасида энг кўп қўлланиладигани 1977 йилда Рон Ривест, Ади Шамир ва Леонард Эйдельманлар томонидан яратилган RSA тизимидир. Улар ҳисоблаш жараёнида катта оддий сонларни топиш осонлиги ва шундай икки сон кўпатмасини кўпайтувчиларга ажратиш амалда мумкин эмаслигини ҳисобга олган ҳолда ушбу тизимни яратганлар.

Қуйида RSA алгоритмини оддий мисол орқали ёритишга ҳаракат қиламиз. Берилган матн “CAB” бўлсин. Иккита кичик оддий сон танлаймиз (Амалда оддий сонларнинг каттаси ишлатилади)

1. Биринчи оддий сон $p=3$ ва иккинчи оддий сон $q=11$ бўлсин.
2. Ушбу сонларнинг кўпайтмасини аниқлаймиз: $n=3*11=33$.
3. $(p-1)(q-1)$ кўпайтмани ҳисоблаймиз : $2*10=20$. Демак, 20 дан кичик бўлган оддий сон танлаймиз, масалан, $d=3$.

4. Шундай e сонини танлаймизки, бу сон (e*3) (mod 20) = 1 шартни қаноатлантирсин. Бундай сон 7 га тенг.
5. Шифрланаётган матн белгиларини алфавит тартиби бўйича мос бутун сонлар орқали ифодалаймиз: A→1, B→2, C→3. У ҳолда матн (3,1,2) кўринишни олади. Берилган матнни {7,33} очиқ калит орқали шифрлаймиз:

$$ШМ1 = (3^7) (mod\ 33) = 2187 (mod\ 33) = 9,$$

$$ШМ2 = (1^7) (mod\ 33) = 1 (mod\ 33) = 1,$$

$$ШМ3 = (2^7) (mod\ 33) = 128 (mod\ 33) = 29.$$

6. Ҳосил бўлган шифрланган матн (9,1,29) га тенг. Ушбу шифрланган матнни {3,33}ёпиқ калит орқали дешифрлаймиз:

$$БМ1 = (9^3) (mod\ 33) = 729 (mod\ 33) = 3,$$

$$БМ2 = (1^3) (mod\ 33) = 1 (mod\ 33) = 1,$$

$$БМ3 = (29^3) (mod\ 33) = 24389 (mod\ 33) = 2.$$

Демак, реал шароитларда RSA алгоритми қуйидагича ишлатилади: ҳар бир фойдаланувчи икки p ва q катта бўлган оддий сонларни танлайди ва мос равишда e ва d оддий сонларини танлайди. p ва q сонлари кўпайтмасидан n ни аниқлайди.

$\{e,n\}$ ёпиқ калит, $\{d,n\}$ – эса очиқ калит сифатида ишлатилади (тескариси ҳам бўлиши мумкин).

Узатиладиган маълумот ёпиқ калит билан шифрланади. Очиқ калит эса олувчига ҳавола этилади. Шифрланган маълумотни дешифрлаш учун фойдаланувчи очиқ калитдан фойдаланади. Ёпиқ калит эгаси уни ошкор қилмаган ҳолда сир сақлаши керак.

2.3.4. Ал-Жамол криптографик тизими

Ушбу тизим 1985 йилд.а миллати араб бўлган АҚШлик аспирант Тоҳир Ал-Жамол томонидан яратилган бўлиб, RSA тизимига ўхшашдир. Унда дискрет логарифм қиймати ҳисобга олинади.

Тизимда икки параметр p ва g ишлатилиб, улардан биринчиси оддий сон, иккинчиси эса бутун сон қийматини қабул қилади.

Мисол учун,

1. Алиев a махфий калит яратади ва унинг асосида $y = g^a \bmod p$ очиқ калитини ҳисоблайди. Агар Валиев Алиевга маълумот юбормокчи бўлса, у шундай k тасодифий сонни танлайдики, бу сон р дан кичик бўлиши керак. Ва ушбу сонлар асосида қуйидагиларни ҳисоблайди :

$$y_1 = g^k \bmod p \quad \text{ва}$$

$$y_2 = m \oplus y^k,$$

бунда $\oplus$ белгиси иккилик саноқ системасида битлар бўйича қўшиш амалини билдиради.

2. Шундан сўнг Валиев Алиевга (y_1, y_2) маълумотини жўнатади.

Алиев олинган маълумотни қуйидаги формула бўйича тиклаб, дешифрлайди :

$$m = (y_1^a \bmod p) \oplus y_2.$$

2.4. Ахборот хавфсизлигини таъминлашда биометрик воситалардан фойдаланиш

Ахборотларга рухсатсиз мурожаат қилишдан ҳимоя қилиш мақсадида аутентификациялашнинг ва назорат қилишнинг биометрик воситалари ишлатилади. Биометрик воситалар фойдаланувчининг айнан кимлигини унинг шахсий хусусиятларига асосланиб аниқлаш имконини берадилар. Улар яхши

самара беришлари билан бирга нархи жиҳатидан қимматроқ. Бундай воситаларда аниқлашнинг қуйидаги услублари қўлланилади:

- шахсий услуб - бармоқ изларининг нусхасини ёки юз тузилишини назорат қилиш асосида;
- квазистатик услуб - қўл геометрияси, кўз хусусиятлари, қўл излари нусхаси, қон томирлари расми асосида;
- квазидинамик услуб – пульс, баллистокардиография, энцефалография асосида;
- динамик услуб – товуш, ёзув шакли, босмалаш (печатлаш) стили асосида.

Карточка кўринишида тайёрланган ва ундаги белгиланган маълумотлар хусусиятларига кўра аниқловчи воситалар кейинги пайтларда кўпроқ қўлланилмоқда. Фойдаланувчининг идентификацион ахборотлари карточкага механик, оптик ёки магнит усуллари ёрдамида юритилади.

Магнит карточкалари ўрнига ишончлилиги юқори ва қалбакилаштирилишдан ҳимояланган интеллектуал карточкалар (smartcard) жорий этилмоқда. Уларда ахборотни сақлаш учун электрон компонентлар (микропроцессор, энергияга боғлиқ бўлмаган ҳолда ишловчи хотира) ишлатилади. Интеллектуал карточкалар учун ISO 7816 ҳалқаро стандарт мавжуд. Интеллектуал карточка хотирасига ахборот кўп маротаба ёзилиши, ўқилиши мумкин. Карточкадан қуйидагиларни сақлашда фойдаланиш мумкин:

- идентификацион ахборотларни;
- шифрлаш калитларини ва улардан криптопроцессор сифатида фойдаланишни;
- ихтиёрий махфий ахборотни.

Баъзи карточкаларда «ўз-ўзини блокировка қилиш» режимида рухсатсиз мурожаат қилишдан ҳимояланиш кўзда тутилган.

2.5. Ахборот хавфсизлигини таъминлашда фойдаланиладиган бошқа воситалар

Ахборотга рухсатсиз мурожаат қилишдан ҳимояловчи воситалар. Бундай воситалар асосан шахсий идентификаторни назорат қилувчи дастурий-аппарат комплекси кўринишида ишлаб чиқилади (Touch Memory (iButton) туридаги электрон идентификатор, микропроцессорли карта ва бошқалар). Бу синфга тегишли воситалар ҳисоблаш техникаси ахборот ресурларига мурожаат қилишни чеклашда, иш сеанслари аудитини ўтказишда, фойдаланиладиган дастурий воситаларни маъмурий бошқаришда қўлланилади. Бундан ташқари уларнинг баъзилари ўзида антивирус функцияларини бажариш ва ахборотларни криптографик ҳимоялаш имкониятларига эга. Тармоқ бўйича улардан фойдаланишда масофадан туриб ишчи компьютерларни маъмурий Бошқариш ва тармоқда ишлаётган ҳар бир компьютер ҳақида статистик маълумотлар олиш, рухсатсиз кириш ва сеанс давомийлиги ҳақидаги маълумотларни назорат қилиш мумкин.

Баённомалар (протоколлар) анализаторлари. Тармоқ хавфсизлигини таъминлаш масалаларини ҳал қилиш жараёнида кўпинча тармоқнинг турли бўғинлари баённомалари ёрдамида узатилаётган ахборотлар пакети, кодлаштирилган ахборотларни ўз аслига ўтказиш ҳақидаги маълумотларни тўплаб, статистик таҳлил қилиш керак бўлади. Унчалик катта бўлмаган корпоратив тармоқларда хавфсизликни таъминлаш учун Expert Sniffer Analyzer (ESA) номли портатив анализатордан фойдаланиш мумкин (уни Turbo Sniffer Analyzer номи билан ҳам аташади). Ҳозирги пайтда ишлаб чиқилаётган ушбу анализаторларнинг янги турлари тармоқ баённомаларини тўлиқ таҳлил қилиш, тармоқ сегментининг мониторингини ўтказиш имконига эга.

Ахборот тизимлари баённомалари дастурий анализаторлари қулай бўлишлари билан бирга камчиликлардан ҳам холи эмас, сабаби бундай анализатор ишлаши учун қўшимча яна битта ишчи станция бўлиши талаб этилади.

Тажриба шуни кўрсатмоқдаки, корхона корпоратив тармоғида хавфсизлик бўйича администратор томонидан алоҳида жиддий назоратни талаб этадиган бўғинни олдиндан билиш жуда қийин. Корпоратив тармоқнинг маълум нуқтасида стационар анализаторларни ўрнатиш зарурати корхонада қабул қилинган хавфсизлик сиёсатидан келиб чиққан ҳолда амалга оширилади.

Бундай анализаторлар ёрдамида:

- ETHERNET и TOKEN RING туридаги баённомаларга асосланган тармоқлар ишини таҳлил қилиш ва назорат қилиш;
- тармоқ бўйича энг фаол маълумот жўнатувчиларни (ёки олувчиларни) аниқлаш, шунингдек катта ҳажмдаги ахборот пакетларини юборувчиларни аниқлаш;
- ахборот пакети манбаи ва хатога эга бўлган пакетларни таҳлил қилиш;
- тармоқ бўйича узатилаётган ахборот оқими айланмаси ҳақидаги маълумотларни йиғиш (TOKEN RING туридаги баённомада эса мурожаат қилиш вақтлари ва тармоқдаги носозликлар ҳақидаги маълумотларни йиғиш);
- ахборот пакетларини сунъий равишда моделлаштириб, улардан тармоқ бўйича ахборот узатиш қобилятини синаш ишларини бажариш;
- тармоқдаги заиф бўғин ва нуқталарни аниқлаш;
- тармоқда ишлатилаётган кўприк ва маршрутизаторлар ишини тасодифан танлаш йўли билан назорат қилиш;
- тармоқ топологиясини чуқур таҳлил қилиш;
- NETWARE туридаги тармоқни текшириш;
- тармоқ мониторинги учун зарур бўлган статистик маълумотлар йиғиш мумкин.

Булардан ташқари анализаторлар кабель линияларини назорат қилиш имкониятига ҳам эга. Тармоқ линиясининг охирига ўрнатилган ёрдамчи қурилма орқали кабель тизимидаги кабель узунлиги, боғланишдаги хатоликлар, (туташ ва ажрашган тугунлардаги), носозликкача бўлган масофани, узилиш

нуқталарини, қисқа туташув нуқтасини ва шу каби бошқа параметрларни аниқлаш мумкин.

Ҳимоя тизимини назорат қилувчи ускунавий воситалар. Корпоратив тармоқнинг ҳимоя тизими доимий назорат натижалари асосида ишончли ёки ишончсиз, деб баҳолаш мумкин. Амалда хавфсизлик бўйича масъул администратор тизимга уюштирилиши мумкин бўлган ҳужумлар, уларнинг турлари ҳақидаги маълумотларни тўплаши ва шунга асосланган ҳолда хавфсизлик сиёсатини юритиши керак. Бунинг учун администратор даврий равишда сунъий ҳужум турини моделлаштириб, назорат қилиши керак.

Ҳозирги пайтда корпоратив тармоқларнинг ҳимоя савиясини назорат қилувчи, ISS фирмасида яратилган Internet Scanner SAFEsuite тизими ишлатилмоқда. Бу тизим ёрдамида хавфсизлик администратори хавфсизлик сиёсати талаб даражасида жорий этилишини назорат қилиш имконига эга.

System Security Scanner модули шахсий компьютерларнинг операцион тизим параметрларининг тўғри созланганлигини, файлларга мурожаат қилиш ҳуқуқларининг ахборот хавфсизлиги сиёсатига мос келишлигини, «троян» дастурлари туридаги хавфли дастурларни кидириб назорат қилиш имконини беради.

Тармоқлараро ҳимоя экрани. Тармоқлараро ҳимоя экрани (инглизча FireWall-тизими ёки немисча Brandmauer) - дастурий-аппарат маҳсулот бўлиб, ташқи тармоқ билан ички тармоқ ўртасида ташқи тармоқдан амалга ошириладиган рухсатсиз мурожаатлар, ҳаракатларни чеклашда (INTERNET - INTRANET маҳсулотларини) ва корпоратив тармоқни сегментларга ажратишда (ENTERPRISE маҳсулотлари) ишлатилади.

Маълумотларни қайта ишлаш дастурлари жараёнларини ҳимоя қилиш механизмлари. Бундай механизмлар ахборот тизимидаги объектларга, асосан ахборот ресурсларига мурожаат қилишни назорат қилишда ишлатиладилар. Бундай механизмларга бир томондан бажарилаётган дастурнинг бошқа дастурлардан тўлиқ изоляция қилиш, иккинчи томондан эса

дастурнинг зарур ҳолларда бошқа дастурлар билан ахборот алмашинувига рухсат берилишини таъминлаш бўлган каби талаблар қўйилади.

Тармоқ ресурсларини ҳимоя қилишда қуйидаги икки ҳолаттга кўпроқ эътибор қаратилади:

- дастурнинг бажарилиши ва унда ахборотларнинг узатилиши жараёнларини рухсатсиз кўришдан (ёки кузатишдан) ҳимоялаш;
- бажарилаётган дастур ва унга тегишли маълумотларни рухсатсиз кўчириш ва тарқатишдан ҳимоялаш.

Бундай ҳимоялашда криптографик усуллардан фойдаланиш механизми яхши самара беради. Бажарилаётган дастур ва унга тегишли маълумотларни рухсатсиз кўчириш ва тарқатишдан ҳимоялаш мурожаат қилишни назорат қилиш механизми ёрдамида таъминланиши мумкин. Бажарилувчи файлларнинг такомиллаштирилиб ўзгартирилишидан ва уларга вируслар жорий этилишидан ҳимоялаш операцион тизимдаги ихтиёрий бажарилувчи файл ҳолатини ўзгартирмасдан сақлаш имконини беради. Бундай ҳимоя файлнинг бажарилиши жараёнида ёки алоҳида назорат натижасида таъминланиши мумкин. Ваколатга эга бўлмаган фойдаланувчининг тизимдаги ҳар кандай дастурни ишга тушириши имкониятидан ҳимоялаш бажарилувчи файлларнинг ўзгартирилишини ёки улардан нусха кўчирилишини олдини олади. Бунда шахсий компьютер тизимли шинасига ўрнатиладиган аппарат модул, дастурни ишга туширишга рухсат беришни ва қаттиқ дискдаги операцион тизимга тегишли хизматчи маълумотларни шифрлашни таъминловчи калит ёрдамида ҳимоялаш амалга оширилади.

Қаттиқ дискни турли фойдаланувчилар томонидан тўсатдан форматлаб юборилишини ҳимоялаш шахсий компьютер тизимли шинасига ўрнатиладиган махсус аппарат қурилма ёки калит ёрдамида амалга оширилади.

Тармоқда фаолият кўрсатувчи баъзи дастурларга масофадан туриб шундай буйруқлар кетма-кетлиги ўрнатилиши мумкинки, улар тизимда сақланаётган махфий ахборотларга мурожаат қилиш ва керакли манзилга етказиб беришни таъминлаб берадилар. Бундай хуфиёна амаллар бажарадиган нотаниш

буйруқлар суқилиб кирган дастурдан ҳимояланиш учун ҳам шахсий компьютер тизимли шинасига махсус аппаратли модуль ўрнатилади.

2.6. Ахборот тизимида алоқа каналлари бўйича ахборот узатиш жараёнларини ҳимоя қилиш воситалари

Ахборот тизимидаги энг заиф жойлардан бири алоқа каналларидир. Бузғунчиларнинг аксарият кўпчилиги айнан мана шу алоқа каналлари орқали ўз мақсадларига эришадилар.

Алоқа каналларига рухсатсиз суқилиб кириш пассив ва актив ҳолда амалга оширилади. Пассив ҳолда бузғунчи алоқа каналида бўлаётган жараёнларни уларни бузмаган ҳолда фақат кузатади. Узатилаётган маълумотлар тушунарли бўлмаса ҳам, бузғунчи маълумотлар билан биргаликда узатилаётган бошқарувчи буйруқларнинг мазмунини билиб олишга ҳаракат қилади. Максад - ахборот тизими объектларининг жойлашган ўрни, идентификаторларини билиб олиш. Ва ниҳоят, пассив суқилишнинг яна бир кўринишида бузғунчи узатилаётган ахборот узунлиги, вакти, сеанслар частотасини аниқлаб олишга ҳаракат қилади.

Каналда узатилаётган ахборотни ҳимоялашда алоқа каналининг икки бўғинли ҳимоялаш шаклидан фойдаланилади. Биринчи бўғинда ахборот узатиш жараёни ҳимояланса, иккинчи бўғинда ахборот шифрланади. Бундай ҳолатда бузғунчи шифрланган ахборот маъносини англай олмайди.

Актив суқилишнинг қуйидаги тоифалари мавжуд:

- узатилаётган ахборот оқимига таъсир кўрсатиш – уларнинг структурасини ўзгартириш, ўчириб ташлаш, бошка ахборот билан алмаштириш, қайта тартиблаш, ва ёлғон маълумотларни жўнатиш;
- ахборот узатилишига тўсқинлик қилиш;
- тизимни умуман бошқа манзилдаги абонент билан боғлаб юбориш ва шу манзилга маълумот узатишни ташкил қилиш.

Бундай суқилиб киришлардан ҳимояланишда ҳар бир узатилаётган ахборот оқими билан биргаликда коммуникацион баённомалардан фойдаланилади. Узатилаётган ахборот оқимининг яхлитлигини таъминлашга қаратилган ҳимоя механизми ахборот узатилишига тўсқинлик қилувчи ҳаракатларни аниқлаш имконини беради. Суқилиб киришдан ҳимоя қилишда жойлардаги абонентлар ахборот узатилиши ва қабул қилиниши ҳақидаги маълумотларни тасдиқловчи назорат қилиш механизмидан фойдаланишлари керак.

Назорат учун саволлар :

1. Ахборот хавфсизлиги тизимининг техник асосини нималар ташкил этади ?
2. Дастурий ва техник воситалар ахборот хавфсизлигини таъминлашнинг қайси йўналишларида фойдаланилмайдилар ?
3. Аппарат воситалари ва схемалар ёрдамида ҳимоя килишнинг моҳияти нимадан иборат ?
4. Ҳимоялашнинг алмаштириш усуллари моҳияти нимадан иборат ?
5. Ҳимоялаш воситаларини қўллашда ташкилий тадбирлар нималарни ўз ичига олиши керак ?
6. Ахборот хавфсизлигини таъминлашда биометрик воситалар нима мақсадда фойдаланиладилар ?
7. Биометрик воситаларда аниқлашнинг шахсий услуби ёрдамида қайси жиҳатга қараб назорат амалга оширилади ?
8. Ахборотга рухсатсиз мурожаат қилишдан ҳимояловчи воситаларга нималар киради ?

III боб. АХБОРОТНИ ҲИМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ

3.1. Криптографиянинг асосий қоидалари ва таърифлари

Ахборотнинг ҳимоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. *Ахборотни шифрлаш* деганда очиқ ахборотни (дастлабки матнни) шифрланган ахборотга ўзгартириш (шифрлаш) ва аксинча (расшифровка қилиш) жараёни тушунилади. Шифрлаш криптотизимининг умумлаштирилган схемаси 3.1-расмда келтирилган.

3.1-расм. Шифрлаш криптотизимининг умумлаштирилган схемаси.

Узатилувчи ахборот матни M криптографик ўзгартириш E_{k1} ёрдамида шифрланади, натижада шифрматн C олинади:

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

бу ерда $k1$ – шифрлаш калити деб аталувчи E функциянинг параметри.

Шифрлаш калити ёрдамида шифрлаш натижаларини ўзгартириш мумкин. Шифрлаш калити муайян фойдаланувчига ёки фойдаланувчилар гуруҳига тегишли ва улар учун ягона бўлиши мумкин. Муайян калит ёрдамида шифрланган ахборот фақат ушбу калит эгаси (ёки эгалари) томонидан расшифровка қилиниши мумкин.

Ахборотни тескари ўзгартириш қуйидаги кўринишга эга:

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

D функцияси E функцияга нисбатан тескари функция бўлиб, шифр матнни расшифровка килади. Бу функция хам $k2$ калит кўринишидаги қўшимча параметрга эга. $k1$ ва $k2$ калитлар бир маъноли мосликка эга бўлишлари шарт. Бу ҳолда расшифровка қилинган M' ахборот M га эквивалент бўлади. $k2$ калити ишончли бўлмаса D функция ёрдамида $M' = M$ дастлабки матнни олиб бўлмайди.

Криптотизимларнинг иккита синфи фаркланади:

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

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка қилиш учун битта калитнинг ўзи ишлатилади. Демак, шифрлаш калитидан фойдаланиш хукукига эга бўлган ҳар қандай одам ахборотни расшифровка қилиши мумкин. Шу сабабли, симметрик криптотизимлар махфий калитли криптотизимлар деб юритилади. Яъни шифрлаш калитидан фақат ахборот аталган одамгина фойдалана олиши мумкин. Шифрлашнинг симметрик криптотизими схемаси 3.2-расмда келтирилган.

3.2-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 бўлади ва шахсий калит элтувчисидан масалан, дискетда ёки смарт-картада сакланади. Шахсий калит

элтувчиси эгасидан бошқа одамларнинг фойдаланишига қарши чоралар кўрилиши шарт.

Симметрик шифрлаш ахборотни "ўзи учун", масалан, эгаси йўқлигида ундан рухсатсиз фойдаланишни олдини олиш мақсадида, шифрлашда жуда қулай хисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантиқий ёки физик дискларни шаффоф(автоматик) шифрлаш бўлиши мумкин.

Симметрик шифрлашнинг ноқулайлиги - ахборот алмашинуви бошланмасдан олдин барча адресатлар билан махфий калитлар билан айирбошлаш заруриятидир. Симметрик криптотизимда махфий калитни алоқанинг умумфойдаланувчи каналлари орқали узатиш мумкин эмас. Махфий калит жўнатувчига ва қабул қилувчига калитлар тарқатилувчи ҳимояланган каналлар орқали узатилиши керак.

Симметрик шифрлаш алгоритмининг маълумотларни абонентли шифрлашда, яъни шифрланган ахборотни абонентга, масалан Internet орқали, узатишда амалга оширилган вариантлари мавжуд. Бундай криптографик тармокнинг барча абонентлари учун бита калитнинг ишлатилиши хавфсизлик нуқтаи назаридан ножоиздир. Хақиқатан, калит обрўсизлантирилганда (йўқотилганида, ўғирлатилганда) барча абонентларнинг хужжат алмашиши хавф остида қолади. Бу ҳолда калитларнинг матрицаси (3.3-расм) ишлатилиши мумкин.

	1	2	3	...	n	
1	k_{11}	k_{12}	k_{13}	...	k_{1n}	1-абонент учун калитлар набори
2	k_{21}	k_{22}	k_{23}	...	k_{2n}	2-абонент учун калитлар набори
3	k_{31}	k_{32}	k_{33}	...	k_{3n}	3-абонент учун калитлар набори
...	...	...	...	...	...	...
n	k_{n1}	k_{n2}	k_{n3}	...	k_{nn}	n-абонент учун калитлар набори

3.3–расм. Калитлар матрицаси

Калитлар матрицаси абонентларнинг жуфт-жуфт боғланишли жадвалидан иборат. Жадвалнинг ҳар бир элементи *i* ва *j* абонентларни боғлашга мўлжалланган ва ундан фақат ушбу абонентлар фойдалана оладилар. Мос ҳолда, калитлар матрицаси элементлари учун қуйидаги тенглик ўринли.

$$K_{ij} = K_{ji}.$$

Матрицанинг ҳар бир *i*- қатори муайян *i* абонентнинг қолган *N*-1 абонентлар билан боғланишини таъминловчи калитлар наборидан иборат. Калитлар набори (тармоқ наборлари) криптографик тармоқнинг барча абонентлари ўртасида тақсимланади. Тақсимлаш алоқанинг *ҳимояланган каналлари* орқали ёки қўлдан-қўлга тарзда амалга оширилади.

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка қилишда турли калитлардан фойдаланилади:

- *очиқ калит* K ахборотни шифрлашда ишлатилади, махфий калит k дан ҳисоблаб чиқарилади;
- *махфий калит* k, унинг жуфти бўлган очиқ калит ёрдамида шифрланган ахборотни расшифровка қилишда ишлатилади.

Махфий ва очиқ калитлар жуфт-жуфт генерацияланади. Махфий калит эгасида қолиши ва уни рухсатсиз фойдаланишдан ишончли химоялаш зарур (симметрик алгоритмдаги шифрлаш калитига ўхшаб). Очиқ калитнинг нусхалари махфий калит эгаси ахборот алмашинадиган криптографик тармоқ абонентларининг ҳар бирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 3.4-расмда келтирилган.

3.4-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.

Асимметрик криптотизимда шифрланган ахборотни узатиш қуйидагича амалга оширилади:

1. Тайёргарлик босқичи:

- абонент B жуфт калитни генерациялайди: махфий калит k_B ва очиқ калит K_B;
- очиқ калит K_B абонент A га ва қолган абонентларга жўнатилади.

2. A ва B абонентлар ўртасида ахборот алмашиш:

- абонент A абонент Bнинг очиқ калити K_B ёрдамида ахборотни шифрлайди ва шифрматнни абонент Bга жўнатади;
- абонент B ўзининг махфий калити k_B ёрдамида ахборотни расшифровка қилади. Ҳеч ким (шу жумладан абонент A ҳам) ушбу ахборотни расшифровка қилаолмайди, чунки абонент Bнинг махфий калити унда йўқ.

Асимметрик криптотизимда ахборотни химоялаш ахборот қабул қилувчи калити k_B нинг махфийлигига асосланган.

Асимметрик криптотизимларнинг асосий ҳусусиятлари қуйидагилар:

1. Очиқ калитни ва шифр матнни ҳимояланган канал орқали жўнатиш мумкин, яъни нияти бузуқ одамга улар маълум бўлиши мумкин.
2. Шифрлаш $E_B: M \rightarrow C$ ва расшифровка қилиш $D_B: C \rightarrow M$ алгоритмлари очиқ.

3.2. Симметрик шифрлаш тизими

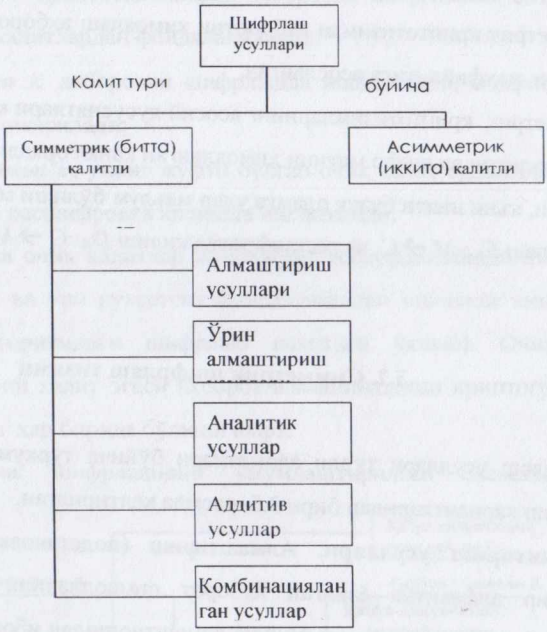
Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш вариантларидан бири 3.5–расмда келтирилган.

Алмаштириш усуллари. Алмаштириш (подстановка) усулларининг моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит символлари билан маълум қоида бўйича алмаштиришдан иборатдир. Энг содда усул сифатида ***тўғридан тўғри алмаштиришни*** кўрсатиш мумкин. Дастлабки ахборот ёзилувчи A_0 алфавитнинг s_{0i} символларига шифрловчи A_1 алфавитнинг s_{1i} символлари мос қуйилади. Оддий ҳолда иккала алфавит ҳам бир хил символлар тўпламига эга бўлиши мумкин.

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича К символлар узунлигига эга бўлган дастлабки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади.

Моноалфавитли алмаштириш алгоритми қуйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

1-қадам. [1xR] ўлчамли дастлабки A_0 алфавитдаги хар бир символ $s_0 \in T(i=\overline{1,K})$ ни A_0 алфавитдаги s_{0i} символ тартиб рақамига мос келувчи $h_{0i}(s_{0i})$ сонга алмаштириш йўли билан рақамлар кетма-кетлиги L_{0h} ни шакллантириш.



3.5-расм. Шифрлаш усулларининг туркумланиши.

2-қадам. L_{0h} кетма-кетлигининг ҳар бир сонини $h_{1i}=(k_1 x h_{0i}(s_{0i})+ k_2)(\mathrm{mod} R)$ формула орқали ҳисобланувчи L_{1h} кетма-кетликнинг мос сони h_{1i} га алмаштириш йўли билан L_{1h} сон кетма-кетлигини шакллантириш, бу ерда k_1-ўнлик коэффицент; k_2-силжитиш коэффиценти. Танланган k_1, k_2 коэффицентлар h_{0i}, h_{1i} сонларнинг бир маъноли мослигини таъминлаши лозим, $h_{1i}=0$ олинганида эса $h_{1i}=R$ алмашинуви бажарилиши керак.

3-қадам. L_{1h} кетма-кетликнинг ҳар бир сони $h_{1i}(s_{1i})$ни [1xR] ўлчамли шифрлаш алфавитнинг мос $s_{1i} \in T_1(i=\overline{1,K})$ символи билан алмаштириш йўли билан T_1 шифрматнни ҳосил қилиш.

4-қадам. Олинган шифрматн ўзгармас b узунликдаги блокларга ажратилади. Агар охирги блок тўлиқ бўлмаса блок орқасига махсус символ-тўлдирувчилар жойлаштирилади(масалан, *).

Мисол. Шифрлаш учун дастлабки маълумотлар қуйидагилар:

T_0=<ҲИМОЯ_ХИЗМАТИ>

A_0=<АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҲ_>

A_1=<ОРЁЬЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЪШБУЮ ҚГН>

R=36; k_1=3; k_2=15; b=4

Алгоритмнинг қадамба-қадам бажарилиши қуйидаги натижаларни олинишига олиб келади.

1-қадам. L_{0h}=<35,10,14,16,31,36,23,10,9,14,1,20,10>

2-қадам. L_{1h}=<12,9,21,17,36,14,12,9,6,21,18,3,9>

3-қадам. T_1=<ХЖЕФНВҲЖТЕҚЁЖ>

4-қадам. T_1=<ХЖЕФ НВҲЖ ТЕҚЁ Ж***>

Расшифровка қилишда блоклар бирлаштирилиб K символли шифрматн T_1 ҳосил қилинади. Расшифровка қилиш учун қуйидаги бутун сонли тенгламани ечиш лозим:

$$k_1 h_{01}+k_2=nR+h_{1i}$$

k_1, k_2, h_{1i} ва R бутун сонлар маълум бўлганда h_{0i} катталиги n ни саралаш орқали ҳисобланади. Бу муолажани шифрматннинг барча символларига тадбиқ қилиш унинг расшифровка қилинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристкаларининг бир хиллигидир. Дастлабки матн қайси тилда ёзилганлигини билган криптоаналитик ушлаб колинган ахборотларни статистик ишлаб, иккала алфавитдаги символлар ўртасидаги мувофиқликни аниқлаши мумкин.

Полиалфавитли алмаштириш усуллари айтарлича юкори криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришни қуйидагича тасаввур этиш мумкин. *N*-алфавитли алмаштиришда дастлабки A_0 алфавитдаги s_{0l} символи A_1 алфавитдаги s_{11} символи билан алмаштирилади ва х. s_{0N} ни s_{NN} символ билан алмаштирилганидан сўнг $S_{0(N+1)}$ символнинг ўрнини A_1 алфавитдаги $S_{1(N+1)}$ символ олади ва х.

Полиалфавитли алмаштириш алгоритмлари ичида ***Вижинер жадвали (матрицаси)*** T_B ни ишлатувчи алгоритм энг кенг тарқалган. Вижинер жадвали [*R*x*R*] ўлчамли квадрат матрицадан иборат бўлиб, (*R*-ишлатилаётган алфавитдаги символлар сони) биринчи қаторида символлар алфавит тартибида жойлаштирилади. Иккинчи қатордан бошлаб символлар чапга битта ўринга силжитилган ҳолда ёзилади. Сиқиб чиқарилган символлар ўнг тарафдаги бўшаган ўринни тўлдиради (циклик силжитиш). Агар ўзбек алфавити ишлатилса, Вижинер матрицаси [36x36] ўлчамга эга бўлади (3.6-расм).

АБВГД.....	.....	.....ЎҚҲҲ_
БВГДЕ.....	.....	.....ҚҲҲ_А
ВГДЕЖ.....	.....	.....ҲҲ_АБ
.....		
_АБВГ.....	.....	.....ЯЎҚҲҲ

3.6-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиган M символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тўлиқ матрицасидан $[(M+1),R]$ ўлчамли шифрлаш матрицаси $T_{(Ш)}$ ажратилади. Бу матрица биринчи қатордан ва биринчи элементлари калит символларига мос келувчи қаторлардан иборат бўлади.

Агар калит сифатида <ҒЎЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта қатордан иборат бўлади. (3.7-расм)

$T_ш$=

АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҲҲ_
ҲҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚ
ЎҚҲҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҲҲ_АБВДЕЁЖ
АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҲҲ_

3.7-расм. «Ғўза» калити учун шифрлаш матрицаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги M символли калит K ни танлаш.

2-қадам. Танланган калит K учун $[(M+1),R]$ ўлчамли шифрлаш матрицаси $T_ш=(b_{ij})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи s_{0r} тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матрицаси $T_ш$ дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

1) K калитнинг алмаштирилувчи s_{0r} символга мос k_m символи аниқланади;

2) шифрлаш матрицаси $T_ш$ даги $k_m = b_{j1}$ шарт бажарилувчи i қатор топилади.

3) $s_{or} = b_{i1}$ шарт бажарилувчи j устун аниқланади.

4) s_{or} символи b_{ij} символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг бўш жойлари махсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан s_{1r} символлари ва мос калит символлари k_m кетма-кет танланади. $T_{ш}$ матрицада $k_m = b_{ij}$ шартни қаноатлантирувчи i қатор аниқланади. i-қаторда $b_{ij}=s_{1r}$ элемент аниқланади. Расшифровка қилинган матнда r - ўрнига b_{ij} символи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Мисол. К=<ҲЎЗА> калити ёрдамида Т=<ПАХТА ҲАРАМИ> дастлабки матнни шифрлаш ва расшифровка қилиш талаб этилсин. Шифрлаш ва расшифровка қилиш механизми 3.7-расмда келтирилган

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

Дастлабки матн ПАХТА_ҒАРАМИ

Калит Ғ ЎЗАҒЎЗАҒЎЗ А

Алмаштирилган

сўнгги матн МЎЯТҒЯЕАНЎФИ

Шифрматн МЎЯТ ҒЯЕА НЎФИ

Калит ҒЎЗА ҒЎЗА ҒЎЗА

Расшифровка

қилинган матн ПАХТ А_ҒА РАМИ

Дастлабки матн ПАХТА_ҒАРАМИ

Ўрин алмаштириш усуллари. Ўрин алмаштириш усулларига биноан дастлабки матн белгиланган узунликдаги блокларга ажратилиб ҳар бир блок ичидаги символлар ўрни маълум алгоритм бўйича алмаштирилади.

Энг осон ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокини матрицага қатор бўйича ёзишни, ўқишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица улчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8x8) учун калитнинг $1{,}6 \bullet 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси $1{,}4 \bullet 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЭҲМлар учун ҳам мураккаб ҳисобланади.

Гамильтон маршрутларига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул қуйидаги қадамларни бажариш орқали амалга оширилади.

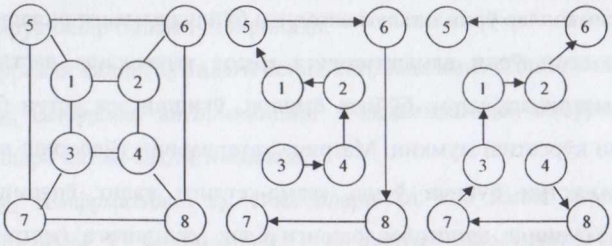
1-қадам. Дастлабки ахборот блокларга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охирги блокдаги бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади (масалан, *).

2-қадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади (3.9-расм).

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

4-қадам. Символларнинг шифрланган кетма-кетлиги белгиланган L узунликдаги блокларга ажратилади. L катталик 1-қадамда дастлабки ахборот бўлинадиган блоклар узунлигидан фарқланиши мумкин.

Расшифровка қилиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



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

Жадвалдан символлар элемент номерлари келиши тартибида ўқилади.

Мисол. Дастлабки матн T_0 «ЎРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Калит ва шифрланган блоклар узунлиги мос ҳолда қуйидагиларга тенг: K=<2,1,1>, L=4. Шифрлаш учун 3.9-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрицалари тўлдирилган маршрутлар 3.10-расмда келтирилган кўринишга эга.

1-қадам. Дастлабки матн учта блокка ажратилади. *Б1*=<ЎРИН_АЛМ>, *Б2*=<АШТИРИШ->, *Б3*=<УСУЛИ**>;

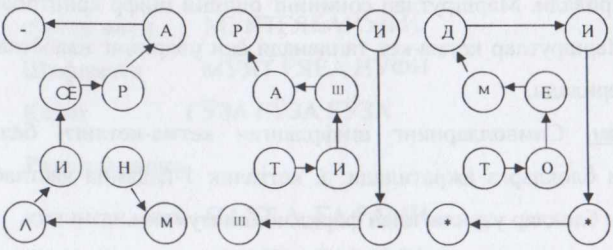
2-қадам. 2,1,1 маршрутли учта матрица тўлдирилади;

3-қадам. Маршрутларга биноан символларни жой-жойига қўйиш орқали шифрматнни ҳосил қилиш.

T_1=<НМЛИЎРА_ТИШАРИ_ШТОЕМДИ**>

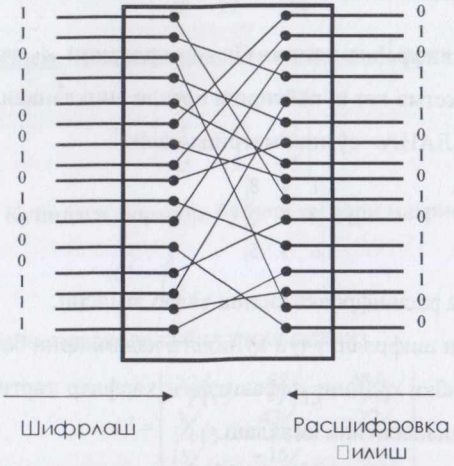
4-қадам. Шифрматнни блокларга ажратиш.

T_1=<НМЛИ ЎРА_ ТИША РИ_Ш ТОЕМ ДИ**>



3.10-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

Амалиётда ўрин алмаштириш усулини амалга оширувчи махсус аппарат воситалар катта аҳамиятга эга (3.11-расм).



3.11-расм. Ўрин алмаштириш схемаси.

Дастлабки ахборот блокининг параллел иккили коди (масалан, икки байт) схемага берилади. Ички коммутация ҳисобига схемада битларнинг блоклардаги ўринлари алмаштирилади. Расшифровка қилиш учун эса схеманинг кириш ва чиқиш йўллари ўзаро алмаштирилади.

Ўрин алмаштириш усулларининг амалга оширилиши содда бўлсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш орқали фош қилиш мумкин. Иккинчидан, агар дастлабки матн узунлиги K символлардан ташкил топган блокларга ажратилса, шифрни фош этиш учун шифрлаш тизимсига биттасидан бошқа барча символлари бир хил бўлган тест ахборотининг K-1 блокини юбориш кифоя.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асосланган шифрлаш усуллари энг кўп тарқалган. Дастлабки ахборотнинг $B_к=||b_j||$ вектор кўринишида берилган k- блокини шифрлаш $A=||a_{ij}||$ матрица калитни $B_к$ векторга кўпайтириш орқали амалга оширилади. Натижада $C_k=||c_i||$ вектор

кўринишидаги шифрматн блоки ҳосил қилинади. Бу векторнинг элементлари $c_i = \sum_j a_{ij} b_j$ ифодаси орқали аниқланади.

Ахборотни расшифровка қилиш C_k векторларини A матрицага тескари бўлган A^{-1} матрицага кетма-кет кўпайтириш орқали аниқланади.

Мисол. T_0=<АЙЛАНА> сўзини матрица-калит

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

ёрдамида шифрлаш ва расшифровка қилиш талаб этилсин.

Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквивалентини аниқлаш.

$$T_5 = <1,10,12,1,14,1>$$

2-қадам. A матрицани B_1={1,10,12} ва B_2={1,14,1} векторларга кўпайтириш.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix} = \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix} = \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix}$$

3-қадам. Шифрланган сўзни кетма-кет сонлар кўринишида ёзиш.

$$T_1 = <137,97,156,65,103,137>$$

Шифрланган сўзни расшифровка қилиш қуйидагича амалга оширилади:

1-қадам. A матрицанинг аниқловчиси ҳисобланади:

$$|A| = -115 .$$

2-қадам. Ҳар бир элементи А матрицадаги a_{ij} элементнинг алгебраик тўлдирувчиси бўлган бириктирилган матрица A^* аниқланади.

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

3-қадам. Транспонирланган матрица A^T аниқланади.

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

4-қадам. Қуйидаги формула бўйича тескари матрица A^{-1} ҳисобланади:

$$A^{-1} = \frac{A^t}{|A|}$$

Ҳисоблаш натижасида қуйидагини оламиз.

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

5-қадам. B_1 ва B_2 векторлар аниқланади:

$$B_1 = A^{-1}C_1; \quad B_2 = A^{-1}C_2.$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix}$$

6-қадам. Расшифровка қилинган сўзнинг сон эквиваленти T_3=<1,10,12,1,14,1> символлар билан алмаштирилади. Натижада дастлабки сўз T_0=<АЙЛАНА> ҳосил бўлади.

Шифрлашнинг аддитив усуллари. Шифрлашнинг ***аддитив усулларига*** биноан дастлабки ахборот символларига мос келувчи рақам кодларини кетма-кетлиги ***гамма*** деб аталувчи қандайдир символлар кетма-кетлигига мос келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашиннг аддитив усуллари ***гаммалаш*** деб ҳам аталади.

Ушбу усуллар учун калит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги калит узунлигига ва унинг статистик характеристкаларининг текислигига боғлиқ. Агар калит шифрланувчи символлар кетма-кетлигидан қисқа бўлса, шифрматн криптоаналитик томонидан статистик усуллар ёрдамида расшифровка қилиниши мумкин. Калит ва дастлабки ахборот узунликлари канчалик фарқланса, шифр-матнга муваффақиятли хужум эхтимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан иборат бўлса, калитни билмасдан туриб шифрматнни расшифровка қилиш амалий жиҳатдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда калит сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг кўп тарқалган ва самарали ҳисобланади. Генератор псевдотасодифий сонларнинг чексиз кетма-кетлигини шакллантиришда нисбатан қисқа 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 чиқиш йўли кетма-кетликларининг тасодифийлиги каби асосий характеристкаларини қатъий математик тарзда ифодалаш мумкин.

Конгруэнт генераторлар ичида ўзининг соддалиги ва самаралилиги билан чизиқли генератор ажралиб тўради. Бу генератор қуйидаги муносабат бўйича сонларнинг псевдотасодифий кетма-кетликларини шакллантиради.

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

бу ерда a ва c – ўзгармаслар, T(0) –туғдирувчи(сабаб бўлувчи) сон сифатида танланган дастлабки катталик.

Бундай датчикнинг такрорланиш даври a ва c катталикларига боғлиқ. m қиймати одатда 2^s га тенг қилиб олинади, бу ерда *s*-ЭХМдаги сўзнинг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг такрорланиш даври *c*-ток сон ва *a* (mod4)=1 бўлгандагина максималь бўлади. Бундай генераторларни аппарат ёки программ воситалари орқали осонгина яратиш мумкин.

Шифрлашнинг комбинацияланган усуллари. Қудратли компьютерлар, тармоқ технологиялари ва нейронли ҳисоблашларнинг пайдо бўлиши ҳозиргача умуман фош қилинмайди деб ҳисобланган криптографик тизимларни обрўсизлантирилишига сабаб бўлди. Бу эса ўз навбатида юқори бардошликка эга криптографик тизимларни яратиш устида ишлашни тақозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. Қуйида энг кам вақт сарфида криптобардошликни жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки босқичда амалга оширилади. Биринчи босқичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи босқичда шифрланган маълумотлар махсус усул бўйича қайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фарқли бўлган сон матрицасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни қўллашда агар шифр гаммаси сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош қилиш жуда қийин. Одатда шифр гаммаси ҳар бир шифрланувчи сўз учун тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг ҳеч қандай қисми маълум бўлмаса, шифрни фақат тўғридан-тўғри саралаш орқали фош этиш мумкин. Бунда криптобардошлик калит ўлчами орқали аниқланади. Шифрлашнинг бу усулидан кўпинча ҳимоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз Кбайтини шифрлаш имконияти мавжуд. Расшифровка қилиш жараёни-калит

маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага кўпайтиришни қўллашда шифрланган матн бир байт узунликдаги f_i векторларга ажратилади ва ҳар бир вектор квадрат матрица $\|M_{ij}\|$ га кўпайтирилади ва шифрланган векторлар шакллантирилади:

$$f_i^* = f_i \cdot \|M_{ij}\|$$

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

Расшифровка қилиш жараёнида шифрланган f^* векторларни тескари матрица $\left(\|M_{ij}^{-1}\|\right)$га кўпайтирилади.

$$f_i = f_i^* \cdot \left\|M_{ij}^{-1}\right\|$$

Комбинацияланган усулларнинг юқори самарадорлигига унинг иккала босқичини аппарат усулда амалга ошириш орқали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка қилиш вақти ошиб кетади. Шу сабабли комбинацияланган усуларни аппарат-дастурий усулда, яъни усулнинг бир босқичи аппарат усулда, иккинчи босқичи дастурий усулда амалга оширилиши мақсадга мувофиқ ҳисобланади.

3.3. Асимметрик шифрлаш тизимлари

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очиқ калит ёрдамида шифрланса, махфий калит ёрдамида расшифровка қилинади. Асимметрик шифрлаш тизимларини очиқ калитли шифрлаш тизимлар деб ҳам юритилади.

Очиқ калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки x маълум бўлса $y=f(x)$ функцияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жихатдан мумкин эмас. Криптографияда яширин деб аталувчи йўлга эга бўлган бир томонли функциялар ишлатилади. z параметрли бундай функциялар қуйидаги хусусиятларга эга. Маълум z учун E_z ва D_z алгоритмларини аниқлаш мумкин. E_z алгоритми ёрдамида аниқлик соҳасидаги барча x учун $f_Z(x)$ функцияни осонгина олиш мумкин. Худди шу тариқа D_z алгоритми ёрдамида жоиз қийматлар соҳасидаги барча y учун тескари функция $x=f^1(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча z ва деярли барча, y учун хатто E_z маълум бўлганида ҳам $f^1(y)$ни ҳисоблашлар ёрдамида топиб бўлмайди. Очиқ калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

Очиқ калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқатда бўлган субъектлар ўртасида махфий калитни алмашиш зарурияти йўқолади. Бу эса ўз навбатида узатилувчи ахборотнинг криптоҳимоясини соддалаштиради.

Очиқ калитли криптотизимларни бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алохида тилга олиш ўринли. Ҳозирда энг самарали ва кенг тарқалган очиқ калитли шифрлаш алгоритми сифатида RSA алгоритмини кўрсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Rivest, Shamir ва Adleman).

Алгоритм модуль арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги қадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-қадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-қадам. Калитнинг очиқ ташкил этувчиси n ҳосил қилинади

$$n=p*q.$$

3-қадам. Қуйидаги формула бўйича Эйлер функцияси ҳисобланади:

$$f(p,q)=(p-1)(q-1).$$

Эйлер функцияси n билан ўзаро туб, 1 дан n гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига эга бўлмаган сонлар тушунилади.

4-қадам. $f(p,q)$ қиймати билан ўзаро туб бўлган катта туб сон d танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи е сони аниқланади

$$e \cdot d = 1 (mod f(p,q)).$$

Бу шартга биноан $e \cdot d$ кўпайтманинг $f(p,q)$ функцияга бўлишдан қолган қолдиқ 1га тенг. е сони очиқ калитнинг иккинчи ташкил этувчиси сифатида қабул қилинади. Махфий калит сифатида d ва n сонлари ишлатилади.

6-қадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блокларга ажратилади, бу ерда $L-L \geq \log_2(n+1)$ шартини қаноатлантирувчи энг кичик бутун сон. Ҳар бир блок [0, n-1] оралиқка тааллукли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот $X(i)$, i=1,l сонларнинг кетма-кетлиги орқали ифодаланади. i нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи $Y(i)$ сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e \pmod n.$$

Ахборотни расшифровка қилишда қуйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d \pmod n.$$

Мисол. <ГАЗ> сўзини шифрлаш ва расшифровка қилиш талаб этилсин. Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. p=3 ва q=11 танлаб олинади.

2-қадам. $n = 3 \cdot 11 = 33$ ҳисобланади.

3-қадам. Эйлер функцияси аниқланади.

$$f(p,q) = (3-1)\cdot(11-1) = 20$$

4-қадам. Ўзаро туб сон сифатида d=3 сони танлаб олинади.

5-қадам. $(e \cdot 3) \cdot (\mathrm{mod}\, 20) = 1$ шартини қаноатлантирувчи e сони танланади. Айтайлик, e=7.

6-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквиваленти аниқланади. А харфига –1, Г харфига-4, З харфига –9. Ўзбек алфавитида 36та харф ишлатилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак бўлади. Дастлабки ахборот иккили кодда қуйидаги кўринишга эга бўлади:

000100 000001 001001.

Блок узунлиги L бутун сонлар ичидан $L \geq \log_2(33+1)$ шартини қаноатлантирувчи минималь сон сифатида аниқланади. n=33 бўлганлиги сабабли L=6.

Демак, дастлабки матн $X(i) =< 4,1,9 >$ кетма-кетлик кўринишида ифодаланади.

7-қадам. $X(i)$ кетма-кетлиги очиқ калит {7,33} ёрдамида шифрланади:

$$Y(1) = (4^7)(\mathrm{mod}\, 33) = 16384(\mathrm{mod}\, 33) = 16$$

$$Y(2) = (1^7)(\mathrm{mod}\, 33) = 1(\mathrm{mod}\, 33) = 1$$

$$Y(1) = (9^7)(\mathrm{mod}\, 33) = 4782969(\mathrm{mod}\, 33) = 15$$

Шифрланган сўз $Y(i)$=<16,1,15>

Шифрланган сўзни расшифровка қилиш махфий калит {3,33} ёрдамида бажарилади.:

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

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

$$Y(1) = (15^3)(\mathrm{mod}\, 33) = 3375(\mathrm{mod}\, 33) = 9$$

Дастлабки сон кетма-кетлиги расшифровка қилинган $X(i)$=<4,1,9> кўринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Келтирилган мисолда ҳисоблашларнинг соддалигини таъминлаш мақсадида мумкин бўлган кичик сонлардан фойдаланилди.

Эль-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. RSA ва Эль-Гамал тизимларининг асосий камчилиги сифатида модуль арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш мумкин. Бу ўз навбатида айтарлича ҳисоблаш ресурсларини талаб қилади.

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

Барча очиқ калитли шифрлаш усуллари учун *NP*-тўлиқ масалани (тўлиқ саралаш масаласи) ечишга асосланган криптотахлил усулидан бошқа усулларининг йўқлиги қатъий исботланмаган. Агар бундай масалаларни ечувчи самарали усуллар пайдо бўлса, бундай хилдаги криптотизим обрўсизлантирилади.

Юқорида кўрилган шифрлаш усулларининг криптобардошлиги калит узунлигига боғлиқ бўлиб, бу узунлик замонавий тизимлар учун, лоақал, 90 битдан катта бўлиши шарт.

3.4. Шифрлаш стандартлари

Россиянинг ахборотни шифрлаш стандарти. Росссия Федерациясида ҳисоблаш машиналари, комплекслари ва тармокларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар махфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усулларида амалга оширилиши мумкин.

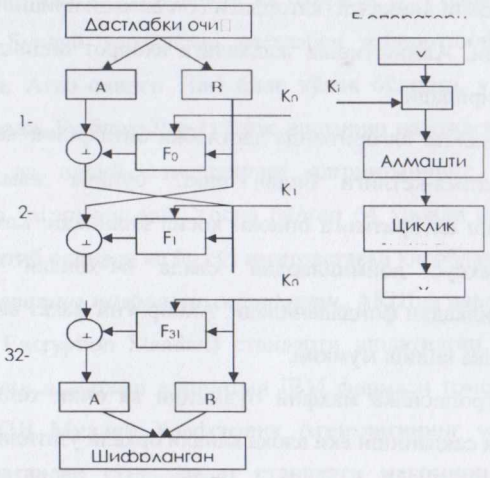
Стандартда ахборотни криптографик ўзгартиришнинг қуйидаги алгоритмлари мавжуд:

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

Бу алгоритмлар учун 8 та 32 хонали иккили сўзларга ажратилган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий ҳисобланади.

Оддий алмаштириш алгоритмининг моҳияти қуйидагича (3.12-расм).

Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали A ва B иккили сўзларга ажратилади. A сўзлар блокнинг кичик хоналарини B сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони i=32 бўлган циклик итерация оператори F_i қўлланилади. Блокнинг кичик битларидаги сўз (биринчи итерациядаги A сўзи) калитининг 32 хонали сўзи билан $mod2^{32}$ бўйича жамланади; ҳар бири 4 битдан иборат қисмларга (4 хонали кириш йўли векторлари) ажратилади; махсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилади; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги B сўзи) билан mod 2 бўйича жамланади.



5.12-расм. Оддий алмаштириш алгоритмида шифрлаш жараёнининг блок-

Ҳар бир i-итерацияда K_j калитнинг (калитлар 8 та) 32 хонали сўзи қуйидаги қоидага биноан танланади

$$K_j = \begin{cases} (i\text{-}1) \bmod 8, & 1 \le i \le 24 \text{ бўлганда,} \\ 32\text{-}i, & i \ge 25 \text{ бўлганда,} \\ 0, & i = 32 \text{ бўлганда.} \end{cases}$$

$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \le i \le 24 \quad \text{бўлганда,} \\ 32 - i, & i \ge 25 \quad \text{бўлганда,} \\ 0, & i = 32 \quad \text{бўлганда,} \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби қуйидаги кўринишда бўлади:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,$

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0,$.

Расшифровка қилишда калитлар тескари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узелларидан иборат. Алмаштириш узели ҳар бирида алмаштириш вектори (4 бит) жойлашган 16 қаторли жадвалдан иборат. Кириш йўли вектори жадвалдаги қатор адресини аниқласа, қатордаги сон алмаштиришнинг чиқиш йўли вектори ҳисобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам ўзгартирилади.

Гаммалаш алгоритмида дастлабки битларнинг кетма-кетлиги гамманинг битлари кетма-кетлиги билан mod2 бўйича жамланади. Гамма оддий алмаштириш алгоритмига биноан ҳосил қилинади. Гаммани шакллантиришда иккита махсус доимийлардан ҳамда 64-хонали иккили кетма-кетилик синхропосилкадан фойдаланилади. Ахборотни фақат синхропосилка борлигида расшифровка қилиш мумкин.

Синхропосилка махфий бўлмайди ва очиқ ҳолда ҳисоблаш машинаси хотирасида сақланиши ёки алоқа канали орқали узатилиши мумкин.

Тескари боғланишли гаммалаш алгоритми гаммалаш алгоритмидан фақат шифрлаш жараёнининг биринчи қадамидаги ҳаракатлар билан фарқланади.

Имитовставка нотўғри ахборотни зўрлаб киритилишидан ҳимоялашда ишлатилади. Имитовставка дастлабки ахборот ва махфий калитни ўзгартириш функцияси хисобланади. У k бит узунликдаги иккили кетма-кетликдан иборат бўлиб, k нинг киймати нотўғри ахборотнинг зўрлаб киритилиши эҳтимоллиги $P_{зк}$ билан қуйидаги муносабат билан боғланган.

$$P_{зк}=\frac{1}{2^k}$$

Имитоставкани шакллантириш алгоритми қуйидаги харакатларнинг кетма-кетлигидан иборат. Очиқ ахборот 64 битли $T(i)$ (i=1,2,3,....,m) блокларга ажратилади, бу ерда m-шифрланувчи ахборот хажми орқали аниқланади. Биринчи блок $T(1)$ оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки ахборот шифрланишда ишлатиладиган калит олинади. Олинган 64 битли иккили сўз иккинчи блок $T(2)$ билан mod2 бўйича жамланади. $T(1)$ блок устида қандай итерация ўзгартиришлари бажарилган бўлса жамлаш натижаси устида ҳам шундай ўзгартиришлар амалга оширилади ва охирида $T(3)$ блок билан mod2 бўйича жамланади. Бундай харакатлар дастлабки ахборотнинг m-1 блоки бўйича такрорланади. Агар охирги $T(m)$ блок тўлиқ бўлмаса, у 64 хонагача ноллар билан тўлдиради. Бу блок $T(m-1)$ блок ишланиш натижаси билан mod2 бўйича жамланади ва оддий алмаштириш алгоритмининг биринчи 16 итерациялари бўйича ўзгартирилади. Ҳосил бўлган 64 хонали блокдан к бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка ҳисобланади.

АҚШнинг ахборотни шифрлаш стандарти. АҚШда давлат стандарти сифатида DES(Data Encryption Standart) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чиқилган бўлиб, АҚШ Миллий Хавфсизлик Агентлигининг мутахасислари томонидан текширилгандан сўнг давлат стандарти мақомини олган. DES

стандартидан нафақат федерал департаментлар, балки нодавлат ташкилотлар, нафақат АҚШда, балки бутун дунёда фойдаланиб келинган.

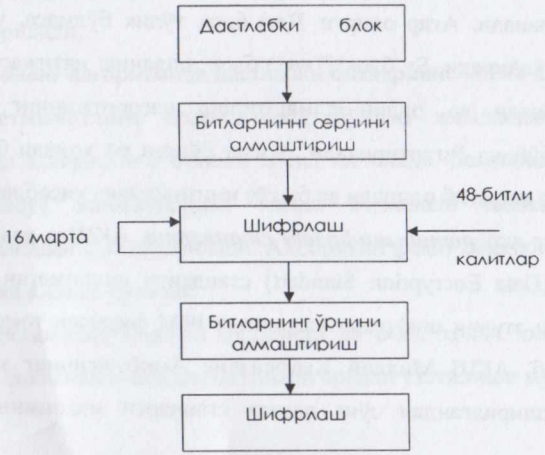
DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади.

Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 3.13–расмда келтирилган.

Ҳозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроқсиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу ЭҲМлар-нинг замонавий ривожи учун жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вакт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).



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

Бу сабаблар АҚШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон қилишига олиб келди. Танлов шартларига биноан алгоритмга қуйидаги талаблар қўйилган эди:

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

Ундан ташқари танловда иштирок этувчилар учун қуйидаги тавсиялар берилган эди:

- ҳам аппарат усулда ҳам программ усулда осонгина амалга оширилувчи амаллардан фойдаланиш;
- 32 хонали процессорлардан фойдаланиш;
- иложи борича шифр структурасини мураккаблаштирмаслик. Бу ўз навбатида барча қизиқувчиларнинг алгоритмни мустақил тарзда криптотахлил қилиб, унда қандайдир хужжатсиз имкониятлар йўқлигига ишонч ҳосил қилишлари учун зарур ҳисобланади.

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

Ҳозирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж.Деймен (J. Daemen) ва В. Райджмен (V.Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокли шифр бўлиб, кодланувчи маълумотларнинг ҳар бир блоки қабул қилинган блок узунлигига қараб 4x4, 4x6 ёки 4x8 ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

Шифрдаги барча ўзгартиришлар қатъий математик асосга эга. Амалларнинг структураси ва кетма-кетлиги алгоритмнинг ҳам 8-битли, ҳам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм структурасида баъзи амалларнинг параллел ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Ўзбекистоннинг ахборотни шифрлаш стандарти. Ушбу "Маълумотларни шифрлаш алгоритми" стандарти Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган ва унда Ўзбекистон Республикасининг "Электрон рақамли имзо хусусида"ги ва "Электрон хужжат алмашинуви хусусида"ги қонунларининг меъёрлари амалга оширилган.

Ушбу стандарт – криптографик алгоритм, электрон маълумотларни ҳимоялашга мўлжалланган. Маълумотларни шифрлаш алгоритми симметрик блокли шифр бўлиб, ахборотни шифрлаш ва расшифровка қилиш учун ишлатилади. Алгоритм 128 ёки 256 бит узунлигидаги маълумотларни шифрлашда ва расшифровка қилишда 128, 256, 512 битли калитлардан фойдаланиши мумкин.

Стандарт ЭҲМ тармоқларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ЭҲМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш қоидасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари қуйидаги камчиликларга эга:

- ахборот алмашувчи икала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига қуйиладиган талабларнинг қатъийлиги;
- калитларни яратиш ва тақсимлаш хизматига қуйиладиган талабларнинг юқорилиги. Сабаби, ўзаро алоқанинг «ҳар ким – хар ким билан» схемасида «n» та абонент учун $n(n\text{-}1)/2$ та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғлиқлиги квадратли. Масалан, n=1000 абонент учун талаб қилинадиган калитлар сони $n(n\text{-}1)/2$=499500. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва воситаларсиз қўллашнинг иложи йўқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криптоалгоритми RSA (5.3 га қаралсин) 1993 йилда стандарт сифатида қабул қилинди. Ушбу криптоалгоритм ҳар тарафлама тасдикланган ва калитнинг етарли узунлигида бардошлиги эътироф этилган. Ҳозирда 512 битли калит бардошликни таъминлашда етарли ҳисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор қувватининг ошиши RSA криптоалгоритмининг тўлиқ саралаш хужумларга бардошлигининг йўқолишига олиб келади. Аммо, процессор қувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

- калитларни махфий тарзда етказиш зарурияти йўқ; асимметрик шифрлаш очиқ калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса ҳимояланган алоқа сеанси бошланишидан аввал махфий калитлар алмашиниши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли боғланишлиги йўқолади; RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига боғлиқлиги чизиқли кўринишга эга (N фойдаланувчиси бўлган тизимда $2N$ калит ишлатилади).

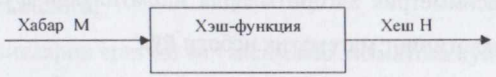
Аммо асимметрик криптотизимлар, хусусан RSA криптотизими, камчиликлардан ҳоли эмас:

- ҳозиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтарилмаслигининг математик исботи йўқ;
- асимметрик шифрлаш симметрик шифрлашга нисбатан секин амалга оширилади, чунки шифрлашда ва расшифровка қилишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, RSAда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;

- очиқ калитларни алмаштириб қуйилишидан ҳимоялаш зарур. Фараз қилайлик "*A*" абонентнинг компьютерида "*B*" абонентнинг очиқ калити "K_B" сақланади. "*n*" нияти бузуқ одам "*A*" абонентда сақланаётган очиқ калитлардан фойдалана олади. У ўзининг жуфт (очиқ ва махфий) "K_n" ва "k_n" калитларини яратади ва "*A*" абонентда сақланаётган "*B*" абонентнинг "K_B" калитини ўзининг очиқ "K_n" калити билан алмаштиради. "*A*" абонент қандайдир ахборотни "B" абонентга жўнатиш учун уни "K_n" калитда (бу "K_B" калит деб ўйлаган ҳолда) шифрлайди. Натижада, бу хабарни "*B*" абонент ўқий олмайди, "*n*" абонент осонгина расшифровка қилади ва ўқийди. Очиқ калитларни алмаштиришни олдини олишда калитларни сертификациялашдан фойдаланилади.

3.5. Хэшлаш функцияси

Хэшлаш функцияси (хэш-функцияси) шундай ўзгартиришки, кириш йўлига узунлиги ўзгарувчан хабар *M* берилганида чиқиш йўлида белгиланган узунликдаги қатор $h(M)$ ҳосил бўлади. Бошқача айтганда, хеш-функция $h(.)$ аргумент сифатида узунлиги ихтиёрий хабар (хужжат) *M* ни қабул қилади ва белгиланган узунликдаги хеш-қиймат (хеш) $H=h(M)$ни қайтаради (3.14-расм).



3.14-расм. Хэшни шакллантириш схемаси

Хэш-қиймат h(M) – хабар M нинг дайджести, яъни ихтиёрий узунликдаги асосий хабар *M*нинг хичлантирилган иккилик ифодаси. Хэшлаш функцияси ўлчами мегабайт ва ундан катта бўлган имзо чекилувчи хужжат *M*ни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлаштиришга имкон

беради. Таъкидлаш лозимки, хеш-функция $h(M)$ қийматининг хужжат Mга боғлиқлиги мураккаб ва хужжат Mнинг ўзини тиклашга имкон бермайди.

Хэшлаш функцияси қуйидаги хусусиятларга эга бўлиши лозим:

1. Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.
2. Хэш-функция чиқиш йўлининг қиймати белгиланган ўлчамга эга.
3. Хэш-функция $h(x)$ ни ихтиёрий "x" учун етарлича осон ҳисобланади. Хэш-функцияни ҳисоблаш тезлиги шундай бўлиши керакки, хэш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.
4. Хэш-функция матн M даги орасига қўйишлар (вставки), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва ҳ. каби ўзгаришларга сезгир бўлиши лозим.
5. Хэш-функция қайтарилмаслик хусусиятига эга бўлиши лозим.
6. Иккита турли хужжатлар (уларнинг узунлигига боғлиқ бўлмаган ҳолда) хэш-функциялари қийматларининг мос келиши эҳтимоллиги жуда кичкина бўлиши шарт, яъни ҳисоблаш нуқтаи назаридан $h(x')=h(x)$ бўладиган $x' \neq x$ ни топиш мумкин эмас.

Иккита турли хабар бита тугунчага (свертка) зичлаштириш назарий жиҳатдан мумкин. Бу коллизия ёки тўқнашиш деб аталади. Шунинг учун хэшлаш функциясининг бардошлигини таъминлаш мақсадида тўқнашишларга йўл қўймасликни кўзда тутиш лозим. Тўқнашишларга бутунлай йўл қўймаслик мумкин эмас, чунки умумий ҳолда мумкин бўлган хабарлар сони хэшлаш функциялари чиқиш йўллари қийматларининг мумкин бўлган сонидан ортиқ. Аммо, тўқнашишлар эҳтимоллиги паст бўлиши 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 қилиб, хэшлаш функциясидан хабар ўзгаришини пайқашда фойдаланиш мумкин, яъни у *криптографик назорат йиғиндисини*

(ўзгаришларни пайқаш коди ёки *хабарни аутентификациялаш коди* деб ҳам юритилади) шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон рақамли имзони шакллантаришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентификациялашда ҳам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули *бир томонлама хеш-функция ёрдамида шифрлаш* ишлатилади. Бу шифрлашнинг ўзига хослиги шундан иборатки, у моҳияти бўйича, бир томонламадир, яъни тескари муолажа – қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) 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 чиқилган ахборот дайджестини ҳисобловчи алгоритм. Уларнинг ҳар бири 128 битли хэш-кодни тўзади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тезкор ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси бўлиб, MD4 алгоритмида хавфсизликнинг оширилиши эвазига тезликдан ютказилган. SHA(Secure Hash Algorithm) – 160 битли *хэш-код*ни тузувчи ахборот дайджестини ҳисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбатан ишончлирок.

3.6. Электрон рақамли имзо

Электрон хужжатларни тармоқ орқали алмашишда уларни ишлаш ва сақлаш харажатлари камаяди, қидириш тезлашади.Аммо, электрон хужжат муаллифини ва хужжатнинг ўзини аутентификациялаш, яъни муаллифнинг хақиқийлигини ва олинган электрон хужжатда ўзгаришларнинг йўқлигини аниқлаш муаммоси пайдо бўлади.

Электрон хужжатларни ауентификациялашдан мақсад уларни мумкин бўлган жинояткорона харакатлардан ҳимоялашдир. Бундай харакатларга қуйидагилар киради:

- *фаол ушлаб қолиш* - тармоққа уланган бузғунчи хужжатларни (файлларни) ушлаб қолади ва ўзгартиради.

- *маскарад* – абонент *C* хужжатларни абонент *B* га абонент *A* номидан юборади;

- *ренегатлик* – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;

- *алмаштириш* – абонент *B* хужжатни ўзгартиради, ёки янгисини шакиллантирадива уни абонент *A* дан олганман дейди;

- *такрорлаш* – абонент *A* абонент *B* га юборган хужжатни абонент *C* такрорлайди.

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

Электрон рақамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хақикийлигини текшириш муаммосини самарали ҳал этишга имкон беради.

Электрон рақамли имзо телекоммуникация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қуйидаги афзалликларга эга:

- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;

- бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;

- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон рақамли имзо-имзо чекилувчи матн билан бирга узатилувчи қўшимча рақамли хабарнинг нисбатан катта бўлмаган сонидир.

Электрон рақамли имзо асимметрик шифрларнинг қайтарувчанлигига ҳамда хабар таркиби, имзонинг ўзи ва калитлар жуфтининг ўзаро боғлиқлигига асосланади. Бу элементларнинг хатто биринг ўзгариши рақамли имзонинг ҳақиқийлигини тасдиқлашга имкон бермайди. Электрон рақамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш–функциялари ёрдамида амалга оширилади.

Электрон рақамли имзо тизимининг қўлланишида бир- бирига имзо чекилган электрон хужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз қилинади. Ҳар бир абонент учун жуфт – маҳфий ва очиқ калит генерацияланади. Маҳфий калит абонентда сир сақланади ва ундан абонент электрон рақамли имзони шакллантиришда фойдаланади.

Очиқ калит бошқа барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон хужжатни қабул қилувчи электрон рақамли имзони текширишда фойдаланади.

Электрон рақамли имзо тизими иккита асосий муолажани амалга оширади:

- рақамли имзони шакллантириш муолажаси;
- рақамли имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очиқ калитидан фойдаланилади.

Рақамли имзони шакллантириш муолажаси.

Ушбу муолажани тайёрлаш босқичида хабар жўнатувчи абонент A иккита калитни генерациялайди: маҳфий калит k_A ва очиқ калит K_A. Очиқ калит K_A унинг жуфти бўлган махфий калити k_A дан ҳисоблаш орқали олинади. Очиқ калит K_A тармоқнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жўнатувчи A аввало имзо чекилувчи матн M нинг хеш функцияси $L(M)$ қийматини ҳисоблайди (3.15-расм).

Хеш-функция имзо чекилувчи дастлабки матн *"M"* ни дайджест *"m"* га зичлаштиришга хизмат қилади. Дайджест *M*–бутун матн *"M"* ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан қисқа сондир. Сўнгра жўнатувчи *A* ўзининг маҳфий калити k_A билан дайджест *"m"* ни шифрлайди. Натижада олинган сонлар жуфти берилган *"M"* матн учун рақамли имзо ҳисобланади. Хабар *"M"* рақамли имзо билан биргаликда қабул қилувчининг адресига юборилади.

3.15-расм. Электрон рақамли имзони шакллантириш схемаси.

Рақамли имзони текшириш муолажаси.

Тармоқ абонентлари олинган хабар *"M"* нинг рақамли имзосини ушбу хабарни жўнатувчининг очиқ калити K_A ёрдамида текширишлари мумкин (3.16-расм).

Электрон рақамли имзони текширишда хабар *"M"*ни қабул қилувчи *"B"* қабул қилинган дайджестни жўнатувчининг очиқ калити *"K_A"* ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хеш-функция *h(M)* ёрдамида қабул қилинган хабар *"M"* нинг дайджести *"m"* ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест *"m"* ва *"m'"* мос келса рақамли имзо ҳақиқий ҳисобланади. Акс ҳолда имзо қалбакилаштирилган, ёки ахборот мазмуни ўзгартирилган бўлади.

3.16–расм. Электрон рақамли имзони текшириш схемаси.

Электрон рақамли имзо тизимининг принципиал жиҳати– фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги махфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни рухсатсиз фойдаланишдан химоялаш зарур. Электрон рақамли имзонинг махфий калитини, симметрик шифрлаш калитига ўхшаб, шахсий калит элитувчисида, ҳимояланган ҳолда сақлаш тавфсия этилади.

Электрон рақамли имзо имзо чекилувчи хужжат ва махфий калит орқали аниқланувчи ноёб сондир. Имзо чекилувчи хужжат сифатида ҳар қандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо қўшилиши орқали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рақамли имзо имзо чекилган хужжат муаллифини идентификацияловчи қўшимча ахборотга эга. Бу ахборот хужжатга электрон рақамли имзо ҳисобланмасидан олдин қўшилади. Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана;
- ушбу имзо калити таъсирининг тугаши муддати;
- файлга имзо чекувчи шахс хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);
- имзо чекувчининг индентификатори (очиқ калит номи);
- рақамли имзонинг ўзи.

Асимметрик шифрлашга ўхшаш, электрон рақамли имзони текшириш учун ишлатиладиган очиқ калитнинг алмаштирилишига йўл қўймаслик лозим. Фараз қилайлик, нияти бузуқ одам "*n*" абонент "*B*" компьютерида сақланаётган очиқ калитлардан, хусусан, абонент *A* нинг очиқ калити K_A дан фойдалана олади. Унда у қуйидаги харакатларини амалга ошириши мумкин:

- очиқ калит K_A сақланаётган файлдан абонент *A* хусусидаги инденцификация ахборотини ўқиши;

- ичига абонент *A* хусусидаги индентификация ахборотини ёзган ҳолда шахсий жуфт калитлари k_n ва K_n ни генерациялаши;

- абонент *B*да сақланаётган очиқ калит K_Aни ўзининг очиқ калити K_n билан алмаштириши.

Сўнгра нияти бузуқ одам "*n*" абонент *B* га хужжатларни ўзининг махфий калити k_n ёрдамида имзо чекиб жўнатиши мумкин. Бу хужжатлар имзосини текширишда абонент *B* абонент *A* имзо чеккан хужжатларни ва уларнинг электрон рақамли имзоларини тўғри ва хеч ким томонидан модификацияланмаган деб ҳисоблайди. Абонент А билан муносабатларини бевосита ойдинлаштирилишигача В абонентда олинган хужжатларнинг хақиқийлигига шубҳа туғилмайди.

Электрон рақамли имзонинг катор алгоритмлари ишлаб чиқилган. 1977 йилда АҚШ да яратилган RSA тизими биринчи ва дунёда машҳур электрон рақамли имзо тизими ҳисобланади ва юқорида келтирилган принципларни амалга оширади. Аммо рақамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузуқ одамга махфий калитни билмасдан, хешлаш натижасини имзо чекиб бўлинган хужжатларнинг хешлаш натижаларини кўпайтириш оркали ҳисоблаш мумкин бўлган хужжатлар имзосини шакллантиришга имкон беради.

Ишончлилигининг юқорилиги ва шахсий компьютерларда амалга оширилишининг қулайлиги билан ажралиб турувчи рақамли имзо алгоритмли 1984 йилда Эль Гамал томонидан ишлаб чиқилди. Эль Гамалнинг рақамли имзо алгоритми (EGSA) RSA рақамли имзо алгоритмидаги камчиликлардан ҳоли

бўлиб, АҚШ нинг стандартлар ва технологияларнинг Миллий университети томонидан рақамли имзонинг миллий стандартига асос каби қабул қилинди.

3.7. Криптографик калитларни бошқариш

Ҳар қандай криптографик тизим крпитографик калитлардан фойдаланишга асосланган. Калит ахбороти деганда ахборот тармоқлари ва тизимларида ишлатилувчи барча калитлар мажмуи тушунилади. Агар калит ахборотларининг етарлича ишончли бошқарилиши таъминланмаса, нияти бузуқ одам унга эга бўлиб олиб тармоқ ва тизимдаги барча ахборотдан ҳоҳлаганича фойдаланиши мумкин. Калитларни бошқариш калитларни генерациялаш, сақлаш ва тақсимлаш каби вазифаларни бажаради. Калитларни тақсимлаш калитларни бошқариш жараёнидаги энг маъсулиятли жараён ҳисобланади.

Симметрик криптотизимдан фойдаланилганда ахборот алмашинувида иштирок этувчи иккала томон аввал махфий сессия калити, яъни алмашинув жараёнида узатиладиган барча хабарларни шифрлаш калити бўйича келишишлари лозим. Бу калитни бошқа барча билмаслиги ва уни вақти-вақти билан жўнатувчи ва қабул қилувчида бир вақтда алмаштириб туриш лозим. Сессия калити бўйича келишиш жараёнини калитларни алмаштириш ёки тақсимлаш деб ҳам юритилади.

Асимметрик криптотизимда иккита калит-очиқ ва ёпиқ (махфий) калит ишлатилади. Очиқ калитни ошкор этиш мумкин, ёпиқ калитни яшириш лозим. Хабар алмашинувида фақат очиқ калитни унинг ҳақиқийлигини таъминлаган ҳолда жўнатиш лозим.

Калитларни тақсимлашга қуйидаги талаблар қўйилади:

- тақсимлашнинг оперативлиги ва аниқлиги;
- тақсимланувчи калитларнинг конфиденциаллиги ва яхлитлиги.

Компьютер тармоқларидан фойдаланувчилар ўртасида калитларни тақсимлашнинг қуйидаги асосий усулларидан фойдаланилади.

1. Калитларни тақсимловчи битта ёки бир нечта марказлардан фойдаланиш.
2. Тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашиш.

Биринчи усулнинг муаммоси шундаки, калитларни тақсимлаш марказига кимга, қайси калитлар тақсимланганлиги маълум. Бу эса тармоқ бўйича узатилаётган барча хабарларни ўқишга имкон беради. Бўлиши мумкин бўлган суиистеъмоллар тармоқ хавфсизлигининг жиддий бузилишига олиб келиши мумкин.

Иккинчи усулдаги муаммо – тармоқ субъектларининг ҳақиқий эканлигига ишонч ҳосил қилишдир.

Калитларни тақсимлаш масаласи қуйидагиларни таъминловчи калитларни тақсимлаш протоколини қуришга келтирилади:

- сеанс қатнашчиларининг ҳақиқийлигига иккала томоннинг тасдиқи;
- сеанс ҳақиқийлигининг тасдиқи;
- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тариқасида Kerberos деб аталувчи калитларни аутентификациялаш ва тақсимлаш тизимини кўрсатиш мумкин.

Иккинчи усулга-тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашишга батафсил тўхталамиз.

Симметрик калитли криптотизимдан фойдаланилганда криптографик ҳимояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий махфий калитга эга бўлишлари лозим. Бу фойдаланувчилар умумий калитни алоқа канали бўйича хавфсиз алмашишлари лозим. Агар фойдаланувчилар калитни тез-тез ўзгартириб турсалар калитни етказиш жиддий муаммога айланади.

Бу муаммони ечиш учун қуйидаги иккита асосий усул қўлланилади:

1. Симметрик криптотизимнинг махфий калитини ҳимоялаш учун очиқ калитли асимметрик криптотизимдан фойдаланиш

2. Диффи-Хеллманнинг калитларни очиқ тақсимлаш тизимидан фойдаланиш.

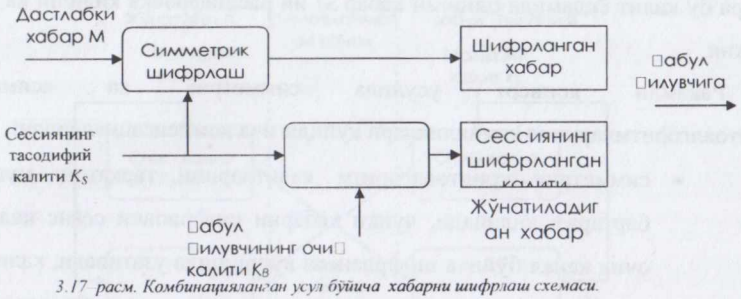
Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптотизим доирасида амалга оширилади. Бундай ёндашишда симметрик криптотизим дастлабки очиқ матнни шифрлаш ва узатишда ишлатилса, очиқ калитли асимметрик криптотизим фақат симметрик криптотизимнинг махфий калитини шифрлаш, узатиш ва кейинги расшифровка қилишда ишлатилади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очиқ калитли асимметрик криптотизимнинг юқори махфийлиги билан махфий калитли симметрик криптотизимнинг юқори тезкорлигининг уйғунлашишга олиб келади. Бундай ёндашиш баъзида *электрон рақамли конверт* схемаси деб юритилади.

Фараз қилайлик, фойдаланувчи A хабар M ни фойдаланувчи B га ҳимояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмоқчи. Унда фойдаланувчиларнинг ҳаракатлари қуйидагича бўлади.

Фойдаланувчи A нинг ҳаракатлари:

1. Симметрик сеанс махфий калит K_S ни яратади (масалан, тасодифий тарзда генерациялайди).
2. Хабар M ни симметрик сеанс махфий калит K_S да шифрлайди.
3. Махфий сеанс калит K_S ни фойдаланувчи (хабар қабул қилувчи) Bнинг очиқ калити K_B да шифрлайди.
4. Фойдаланувчи B адресига алоқанинг очиқ канали бўйича шифрланган хабар M ни шифрланган сеанс калити K_S билан биргаликда узатади.

Фойдаланувчи A нинг харакаталарини 3.17-расмда келтирилган хабарларни комбинацияланган усул бўйича шифрлаш схемаси орқали тушуниш мумкин.

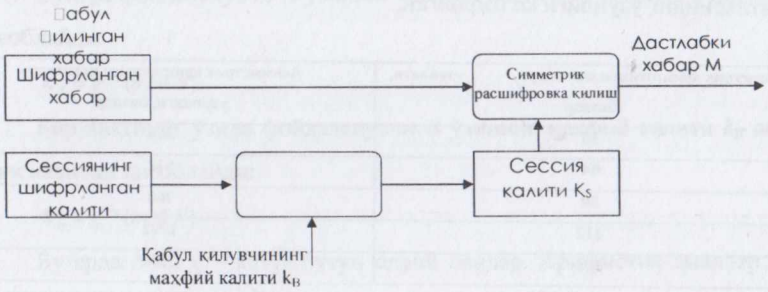


3.17-расм. Комбинацияланган усул бўйича хабарни шифрлаш схемаси.

Фойдаланувчи *B* нинг харакатлари (электрон рақамли конвертни-шифрланган хабар *M* ни ва шифрланган сеанс калити K_S ни олганидан сўнгги) қуйидагича:

1. Ўзининг махфий калити k_B бўйича сеанс калити K_S ни расшифровка килади.
2. Олинган сеанс калити K_S бўйича олинган хабар *M* ни расшифровка қилади.

Фойдланувчи *B* нинг харакатларини 3.18-расмда келтирилган хабарларни комбинацияланган усул бўйича расшифровка қилиш схемаси орқали тушуниш мумкин.



3.18-расм. Комбинацияланган усул бўйича хабарни расшифровка қилиш.

Олинган электрон рақамли конвертни фақат қонуний қабул қилувчи-фойдаланувчи *B* очиши мумкин. Фақат шахсий махфий калит k_B эгаси бўлган фойдаланувчи *B* махфий сеанс калити K_S ни тўғри расшифровка қилиш ва

сўнгра бу калит ёрдамида олинган хабар M ни расшифровка қилиши ва ўқиши мумкин.

Рақамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари қуйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини тарқатиш муаммоси бартараф қилинади, чунки хабарни шифрловчи сеанс калити K_S очиқ канал бўйича шифрланган кўринишда узатилади, калит K_Sни расшифровка қилиш учун асимметрик криптоалгоритмдан фойдаланилади;
- бу ҳолда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо бўлмайди, чунки асимметрик алгоритм бўйича фақат қисқа калит K_S шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм бўйича шифрланади.

Натижада тезкор шифрлаш билан биргаликда калитларнинг қулай тақсимланиши амалга оширилади.

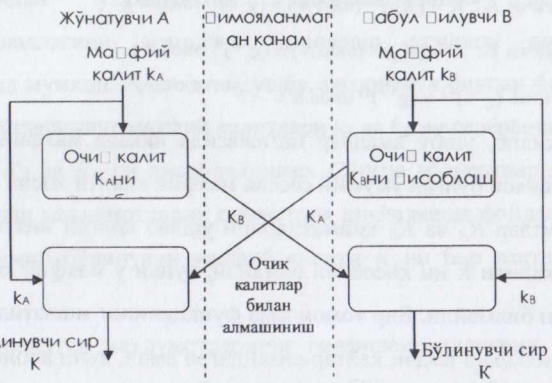
3.1-жадвалда кўп учрайдиган симметрик ва асимметрик криптотизимлар калитларининг узунлиги келтирилган.

3.1-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 очиқ тақсимлаш усули* фойдаланувчиларга калитларни ҳимояланмаган алоқа каналлари орқали алмашишга имкон беради. Унинг хавфсизлиги чегараланган соҳада дискрет логарифмларни ҳисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулининг моҳияти қуйидагича (3.19-расм).



3.19–расм. Диффи-Хеллманнинг калитларни очиқ тақсимлаш схемаси

Ахборот алмашинувида иштирок этувчи фойдаланувчилар А ва В мустақил равишда ўзларининг махфий калитларини k_A ва k_B ни генерациялайдилар (k_A ва k_B калитлар фойдаланувчилар А ва В лар сир сақловчи тасодифий катта бутун сонлар).

Сўнгра фойдаланувчи А ўзининг махфий калити k_A асосида очиқ калитни ҳисоблайди:

$$K_A = g^{K_A} (\mathrm{mod}\, N).$$

Бир вақтнинг ўзида фойдаланувчи B ўзининг махфий калити k_B асосида очиқ калитни ҳисоблайди:

$$K_B = g^{K_B} (\mathrm{mod}\, N).$$

Бу ерда N ва g – катта бутун оддий сонлар. Арифметик амаллар Nнинг модулига келтириш орқали бажарилади. N ва g сонларни сир сақлаш шарт эмас, чунки одатда, бу қийматлар тармоқ ва тизимдан фойдаланувчиларнинг барчаси учун умумий ҳисобланади.

Сўнгра фойдаланувчилар А ва В ўзларининг очиқ калитларини ҳимояланмаган канал орқали алмаштирадилар ва умумий сессия махфий калити Kни (бўлинувчи сирни) ҳисоблашда ишлатадилар:

фойдаланувчи А: $K = (K_B)^{k_A} (\mathrm{mod}\, N) = (g^{k_B})^{k_A} (\mathrm{mod}\, N)$,

фойдаланувчи В: $K' = (K_A)^{k_B} (\mathrm{mod}\, N) = (g^{k_A})^{k_B} (\mathrm{mod}\, N)$,

бунда $K = K'$, чунки $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} (\mathrm{mod}\, N)$.

Шундай қилиб, ушбу амаллар натижасида иккала махфий калит k_A ва k_Bларнинг функцияси бўлган умумий сессия махфий калити ҳосил қилинади.

Очиқ калитлар K_A ва K_B қийматларини ушлаб қолган нияти бузуқ одам сессия махфий калити K ни ҳисоблай олмайди, чунки у махфий калитлар k_A ва k_B қийматларини билмайди. Бир томонлама функциянинг ишлатилиши сабабли очиқ калитни ҳисоблаш амали қайтарилмайдиган амал, яъни абонентнинг очиқ калити қиймати бўйича унинг махфий калитини ҳисоблаш мумкин эмас.

Диффи-Хеллман усулининг ноёблиги шундан иборатки, абонентлар жуфти тармоқ орқали очиқ калитларни узатганларида фақат ўзларига маълум махфий сонни олиш имкониятига эга. Сўнгра абонентлар узатилаётган ахборотни маълум текширилган усулни – олинган умумий сессия махфий калитидан фойдаланган ҳолда симметрик шифрлашни ишлатиб ҳимоялашга киришишлари мумкин.

Диффи-Хеллман схемаси маълумотларни ҳар бир сеансда янги калитларда шифрлаш имконини беради. Бу сирларни дискетларда ёки бошқа элтувчиларда сақламасликка имкон беради, чунки бундай сақлаш уларни рақиблар ёки нияти бузуқ одамлар қулига тушиб қолиш эҳтимоллигини оширади.

Диффи-Хеллман схемаси *узатилаётган маълумотларнинг конфиденциаллигини ва аутентлигини (аслига тўғрилигини) комплекс ҳимоялаш усулини* ҳам амалга ошириш имконини беради. Алгоритм фойдаланувчига рақамли имзони ва симметрик шифрлашни бажаришда бир хил калитларни шакллантириш ва ишлатиш имконини беради.

Маълумотлар яхлитлигини ва конфиденциаллигини бир вақтда ҳимоялаш учун шифрлаш ва электрон рақамли имзодан комплекс фойдаланиш мақсадга мувофиқ ҳисобланади. Диффи-Хеллман схемаси ишлашининг оралиқ

натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллагини комплекс ҳимоялаш усулини амалга оширишда фойдаланиш мумкин. Ҳақиқатан, ушбу алгоритмга биноан фойдаланувчилар A ва B аввал ўзларининг махфий калитлари k_A ва k_B ни генерациялайдилар ва очиқ калитлари K_A ва K_B ни ҳисоблайдилар. Сўнгра абонентлар A ва B бу оралиқ натижалардан маълумотларни симметрик шифрлашда фойдаланилиши мумкин бўлган умумий бўлинувчи махфий калити K ни бир вақтда ҳисоблаш учун ишлатади.

Узатилаётган маълумотларнинг конфиденциаллигини ва аутентилигини комплекс ҳимоялаш усули қуйидаги схема бўйича ишлайди:

- абонент A рақамли имзонинг стандарт алгоритмидан фойдаланиб, ўзининг махфий калити k_A ёрдамида хабар M га имзо чекади;

- абонент A ўзининг махфий калити k_A ва абонент B нинг очиқ калити K_B дан Диффи-Хеллман алгоритми бўйича умумий бўлинувчи махфий калити K ни ҳисоблайди.

- абонент A олинган ўзаро бўлинувчи махфий калитда алмашинув бўйича шериги билан келишилган симметрик шифрлаш алгоритмидан фойдаланган ҳолда хабар M ни шифрлайди;

- абонент B шифрланган хабар M ни олиши билан ўзининг махфий калити k_B ва абонент A нинг очиқ калити K_A дан Диффи-Хеллман алгоритми бўйича ўзаро бўлинувчи махфий калит K ни ҳисоблайди;

- абонент B олинган хабар M ни калити K да расшифровка қилади;

- абонент B абонент A нинг очиқ калит K_A ёрдамида расшифровка қилинган хабар M имзосини текширади.

Диффи-Хеллман схемаси асосида тармоқ сатҳида ҳимояланган виртуал тармоқлар VPN қурилишида қўлланилувчи криптокалитларни бошқариш протоколлари SKIP (Simple Key Management for Internet Protocols) ва IKE (Internet Key Exchange) ишлайди.

Назорат учун саволлар :

1. Компьютер стеганографиясининг моҳияти нимадан иборат ?
2. Криптографияда ўринларни алмаштириш усули қандай усул ?
3. Криптографияда ассимметрик алгоритмларнинг ўзига хос хусусиятлари нималардан иборат ?
4. Ассимметрик алгоритмларда очиқ ва ёпиқ калитларнинг вазифаси нимадан иборат?

IV боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ИСТИҚБОЛЛАРИ

Ахборот технологиялари, инфраструктуралари ривожланиши ва мураккаблашуви билан улардаги ахборот хавфсизлиги муаммолари аҳамияти янада ошиб бормоқда. Сабаби, турли хил корхоналар, давлат органлари маҳкамалари ахборот айирбошлашда янги усулларни жорий этмоқдалар, тижорат соҳасида янги технологиялар ва қурилмалардан фойдаланмоқдалар. Буларнинг барчаси ахборот хавфсизлиги нуқтаи-назаридан таҳдидлар сонининг ошишига олиб келмоқда. Булардан ташқари таҳдидлар шиддатли тус олмоқда, чунки хакерлар, спамерлар ва бошқа бузғунчилар, ахборот технологияларида қўлланиладиган хавфсизлик чоралари ва воситалари имкониятларини билган ҳолда, уларни четлаб ўтиш имконига эга бўлган ҳужумлар уюштирмоқдалар.

Таҳдидларнинг манбаини аниқлаш, уларнинг турлари ва амалга ошириш усулларининг кенг кўлами компьютерларда, тармоқларда, ахборот тизимларида, Интернет тармоғида ахборот хавфсизлигини таъминлашга қаратилган кўплаб технологиялар, воситалар яратилишига олиб келди. Яратилган дастурий таъминот асосида корхоналар хавфсизлик сиёсатига мувофиқ равишда ахборотнинг яхлитлигини, унга мурожаат килиш имкониятини, махфийлигини таъминлашлари мумкин бўлди. Бундай дастурий таъминот асосида вируслардан ҳимояланиш, муҳим бўлган маълумотларни шифрлаш, ҳужумларни аниқлаш ва бартараф этиш, тизимдаги заифликларни аниқлаш мумкин бўлди.

4.1. Ахборот технологиялари соҳасидаги таҳдидлар

4.1.1. Ҳужумлар сонининг ўсиши

Америка Қўшма Штатлари компьютер хавфсизлиги институти (Computer Security Institute, CSI), «2007 CSI Computer Crime and Security Survey» номли ҳисоботи маълумотларига кўра, сўровда қатнашган компанияларнинг 26% и ўзларида 10 дан ортиқ хавфсизликка қарши қаратилган бузғунчилик ҳаракатлари амалга оширилганлигини эътироф этганлар. 2004 йилда сўровда қатнашган компанияларнинг 12% ида, 2005 ва 2006 йилларда 9% ида шундай ҳолат кузатилган. Хавфсизлик борасида бузғунчилик ҳаракатларига дуч келган компаниялар салмоғи камайгани билан (2007 йилда сўралган компаниялардан 46% и, 2005 йилда 56% и, 2006 йилда йилда 53 % и) таҳдидлар шиддатли тус олиши билан бирга бузғунчилар компаниялар маълумотларини яширин ўғирлашда тажрибалари ошганликлари кузатилган.

Уюштириладиган ҳужумлар алоҳида танлаб олинган компанияларга қаратилиши (бундай ҳолат сўровда иштирок этган компанияларнинг 5% ида кузатилган) ҳужумни аниқлаш ва унинг олдини олишда мураккабликлар туғдирган. Сабаби, ҳужум уюштиришни амалга оширувчи дастур коди антивирус дастурлари базасидан ўрин олмаган ўзига хос кодга эга бўлган. Натижада баъзи компаниялар ўзларига ҳужум уюштирилганлигини билмаганлар ҳам.

Ахборотга қаратилган ҳужумлар компанияларга катта миқдорда молиявий зарар етказмоқдалар. Энг кўп зарар компьютер вируслари ҳиссасига тўғри келади. 3.1.1-жадвалда 2007 йилда АҚШ компаниялари томонидан кўрилган зарар миқдорлари келтирган.

4.1.1-жадвал. 2007 йилда АҚШ компанияларига энг кўп молиявий зарар етказган таҳдидлар 10 талиги, (манба: CSI, 2007)

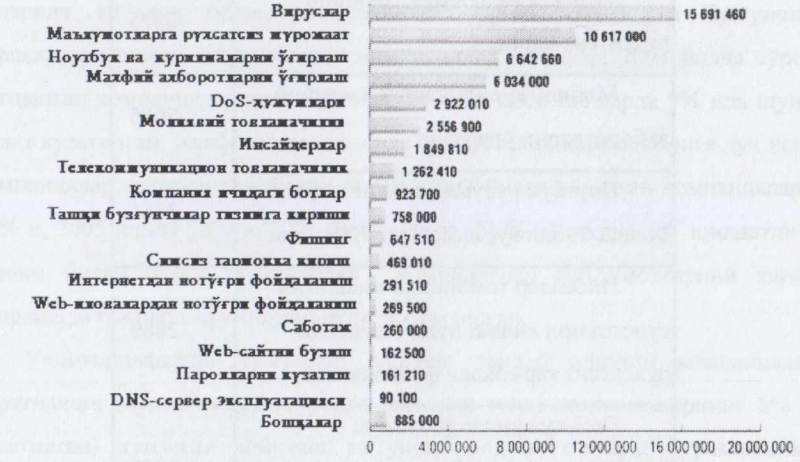
Ахборот технологиясига бўлган таҳдид	Зарар миқдори, минг дол-

	ларда.
Вируслар	8391
Тизимга ташқи бузғунчининг рухсатсиз кириши	6875
Мобиль қурилмалардан махфий ахборотларни ўғирлаш	5685
Ноутбук русумли компьютерлар ва Бошқа мобил қурилмаларни ўғирлаш	3881
Инсайдер томонидан ваколатни суистеъмол қилиш йўли билан ёки рухсатсиз тармоқдан фойдаланиш	2889
DoS-ҳужумлар (Denial of Service — хизмат кўрсатишдан воз кечиш)	2888
Компания ичида ботлар	2869
Фишинг	2752
Саботаж	1056
Маълумотларга рухсатсиз мурожаат қилиш	1042
Web-сайтни бузиш	725

2007 йилда АҚШ компанияларининг ўртача зарар миқдори 350,4 минг долларни ташкил этди. 2006 йилда бу кўрсаткич 168 минг долларни ташкил этган.

CSI/FBI Computer Crime and Security Survey ҳисоботи маълумотларига кўра, 2006 йилда АҚШ бўйича ахборот тизимлари ва уларнинг

инфраструктураларига бўлган ҳужумлар натижасида кўрилган зарар миқдори жами 52 494 290 долларни ташкил этган (4.1.1-расм).



2006 йил бўйича жами зарар – 52 494 290 доллар.

4.1.1-расм. 2006 йилда АҚШ компанияларида ҳужумлар натижасида кўрилган зарар миқдори тақсимоти.

4.1.2. Ички таҳдидлар

Анъанавий равишда ташқи таҳдидлар (биринчи навбатда вируслар таҳдиди) энг хавфли таҳдидлар деб ҳисобланиб, уларга алоҳида эътибор бериб келинган. Бироқ кейинги йилларда ички таҳдидлар, айникса инсайдерлар таҳдидлари вируслар таҳдидларидан ўзиб кетган. Computer Economics тадқиқот марказининг «Trends in IT Security Threats: 2007» номли ҳисоботида келтирилган молиявий зарар миқдори бўйича инсайдерлар таҳдиди биринчи ўринни эгаллаган. Malware-таҳдидлар кўпгина компаниялар томонидан уларга қарши ҳимоя чоралари етарли даражада йўлга қўйилмаганлиги боис мустаҳкам 3-ўринни эгаллаганлар. Иккинчи ўринни спам маълумтлари эгаллаган. 4.1.2.1-жадвалда энг хавфли таҳдидлар 10 талиги маълумотлари келтирилган.

4.1.2.1-жадвал. Энг хавфли таҳдидлар ўнталиги

(манба: Computer Economics, 2007)

Рейтингдаги ўрни	Таҳдид тури
1	Инсайдерлар
2	Спам
3	Malware-таҳдидлар (компьютер вируслари, чувалчанглар, троян дастурлари, adware- ва spyware-дастурлари)
4	Ташқи бузғунчилар томонидан рухсатсиз кириш
5	Ахборот ташувчи воситаларга бўлган жисмоний таҳдидлар
6	Электрон товламачилик
7	Фарминг (Pharming) -ҳужумлар
8	Фишинг (Phishing) – ҳужумлар
9	Электрон бузғунчилик ва саботаж
10	DoS-ҳужумлар

Шунга ўхшаш хулосага CSI мутахассислари ҳам келишган. Уларнинг маълумотларига кўра, 2007 йилда инсайдерлар ҳужумлари 59% компанияларда амалга оширилган.

4.1.2.1-расм. 2000-2007 йилларда ахборотга нисбатан амалга оширилган ҳужумлар динамикаси (Манба: CSI, 2007).

Вируслар ҳужумлари 52%, махфий ахборот ташувчи воситалар ўғирланиши (биринчи навбатда ноутбук компьютерлари) 50% компанияларда рўй берган. 3.1.2.1-расмда 2000-2008 йилларда амалга оширилган ҳужумлар динамикаси келтирилган.

SiliconRepublic.com сайтининг маълумотларига кўра, иш жойини алмаштирган америкалик ходимларнинг 45% и ўзлари билан эски иш жойларидаги корпоратив ахборотларни олиб кетишган экан. Бундай маълумотлар кўпинча флэш-карталар ёки ноутбуклар ёрдамида олиб чиқиб кетилган. Баъзи собиқ ходимлар бундай ахборотларни ўз электрон почта қутиларига жўнатиш орқали олиш имконига эга бўлганлар. Шунинг учун сўровда катнашган компанияларнинг 53% и ўз копанияларига тегишли махфий ахборотларни уларга рақобатчи бўлган компаниялар бемалол ишлатаётганликларини эътироф этганлар. 63% респондентлар эса рақобатчилар компанияга тегишли ишланмалардан бемалол фойдаланаётганликларини маълум қилишган. Бунга ўхшаш маълумотлар «2007 E-Crime Watch Survey» ҳисоботида ҳам берилган. Унга кўра, 36% ҳолатларда махфий ахборотлар инсайдерлар томонидан мобил курилмалар ёрдамида ташқарига олиб чиқиб кетилган. 35% ҳолатларда эса ўз ваколатларидан фойдаланиб, ресурсларга мурожаат қилиш орқали олиб чиқиб кетганлар. 31% ҳолатларда инсайдерлар

махсус дастурлардан (паролларни синдирувчи, пакетлар сниффери) фойдаланиб махфий ахборотларни қўлга киритганлар.

CERT.UZ сайти маълумотларига кўра, 2007 йилда Ўзбекистон Республикасида қуйидаги ҳолатлар қайд қилинган:

• провайдерларнинг 70% серверлари тўғри созланмаганликлари натижасида заифликларни келтириб чиқарган. Шунингдек сервердан фойдаланувчилар ваколатларини тақсимлашда эътиборсизликка йўл қўйилган;

• давлат органлари сайтларининг 40% и ахборот хавфсизлиги нуқтаи-назаридан талабларга жавоб бермаслиги маълум бўлган.

Бузғунчилик борасидаги статистик маълумотлар қуйидагича :

• 70% бузиб киришлар зарар етказувчи дастурлар орқали фойдаланувчилар шахсий маълумотларини ва паролларини ўғирлаш мақсадида амалга оширилган. Зарар етказувчи дастурлар асосанг электрон почта хатига бириктирилган файлни ишга тушириш, Web-сайтларга кириш, ахборот ташувчи воситалар орқали фаоллашганлар;

• 15% бузиб киришлар Web-иловалардаги хатоликлар ва камчиликлар, бепул тарқатиладиган скриптлардан фойдаланиш натижасида амалга оширилган;

• 10% бузиб киришлар сервер администраторлари эътиборсизликлари оқибатида амалга оширилган (содда пароллардан фойдаланиш ва бошқалар);

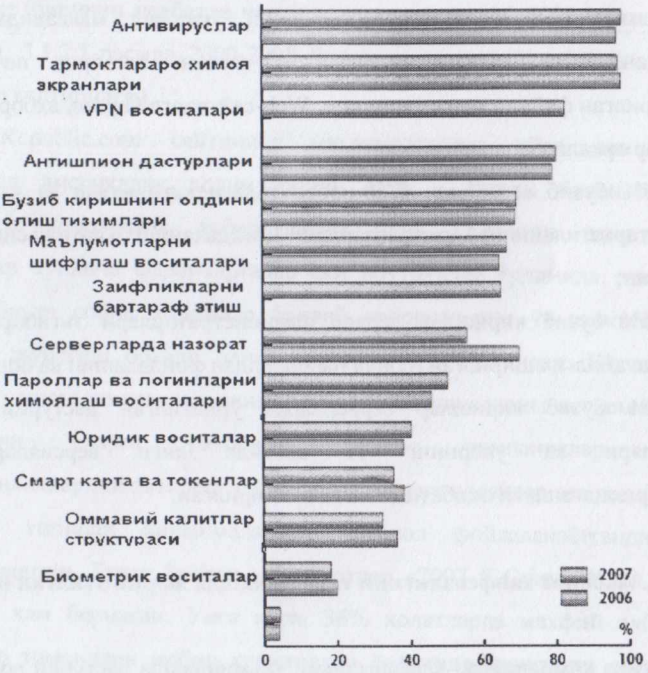
• 5% бузиб киришлар серверларда ўрнатилган дастурий таъминот заифликлари ва уларнинг ўз вақтида янги версиялари билан алмаштирилмаганлиги оқибатида амалга оширилган.

4.2. Ахборот хавфсизлигини таъминлашда жорий этилган воситалар

Кўпгина компаниялар хавфсизликни таъминлашда дастурий воситалардан фойдаланадилар. «2007 CSI Computer Crime and Security Survey» ҳисоботи маълумотларига кўра, америка компанияларининг 97% и турли хил таҳдидларнинг олдини олишда тармоқлараро ҳимоя экранларидан

фойдаланишган. Копанияларнинг 98% и антивитрус дастурлари билан, 84% и VPN воситалари билан, 80% и антишпион дастурлари билан, 69 % и рухсатсиз бузиб киришлар олдини олишга қаратилган тизимлар билан қуролланган (4.2.1-расм).

Компанияларнинг ахборот хавфсизлигини таъминлаш учун ҳаражатлари ҳам ошиб бормокда. Жумладан «2007 Global Security Survey» ҳисоботи маълумотларига кўра, 2007 йилда ахборот хавфсизлиги борасида экспертлар маслаҳатлари, ахборотга мурожаатларни чеклаш, қурилмаларда хавфсизлик тизимини шакллантириш, рухсатсиз тизимга кириш ва хоналарга киришни назорат қилиш тизимлари учун ҳаражатлар салмоғи сезиларли даражада ошганлиги таъкидланган.



4.2.1-расм.

Ахборот хавфсизлигини таъминлашда ишлатиладиган воситалар.

(манба: «2007 CSI Computer Crime and Security Survey» ҳисоботи)

4.2.2-расм. Ахборот хавфсизлигини таъминлаш харажатлари динамикаси

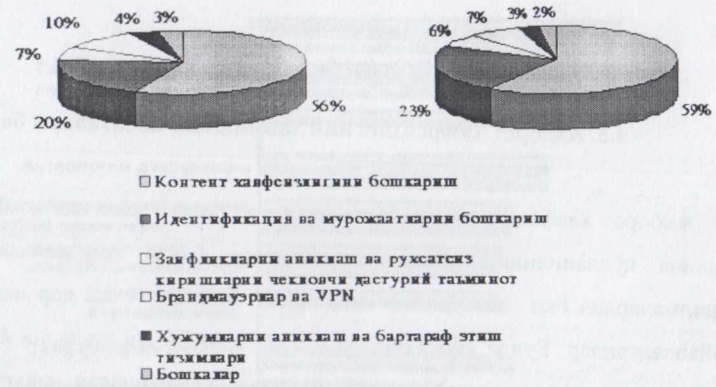
(Манба: «2007 Global Security Survey» ҳисоботи)

4.3. Ахборот хавфсизлигини таъминлаш воситалари бозори

Ахборот хавфсизлигини таъминлаш воситалари турли хил компанияларда турлича қўлланилиши кузатилган. Масалан, баъзи компаниялар аппарат қурилмалардан ёки дастурий воситалардан, баъзилари эса ҳар икки туридан фойдаланганлар. Бунда компаниялар ўзлари яратган воситаларни ёки ахборот хавфсизлиги воситаларини ишлаб чиқувчи компаниялар маҳсулотларини жорий этиб келганлар. Шунинг учун ахборот хавфсизлигини таъминлаш воситалари бозорини (IT Security Market) шартли равишда учта сегментга ажратиш мумкин: ахборот хавфсизлиги бўйича хизмат кўрсатиш бозори (Security Services Market), дастурий воситалар бозори (Security Software Market), аппарат воситалари бозори (Security Hardware Market). Охирги икки бозор кесишиш соҳаси кенгайиб бормоқда. Сабаби, битта воситани у ёки бу бозордан излаб топиш мумкин.

Дастурий таъминот воситалари бозорида контент хавфсизлигини бошқариш ва идентификация, мурожаатларни бошқариш воситаларига талаб

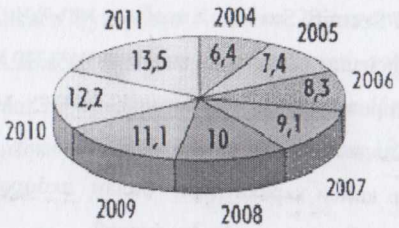
ортган. Уларнинг биргаликдаги савдо хажми салмоғи 75% ни ташкил этган. Контент хавфсизлигини бошқариш воситалари биринчи навбатда компаниядан Интернет тармоғига узатиладиган ахборот окимини ва Интернетдан компания тармоғига келиб тушадиган ахборот окимини назорат қилишда ишлатиладилар. Шунингдек бундай воситалар компания локал тармоғида сақланаётган ахборотларни, корпоратив электрон почта хатларини, ходимларнинг Интернет тармоғи билан ишлашларини назорат киладилар. 2005 йилда Осиё-Тинч океани региони дастурий таъминот бозорида контентни назорат қилиш воситалари салмоғи 56% ни ташкил этган (4.3.1-расм).



4.3.1-расм. Ахборот хавфсизлигини таъминлаш воситаларининг Осиё-Тинч океани минтақаси бозорларидаги 2005-20011 йилларда тақсимоти, % (манба: IDC, 2007)

IDC компанияси башоратига кўра 2011 йилга бориб контент хавфсизлигини бошқариш воситалари салмоғи 82% ни ташкил этиши кутилмоқда. Идентификация ва мурожаатларни бошқариш воситалари 7% ни ташкил этиши кутилмоқда. Брандмауэрлар ва VPN лар бозордаги салмоғи 10% ни ташкил этиши кутилмоқда.

Gartner тадқиқот маркази маълумотларига кўра хавфсизликни таъминловчи дастурий воситалар бозори 2007 йилда 10,4 % га ошган савдо ҳажми 9,1 миллиард долларни ташкил этган (3.3.2-расм.). Шулардан 53,8% и (яъни 4,9 миллиард доллар) антивирус дастурлари ҳиссасига тўғри келади. IDC маълумотларига кўра, энг кўп ўсиш суръати Осиё-Тинч океани регионида (Япония бундан мустасно) йилига 15,5% ни ташкил этиши кузатилган. Якин Шарк, Африка минтакаси бозорида ўсиш суръати 14,7% ни, Шарқий Европада 13,6% ни, Ғарбий Европада 9,2% ни ташкил этган..



4.3.2-расм. 2004-20011 йилларда ахборот хавфсизлигини таъминлаш дастурий воситалари бозори ҳажми, миллиард доллар ҳисобида (манба: Gartner, 2007).

IDC маълумотларига кўра бозор ҳажми 16% га ўсиши ва 2010 йилда 67 миллиард долларни ташкил этиши кутилмоқда. Дастурий воситалар бозорининг ўсиш суръати 12% ни ва 2010 йилда 20,5 миллиард долларни ташкил этиши кутилмоқда. 2010 йилда хавфсизликни таъминловчи аппарат (Security Hardware Market) ва дастурий воситаларнинг (Security Software Market) умумий савдо ҳажми 34,4 миллиард долларни ташкил этади. Gartner маълумотларига кўра, фақат дастурий воситалар бозори ҳажми 2011 йилда 13,5 миллиард долларни ташкил этиши башорат қилинган.

Дастурий воситалар бозорига ўз маҳсулотларини ишлаб чиқарувчи етук компаниялар - Symantec, Check Point, RSA Security, Computer Associates ва IBM

бўлиб, улар орасида бозордаги жами маҳсулотларнинг 31% ини ишлаб чиқарган Symantec компанияси карвонбошилик килмоқда.

Назорат учун саволлар:

1. 2007 йилда АҚШ компанияларига энг кўп молиявий зарар етказган таҳдидлар қайсилар?
2. «2007 Global Security Survey» ҳисоботи маълумотларига кўра, 2007 йилда ахборот хавфсизлиги борасида қайси хизматлар учун ҳаражатлар ошган?
3. CSI/FBI Computer Crime and Security Survey ҳисоботи маълумотларига кўра, 2006 йилда жаҳон бўйича қайси таҳдидлар энг кўп зарар келтирган?
4. Инсайдерлар қайси ҳаракатлари билан ахборот тизимлари ва уларнинг инфраструктурасига зарар етказадилар?
5. Компаниялар ахборот хавфсизлигини таъминлаш борасида қайси воситалар билан кўпрок қуролланганлар ?
6. Ахборот хавфсизлигини таъминлаш ҳаражатлари динамикасини қандай тавсифлаш мумкин?
7. Ахборот хавфсизлигини таъминлаш воситалари бозорини қандай тавсифлаш мумкин?
8. CERT.UZ сайти маълумотларига кўра, 2007 йилда Ўзбекистон Республикасида қайси ҳолатлар қайд қилинган?

Фойдаланилган адабиётлар рўйхати

1. Ўзбекистон Республикаси Конституцияси. 8 декабрь 1992 йил.
2. Ўзбекистон Республикаси «Давлат сирларини сақлаш тўғрисида»ги Қонуни, 7 май 1993 йил.
3. Ўзбекистон Республикаси «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги Қонуни 24 апрель 1994 йил
4. «Электрон ҳисоблаш машиналари учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси тўғрисида»ги Қонуни. 6 май 1994 йил.
5. Ўзбекистон Республикаси Фукаролик Кодекси, 29 август 1996 йил.
6. «Ўзбекистон Республикаси ахборот ресурсларини тайёрлаш ва уларни маълумотларни узатиш тармоқларида, шу жумладан, Интернетда таркатиш тартиби тўғрисида низом». Вазирлар Маҳкамасининг 1999 йил 26 мартдаги 137-сон карорига илова.
7. «Ахборотлаштириш тўғрисида»ги Ўзбекистон Республикаси Қонуни. 2003 й. 11.12. // Ўзбекистон Республикаси қонун ҳужжатлари тўплами, 2004, №6.
8. «Электрон ракамли имзо тўғрисида»ги Ўзбекистон Республикаси Қонуни. 2003 й. 11.12. // Ўзбекистон Республикаси қонун ҳужжатлари тўплами, 2004, №4.
9. «Электрон ҳужжат айланиши тўғрисида»ги Ўзбекистон Республикаси Қонуни. 2004 й. 29.04. // Ўзбекистон Республикаси қонун ҳужжатлари тўплами, 2004, №8.
10. «Электрон тижорат тўғрисида»ги Ўзбекистон Республикаси Қонуни. 2004 й. 29.04. // Ўзбекистон Республикаси қонун ҳужжатлари тўплами, 2004, №8.
11. Постановление Президента Республики Узбекистан ПП-167 «О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем» от 5 сентября 2005 г.

12. Ўзбекистон Республикаси «Муаллифлик ҳуқуқи ва турдош ҳуқуқлар тўғрисида»ги Қонуни. 20.07.2006 йил.// Ўзбекистон Республикаси қонун ҳужжатлари тўплами, 2006, №28-29.
13. Ўзбекистон Республикаси Жиноят Кодекси, 24.09.2008 йил.
14. М. Арипов, Ю. Пудовченко, К. Арипов «Основы Интернет» 2002 йил. Тошкент, 194 бет.
15. М. Арипов, Ю. Пудовченко, «Основы криптологии» Учебное пособие, Ташкент 2004, 138 с.
16. Арипов М., Мухаммадиев Ж. «Информатика. Информацион технологиялар» Тошкент, 2004, 330 бет (Ҳукукшунослик мутахассисликлари учун дарслик)
17. Арипов М., Кобилжанова Ф.А Юлдашев З.Х. «Информатика, Информационые технологии». Ташкент 2005, 350с.
18. Ғаниев С.К., Каримов М.М., Ташев К.А. «Ахборот хавфсизлиги» Техника олий ўқув юртлари бакалавриат боскичи талабалари учун ўқув қўлланма. «Aloqachi»-2008.
19. Баричев С. «Криптография без секретов» – Санкт-Петербург: "Питер-Пресс", 2000 год.
20. Воробьев С. «Защита информации в персональных ЭВМ» М.: "Мир", 1993 год.
21. Громов В.И., Васильев Г.А. «Энциклопедия компьютерной безопасности» (сборник). М.: МГУ, 1999 год.
22. Джой Крейнак. «Интернет» – Санкт-Петербург: "Питер", 1999 год.
23. Жельников В. «Криптография от папируса до компьютера» М.: Dore Print, 1999 год.
24. Ғуломов С.С. ва бошк. «Ахборот тизимлари ва технологиялари» Т.: "Шарк", 2000 йил.
25. В.И.Ярочкин. «Информационная безопасность» Учебник для вузов. 2004 г.
26. Щербаков А.Ю. «Введение в теорию и практику компьютерной безопасности» М.: Издательство Молгачева С.В., 2001

27. Башлы П.Н. «Информационная безопасность» Ростов-на-Дону. Издательство «Феникс», 2006.
28. Донцов Д. «Как защитить компьютер от ошибок, вирусов, хакеров» – СПб.: Питер, 2006.
29. Яремчук С. «Защита вашего компьютера от сбоев, спама, вирусов и хакеров на 100%» СПб.:Питер, 2007.
30. «Компьютер-пресс» журнали сонлари

Интернет ресурслари

31. Масофадан ўқитиш университети http://www.intuit.ru
32. Антиспамерлар: http://mailwasher.net, http://www.energosoft.net, http://www.nospam.net
33. Интернет тармоғида ишлашда ва дастурий таъминотни аутентификация қилиш ҳамда рухсат этилмаган фойдаланишдан ҳимоялаш тизимларини яратиш ва ишлаб чиқариш – Aladdin Knowledge Systems Ltd (http://www.aladdin.ru)
34. Технологические аспекты информационной безопасносни. http://www.infobez.ru
35. Корпоратив тармоқларни рухсат этилмаган мурожатлардан ҳимоялаш тўғрисида: http://www.cysco.com, http://ca.com (Computer Associates), http://www.symantec.ru
36. PGP интернет-ресурси: http://www.pgp.net, http://www.pgp.com, http://www.pgpi.org - ҳалқаро сервери.
37. Электрон рақамли имзо тавсифлари: http://www.w3.org/TR/xml-c14n, http://www.w3.org/Signature
38. Компьютер-Пресс журнали : http://www.compress.ru
39. Ахборот хавфсизлиги технологиялари яратиш бўйича инновацион компания: http://www.infowatch.ru

40. Computer Economics илмий тадқиқот маркази: http://www.computereconomics.com
41. Буюк Британиянинг Virus Bulletin журнали: http://www.virusbtn.com
42. InformationWeek Business Technology Network: www.informationweek.com
43. Антивирус дастурлари бўйича холис таҳлил ўтказувчи тадқиқот маркази: http://www.av-comparatives.org
44. http:// www.insidepro.com
45. Элкомсофт компанияси (Россия): http://www.elcomsoft.com
46. www.sysinternals.com
47. www.f-secure.com
48. www.chemtable.com
49. www.wisecleaner.com
50. Ўчирилган файлларни тиклаш дастурлари: Undelete Plus (www.Undelete-Plus.com), Recuva (www.Recuva.com), Flash Recovery ToolBox (www.filerecoveryangel.com)
51. AdSubtract 3.0 антиреклама дастури: **www.Intermute.com**
52. Спам мавзуларининг статистикаси: www.spamtest.ru
53. Касперский Лабораторияси: www.kaspersky.ru
54. Eset компанияси: http://www.eset.com, http://www.esetnod32.ru
55. АҚШ компьютер хавфсизлиги институти (CSI): www.gosci.com
56. Ахборот технологиялари бозорини тадқиқ этувчи компания -International Data Company (АҚШ): www.IDC.com
57. Ахборот технологиялари бўйича тадқиқотлар олиб борувчи Gartner компанияси: www.Gartner.com
58. Agnitum компанияси (Россия, Санкт-Петербург): www.agnitum.com
59. Компьютер можароларига муносабат билдирувчи Марказ: www.cert.uz
60. Ўзбекистон Республикаси компьютер ва ахборот технологияларини ривожлантириш Маркази: www.uzinfocom.uz
61. Ўзбекистон Республикаси ахборот хавфсизлиги электрон журнали: www.security.uz

Намунавий тест саволлари

1. Хавфсизлик деганда ...

a) душман томонга уюштириладиган ҳужум тушунилади.

b) шахснинг, корхонанинг, давлатнинг муҳим ҳаётий манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати тушунилади.

c) шахснинг, корхонанинг, давлатнинг ноқонуний фойда кўришдан ҳимояланганлик ҳолати тушунилади.

d) уюштирилмаган ҳужумга қарши ҳужум уюштириш тушунилади.

2. Ахборотга мурожаат қилиш имкониятини таъминлаш нимани англатади?

a) Белгиланган вақт оралиғида ваколатга эга бўлган ахборот фойдаланувчилари ва субъектлари учун ахборот ёки у билан боғлиқ сервисга мурожаат қилиб фойдаланиш имкониятини таъминлашни англатади.

b) Сақланаётган ахборот ваколатга эга бўлмаган субъектлар томонидан ўзгартирилишидан, яъни ахборот тузилиши ва маъноси қандай берилган бўлса, шундай сақлашни таъминлашни англатади.

c) Ахборотга ваколати бўлмаган субъектлар томонидан мурожаат қилиб, ундан ошкор ҳолда фойдаланишдан ҳимоя қилишни англатади.

d) Узатилаётган ахборот ўзгартирилган ҳолда бўлса ҳам жойдаги фойдаланувчига келиб тушиши имкониятини таъминлаш тушунилади.

3. Ахборотнинг статик яхлитлиги деганда ...

a) ахборотларни қайта ишлаш жараёнида бир ахборотни қайта ишлаш натижасида тўғри натижавий ахборот олиниб, ўзгартирилмаган ҳолда тегишли бўғинга етказилиши тушунилади.

b) компьютер хотирасига киритилган маълумотнинг кодлаштирилиши тушунилади.

c) белгиланган объект ҳақидаги маълумотлар ўзгармай сақланиши тушунилади.

d) ахборотнинг компьютер хотирасидан чиқариш қурилмасига қайта шифрланиб чиқарилиши тушунилади.

4. Таҳдид деганда ...

a) кимларнингдир манфаатларига зиён етказувчи рўй бериши мумкин бўлган воқеа, таъсир, жараён тушунилади.

b) ҳужумни амалга оширишга қаратилган ҳаракат тушунилади.

c) заифликларни аниқлаш ва ундан фойдаланиш чораларини ишлаб чиқиш тушунилади.

d) Ҳали содир этилмаган, лекин содир этилиши кутилаётган воқеа ёки жараён тушунилади.

5. Ахборот муносабатлари субъектлари манфаатларига қаратилган таҳдид деб нимага айтилади?

a) Ахборот тизими фойдаланувчиларига нисбатан ишлатиладиган зўравонлик ва куч ишлатишга айтилади.

b) Ахборотга ёки ахборот тизимига салбий таъсир этувчи потенциал рўй бериши мумкин бўлган воқеа ёки жараён аталади

c) Ахборот тизими инфраструктурасига нисбатан амалга ошириладиган кўпорувчилик ҳаракатларига айтилади.

d) Барча жавоблар тўғри.

6. Фойдаланувчиларнинг воз кечишлари натижасида келиб чиқадиган таҳдидлар ...

a) белгиланган тартиб ва қоидаларга риоя қилмасликдан, атайлаб ёки тасодифан ҳаракатлар туфайли тизимнинг ишдан чиқишидан, йўл қўйилган хатоликлар ва носозликлардан келиб чиқади.

b) дастурий ва техник таъминотдаги узилиш ва носозликлардан келиб чиқади.

c) ташқи хотирада сақланаётган маълумотларнинг бузилишидан келиб чиқади.

d) ахборот тизими билан ишлаш ҳохишининг йўқлиги, касбий тайёргарлик савияси пастлиги, нормал шароитнинг йўқлигидан келиб чиқади.

7. Зарар етказувчи дастурлар қайси жиҳатлари билан ажралиб турадилар?

a) Бузиш функцияси билан, таркалиш усули билан, ташқи кўриниши билан.

b) Табиий равишда жорий этилиши билан, тизимни бир зумда ишдан чиқариши билан.

c) Жуда тез таркалиши билан, мураккаб буйруқлардан иборатлиги билан.

d) Инсон саломатлигига таъсири билан

8. Ахборот тизимларида ахборот хавфсизлигини таъминлашга оид раҳбарият томонидан қабул қилинган чора-тадбирлар қайси бўғинга тегишли?

a) ҳуқуқий бўғинга

b) маъмурий бўғинга

c) амалий бўғинга

d) дастурий ва техник бўғинга

e) Барча бўғинларга

9. "Ахборотлаштириш тўғрисида"ги Қонуннинг нечанчи моддаси "Ахборот ресурслари ва ахборот тизимларини муҳофаза қилиш" номи билан аталган?

a) 19-моддаси

b) 3-моддаси

c) 10-моддаси

d) 20-моддаси

10. Турли давлатларнинг ахборот хавфсизлиги бўйича стандартлаш базаларининг шаклланишига нима асос бўлди?

a) Европа давлатлари - Франции, Германии, Нидерландия ва Буюк Британия вакилларининг ҳамкорликда ишлаб чиқилган "Уйғунлаштирилган мезонлар" асос бўлди.

b) "Ахборот технологияларида ахборот хавфсизлигини баҳолаш мезонлари" номли ISO/IEC 15408 стандарт асос бўлди.

c) Дунёда биринчи бўлиб АҚШ да яратилган ва кенг кўламда фойдаланилган "Ишончли компьютер тизимларини баҳолаш мезонлари" номли стандарти асос бўлди.

d) Ахборот хавфсизлиги масалаларини тўлиқ ва чуқур талқин қилувчи, кейинчалик шартли равишда X.800 номи берилган техник хусусиятлар асос бўлди.

11. "Оранжевая книга"да ишончлиликнинг қайси поғоналари келтирилган?

a) 2 поғонаси – B ва A белгиланган. B ишончлилик даражаси паст, A ишончлилик даражаси юқори бўлган тизимлар учун мўлжалланган.

b) 3 поғонаси A, B, C поғоналари белгиланган. A ишончлилик даражаси паст, C юқори бўлган тизимлар учун мўлжалланган.

c) 5 поғонаси – I, II, III, IV ва V белгиланган. I поғона ишончлилик даражаси юқори, V поғона паст бўлган тизимлар учун мўлжалланган.

d) 4 поғонаси - D, C, B ва A белгиланган. D поғонаси ишончлилик даражаси паст ва талабга жавоб бермайдиган тизимлар, A поғонаси юқори талабларга жавоб берувчи тизимлар учун мўлжалланган

12. Ахборотларни ҳимоялашнинг алмаштириш усуллари моҳияти нимадан иборат?

a) Тизимда сақланаётган ахборот алоқа линиялари бўйича узатилишида маълум қоидага кўра кодлаштирилиб, ундан очиқ ҳолда бевосита фойдаланиш имконияти баратараф этилади.

b) Махсус техник ишланмалар асосида ахборотни қайта ишловчи қурилмалар ва воситаларда ахборотни назорат қилиш ва ҳимоя қилишни таъминлаш амалга оширилади.

c) Алоқа каналларини ҳимоя қилишда, кераксиз ва ҳалақит қилувчи электромагнит нурларини бартараф этилади.

d) Ахборот тизимидаги жараёнларда ва дастурлардан фойдаланишда фаолият кўрсатувчи персонални назорат қилиш амалга оширилади.

13. Биометрик воситаларда аниқлашнинг квазистатик услуби ёрдамида ...

a) фойдаланувчи қўл геометрияси ёки кўз хусусиятлари ёки қўл излари нусхаси ёки қон томирлари расмига қараб аниқланади.

b) фойдаланувчи бармоқ изларининг нусхаси ёки юз тузилиши назорат қилиниб, аниқланади.

c) фойдаланувчи пульси, баллистокардиография, энцефалография натижалари назорат қилиниб аниқланади.

d) фойдаланувчи товуши ёки ёзув шакли ёки босмалаш (печатлаш) стили назорат қилиниб аниқланади.

14. Электрон ҳужжат айирбошлашни ҳимоялашда унинг яхлитлигини ва бегоналар томонидан фойдаланиш имкониятидан сақлашни таъминлашда қайси усул ва воситалар қўлланилади?

a) Электрон рақамли имзо

b) Криптографик усуллар

c) Биометрик усуллар

d) Баённомалар анализаторлари

e) a ва b жавоблар тўғри.

15. Троян дастурлари...

a) бошқа дастурларга жорий этилиб, зарарланган файлларни ишга туширишни бошкариш мақсадида уларга ўзларининг кодларини киритадилар.

b) компьютерда фойдаланувчининг рухсатисиз маълум амалларни бажаришга киришадилар, яъни маълум шароитларда дискдаги маълумотларни ўчирадилар, тизимнинг "осилиб" қолишига олиб келадилар, махфий ахборотларни ўғирлайдилар ва хоказо.

c) тармоқ бўйича бошқа компьютерлар адресларини ҳисоблаб, шу адреслар бўйича ўз нусхаларини юборадилар.

d) компьютерда фойдаланувчи рухсати билан маълум амалларни бажарадилар, яъни маълум файллардан нусха кўчирадилар, папка ичига янги файл киритадилар ва хоказо.

16. Жорий этилиш усулига кўра вируслар ...

a) файлга, юкловчи дастурларга ва бир вактнинг ўзида ҳам файл, ҳам юкловчи дастурларга жорий этилувчи турларга бўлинадилар.

b) резидент ва норезидент вирусларга ажратиладилар.

c) чалғитиб, ҳалал берувчи, хавфли бўлмаган ва хавфли турларга ажратиладилар.

d) "йўлдош", файл тизими структурасидаги, стелс ва "рух" вирусларга ажратиладилар.

17. Вирус сигнатураси – ...

a) вируснинг барча нусхаларида ва фақат нусхаларида учрайдиган код бўлаги бўлиб, маълум узунликка эгадир.

b) вируснинг ўзини-ўзи шифрлаш хусусиятидир.

c) вируснинг ўзини тизимда яширувчи бўлаги бўлиб, бир папкадан иккинчисига сакраб ўтади.

d) вируснинг ошкор равишда фойдаланувчи томонидан аникланиши мумкин бўлган бўлагидир.

18. Компьютернинг вирус билан зарарланишининг нисбий аломатларидан кайси бири нотўғри?

a) Ташки хотира ресурсларига умуман мурожаат килиш имконияти йўқлиги.

b) Компьютерда аввал киска вакт ичида ишга тушувчи бирор дастурнинг жуда секинлик билан ишга тушиши.

c) Операцион тизимнинг юкланмаслиги.

d) Баъзи керакли файл ва папкаларнинг йўколиб қолиши ёки улар сиғимларининг ўзгариши.

19. Ёлғон салбий огоҳлантиришда...

a) антивирус дастури хеч кандай вирус йўклиги ҳақида маълумот берадику, лекин аслида тизимда вирус ҳақиқатан ҳам мавжуд бўлади.

b) антивирус дастури тизим нормал ҳолда ишлаётганлиги ҳақида маълумот беради.

c) антивирус дастури тизимда жиддий бузилишлар мавжудлиги ҳақида огоҳлантирувчи маълумотлар беради.

d) антивирус дастури фойдаланувчига тизимда вирус мавжудлиги ҳақида маълумот берадику, лекин аслида бундай вирус мавжуд бўлмайди.

20. SAM файли қаерда сақланади?

a) Компьютер администраторининг сейфида.

b) Winnt_root\System32\Config каталоги ичида сақланади.

c) Program Files\Common Files\ODBS каталоги ичида сақланади.

d) CMOS хотрада сақланади.

21. MS Word 2002 (MS Office XP да) да файлни очиш учун паролли ҳимоя параметрларини ўрнатиш кетма-кетлигини аниқланг.

a) Бош менюдан Файл > Сохранить > файл номи ва пароли киритилиб > ОК босилади.

b) Бош менюнинг Сервис > Установить защиту > «Запретить любые изменения» банди белгиланиб, пароль киритилади ва тасдиқланади.

c) Бош менюдан Сервис > Параметры > «Безопасность», «Пароль для открытия файла» майдонига файлни очиш учун пароль маълумотини киритиб, тасдиқлаш керак..

d) Бош менюдан Сервис > Параметры > «Сохранение», «Пароль для открытия файла» майдонига файлни очиш учун пароль маълумотини киритиб, тасдиқлаш керак.

22. MS Excel XP да актив варак (Лист) да ячейкалар ичидаги маълумотларни ва ва диаграмма маълумотларини ҳимоялаш учун қайндай иш тутиш керак?

a) Сервис > Защита > Защитить лист буйруклар кетма-кетлиги бажарилиб, очилган ойнадан ҳимоя қилинадиган объектлар белгиланади ва пароль маълумоти киритилади.

b) Сервис > Защита > Защитить лист буйруклар кетма-кетлиги бажарилиб, очилган ойнадан ҳимоя қилинмайдиган объектлар белгиланади ва пароль маълумоти киритилади.

c) Сервис > Безопасность > Защита > Защитить лист буйруклар кетма-кетлиги бажарилиб, очилган ойнадан «Объекты» банди белгиланиб, пароль маълумоти киритилади.

d) Файл > Сохранить > Сервис > Параметры > Защитить лист кетма-кетлигини бажариб, очилган ойнада «Содержимое» банди белгиланиб, пароль маълумоти киритилади.

23. Брадмауэрланинг уланиш даражасида ишловчи турлари …

a) ишлаш жараёнида кирувчи ва чикувчи трафик маълумотларини ўзига кўчириб оладилар ва улар оркали ташки тармокка уланиш мумкинми ёки йўклигини аниклайдилар.

b) Интернетнинг муайян хизмат тури бўйича чеклашларни амалга оширишиб хавфсизликни таъминлайдилар.

c) хавфсизликни келаётган пакетларни фильтрлаш йўли билан таъминлайдилар.

d) Хавфсизликни тармок компонеталари мониторингини ўтказиб бориш асосида таъминлайдилар

24. Локал тармокка Интернет оркали уюштириладиган пакетлар сниффери хужуми…

a) хакер-бузгунчи тармок жойлашган корпорация худудида ёки унинг ташкарисидан туриб ўзини тармокка кириш учун ваколати бор мутахассис килиб кўрсатиши оркали амалга оширилади.

b) тармок операцион тизими ташкил этувчиларининг ёки тегишли дастурларнинг бузилиши натижасида тармок тизимига ваколатга эга бўлган фойдаланувчиларнинг кириши тўсиб қўйилиши максадида уюштирлади.

c) тармок картасидан фойдаланиб физик канал оркали юборилаётган барча ахборот пакетларини қайта ишлаш максадида махсус дастурга юбориш максадида уюштирилади.

d) ваколатга эга бўлган фойдаланувчининг тармокка кириши учун белгиланган парол маълумотини кўлга киритиш максадида уюштирилади.

25. Локал тармокдаги трафикни ошкор килиш …

a) тармоқ бўйича узатилаётган маълумотни рухсатсиз эгаллаб, ундан фойдаланиш ёки бошқаларга ошкор қилишга уринишларида рўй беради.

b) рухсати бўлмаган фойдаланувчилар томонидан тасодифан ёки ғаразли равишда керакли файл ва дастурларга ўзгартиришлар киритишга ҳаракат қилишлари натижасида рўй беради.

c) Бошқа фойдаланувчи томонидан асл жўнатувчи номини қалбакилаштириб маълумот узатиш учун амалга ошириладиган ҳаракатлар натижасида рўй беради

d) тармоқнинг муҳим бўғинларида ресурсларга мурожаат қилиш имконияти йўқлигидан ёки аппарат ва дастурий таъминот носозлиги туфайли рўй беради.

26. Бузғунчиларнинг Интернет тармоғи бўйича ҳужум уюштиришлари муваффақиятли амалга оширилишининг сабабларидан бири …

a) канал бўйича узатилаётган маълумотларни осонликча кузатиш имкони мавжудлиги

b) Internet Explorer каби браузер дастури интерфейсининг мукаммал ишланмаганлиги.

c) операцион тизим компоненталарининг нотўғри созланганлиги.

d) Интернетга уланишдаги модем қурилмаси имкониятлари пастлиги.

27. … троян дастурлари туркумига мансуб бўлиб, компьютерга масофадан вируслар оркали ёки Бошқа йўллар билан жорий этиладилар. Нукталар ўрнига мос жавобни танланг.

a) Вируслар

b) Чувалчанглар

c) Фишинг маълумотлари

d) Ботлар

28. Қайси хизматлар сеанлари давомида узатилаётган маълумотлар осонликча бузғунчилар томонидан қўлга киритиладилар?

a) Электрон почта, TELNET ва FTP хизматларида

b) UseNet ва FTP хизматларидан

c) TelNet ва WWW хизматларидан

d) WWW ва UseNet хизматларидан

29. Ахборот йиғиш учун юборилган спамда қандай маълумотлар берилади?

a) Фойдаланувчининг банкдаги ҳисоб рақами ўзгарганлиги ҳақидаги маълумот юборилиб, уни аниқлаштириш мақсадида эски ҳисоб рақамини тасдиқлаш сўралади.

b) Мажбурий тўловларни тўлаш ҳақидаги маълумотлар юборилади.

c) Сўров баҳона бирор бир анкета тўлдирилиши талаб этилади ва анкетани кўрсатилган манзилга юбориш сўралади.

d) У ёки бу товарни харид қилишга ундовчи таклифлар берилади.

30. Web-серверларда тармоқни ҳимоя қилишдаги заифликлар нима туфайли ҳосил бўлади?

a) Web-серверларда тармоқни ҳимоя қилишдаги заифликлар деярли йўқ, шунинг учун улар хавфсизликни бартараф эта оладилар.

b) Серверга ўрнатилган ихтиёрий скрипт хатоликлари туфайли маҳаллий тармоқни ҳимоя қилишдаги заифликлар келиб чиқади.

c) Web-сервердан фойдаланувчиларнинг малакалари паст бўлганлиги туфайли.

d) Web-сервер ўрнатилган компьютер тезкорлиги талабга жавоб бера олмаслиги туфайли.

31. Ахборот хавфсизлиги деб ...

a) ахборот тизимидаги ахборотларнинг турли шахслардан бекитилиб, ҳимояланганликка айтилади.

b) ахборот тизими субъектларининг ва ташкил этувчиларининг ҳолатини сақлашга айтилади.

c) ахборот тизимида тасодифий ёки ғаразли равишда ахборот эгасига ёки унинг фойдаланувчисига зиён етказувчи ҳуружлардан ҳимояланганликка айтилади.

d) Ахборотларнинг бошқа субъектларга бериб юборилишини олдини олиш тушунилади.

32. Ахборотнинг динамик яхлитлиги деганда ...

a) белгиланган объект ҳақидаги маълумотлар ўзгармай сақланиши тушунилади.

b) ахборотларни қайта ишлаш жараёнида бир ахборотни қайта ишлаш натижасида тўғри натижавий ахборот олиниб, ўзгартирилмаган ҳолда тегишли бўғинга етказилиши тушунилади.

c) компьютер хотирасига киритилган маълумотнинг кодлаштирилиши тушунилади.

d) ахборотнинг компьютер хотирасидан чиқариш қурилмасига қайта шифрланиб чиқарилиши тушунилади.

33. Хавфли дарча деб ...

a) Заифликлар маълум бўлган вақтдан то уларни бартараф этилгунга қадар бўлган вақт оралиғига айтилади.

b) Ахборот тизимига уюштириладиган хужум давомийлигига айтилади.

c) Ахборот тизими ресурсларини ўғирлаб кетиш учун мўлжалланган дарчага айтилади.

d) Ахборот тизими ишлаётган компьютер монитори экранидаги душманга кўриниб турган маълумотлар дарчасига айтилади.

34. Ахборот муносабатларини қўллаб-қувватловчи инфраструктуранинг рад этиши натижасида келиб чиқадиган таҳдидлар ...

a) Белгиланган тартиб ва қоидаларга риоя қилмасликдан, атайлаб ёки тасодифан ҳаракатлар туфайли тизимнинг ишдан чиқишидан, йўл қўйилган хатоликлар ва носозликлардан келиб чиқ ади.

b) Алоқа, электр таъминоти, сув ва иссиқлик таъминоти, совутиш тизимларидаги носозликлардан келиб чиқади.

c) Хоналар ва улардаги жиҳозларнинг бузилиши, авария ҳолатига келиши натижасида вужудга келади.

d) b ва c жавоблар тўғри.

35. "Давлат сирларини сақлаш борасидаги бурч, уларни ошкор этганлик ёки қонунга хилоф равишда махфийлаштирганлик учун жавобгарлик" номли модда қайси ҳужжатда ёритилган ?

a) Конституцияда

b) "Давлат сирларини сақлаш тўғрисида" ги қонунда

c) "Ахборот олиш кафолатлари ва эркинлиги тўғрисида" ги қонунда

d) Фуқаролик Кодексида

e) Жиноят кодексида

36. Ахборот хавфсизлигида «хавфсизлик сиёсати» – ...

a) ахборотни ўғирланиб, йўқ килиниши олдини олишга қаратилган чора-тадбирлар гуруҳи.

b) корхона ёки компанияда компьютер фойдаланувчиларига тушунтириладиган кўрсатмалар.

c) ахборотни тўплаш, қайта ишлаш ва тарқатишни ташкил этишга қаратилган қонунлар, қоидалар ва меъёрий ҳужжатлар тўплами.

d) ахборот тизими архитектураси ва жорий этилишида унга бўлган ишончлилик мезони бўйича бериладиган баҳо.

37. Маълумотларо базасини шифрлаш ...

a) нинг самараси жуда паст. сабаби, бузғунчилар уларни осонликча бузиб тиклашлари мумкин.

b) фақат махфий ахборотларни ҳимоялашдагина юкори самара бериши мумкин.

c) натижасида ундаги айрим объектлар яширин ҳолда сақланиши мумкин.

d) натижасида маълумотлар базаси Бошқа дастурлар ёрдамида очилиши ва ўқилиши тақиқланади.

38. Локал тармокка Интернет орқали уюштириладиган IP-спуфинг ҳужуми...

a) хакер-бузғунчи тармок жойлашган корпорация ҳудудида ёки унинг ташкарисидан туриб ўзини тармокка кириш учун ваколати бор мутахассис килиб кўрсатиши орқали амалга оширилади.

b) тармоқ картасидан фойдаланиб физик канал орқали юборилаётган барча ахборот пакетларини қайта ишлаш мақсадида махсус дастурга юбориш мақсадида уюштирилади.

c) тармоқ операцион тизими ташкил этувчиларининг ёки тегишли дастурларнинг бузилиши натижасида тармоқ тизимига ваколатга эга бўлган фойдаланувчиларнинг кириши тўсиб қўйилиши мақсадида уюштирлади.

d) ваколатга эга бўлган фойдаланувчининг тармоққа кириши учун белгиланган парол маълумотини кўлга киритиш мақсадида уюштирилади.

39. Локал тармоққа Интернет орқали уюштириладиган DoS ҳужуми …

a) хакер-бузғунчи тармоқ жойлашган корпорация ҳудудида ёки унинг ташқарисидан туриб ўзини тармоққа кириш учун ваколати бор мутахассис килиб кўрсатиши орқали амалга оширилади.

b) тармоқ операцион тизими ташкил этувчиларининг ёки тегишли дастурларнинг бузилиши натижасида тармоқ тизимига ваколатга эга бўлган фойдаланувчиларнинг кириши тўсиб қўйилиши мақсадида уюштирлади.

c) тармоқ картасидан фойдаланиб физик канал орқали юборилаётган барча ахборот пакетларини қайта ишлаш мақсадида махсус дастурга юбориш мақсадида уюштирилади.

d) ваколатга эга бўлган фойдаланувчининг тармоққа кириши учун белгиланган парол маълумотини кўлга киритиш мақсадида уюштирилади.

40. Аутентификация ёрдамида ...

a) тизимда ишловчи шериклар (фойдаланувчилар) ҳақиқатан ҳам тизимда ишлаш ваколатига эга эканликларини ва маълумотларнинг ҳакикийлигини текшириш таъминланади.

b) ваколатга эга бўлмаганлар тармоқ ахборот ресурсларига мурожаат қилишларига рухсат берилади.

c) компьютер ресурслари текширилиб, таҳлил қилинади ва бу пайтда бирорта фойдаланувчи унда ишлаш имконига эга бўлмайди.

d) b ва c жавоблар тўғри.

41. Фармер ҳаракатлари давомийлигини аниқланг.

a) узлуксиз равишда

b) бир ойлик вақт давомида

c) 1 ёки 2 кунлик қисқа вақт ичида

d) бир хафталик вақт оралиғида

42. Интернет тармоғидаги заифликлардан бири - ...

a) алоқа каналлари бўйича узатилаётган маълумотларни осонликча кузатиш мумкинлиги.

b) маълумотлар узатишнинг ягона протоколи асосида бутун жаҳон миқёсидаги тармокларнинг ўзаро боғланиши.

c) локал тармокдаги алохида олинган ишчи станциядан бевосита Интернет ресурсларига мурожаат қилиш имконияти мавжудлиги.

d) кўпгина фойдаланувчилар ўз фаолиятларини Интернетсиз тасаввур қила олмасликлари.

43. Спам билан курашишнинг дастурий услубида нималар кўзда тутилади?

a) Электрон почта қутисига келиб тушадиган спамлар меъёрий хужжатлар асосида чекланади.

b) Электрон почта қутисига келиб тушадиган маълумотлар дастурлар асосида фильтрланиб чекланади.

c) Электрон почта қутисига келиб тушадиган спамлар оммавий равишда чекланади.

d) Электрон почта қутисига келиб тушадиган спамлар минтақавий худудларда чекланади.

44. Брандмауэрларнинг асосий вазифаларидан бири қайси қаторда келтирилган?

a) Интернет тармоғи орқали уюштириладиган ташқи ҳужумларни тўсиш

b) Компьютер қурилмалари ишининг нормал ҳолда ташкил этилишини таъминлаш.

c) Ташқи хотира воситаларидаги ахборотларнинг ишончли ҳимоясини ташкил этиш.

d) Интернет тармоғи оркали вирусларнинг маҳаллий компьютерга жорий этилишини чеклаш.

45. Брандмауэрларнинг технологик жиҳатлари бўйича камчиликларидан бири қайси қаторда келтирилган?

a) Улар фойдаланувчининг нормал ҳолда ишлашига ҳалал берадилар.

b) Интернет тармоғидан келаётган ахборотларнинг айримларинигина назорат қила оладилар.

c) Фойдаланувчининг электрон хатга бириктирилган файллардан ихтиёрий тарзда фойдаланиш имкониятларини яратишлари

d) Тизимнинг меҳнат унумдорлигига таъсири

46. Фойдаланувчиларнинг воз кечишлари натижасида келиб чиқадиган таҳдидлар ...

a) Белгиланган тартиб ва қоидаларга риоя қилмасликдан, атайлаб ёки тасодифан ҳаракатлар туфайли тизимнинг ишдан чиқишидан, йўл қўйилган хатоликлар ва носозликлардан келиб чиқади.

b) Ахборот тизими билан ишлаш ҳохишининг йўқлиги, касбий тайёргарлик савияси пастлиги, нормал шароитнинг йўқлигидан келиб чиқади.

c) Дастурий ва техник таъминотдаги узилиш ва носозликлардан келиб чиқади.

d) Ташқи хотирада сақланаётган маълумотларнинг бузилишидан келиб чиқади.

47. Ўзбекистонда ахборотлаштириш қоидаларини бузиш кўп миқдорда зарар ёхуд жиддий зиён етказилишига сабаб бўлса, қандай жазо чоралари кўрилади?

a) Энг кам иш ҳакининг 75 бараваригача миқдорда жарима ёки 3 йилгача озодликдан махрум этиш.

b) 3 йилдан 6 йилгача озодликдан маҳрум этиш.

c) Энг кам ойлик иш ақининг эллик бараваригача миқдорда жарима ёки бир йилгача ахлоқ тузатиш ишлари билан жазоланади.

d) 2 йилдан 5 йилгача озодликдан маҳрум этиш ёки зарар миқдорини қоплаш билан бирга энг кам иш ҳақининг 100 бараваригача жарима.

48.Қайси ҳужжатда ахборот борасидаги хавфсизлик тушунчасига «ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлик ҳолати», деб таъриф берилган?

a) «Ахборотлаштириш тўғрисида» Қонунда

b) Ўзбекистн Республикаси Конституциясида

c) «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги Қонунда

d) Россия Федерациясида қабул килинган "Ҳалкаро ахборот айирбошлашда иштирок этиш тўғрисида"ги Қонунда

49. Ўзбекистонда зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш худди шунингдек махсус вирус дастурларини ишлаб чиқиш, улардан қасддан фойдаланиш ёки уларни қасддан тарқатиш ҳолати қайд килинса, қандай жазо чоралари кўрилади?

a) Энг кам ойлик иш ҳақининг етмиш беш бараваридан икки юз бараваригача миқдорда жарима ёки муайян ҳуқуқдан маҳрум килиб, уч ойдан олти ойгача қамоқ билан жазолаш.

b) Энг кам ойлик иш ҳақининг юз бараваридан уч юз бараваригача миқдорда жарима ёки икки йилгача озодликдан маҳрум қилиш билан жазоланади

c) Энг кам ойлик иш ҳақининг етмиш беш бараваригача миқдорда жарима ёки уч йилгача аҳлоқ тузатиш ишлари билан жазолаш.

d) 2 йилдан 5 йилгача озодликдан маҳрум этиш ёки зарар миқдорини қоплаш билан бирга энг кам иш ҳақининг 100 бараваригача жарима.

50. Ҳимоялаш воситаларини қўллашда ташкилий тадбирлар нималарни ўз ичига олиши керак?

a) Тизимда сақланаётган ахборотлар алоқа линиялари бўйича узатилишида маълум қоидага кўра кодлаштирилиб, ундан очиқ ҳолда бевосита фойдаланиш имконияти баратараф этиш каби тадбирларни.

b) Ахборот тизимидаги жараёнларда ва дастурлардан фойдаланишда фаолият кўрсатувчи персонални танлаш ҳамда назорат қилиш, ахборотни қайта ишлаш жараёнларининг тартиб-қоидаларига қатъий риоя қилинишини таъминлаш каби тадбирларни

c) Ахборот тизимидаги жараёнларда ва дастурлардан фойдаланишда барча фойдаланувчилар учун ахборотга мурожаат қилиш имкониятини яратишга қаратилган тадбирларни.

d) Ахборот тизимидаги жараёнларни ва дастурлардан фойдаланишни тўғри ташкил этишни

Глоссарий

Ахборот хавфсизлиги бўйича атамалар ва таянч иборалар луғати

ACSCII (American Standart Code for Information Interchange) – маълумот алмашиш учун мўлжалланган Америка стандарт кодлаштириш жадвали.

Java-вируси - Java тилида тузилган апплетларга жорий этиладиган вирус.

SYN –тошқини - кўплаб сондаги пакетларни жўнатиш ҳисобига тармоқ драйвери бундай пакетларни қайта ишлаш имконига эга бўлмай, тизимнинг ишдан чиқишига олиб келувчи ҳаракат.

Telnet протоколи – масофадан туриб тармоқ компьютерини бошқариш имконини яратувчи қоидалар, дастурлар тўплами.

Абонент [abonent, subsriber, user] – ҳисоблаш техникаси хизматларидан фойдаланиш ҳуқуқига эга бўлган шахс (бир гуруҳ фойдаланувчилар, ташкилот).

Авторизация [Authorization] – фойдаланувчига, дастурга ёки жараёнга мурожаат қилиш имконини бериш. Шахсга (бир гуруҳ шахсларга) муайян амалларни бажариш ваколатини бериш.

Актив ҳужум – тизимдаги маълумотлар яхлитлигини бузилишига олиб келувчи ҳужум.

Алгоритм [algorithm] - ижрочи учун маълум бир масалани ечишга қаратилган чекли сондаги кўрсатмаларнинг аниқ кетма-кетлиги.

Алдов [Spoofing] – фойдаланувчини ёки тизимни нотўғри амал бажаришга ундовчи ғаразли ҳаракат.

Алоқа линияси трафиги таҳлили ([Traffic analysis] –алоқа тармоғи пунктларни боғловчи линиядан ўтказилаётган маълумотлар оқимини тадқиқ этиш (маълумот мавжудми, йўқми,йўналиши, частотаси).

Анализатор [Analyzer] – дастурлаш тизимида берилган дастурни таҳлил этувчи алгоритм.

Антивирус – компьютер вирусини аниқловчи ва уни тизимдан ўчириб юборувчи дастур. Агар вирус тизимдан ўчирилмаса, вирус билан зарарланган дастурнинг ўзи ўчириб юборилади.

Аппарат узилиши [Hardware interrupt] – ташқи қурилма томонидан содир этиладиган ёки бажарилаётган дастурдаги хато буйруқ туфайли содир бўладиган узилиш.

Апплетлар – турли хил дастурлаш тилларида яратилган унчалик катта бўлмаган дастурлар бўлиб, автоматик тарзда Web-браузер томонидан юкланадилар ва бажариладилар

Архив [Archives] - 1) Ташқи хотирада сақланаётган ҳозирда умуман керак бўлмаган, ёки вақтинча фойдаланилмайдиган ёки қисман фойдаланиладиган маълумотлар тўплами. 2) Маълумотлар ва дастурларнинг ташқи хотирада архиватор дастури ёрдамида зичлаштирилган ҳолда сақланиши.

Асимметрик шифр [Asymmetric cipher] – шифрлаш калити дешифрлаш калитига мос келмайдиган шифр.

Атрибут [Attribute] - маълумотлар хусисиятларини тавсифловчи аломат – номи, тури, узунлиги, миқдори, тасвирлаш тизими.

Аутентификатор – фойдаланувчини айрим хусусиятига кўра фарқлаб олишда қўлланиладиган аутентификация воситаси.

Аутентификация [Authenticate] - ўз идентификаторини маълум қилган субъект, ҳақиқатан ҳам ўзини маълум қилаётган, айнан ўша субъектлигига ишонч ҳосил қилиш жараёнидир. Аутентификация сўзининг синоними сифатида кўпинча «ҳақикийлигини текшириш» ибораси ишлатилади.

Ахборот [Information] – кишилар, нарсалар, табиатда рўй берадиган ҳодисалар, жараёнлар ҳақидаги маълумотлар.

Яна - табиатдаги объектлар, ҳодисалар, уларнинг хусусиятлари, ҳолатлари ҳақидаги маълумотлар тўплами бўлиб, объект ёки ҳодиса ҳақидаги мавҳумлик даражасини камайтириш имконини беради.

Ахборот инфраструктураси - ахборот билан ишлашда зарур бўлган электр, иссиқлик, сув таъминоти, совутгичлар, коммуникация воситалари ва ходимлар.

Ахборот муносабатлари субъекти – ахборот ресурсига нисбатан муайян ваколатга эга бўлган (мулкдори, эгаси, фойдаланувчиси) жисмоний ёки юридик шахс.

Ахборот муносабатлари субъектлари манфаатларига қаратилган таҳдид - ахборотга ёки ахборот тизимига салбий таъсир этувчи потенциал рўй бериши мумкин бўлган воқеа, таъсир ёки жараён.

Ахборот муҳофазаси - ахборот хавфсизлигини таъминлашга қаратилган тадбирларнинг мажмуи.

Ахборот ресурси - ахборот тизими таркибидаги электрон шаклдаги ахборот, маълумотлар банки, маълумотлар базаси.

Ахборот ресурсларининг ёки ахборот тизимларининг мулкдори - ахборот ресурсларига ёки ахборот тизимларига эгалик қилувчи, улардан фойдаланувчи ва уларни тасарруф этувчи юридик ёки жисмоний шахс.

Ахборот ресурсларининг ёки ахборот тизимларининг эгаси - қонун билан ёки ахборот ресурсларининг, ахборот тизимларининг мулкдори томонидан белгиланган ҳуқуқлар доирасида ахборот ресурсларига ёхуд ахборот тизимларига эгалик қилувчи, улардан фойдаланувчи ва уларни тасарруф этувчи юридик ёки жисмоний шахс.

Ахборот технологияси - ахборотни тўплаш, сақлаш, излаш, унга ишлов бериш ва уни тарқатиш учун фойдаланиладиган жами услублар, қурилмалар, усуллар ва жараёнлар тўплами.

Ахборот тизими - ахборотни тўплаш, сақлаш, излаш, унга ишлов бериш ҳамда ундан фойдаланиш имконини берадиган, ташкилий жиҳатдан тартибга солинган жами ахборот ресурслари, ахборот технологиялари ва алоқа воситалари.

Ахборот тизимининг хавфсизлиги [Information system security] – ахборот тизимини носозликлардан, унга рухсатсиз мурожаат қилишдан, таркибий яхлитлигини бузишдан ҳимоялашда қўлланиладиган чора-тадбирлар тўплами.

Ахборот узатишнинг ишончлилиги [Data transmission validity] – қабул қилинган ахборотнинг узатилган ахбортга мослиги.

Ахборот хавфсизлиги [Information security] - ахборот тизимида тасодифий ёки ғаразли равишда ахборот эгасига ёки унинг фойдаланувчисига зарар етказувчи таҳдидлардан ҳимояланганлик ҳолати.

Яна – ахборотнинг техник қурилмаларда қайта ишланиши жараёнида яхлитлиги, махфийлиги ва унга мурожаат қилиш имкониятининг таъминланганлик ҳолати.

Ахборот хавфсизлиги концепцияси – ахборот хавфсизлигини таъминлаш бўйича фикрлар, қоидалар ва умумий техник талаблар тизими.

Ахборот хавфсизлиги мезони – ахборотга ҳуруж қиладиган турли таҳдидлар таъсири натижасида унинг хавфсизлик даражасини характерловчи кўрсаткич.

Ахборот хавфсизлиги самарадорлиги [information techmical protection efficiency] – ахборот хавфсизлигини таъминланганлик даражасининг хавфсизлик мақсадларига мослиги.

Ахборот хавфсизлиги соҳасидаги сертификациялаш тизими – ахборот хавфсизлиги соҳасида ўз тартиб-қоидалари ва бошқариш тизими асосида дастурий-техник воситаларнинг талабларга мос келиши ёки хавфсизлик мезонларга мослигини сертификациялаш тизими.

Ахборот хавфсизлигини бошқариш – тегишли усул ва воситалардан фойдаланган ҳолда ахборот хавфсизлигини таъминлашни Бошқариш.

Ахборот хавфсизлигини таъминлаш бўйича ташкилий тадбирлар - ахборот тизимидаги жараёнларда ва дастурлардан фойдаланишда фаолият кўрсатувчи персонални танлаш ҳамда назорат қилиш, ахборотни қайта ишлаш жараёнларининг тартиб-қоидаларига қатъий риоя қилинишини таъминлаш каби тадбирлар.

Ахборот хавфсизлигини таъминлаш механизмларининг кафолатланганлиги – ахборот хавфсизлигини таъминлашда фойдаланиладиган механизмларнинг функционал талабларга мос келишини баҳолаш.

Ахборот хавфсизлигини таъминлашнинг техник чоралари – ахборот хавфсизлигини таъминлашда техник воситалар ва усулларни жорий этиш чора-тадбирлари.

Ахборот хавфсизлигини таъминлашнинг ҳуқуқий бўғини – ҳуқуқий-меъёрий ҳужжатлар асосида ҳуқуқбузарлик ва ахборот хавфсизлиги

бузғунчиларига нисбатан жамиятда салбий муносабат шаклланишига ва жамиятда ахборот хавфсизлиги соҳаси бўйича саводхонликни, маданиятни оширишга, ахборот хавфсизлигини таъминлашга қаратилган воситаларни жорий этишга йўналтирилган чора-тадбирлар.

Ахборотга мурожаат қилиш имкониятини таъминлаш - белгиланган вақт оралиғида ваколатга эга бўлган ахборот фойдаланувчилари ва субъектлари учун ахборот ёки у билан боғлиқ сервисга мурожаат қилиб фойдаланиш имкониятини таъминлаш.

Ахборотга рухсатсиз мурожаат [Unauthorized (illegal) access] – ваколатга эга бўлмаган фойдаланувчининг ахборотдан фойдаланиш, уни ўзгартириш ёки бузиш мақсадида мурожаати.

Ахборотга рухсатсиз мурожаат қилиш ҳаракати [Hacking] – тармоқ бўйича мурожаатларни назорат қилувчи воситаларни четлаб ўтиб, ахборот ресурсига мурожаат қилиш имконини қўлга киритишга қаратилган ҳаракат.

Ахборотлар алмашинуви [Data commuunication] – маълумотларни кодлаштириш, декодлаштириш, назорат қилиш билан бирга уларни қабул қилиш ва узатиш жараёни.

Ахборотлаштириш - юридик ва жисмоний шахсларнинг ахборотга бўлган эҳтиёжларини қондириш учун ахборот ресурслари, ахборот технологиялари ҳамда ахборот тизимларидан фойдаланган ҳолда шароит яратишнинг ташкилий ижтимоий-иқтисодий ва илмий-техникавий жараёни.

Ахборотни автоном равишда ҳимоялаш воситаси – ахборотни қайта ишлашнинг техник воситалари таркибига кирмаган, махсус ҳимоялаш қурилмаси.

Ахборотни аппарат воситалари ёрдамида ҳимоялаш – ахборотни қайта ишлашнинг техник воситалари тўпламига кирувчи махсус ҳимоялаш қурилмаси ёки ускунаси.

Ахборотни бузиш [Data erasing] – компьютер тизими хотирасида сақланаётган ахборотни ўчириш.

Ахборотни ёзиб-сақлашдан ҳимоялаш [Writeprotect] – дискдаги ёки оператив хотирадаги ахборотга ўзгартиришлар киритиб, сақлашдан ҳимоялаш усули.

Ахборотни йўқ қилиш – ахборот ташувчи воситада сақланаётган ахборотни тасодифан ёки ғаразли мақсадда (касддан) ўчириб ташлаш, шу жумладан, бундай воситани ўғирлаш.

Ахборотни қалбакилаштириш [Forgery] – қайта ишлаш жараёнида муайян ғаразли мақсадга эришиш учун ахборотга рухсатсиз ўзгартиришлар киритиш.

Ахборотни криптографик ҳимоялаш воситалари [Cryptographic information protection facility] – ахборот хавфсизлигини таъминлаш мақсадида ахборотни криптографик алмаштиришни амалга оширувчи ҳисоблаш машинаси воситалари.

Ахборотни криптографик ҳимоялаш усули – ахборотни шифрлаш тамойилига асосланган усул. Ушбу усул дастурий ёки аппарат воситалари ёрдамида жорий этилиши мумкин.

Ахборотни модификация қилиш (унга ўзгартиришлар киритиш) – ташки хотирада сақланаётган ахборотни қайта ишлаш жараёнида унинг ҳажми ёки мазмунини ўзгартириш.

Ахборотни ҳимоялашнинг техник воситалари [information technical protection facilities] – ахборотнинг бир ёки бир неча техник каналлардан чикиб кетиши олдини олишда қўлланиладиган техник воситалар.

Ахборотни чеклаш – ахборотга мурожаат килиш, ундан фойдаланишни чеклаш.

Ахборотни шифрлаш - ахборотни мазмун-моҳиятини яшириш мақсадида бошқа кўринишга алмаштириш жараёни.

Ахборотнинг кимматлилиги [Information value] – ахборотнинг инсон фаолиятининг турли йўналишларида амалда фойдалана олиш хоссаси.

Ахборотнинг эскириши [Ageing of information] – ахборотнинг вакт давомида ўзининг амалий аҳамияти ва кимматлилик хоссасини йўқотиш жараёни.

Ахборотнинг яхлитлиги [Integrity] – ахборот тизимидаги маълумотлар таркибининг бузилмаган ҳолда сақланиши ҳолати.

Биометрик маълумотлар – фойдаланувчининг шахсий хусусиятларига (товуш тембри, бармоқ излари, кафтининг шакли ва шу кабилар) қараб аутентификация воситаси орқали аниқлашда ишлатиладиган маълумотлар.

Бош пароль [Master password] - 1) Муайян пароллар тўплами учун умумий бўлган ўзак сўз. 2) Пароллар каталогини ҳимоялашда ишлатиладиган пароль.

Брандмауэр - тармоқни икки ёки ундан ортиқ қисмга ажратиб, унинг бир қисмидан иккинчи бир қисмига ахборот узатилиши қоидалари ва шартларини аниқловчи тизимдир. Яна - ташқи тармоқ билан ички тармоқ ўртасида ташқи тармоқдан амалга ошириладиган рухсатсиз мурожаатлар, ҳаракатларни чеклашда ва корпоратив тармоқни сегментларга ажратишда ишлатиладиган дастурий-техник воситадир.

Бузғунчи [Intruder] – тизимдан рухсатсиз фойдаланишга уринувчи ёки фойдаланувчи шахс ёки ташкилот.

Бузиб кириш [Penetration] – ҳимоя механизмларини барбод этиб, тизимга муваффақиятли кириш.

Верификация [verification] – икки даражадаги ҳисоблаш техникаси хусусиятларини солиштириб, бир-бирига мослиги таққослаш жараёни (масалан, хавфсизлик сиёсатини ахборот тизимига мослиги).

Яна – дастурлашда дастурнинг тўғри ишлашини исботлаш.

Воз кечиш [Failure] – ҳисоблаш тизими таркибидаги қурилма, дастур ёки персонал ўзига юклатилган вазифани бажара олмайдиган вазият.

Воситачи сервер (прокси-сервер) [Proxy server] - компания ходимларининг Интернет ресурсларига мурожаат қилишларини бошқарувчи дастур. Ушбу дастур ёрдамида ваколатга эга бўлган фойдаланувчи IP-адреси прокси-сервер дастури ўрнатилган сервер IP-адреси билан никобланади.

Гаммалаштириш - бошланғич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилиши.

Давлат сири – Давлат томонидан қўриқланадиган ва махсус рўйхатлар билан чегаралаб қўйиладиган алоҳида аҳамиятли, мутлақо махфий ва махфий ҳарбий, сиёсий, иқтисодий, илмий-техникавий ва ўзга хил маълумотлар.

Дастурий "бомба" – дустурнинг маълум қисмига хуфёна тарзда киритилган, маълум шартлар ёки вазият рўй берганида бир ёки бир неча бор ишга тушувчи буйруқлар кетма-кетлиги.

Дастурий воситалар [software] – дастурлар ва улардан фойдаланиш бўйича ҳужжатлардан ташкил топган воситалар тўплами.

Дастурий таъминотни ҳимоялаш воситалари [Software protection device] – дастурий таъминотга рухсатсиз мурожаатларни чеклашда ишлатиладиган воситалар.

Дастурни авторизациялаш [Program authorization] – тизимли дастурга ёки фойдаланувчи дастурига мурожаат қилишга Бошқа дастурлар томонидан чекловларни ўрнатиш.

Дастурнинг «осилиб» қолиши [Program hangup] – дастурнинг кўзда тутилмаган вазиятда тўхтаб қолиши, масалан, операцион тизим ишга тайёр бўлмаган, процессорга уланмаган қурилмага мурожаат қилиш буйруғи бажаришида рўй беради.

Демон [Demon] – тизимда ишлаётган дастур яхлитлигини бузмасдан унинг ишини назорат қилувчи ва вақти-вақти билан уни тўхтатувчи дастур.

Дешифрлаш [Decipherement] – шифрлаш амалига тескари бўлган, берилган шифрланган матнни ўз ҳолига тиклаш билан боғлиқ амал.

Домен [Domain] – мурожаат қилиш мумкин бўлган объект, дастур ёки Web-саҳифа адресининг иерархик структурага эга бўлган ўзига хос такрорланмайдиган қисми.

Ёлғон ахборот [False information] – ахборот хоссалари ва аломатларини бузиб кўрсатувчи, реал воқеликка зид келувчи ахборот.

Ёлғон ижобий огоҳлантириш – бунда антивирус дастури фойдаланувчига тизимда вирус мавжудлиги ҳақида маълумот беради, бироқ аслида бундай вирус мавжуд бўлмайди.

Ёлғон салбий огоҳлантириш – бунда антивирус дастури ҳеч қандай вирус мавжуд эмаслиги ҳақида маълумот беради, бироқ аслида тизимда вирус ҳақиқатан ҳам мавжуд бўлади.

Ёпиқ ахборот [Private information] – ваколатга эга бўлган органлар томонидан фойдаланишга рухсат бериладиган махфий маълумотлардан иборат ахборот.

Жисмоний хавфсизлик [physical security] – ахборотни жисмоний ҳимоялашда фойдаланиладиган тўсиқлар,назорат жойлари, жисмоний таҳдидлар (бинога, хонага рухсатсиз кириш, ахборот ташувчи воситаларни ўғирлаш, ёнғин, сув тошқини ва шу кабилар) олдини олишга қаратилган чора-тадбирлар.

Журнал [Journal,log] – ҳисоблаш техникасида операцион тизим ёки бошқа дастурий тизим юритадиган маълумотлар, ходисалар, узилишларга оид статистик маълумотларни ҳисобга оладиган файл.

Заифлик [Vulnerability] – таҳдидлар ҳуружи натижасида тизим ҳимоясининг бузилишига олиб келувчи тизимнинг хусусияти.

Зарарланиш [Infection] – ҳисоблаш техникасида вируснинг ўз нусхаси яратилиб, бошқа дастурлар, тизимли соҳаларга жорий этилиши ва яхлитлининг бузилиши.

Идентификатор [Identifier] – субъект ёки объектни ўзига хос аломатларига кўра аниқлаш воситаси. Фойдаланувчилар учун асосий восита пароль маълумотидир.

Идентификация [Identification] - бир томоннинг (фойдаланувчи, дастур, техник қурилма) бошқа бир томонга (масалан, бошқа бир дастурга) ўзининг такрорланмайдиган, уникал номини маълум қилиш жараёни.

Инсталляция [Installation] - дастурий маҳсулни компьютерга ўрнатиб созлаш.

Интерфейс (маълумотларни қайта ишлаш тизимларида) [interface (in data pro cessing systems)] – пооцессор томонидан тақдим этиладиган мулокот ойнаси, хизматлар кўлами.

Ишончлилик [Trusted funcionality] – хавфсизлик хоссаларининг муайян мезонларга мослиги.

Калит (шифрлашда қўлланиладиган) – ахборотни криптографик алгоритм асосида алмаштириш параметрларининг муайян махфий холати. Ахборотни шифрлаш ва дешифрлаш учун ишлатиладиган муҳим ҳимоя объекти.

Кафолатланганлик даражаси – ахборот тизими архитектураси ва жорий этилишида унга бўлган ишончлилик мезони бўйича бериладиган баҳо.

Кафолатлар [Assurance] – хавфсизлик сиёсатининг тўғри ва намунали бажарилиши нуктаи-назаридан тизим архитектураси ва хавфсизликни таъминлаш воситаларига бўлган ишонч мезони.

Кераксиз ахборот [Garbage] – ЭҲМ хотирасида сақланаётган, лекин кейинчалик фойдаланилмайдиган (эскирган, ишончли бўлмаган, бузилган) ахборот.

Клавиатурани чеклаш [Keyboard lockout] – компьютер клавиатураси оркали маълумотлар киритилишини операцион тизим томонидан чеклаш.

Код [Code] – ахборотни қулай ва ихчам кўринишда тасвирлаш воситаси.

Компаньон вирус – тизимда бирор бир файлнинг худди ўзига ўхшаш иккинчи бир нусхасини яратиб қўювчи вирус.

Компьютер вируси – ўз нусхасини компьютер тизимларига ва/ёки компьютер тармокларига тарқатиб, уларнинг конуний фойдаланувчилари манфаатларига зид равишда маълум бир ғаразли амалларни бажарувчи буйруқлар кетма-кетлигидир.

Компьютер жинояти – ўз рақобатчисига моддий зарар етказиш ёки ўзининг ғаразли максадига эришиши учун ахборот тизимига рухсатсиз мурожаат қилиш, ундаги ахборотларга ўзгартириш (қалбакилаштириш), ўчириш ёки тизим яхлитлигини бузишга каратилган ҳаракатлар.

Криптографик калит [Cryptology key] – ахборотни шифрлаш ва дешифрлашда қўлланиладиган белгилар кетма-кетлиги.

Криптографик химоя [Cryptosecurity(criptographical security)] – ахборотни криптографик алмаштиришлар усули билан ҳимоялаш.

Криптография [Cryptography] – ахборотни унинг мазмун-моҳиятини яшириш максадида алмаштириш ҳамда алмаштириш натижасида ҳосил қилинган ахборотни дастлабки ҳолатга қайтариш тамойиллари, воситалари ва усуллари.

Макровирус - маълумотларни қайта ишлаш тизимига (матн мухаррирлари, электрон жадваллар ва шу кабиларга) ўрнатилган макротиллар

имкониятларидан фойдаланувчи, макрослар ўрнига ўз кодини жойлаштирувчи вирус.

Мантиқий "бомба" [Logic bomb] – зарар етказувчи дастурда маълум шартлар бажарилганида ёки воқеа рўй берганида фаоллашувчи тизимга рухсатсиз мурожаат қилиб, унинг яхлитлигини бузувчи буйруқлар кетма-кетлиги.

Махфий ахборот [Sensitive information] - ўз эгаси томонидан ошкор қилинмайдиган, тижорат ёки шахсий сирга эга бўлган ҳимояланадиган ахборот. Яна - мурожаат қилиш имконияти фақат ваколатга эга бўлган тор доирадаги фойдаланувчиларгагина берилган ахборот.

Маълумотлар базаси [database] - маълум бир соҳага тегишли бўлган муайян объектлар ҳақидаги структуралаштирилган маълумотлар тўплами.

Маълумотлар базаси администратори [Data administrator] – маълумотлар базасини юритиш, ундан фойдаланиш, такомиллаштиришга жавоб берувчи, маълумотлар базаси таркиби ҳақида тўлиқ тасаввурга эга бўлган масъул ходим (бир гуруҳ ходимлар).

Маълумотлар базасини маъмурий бошқариш [database administration] – маълумотлар базаси маълумотларини аниқлаш, ташкил этиш, Бошқариш ва ҳимоялаш вазифаларини бажариш.

Маълумотлар базасини тиклаш [database recovery] - 1) Маълумолтлар базасини тўлиқ ёки қисман қайта юклаш. 2) Маълумотлар базасини заҳира нусхаси орқали тиклаш..

Маълумотлар нусхасини кўчиришдан ҳимоялаш [Copyprotection] – ташқи хотирада сақланган ахборотнинг нусхасини бошқа хотира соҳасига кўчиришни тақиқлаш учун дастурий-техник воситадан фойдаланиш..

Маълумотлар хавфсизлиги [Data security] – маълумотларни рухсатсиз (тасодифан ёки ғаразли равишда) ўзгартириш, бузиш ёки ошкор қилишдан ҳимоялаш.

Маълумотларни кодлаштириш [Coding, encoding] – муайян объектлар ҳақидаги маълумотларни белгиланган қоидага кўра ихчам шаклда ифодалаш ва

компьютерда қулай равишда кайта ишлаш максадида амалга ошириладиган жараён.

Маълумотларни авторизациялаш [Data authorization] – маълумотлар базасида маълумотларнинг махфийлик даражасини аниклаш ва ўрнатиш.

Маълумотларни тиклаш [Data recovery] – ташки хотира воситасидан ўчиб кетган маълумотларни захира нусхаси оркали ёки махсус тикловчи дастурлар оркали тиклаш.

Маълумотларни химоялаш тизими [Security system] – маълумотларни рухсатсиз ўчириш, ўзгартириш, фойдаланишдан химоялашни таъминловчи аппарат, криптографик воситалар, чора-тадбирлар мажмуаси.

Муаллифлик хукуки - ижодий мехнати билан асар (илмий ихтиро, адабий асар, ижро этиладиган постановка, фонограмма, кўрсатув, компьютер дастури) яратган жисмоний шахснинг асаридан фойдаланиш ва уни тарқатиш билан боғлиқ бўлган муносабатларни мувофиклаштирувчи хукукий меъёрлар тўплами

Мурожаат қилиш имконияти [access] – маълумотларни кайта ишлаш тизимига маълумотларни тақдим этиш ёки ундан излаш, ўкиш амаллари оркали маълумотларни олиш имконияти. Субъект ва объект ўртасида ахборот алмашинувини таъминлашга қаратилган ўзаро харакатларни амалга ошириш имконияти.

Мурожаат қилиш қоидаларини бузувчи модели – ахборот ресурсига рухсатсиз мурожаат қилувчи абстракт тавсифи. Бузувчи моделига троян дастури, мантиқий «бомба», компьютер вируси мисол бўла олади.

Мурожаатларни бошқарувчи администратор [Access administrator] – маълумотлар банкига қайси фойдаланувчилар мурожаат қилишларини таксимловчи, мурожаатларни ташкил этувчи масъул ходим.

Мурожаатларни чеклаш – хотира соҳасига мурожаат қилишни аппарат ёки дастурий восита асосида чеклаш.

Никобланиш (Маскарад) [Mascquerade] – фойдаланувчининг бошка фойдаланувчи номидан тизимга кириши.

Носозликларни аниқлаш [Fault diagnostics] – электрон ҳисоблаш машиналарида ёки ташқи қурилмаларда носозлик рўй берган жойни излаш, носозлик келиб чиқиши сабабини аниқлаш.

Норезидент вирус - оператив хотирани эгалламайдиган, ўз коди жорий этилган дастур ишлаганида фаол бўладиган вирус.

Операцион тизим (ОТ) [Operating system (O.S.)] – Электрон ҳисоблаш машиналари қурилмалари, ресурслари ишини мувофиқлаштирувчи ва бошқарувчи, фойдаланувчи билан мулокотни ташкил этувчи дастурий таъминотнинг асосий қисми.

"Оранжевая книга" [Orange book] – тўлиқ номи "Department of Defence Trusted Computer System Evalution Criteria" DOD 5200.28STD ("Мудофаа вазирлиги компьютер тизимлари хавфсизлигини баҳолаш мезонлари "). АҚШнинг ушбу стандартида давлат манфаатлари учун яратиладиган ва фойдаланиладиган компьютер тизимлари хавфсизлиги 4 та синф - A, B,C,D ишончлилик даражалари асосида баҳоланиши кўзда тутилган.

Очиқ ахборот – давлат, хизмат, тижорат ёки шахсий сирдан иборат бўлмаган, матбуотда эълон қилиниши мумкин бўлган ахборот.

Пакетли даражада ишловчи брандмауэр [packet-filtering firewall] – тармоқ бўйича кирувчи ёки чиқувчи маълумотлар пакетларини фильтрлаш асосида узатилишини таъминловчи брандмауэр. Фильтрлаш пакет сарлавҳасидаги маълумотлар асосида амалга оширилади..

Паразит вирус – файлнинг муайян жойига ўз кодини киритиб, унинг таркибини ўзгартирувчи, лекин унинг ишига халақит қилмайдиган вирус.

Пароль [Password] – ҳарф, рақам ва белгилардан иборат кодлаштирилган махфий сўз бўлиб, компьютер билан мулокот қилишда киритиладиган ва тизимга мурожаат қилиш имконини берувчи восита.

Пароль ёрдамида ҳимояланиш [Password protection] –мурожаат қилишни пароль асосида чеклаш ҳисобига маълумотларни ҳимоялаш.

Пассив таҳдид [Passive threat] – тизим ишлашига халақит қилмасдан ахборотга рухсатсиз мурожаат қилиш имконияти.

Пассив ҳужум – тизимдаги маълумотлар оқимини ўрганиш, таҳлил қилиш, кузатиш ҳаракатлари.

Персонал хавфсизлиги [Personnel security] – айрим критик ахборотларга мурожаат қилувчи персонал ваколати ҳақиқийлигини кафолатлаш усули.

Плагин [Plug-in] – асосий дастур функционал имкониятларини оширишга қаратилган динамик равишда юкланадиган кутубхона файллари тўплами.

Полиморф вирус - Сигнатурасини турли хилда шифрлаш ҳисобига ўз кодини ўзгартириш хусусиятига эга бўлган вирус.

Портлаш [Blowup] – ҳисоблаш тизимида тегишли огоҳлантирувчи маълумот бериладиган авариялы ҳолат бўлиб, унда бажарилаётган дастур иши чекланиб, тўхтатилади.

Почта "бомба"си – кўп сонли хатлар юбориш ҳисобига электрон почта серверини ишдан чиқариб, унинг сайтини чеклашга қаратилган ҳужум воситаси.

Протокол [Protocol] - икки ёки ундан ортиқ компьютерларнинг ўзаро ахборот алмашинуви доирасини белгиловчи қоидалар, битимлар, сигналлар узатилиши ва дастурларнинг расман қабул қилинган тўплами.

Рақамли имзо [Digital signature] – аутентификация жараёнини таъминлаш учун ахборот узатувчиси томонидан ҳавола этиладиган қўшимча ахборот. Маълумотлар блокини криптографик алмаштиришлар натижасида ўзгартириб, уни олувчига ҳақиқий узатувчи кимлигини аниқлаш имконини берувчи, малумотлар блокини яхлитлигини таъминлашда ишлатиладиган маълумотлар кетма-кетлиги.

Резидент [Resident] – оператив хотирада доимо сақланувчи маълумотлар.

Резидент вирус – ўз кодини ёки унинг маълум бир қисмини компьютер оператив хотирасига жойлаштириб, операцион тизим орқали дискдаги файл ва дастурларга мурожаат қилишни эгаллаб олувчи вирус.

Рухсатсиз мурожаатлардан ҳимояланиш [Protection from unauthorized access] – тизимдаги дастурлар ва маълумотларга рухсатсиз мурожаат қилишни чеклаш учун аппарат, дастурий ва криптографик воситалардан фойдаланиш. Бундай

ҳимояланишда энг кўп қўлланиладиган дастурий усул пароль тизимидан фойдаланишдир.

Рухсатсиз мурожаатлардан ҳимоялаш воситалари [Protection facility] – тизимга рухсатсиз мурожаатларни чеклаш максадида фойдаланиладиган дастурий, техник ва дастурий-техник воситалар.

Рўйхатга киритилмаган фойдаланувчи [Unauthorized user] – компьютер тизимида авторизация параметрлари киритилмаган фойдаланувчи.

Рўйхатга олинган фойдаланувчи [Authorized user] - тизимда идентификация ва аутентификация параметрлари қайд этилган фойдаланувчи.

Сигнатура [Signature] - вируснинг барча нусхаларида ва фақат нусхаларида учрайдиган ўзига хос бўлган код бўлагидир.

Скрипт (инглизча script - сценарий) - HTML форматида тайёрланган ҳужжатни кўрсатиб, намойиш этилганда Web-саҳифада ижро этиладиган дастур. Ҳозирги вақтда HTML-ҳужжатида сценарийлар ёзиш бўйича Java, JavaScript, VBScript ва шунга ўхшаш тиллар ишлатилади.

Спам [spam] - фойдаланувчиларнинг қизиқиш ёки эҳтиёжлари ҳисобга олмаган ҳолда уларга электрон почта орқали юборилади ган аноним хат-хабар.

Стеганография – ахборот мавжудлигини яшириш тамойиллари, воситалари ва усуллари. Стеганография ёрдамида дастурий таъминотни никоблаш, муаллифлик ҳуқуқларини ҳимоялаш ишлари амалга оширилади.

Стелс вирус [Stealth virus] – диск ёки бошқа ташқи хотира воситаси (баъзида оператив хотира) соҳасида ўзининг мавжудлигини яшириш мақсадида махсус алгоритмдан фойдаланувчи вирус.

Тармоқ хавфсизлиги [Network security] – тармоққа рухсатсиз киришдан, унинг нормал ҳолатда ишлашига халақит қилувчи ҳаракатлардан ёки унинг таркибий қисмлари бузилишидан сақлашга қаратилган чора-тадбирлар.

Таҳдид [threat] - кимларнингдир манфаатларига зиён етказувчи, рўй бериши мумкин бўлган воқеа, таъсир, жараён

Ташхис (Диагностика) [diagnostics] – объектлар ҳолатини назорат қилиш ва бошқаратлаш..

Тег (tag) - HTML-ҳужжатнинг бошқарувчи белгиси. Теглар ёрдамида саҳифадаги саҳифа элементларининг аксланишини бошқариш мумкин. Масалан матн шрифти, ранги, мурожжатларни ташкил қилиш ва хоказолар.Тег – элементнинг саҳифадаги таъсир кўрсатиш доирасини аниқлайди ва бир элементни бошқа элементдан ажратиб туради. Тег матни одатда < ва > белгилари орасида жойлаштирилади. Тег охири эса /* белгиси билан якунланади.

Тижорат ахбороти [Commercial information] – ахборот эгаси томонидан унинг хоҳиши ва шартларига кўра тарқатиладиган ахборот, олди-сотди объекти.

Тижорат сири – ошкор қилиниши ўз эгасига моддий ёки маънавий зарар келтирадиган, давлат корхонаси ёки хусусий корхона фаолиятига тааллукли махфий ахборот.

Тизим администратори [System administrator] – тизимдан фойдаланиш, уни қўллаб-қувватлаш бўйича масъул ходим

Тизим химояси [System security] – тизимга рухсатсиз мурожаат қилишни чеклаш учун бажариладиган чора-тадбирлар йиғиндиси.

Тизимли калит [System key] – тизимни, ёки тизим воситаларини хавфсизлигини таъминлашда, рухсатсиз мурожаатлардан чеклашда ишлатиладиган калит (маълумот).

Тизимли узилиш [operation code trap] – тизим иши билан уйғун равишда оддий узилиш сигнали натижасида рўй берадиган вазиятга ўхшаш ҳолат. Тизимли узилиш тизимли дастурлар иши, қурилмаларга берилган буйруқлар, тизимга нотўғри киритилган буйруқлар натижасида рўй беради.

Тизимнинг «осилиб» қолиши [System quiescing] – янги вазифаларни тизим томонидан инкор этилиши ёки қабул қилинмаслиги.

Трафик [Trafic] – маълумотлар узатиш тармоғидаги хабарлар оқими, алока линиясининг ишчи қуввати.

Троян дастури [Trojan horse] – фойдаланувчининг ахборотларини йиғиш, ўғирлаш, бузиш, ўзгартириш ёки компьютер тизимини ишдан чиқариш ёки

унинг ресурсларидан фойдаланиш максадида рухсатсиз амаллар бажарувчи зарарли дастур.

Файлни тиклаш [File recovery] – файл яхлитлигини таъминлаш мақсадида махсус дастур ёки буйруқ орқали тиклаш.

Фаол таҳдид [Active threat] – тизим ҳолатини ғаразли равишда рухсатсиз ўзгартиришга қаратилган таҳдид.

Фаол ташкил этувчилар - Web-браузер томонидан автоматик тарзда юкланадиган ва бажариладиган дастурларга мурожаат қилувчи Web-саҳифалар.

Фаол яшириш [active hiding] – ахборот ташувчи воситани аниқлашни чигаллаштирувчи ахборотни техник ҳимоялаш усули

Форматни ўзгартириш [Format altration] – дискдаги маълумотларни кўчириб олишдан ҳимоялаш мақсадида дискни ностандарт усулда форматлаш. Бундай ўзгартириш натижасида дискдаги файлларни хизматчи дастурлар орқали кўчириш чекланади.

Хабар маълумотларини эгаллаб олиш [Message wiretapping] – алока линиясига махсус терминални рухсатсиз улаб, линиядаги хабарларни қабул қилиш ва улардан фойдаланиш.

Хавфли дарча – тизимда заифликлар маълум бўлган вақтдан то уларни бартараф этилгунга қадар бўлган вақт оралиғи. Рухсатсиз мурожаатларни чеклаш тизимини хатлаб ўтиш имконини яратувчи ҳисоблаш тизими аппарат қурилмалари носозликлари ва дастурий таъминотдаги мавжуд хатоликлар.

Хавфсиз зона [safety zone] – тегишли хавфсизлик даражаси таъминланган соҳа.

Хавфсизлик [Safety (security)] - шахснинг, корхонанинг, давлатнинг мухим ҳаётий манфаатларининг ташқи ва ички таҳдидлардан ҳимояланганлик ҳолати. Яна – маълумотлар ва файллардан рухсатсиз фойдаланишдан, уларни ўзгартиришдан ҳимояланганлик ҳолати.

Хавфсизлик сиёсати [security policy] - ахборотни тўплаш, қайта ишлаш ва тарқатишни ташкил этишга қаратилган қонунлар, қоидалар ва меъёрий ҳужжатлар асосида корхонанинг ахборот хавфсизлигини таъминлаш бўйича ишлаб чиқилган чора-тадбирлари мажмуидир.

Хавфсизлик хизмати [Security service] – узатилаётган маълумотлар ва алока тизими хавфсизлигини таъминловчи масъул ходимлар ва техник воситалар..

Хакер [Hacker] – муайян ваколатга эга бўлмасдан туриб тизимли дастурий таъминотга ўзгартириш киритишга ҳаракат қилувчи фойдаланувчи. Фойдали ва яхши ҳужжатлаштирилмаган дастур яратувчиларни ҳам хакерлар деб аташади. Сабаби, уларнинг дастурлари кўзда тутилмаган ҳолатларни келтириб чикаради.

Хатоликлар журнали [Journalizing] – тизимдаги хатоликлар ва носозликлар қайд қилинувчи файл.

Хизмат кўрсатишдан воз кечиш [Denial of service] – тизимнинг маълум қисмини носозлик ҳолатига келтиришга қаратилган ихтиёрий ҳаракат ёки амаллар кетма-кетлиги.

Хизмат сири – фан, техника, ишлаб чиқариш, бошқариш соҳаларига тааллукли, давлат томонидан ҳимояланадиган ва ошкор қилиниши тақиқланган маълумотлар.

Хусусий маълумот [Data privacy] – ўз эгаси ва чекли сондаги фойдаланувчиларгина мурожаат қилиши мумкин бўлган маълумотнинг ҳолати.

«Чувалчанг» [Worm] - мустакил равишда, яъни бошка дастурларга сукилиб кирмасдан ўз нусхасини тизимда кўпайтириш ва бажариш имкониятига эга бўлган буйруклар кетма-кетлигидан иборат код.

Шахсий идентификация номери [Personal Identification Number (PIN)] – мурожаатлар бошқариладиган тизимга кириш учун ишлатиладиган фойдаланувчининг шахсий коди.

Шифр [Cipher] – очиқ ахборотни маълум қоидаларга кўра калит асосида ёпиқ ахборотга алмаштиришда ишлатиладиган восита.

Шифрлаш - маълум алгоритм асосида бошланғич матнни унинг маъносини англаб бўлмайдиган кўринишдаги матнга алмаштириш.

Шифрланган матн [Ciphertext] – берилган очиқ матннинг мазмун-мохиятини яшириш максадида шифрлаш натижаси. Электрон хатнинг ёки маълумотнинг шифрланган шакли

Шифрланган маълумотлар [Cipher data] – компьютер хотирасида шифрланган ҳолда сақланадиган ахборот, яъни маълумотларни криптографик ҳимоялаш усули жорий этилган ахборот.

Шифрлаш гаммаси - очиқ ахборотни шифрлаш ва дешифрлаш учун берилган алгоритм асосида ишлаб чиқиладиган тасодифий иккилик рақамлар кетма-кетлиги.

Шифрлаш алгоритми – калитли маълумот асосида ахборотни бир шаклдан иккинчи бир шаклга алмаштириш учун ишлатиладиган математик қоидалар тўплами.

Шифрлашнинг RSA усули [RSA Encryption] – Ривест, Шамир ва Адлеманлар томонидан ҳавола этилган шифрлаш усули. Ушбу усулда ахборотни шифрлаш учун ишлатиладиган калит уни дешифрлашда ишлатиладиган калит билан устма-уст тушмайди. Шунинг учун ушбу усул икки калитли ёки очиқ калитли усул деб аталади.

Электрон почта [Electronic mail (computer mail)] – ҳисоблаш тизими фойдаланувчилари ўртасида ўзаро хабарлар алмашиш тизими.

Юкловчи вирус [Boot virus] – дискларнинг бошланғич секторларида жойлашган юкловчи дастур ўрнига ўз кодини ёзиб қўювчи вирус

Яшириш [hiding] – ахборотни техник ҳимоялаш усули бўлиб, унда ахборот ташувчи восита ёки унда сақланаётган маълумотлар яққол кўрсатилмайди.

Ҳимоя воситаларининг мажмуаси [Trusted computing base] – ҳисоблаш техникаси ёки ахборот тизими воситаларига, улардаги ахборотларга рухсатсиз мурожаатлардан ҳимоялашни таъминлайдиган дастурий ва техник воситалар тўплами.

Ҳимоя модели [Protection model] – аахборот хавфсизлигини таъминлашда қўлланиладиган дастурий-техник воситалар ва ташкили чора-тадбирларнинг биргаликда мажмуасини абстракт тавсифи.

Ҳимояланган файл [Protected file] – пароль оркали мурожаат қилинадиган файл.

Ҳимоялашнинг аппарат воситалари – ахборотдан рухсатсиз фойдаланиш, уни кўчириш, ўгирлаш ёки ўзгартирилишидан ҳимоя қилишда ишлатиладиган механик, электромеханик, электрон, оптик, лазерли, радиотехник ва бошқа қурилмалар, тизимлар ва мосламалар.

Ҳимояни кафолатлаш [Security accredidation] – қайта ишланадиган ахборот хавфсизлиги стандарт талаблар ва бошқа меъёрий ҳужжатларга мос келишини тасдиқловчи сертификат ёки шаҳодатноманинг мавжудлиги.

Ҳисоблаш тармоғи (Компьютер тармоғи) [Network] - узатиш каналлари орқали ўзаро боғланган электрон ҳисоблаш машиналари мажмуи.

Ҳисоблаш тармоғининг ҳимояси [Network security] – фойдаланувчиларнинг тармоқ элементлари ва ресурсларига рухсатсиз мурожаатларини аппарат, дастурий ва криптографик воситалар ёрдамида чеклаш.

Ҳисоблаш техникаси (ахборот тизими) хавфсизлик синфи [Protection class of computer (information) system] - хавфсизлик талаблари бўйича ҳисоблаш техникаси (ахборот тизими) хавфсизлиги таъминланганлиги бўйича баҳолаш мезони.

Ҳужум [Attack] – тизимнинг камчилик ва заиф томонларидан фойдаланиб бузғунчининг тизимнинг яхлитлигини, унга мурожаат қилиш имкониятини ва қайта ишланадиган ахборот бирлигини бузишга қаратилган, олдиндан ўйлаб қилинган ҳаракатлари.

Ҳужум уюштирувчи [Attacker] – компьютер тизимида ўз ҳаракатлари билан ахборот хавфсизлигини бузувчи субъект.

Абдурахимов Дониёр Баҳодирович

Жўраев Умиджон Сайфуллаевич

Тоштемиров Дониёр Эшбоевич

АХБОРОТЛАРНИ ҲИМОЯЛАШ

фанидан услубий қўлланма

Босишга рухсат этилди 29.08.2016. Бичими 60x84 1/16
Офсет қоғози. Times New Roman шрифтида терилди.
11 б.т. Адади 50 нусха

Гулистон давлат университети босмахонасида чоп этилди.
Гулистон ш. 4-мавзе, ГулДУ бош бино, Tel:225-40-42