ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ТОШКЕНТ ДАВЛАТ ИҚТИСОДИЁТ УНИВЕРСИТЕТИ

А.К. Машарипов, Т.А. Зокирова,
Ш.Т. Эрматов, Р.М. Ходиева, М.А. Мусаева

КОМПЬЮТЕР ТИЗИМЛАРИДА АХБОРОТНИ ҲИМОЯ ҚИЛИШ

Ўқув қўлланма

ТОШКЕНТ - 2006

Муаллифлар: А.К. Машарипов, Т.А. Зокирова, Ш.Т. Эрматов, Р.М. Ходиева, М.А. Мусаева. Компьютер тизимларида ахборотни ҳимоя қилиш. Ўқув қўлланма. − Т.: ТДИУ, 2006, − б.

Тақризчилар: И.Х. Сиддиқов
О.А. Абдуллаев

МУНДАРИЖА

КИРИШ

Инсониятнинг XXI асрга кириб келиши жамият ҳаётининг ҳамма сохаларида ахборот технологияларини жадал ривожланиши билан чамбарчас боғлиқдир. Ахборот тобора кўп жиҳатдан давлатнинг стратегик ресурси, ишлаб чиқарувчи кучи ва қимматбаҳо маҳсулоти бўлиб бормоқда. Бу давлатларни, ташкилотларни ва алоҳида олинган фуқароларни оппонентларга тегишли бўлмаган ахборотга эга бўлиш ҳисобига, ҳамда рақобатчининг ахборот ресурсларига зарар етказиш ва ўзининг ахборот ресурсларини ҳимоя қилиш ҳисобига устунликка эришишга интилишини келтириб чиқаради. Ахборотни ҳимоя қилиш муаммоси жуда қадим замонлардан бери инсониятни ташвишга солиб келмоқда. Ахборотни ҳимоя қилиш зарурлиги ҳам ҳарбий, ҳам дипломатик хабарларни махфий узатиш заруратидан пайдо бўлган. Масалан, антик спартакчилар ўзларининг ҳарбий хабарларини шифрлаганлар. Хитойликларда хабарларни иероглифлар ёрдамида оддийгина ёзиш уни ўзга юртликлар учун махфий қилиб қўйган.

Замонавий компьютер тизимларини яратилиши ва глобал ахборот тармоқларини пайдо бўлиши ахборотни ҳимоя қилиш муаммосини характерини ва диапазонини кескин ўзгартирди. Кенг компьютерлаштирилган ва ахборотлаштирилган замонавий жамиятда реал қадриятларга эга бўлиш, уларни бошқариш, қадриятларни узатиш ва уларга мурожаат қилиш кўпинча номоддий ахборотларга, яъни мавжуд бўлиши физик ташувчидаги бирорта ёзув билан боғланиши мажбурий бўлмаган ахборотларга асослангандир. Шунга ўхшаш, баъзида юқори ахамиятга эа бўлган махфий ахборотни ишлатишга, ўзгартиришга, нусхалашга жисмоний ва ҳуқуқий шахсларнинг ваколатлари аниқланади. Шунинг учун ахборотни махфийлиги ва бутунлигини таъминлаш билан боғлиқ бўлган барча керакли функцияларни амалга ошириш учун самарали воситаларни яратиш ва ишлатиш жуда муҳимдир.

Ахборот ёки ўта муҳим бўлганлиги сабабли бундай ахборотни сақлайдиган, қайта ишлайдиган ёки узатадиган компьютер тизимларига нисбатан турли-туман ёмон ниятли ҳаракатлар қилиш мумкиндир. Масалан, бузғунчи ўзини бошқа фойдаланувчи каби кўрсатишга интилиши, алоқа каналини билдирмасдан эшитиб олиши ёки тизим фойдаланувчилари алмашаётган ахборотни ушлаб олиши ва ўзгартириши мумкин. Замонавий компьютер тизимлари ва тармоқлари, Интернет ёмон ниятли кишиларга муҳим махфий ахборотни ўғирлаш, бузиш ёки тўсиқларга учратиш мақсадида корхоналар ва ташкилотларнинг ички тармоқларига бостириб кириш учун кўплаб имкониятлар яратадилар. Шу сабабли ҳозирда инсонларни ва жамиятни ахборот хавфсизлигини ва ахборотни ҳимоя қилишни таъминлаш муаммосини комплекс ечишни долзарб равишда кераклиги пайдо бўлмоқда.

Шу билан бирга таъкидлаш керакки, ўтказилаётган afjkв тадқиқотларга қарамасдан, ахборот хавфсизлигини яхлит тизимини яратишни умумлашган назарияси ва амалий концепцияси (йўна-лиши) ҳанузгача яратилмаган. Шунинг учун махфий ахборот билан ишлаган шахсларга ахборот хавфсизлигини таъминлаш масалаларини барча жабҳаларида, уларнинг комплексли ва ўзаро

келишилган характерини тушунган ҳолда, етарлича тайёргарликка ва мутахассис сифатида мўлжалашга билишга эга бўлишлари керак.

Мақсадларга қарашлар тизими каби ахборот хавфсизлиги кон-цепцияси, ахборот хавфсизлигини таъминлаш усуллари ва уни ҳимоя қилиш воситалари умумий кўринишда учта оддий саволга жавоб бериши керак: нимани, нимадан ва қандай ҳимоя қилиш керак ?

- « Нимани ҳимоя қилиш керак?» саволи билан ҳимоя қилиш обьекти тушунчаси, яъни ахборотларни йиғиш, сақлаш, узатиш ва қайта ишлаш учун мўлжалланган физик, аппаратли, дастурли ва ҳужжатли воситаларнинг комплекси боғлангандир.
- «Нимадан ҳимоя қилиш керак» саволи хавф (таҳдид) тушунчаси билан, яъни ахборотни йўқотилишига ёки очиқ эълон қилинишига олиб келадиган, ҳимоя қилиш обьектига ноқонуний таъсир этишни потенциал имкониятлари боғлангандир.
- «Ахборотни қандай ҳимоя қилиш керак» саволи билан ҳимоя қилиш тизимининг тушунчаси, яъни тадбирлар ва воситалар клмплекси, ҳамда улар асосида ҳимоя қилиш обьектини хавфсизлигини хавфларини турли-туман кўринишларини пайқашга, қайтаришга ва йўқ қилишга йўналтирилган фаолият ажралмас равишда боғлангандир.

Ушбу маърузалар матнида бу саволларни очиб беришга маълум бир интилишлар ва уларнинг ечимларини топишга ҳаракат қилинган. Улар « Компьютер тизимларида ахборотни ҳимоя қилиш » курсини ўқув дастурига мос равишда республикамизнинг олий ўқув юртларини иқтисодиёт йўналишларини талабалари учун ёзилган.

1 боб. АХБОРОТЛАРГА НИСБАТАН ХАВФСИЗЛИКЛАРНИНГ АСОСИЙ ТУШУНЧАЛАРИ

1.1. Замонавий ахборотлашган жамиятда ахборот хавфсизлиги

Ахборотлаштириш замонавий жамият ҳаётининг характерли сифати (хислати) ҳисобланади. Янги ахборотли воситалари ва технологиялар халқ хўжалигининг ва инсон фаолиятининг барча соҳаларига фаол татбиқ қилинмоқда. Улар космик кемаларни ва самолётларни бошқарадилар, атом электростанцияларнинг ишини назорат қилади, турли хил давлат ва хусусий тузилмаларга хизмат кўрсатадилар, аҳолига жуда кўп миқдордаги ахборот хизматларини тақдим этади ва ҳ.к.[2,5]

Компьютерлар, компьютер тизимлари ва тармоқлари. Ахборотни сақлаш ва қайта ишлашни, уни истеъмолчиларга тақдим этишни, шу билан бирга энг замонавий ахборот технологияларини қўллашни амалга оширадиган ахборотни қайта ишлайдиган барча автоматлаштирилган тизимларининг асоси ҳисобланади. Ахборот технологиялари воситалари ва усулларининг гуркираб ривожланиши ва мураккаблашиши билан бир қаторда жамиятнинг унда ишлатилаётган ахборот хавфсизлигига боғлиқлиги даражаси ортади.

Ахборот хавфсизлигини таъминлаш муаммолари инсониятни жуда қадим замонлардан бери ташвишлантириб келмоқда. Ахборотни ҳимоя қилишнинг зарурлиги ҳам харбий, ҳам дипломатик маълумотларни узатиш эҳтиёжидан келиб чиққан. Масалан, антик спартакчилар ўзларининг ҳарбий маълумот-ларини шифрлаганлар. Хитойликларда иероглифлар ёрдамида маълумотни оддий ёзиш уни ўзга юртликлар учун сирли қилиб қўядилар. Ахборотни узатишда унинг хафсизлигини таъминлаш мақсадида шу вактгача энг ишончли ва оддий канал - курьерлик канали ишлатилмоқда. Бундай алоқа тизимларининг хавфсизлиги курьернинг ишончлигига ҳам, маълумотни фош этиш мумкин бўлган вазиятларга тушмаслик қобилиятига ҳам боғлиқ бўлади.

Замонавий ахборотлашган жамиятда кўпроқ «ахборот» тушунчаси сотиб олиш, сотиш, бирор бошқа нарсага алмаштириш ва ҳ.к. мумкин бўлган махсус товарнинг белгиланиши каби ишлатилади. Бунда ахборотнинг нархи унинг ўзи жойлашган компьютер тизимининг ўзидан юзлаб ва минглаб марта ошиб кетади. Шунинг учун, табиийки, ахборотни рухсат этмасдан туриб мурожаат этиш, била туриб ўзгартиришдан, ўғирлашдан, йўқ қилиш ва бошқа жиноий ҳаракатлардан ҳимоя қилишнинг жиддий зарурлиги келиб чиқади.

Замонавий компьютер тизимлари ҳамда тармоқларининг яратилиши, ривожланиши ахборот хавфсизлигини таъминлаш муаммосининг характерини ва диапазонини тубдан ўзгартирди. Ахборотлашган жамиятда ҳақиқий аҳамиятликка эга бўлиш, уларни бошқариш, ёки уларга мурожаат қилиш кўпинча ҳақиқий бўлмаган ахборотга, яъни мавжуд бўлиши физик ташувчида бирор-бир ёзиш билан мажбурий боғланмаган ахборотга, асосланган. Шунга ўхшаш шаклда баъзида физик ва ҳуқуқий шахсларнинг катта аҳамиятга эга бўлган у ёки бу махфий ахборотни ишлатишга, модификациялашга ёки нусхалашга ваколатлари ҳам аниқланади.

Ахборот хавфсизлигини таъминлаш муаммоси Интернетнинг ишлаш шароитларида мухим аҳамият касб этади. Мутлақ кўпчилик компаниялар ва ташкилотлар бугунги кунда ўзларининг локал тармоқларини Интернетга, унинг ресурсларидан ва афзалликларидан фойдаланиш учун уламоқдалар. Улар Интернетни турли мақсадларда ишлатадилар, бунга электрон почта билан алмашиниш, қизиқиб қолган шахслар ва ташкилотлар ўртасида ахборотларни олиш ва тарқатиш ва ҳ.к. киради. Бош тармоққа уланиш катта афзалликларни беради, аммо бунда уланаётган локал ёки корпоратив тармоқдаги ахборот хавфсизлигини таъминлашда жиддий муаммолар пайдо бўлади. Ўзининг идеологиясидаги очиқлилик туфайли Интернет ёмон ниятли кишиларга, муҳим ва махфий ахборотни ўғирлаш, халақитларга учратиш ва бузиш мақсадида корхона ва ташкилотларнинг ички тармоқларига бостириб кириш учун кўп имкониятлар яратиб беради. Ахборот жуда аҳамиятли ёки ўта мухим бўлганлиги сабабли бундай ахборотни сақлаётган, қайта ишлаётган ёки узатаётган компьютер тизимларига ва тармоқларига нисбатан турли хил ёмон ниятли ҳаракатлар бўлиши мумкиндир. Масалан, бузувчи киши ўзини тизимнинг бошқа фойдаланувчиси қилиб кўрсатишга интилиши мумкин, алоқа каналини билдирмасдан эшитиши ёки тармоқ фойдаланувчилари алмашаётган ахборотни ушлаб олишлари ва ўзгартиришлари мумкин. Тизимнинг фойдаланувчиси бузғунчи бўлиши мумкин, у ўзи ҳақиқатда шакллантирган маълумотдан бўйин товлаши мумкин ёки ҳақиқатда ҳам узатилмаган маълумотни улар томонидан олинганлигини тасдиқлашга интилиши мумкин. У мурожаат қилиши мумкин бўлмаган ахборотга мурожаат қилишга рухсат олиш учун ўзининг ваколатларини кенгайтиришга интилиш ёки бошқа фойдаланувчиларнинг ҳуқуқларини тақиқланган ҳолда ўзгартириб тизимни бузишга мумкин. Шу муносабат билан, замонавий ахборотлашган жамиятда глобал ва бошқа тармоқларнинг улкан афзалликлари мавжудлиги билан бир қаторда, уларда ахборотни ҳимоя қилиш бўйича ўзига хос муаммоларни ҳам ечишга тўғри келади. Шунинг учун ахборотнинг махфийлиги ва бутунлигини таъминлаш билан боғлиқ бўлган барча керакли ишларни амалга ошириш учун самарали воситаларни яратиш ва қўллаш жуда муҳимдир.

1.2. Ахборотни ҳимоя қилиш - комьютер тизимлари ва тармоқлари ривожланишининг қонуниятидир

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

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

Ахборотни ҳимоя қилиш - бу:

* ахборотнинг физик бутунлигини таъминлаш, яъни ахборот элементларини тўсиқларга учрашига ва йўқолишига йул қўймаслик;
* ахборот бутунлигини сақлашда унинг элементларини алмаштиришга (модификацияга) йўл қўймаслик;
* мос ваколатларга эга бўлмаган шахслар ёки жараёнлар томонидан тақиқланган ахборотни олинишига йўл қўймаслик;
* эгаларига узатилаётган ресурслар фақатгина томонлар келишган шартларга мос равишда ишлатилишига ишонч ҳосил қилиниши керак.

Компьютер тизимларида ахборотни ҳимоя қилиш муаммоси уларнинг яратилиши билан деярли бир вақтнинг ўзида ахборот устида ёмон ниятли ҳаракатларнинг аниқ фактлари туфайли келиб чиқди. Компьютер жиноятларининг аксарият энг кўпчилиги молия банк ахборотларини қайта ишлаш тизимларида амалга оширилади. Кўп сонли мутахассисларнинг баҳолашларига қараганда бу тизимларга ҳар бир тақиқланган кириб олишдан келаётган зарар 100000 дан 1,5 млн. долларгача баҳоланмоқда.

Компьютер тизимлари ва тармоқларининг эволюцион ривожланиши, Интернетни татбиқ қилиниши билан бундай жиноятлар айникса кенг кулоч ёйдилар. Бу эса қонуниятлидир, негаки агар ЭҲМ нинг фаол ишлатилишининг биринчи ўн йиллигида компьютерларга асосан телефон тармоғи орқали уланиб олган “хакерлар” ёки «электрон қароқчилар» асосий хавф-хатарга эга бўлган бўлса, унда компьютер тизимларини ва тармоқларини оммавий ишлатиш даврида ахборотнинг ишончлилиги ва бутунлигини бузишга компьютер вируслари дастурлари ва Интернет глобал тармоғи орқали хавф солинмоқда.

Компьютер тизимлари ва тармоқларининг ишлаш тажрибаси шуни кўрсатмоқдаки, тақиқланган ахборотга мурожаат қилишни етарлича кўпгина усуллари бор:
* кўриб чиқиш;
* маълумотларни нусхалаш ва алмаштириш;
* линияларга ва алоқа каналларига уланиш натижасида ёлғон дастур ва хабарларни киритиш;
* созловчи ва халокатли дастурларни ишлатиш;
* ахборотни унинг ташувчиларидаги қолдиқларини ўқиш;
* электромагнит нурланишли ва тўлқин характерли хабарларни қабул қилиш;
* махсус дастурли ва аппаратли сўндиргичларни ишлатиш ва ҳ.к.

Табиийки, керакли тақиқланган ахборотга кириб боришнинг бу ва бошқа усуллари, йўллари компьютер тизимлари ва тармоқларининг қонуний ривожланиши билан пайдо бўлдилар ва ривожландилар, Демак, ахборотни ҳимоя қилиш буйича алоҳида локал (жуда муҳим бўлса ҳам) тадбирларни ишлаб чиқиш ва татбиқ қилиш эмас, балки ахборот хавфсизлигининг кўп поғонали, узлуксиз, комплекс ва бошқариладиган тизимини яратиш керакдир.

Ҳозирги вақтда нафақатгина давлат ёки ҳарбий сирни ўз ичига олган ахборотни, балки кичик масштаблардаги - тижорат ва махфий (шахсий) маъноли ахборотни ҳам ҳимоя қилмоқ керак.

1.3 Ахборотни ҳимоя қилиш муаммосининг долзарблилиги

Ахборот хавфсизлигини таъминлаш муаммосининг долзарблиги ва муҳимлиги қуйидаги сабаблар билан шартлангандир:

- замонавий компьютерларни ишлатиш соддалиги билан бир вақтда уларнинг ҳисоблаш қувватининг кескин ошиши;
- компьютерлар ва бошқа автоматлаштириш воситалари ёрдамида йиғилаётган, сақланаётган ва қайта ишланаётган ахборот сиғимининг кескин ошиши;
- турли ҳил вазифали ва турли ҳил тегишли ахборотларни умумий маълумотлар базасига мужассамлантирилиши;
- фаолиятнинг энг турли соҳаларида ишлатишда жойлашган шахсий компьютерлар нархининг ўсишини юқори темплари (суръатлари);
- ҳисоблаш ресурсларига ва маълумотлар базасига бевосита мурожаат қилиш рухсатига эга бўлган фойдаланувчилар доирасининг кескин ошиши;
- ахборот хавфсизлигининг хаттоки минимал талабларини ҳам қаноатлантирмайдиган дастур воситаларинг гуркираб ривожланиши;
- тармоқли технологияларнинг ўзаро таркатилиши, локал ва регионал тармоқларни глобал тармоқларга бирлаштирилиши;
- бутун дунёда ахборотни қайта ишлаш тизимлари хавфсизлигининг бузилишига деярли тўсқинлик қилмайдиган Интернет глобал тармоғининг ривожланиши;
- Интернет глобал тармоғининг очиқлиги ва назорат қилинмаслиги идеологияси.

Ҳозирги вақтда ахборотни ҳимоя қилиш муаммосини ечишнинг долзарблиги ҳимоя қилиш тадбирларига сарфланаётган ҳаражатларнинг янада ўсиб бораётганлиги билан тасдиқланади. Охирги ўн йилликда ахборот хавфсизлигини таъминлашга сарф қилинган воситаларнинг хажми, масалан АҚШда, XX асрнинг 90-йиллар бошига нисбатан деярли уч марта ошди ва тахминан 3,6 млрд. долларни ташкил этди. ғарбий Европада саноат фирмалари, давлат муассасалари ва ўқув юртлари томонидан ўзларининг компьютерларининг хавфсизлигини таьминлашга деярли 1,7 млрд. марка сарфланади.

Ҳимоя қилишнинг ишончли тизимини қуриш учун яна йирик моддий ва молиявий ҳаражатлар талаб этилади. Бу эса ўзини оқлайди, негаки ахборотнинг ишончлиги ва бутунлигининг бузилишининг оқибатлари энг оғир оқибатларга олиб келиши мумкин.

1.4. “Компьютер тизимларида ахборотни ҳимоя қилиш” курсининг асосий мақсадлари ва вазифалари

Янги ахборот технологиялари, компьютер тизимлари ва тармоқлари ҳамда Интернет ривожланишининг замонавий босқичи ахборот хавфсизлигини

таъминлаш муаммосини тизимли ўрганиш қатъиян зарурлигини аниқлаб берди. Шу муносабат билан мутахассисларга, уларнинг ахборот салоҳиятига ва маданиятига янада юқорироқ талабларни қўймоқда. Компьютер воситаларидан фойдаланувчилар янги ахборот технология-ларининг замонавий усулларини ва воситаларини қанчалик яхши билсалар ва ишлата олишларига ташкилот ва муассасаларнинг ишлаш самарадорлиги ҳам, мутахассиснинг муваффақияти ва равнақига ҳам боғлиқ бўлади.

«Компьютер тизимларида ахборотни ҳимоя қилиш" ўқув курси "Информатика" умумий йўналишининг ҳали яхши ўзлаштирилмаган сегментини ўрганишга йўналтирилгандир ва шахсий компьютерларда ҳам, локал ва глобал тармоқларда ҳам ахборот хавфсизлигини таъминлашнинг замонавий усулларига ва воситаларига бағишлангандир.

Ўқув курси шунга мўлжалланганки, уни ўрганиш натижасида:

- компьютер тизимлари ва тармоқларининг ахборот хавфсизлиги тўғрисида талабаларда асосий билимларни шакллантириш;
- ахборотни ҳимоя қилишнинг назарий - услубий ва услубий асосларини бериш;
- компьютер тизимлари ва тармоқларида ахборот хавфсизлигини таъминлаш учун талабаларга замонавий усулларни ва воситаларни ишлатишга амалий ўргатиш;
- ахборотни ҳимоя қилиш бўйича турли хил дастурларга аппаратли воситаларда эркин фойдаланиш имконини берадиган билимлар билан талабаларни таъминлаш;

Курсни ўзлаштириш натижасида талаба;

- компьютер тизимлари ва тармоқларида ахборот хавфсизлигининг кутилаётган хавфлари моҳиятини ва оқибатларини тушуниш;
- компьютер тизимлари ва тармоқларида ахборотни ҳимоя қилиш бўйича асосий талабларни ва принципларни ўзлаштириш;
- компьютер тизимлари ва тармоқларида ахборотнинг керакли хавфсизлигини таъминлайдиган замонавий усулларни ва воситаларни билиш;
- компьютер воситаларини, ахборот бутунлигини ва ишончлилигини бузадиган вируслар ва бошқа манбаларнинг мавжудлигига тизимли текширишни таъминлашни, ва уларни бартараф этиш бўйича зарур чоралар кўришни билиш;
- ахборотни ҳимоя қилиш бўйича замонавий амалий тизимларни ва дастур маҳсулотларини ишлатишни билиш керак.

Шундай қилиб, замонавий ахборотлашган жамиятда, бозор муносабатлари жамиятда ахборот махсус товар (маҳсулот) бўлиб колмоқда, бунда кўпинча ахборотнинг нархи компьютер тизимини ўзин уни комплекс ҳимоя қилиш тизими билан бирга миқдори биргаликдаги нархидан келмоқда. Охирги вақтларда кузатилаётган компьютер тизимларининг ривожланиши қонунияти ахборотни химря килиш тизимини тўлиқ қонуний ривожлантиришни келтириб чиқаради. Компьютер тизимида етарлича ахборотни ҳимоя қилишни ташкил этиш муаммоси, шубхасиз, долзарбдир. Мухимлилик долбзарблилик муаммосини келтириб чиқарадиган сабаблардан ташқари ахборротни ҳимоя қилишда шаклланиши

ажратилаётган ва тобора ўсиб бораётган сарф–харажатларни таъкидлаш мумкин (фақатгина АҚШда ва ғарбий Европа мамлакатларида бу харажатлар 6 млрд. долларни ташкил этади.)

Асосий атамалар

Компьютер тизимлари ва тармоқлари (КТ ва Т); Интернет глобал тармоғи; ахборотлаштириш; ахборот кенглиги; тўсиқ; модификация; ахборотни йўқотиш; ахборотни ҳимоя қилиш; тизим ва тизимли ёндашиш; хакерлар ёки «электрон қароқчилар»; компьютер вируслари, тақиқланган ахборотга мурожаат қилиш; ахборот хавфсизлигининг кўп поғонали, узлуксиз, комплексли ва бошқариладиган тизими.

Назорат саволлари

1. Замонавий ахборотлашган жамият нима?
2. Ахборот кенглиги деганда нима тушунилади?
3. Компьютер тизимлари ва тармоқлари ривожланишининг қандай анъаналари бор?
4. Ахборотнинг қандай бозор тушунчалари бор?
5. Ахборот хавфсизлигига таъриф беринг.
6. Интернет глобал тармоғи шароитларида ахборот хавфсизлигининг қандай характерли хусусиятлари бор?
7. Компьютер тизимлари ва тармоқларида бузғунчининг мумкин бўлган ёмон ниятли ҳаракатларини санаб беринг.
8. Ахборотни ҳимоя қилиш деганда нима тушунилади?
9. Ахборотни ҳимоя қилиш нимани билдиради?
10. Замонавий хакерларга ва электрон қароқчиларга тавсифлар беринг.
11. Компьютер тизимлари ва тармоқлари ривожланишининг замонавий босқичида ахборот бутунлиги бузилишининг спецификаси қандай?
12. Тақиқланган ахборотга мурожаат қилишнинг асосий усулларини санаб беринг.
13. Ахборотни ҳимоя қилиш муаммосининг долзарблиги ва муҳимлиги қандай асосий сабаблар билан шартланган?
14. «Компьютер тизимларида ахборотни ҳимоя қилиш» курсининг асосий мақсадлари ва вазифалари қандай?

Тавсия этиладиган адабиётлар:

1. Каримов И.А. Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникация технологияларини жорий этиш тўғрисида Фармони. //Ишонч, газета, 2002 йил 1 июн.

2. Михаель А. Бенкс. Информационная защита ПК. – СПБ.: Корона – Принт, 2001. – 272 с.

3. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.

4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

5. Камилов Ш.М., Зокирова Т.А., Мусаева М.А. Microsoft Office ҳужжат ва дастурларини тақиқланган мурожаат этишдан сақлаш. Услубий қулланма. Т., 2004.

2 боб. КОМПЬЮТЕР ТИЗИМЛАРИ ВА ТАРМОҚЛАРИНИНГ АХБОРОТ ХАВФСИЗЛИГИ.

2.1. Асосий тушунчалар ва таърифлар

Компьютер тизимлари ва тармоқлари ахборот хавфсизлигининг асосий тушунчаларини киритамиз ва аниқлаймиз.

Компьютер тизимлари ва тармоқларининг хавфсизлиги деганда улар меъёрий ишлаш жараёнига тасодифий ёки олдиндан мўлжалланган аралашишидан, ҳамда уларнинг ташкил этувчиларини ўғирлашга, ўзгартиришга ёки бузишга бўлган интилишлардан ҳимоя қилинганлиги тушунилади.[21; 15-30]

Тизимларнинг хавфсизлиги қайта ишланаётган ахборотни махфийлигини ва бутунлигини, ҳамда компьютер тизимлари ва тармоқларини ташкил этувчиларини ва ресурсларини мурожаат қилишлиги ва сақлаб қўйишлигини таъминлаш бўйича керакли чораларни қабул қилиш билан эришилади.

Ахборотга мурожаат қилиш деганда ахборот билан танишиб чиқиш, уни қайта ишлаш, хусусан нусхалаш, ўзгартириш ва йўқотиш тушунилади. Ахборотга рухсат этилган ва тақиқланган мурожаат қилиш турлари мавжуддир.

Ахборотга рухсат этилган мурожаат қилиш - бу, мурожаат қилиш чекланишларига ўрнатилган қоидаларни бузмайдиган, ахборотга мурожаат қилишдир.

Ахборот тақиқланган мурожаат қилиш мурожаат қилиш чекланишларига ўрнатилган қоидаларни бузилиши билан тавсифланади. Тақиқланган ахборотга мурожаат қилишни амалга оширадиган шахс ёки жараён мурожаат қилиш чекланишлар қоидаларнини бузувчилар ҳисобланади. Тақиқланган мурожаат қилиш компьютер қоида бузилишларининг энг кенг тарқалган кўриниши ҳисобланади.

Маълумотларнинг махфийлиги - бу маълумотларга тақдим этилган ва уларни ҳимоя қилишни талаб этилган даражасини аниқлайдиган мақомдир. Моҳияти бўйича ахборотнинг махфийлиги - рухсат этилган ва текширишдан ўтган (муаллифлаштирилган) тизим субъектларига (фойдаланувчиларга, жараёнларга, дастурларга) маълум бўлиши керак бўлган ахборотнинг хоссасидир. Тизимнинг қолган бошқа субъектлари учун бу ахборот номаълум ва ёпиқ бўлиши керак.

Тизим субъекти - тизимнинг фаол ташкил этувчиси бўлиб, у объектдан объектга ахборот оқишининг ёки тизим ҳолатини ўзгартиришни сабабчиси бўлиши мумкин.

Тизим объекти - тизимнинг ахборотни сақлайдиган, қабул қиладиган ёки узатадиган пассив ташкил этувчисидир. Объктга мурожаат қилиш ундаги мавжуд бўлган ахборотга мурожаат қилишни билдиради.

Ахборотнинг бутунлиги, агар тизимлардаги маълумотлар бошланғич ҳужжатлардаги ёки манбалардаги маълумотлардан семантиқ нуқтаи назардан фарқ қилмасалар, яъни агар уларнинг тасодифан ёки олдиндан мўлжалланган тўсиқлари ёки бузилишлари амалга ошмаган бўлса, таъминланади.

Тизимнинг ташкил этувчисини ёки ререурсининг бутунлиги - тизим тасодифий ёки олдиндан мўлжалланган тўсиқлар ёки бузувчи таъсирлар шароитларда ишлаганда ташкил этувчининг ёки ресурснинг семантиқ маънода ўзгармай қолиши хоссасидир.

Тизимининг ташкил этувчисига ёки ресурсига мурожаат қила олишлик - ташкил этувчининг ёки ресурснинг тизимнинг қонуний муаллифлаштирилган субъектлари учун мурожаат қила олишлик хоссасидир.

Тизим хавфсизлигининг хавфи деганда унинг хавфсизлигига тўғридан тўғри ёки бевосита талофат етказиши мумкин бўлган таъсирлар тушинилади.

Хавфсизлик талофати тизимларда мавжуд бўлган ва қайта ишланаётган ахборотнинг ҳимояланганлик ҳолатининг бузилишини кўзда тутади.

Тизимнинг боғлиқлиги - хавфнинг пайдо бўлишини ва амалга ошиши мумкинлигини билдирадиган тизимнинг бирор-бир муваффақиятсиз хоссасидир.

Компьютер тизимларига ҳужум - тизимнинг у ёки бу боғлиқлигини қидириш ва ишлатиш маъносини билдирадиган, ёмон ниятли киши томонидан бажариладиган ҳаракатдир. Шундай қилиб, ҳужум - хавфсизлик хавфини амалга оширишдир.

Хавфсиз ёки ҳимоя қилинган тизим - хавфсизлик хавфларига муваффақиятли ва самарали қарши турадиган, зарур ҳимоя қилиш воситаларига эга бўлган тизимдир.

Ҳимоя қилиш воситалари комплекси - компьютер тизимлари ва тармоқларининг ахборот хавфсизлигини таъминлаш учун яратиладиган ва қўллаб - қувватланадиган дастурли ва аппарат воситалари кўринишига эгадир. Ушбу комплекс маълум бир ташкилотда қабул қилинган хавфсизлик сиёсатига мувофиқ яратилади ва қўллаб қувватланади.

Хавфсизлик сиёсати - ҳимоя қилиш воситаларининг ишлашини ахборот хавфсизлигининг хавфи берилган тўпламидан меъёрлар, қоидалар ва амалий тавсияномаларнинг йиғиндисидир.

2.2 Компьютер тизимлари ва тармоқлари хавфсизлигининг асосий хавфлари

Таъсир этиш мақсади бўйича хавфсизлик хавфини учта асосий тури фарқланади;

1. Ахборот махфийлигининг бузилиш хавфи.
2. Ахборот бутунлигининг бузилиш хавфи.

3. Тизимнинг ишлаш лаёқатлилигининг бузилиш хавфи (хизмат кўрсатишдаги инкор этишлар).

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

Компьютер тизимларида сақланаётган ёки алоқа канали бўйича узатилаётган ахборот бутунлигини бузилиши хавфи унинг сифатини ва ишончлилигини бузилишига ёки тўлиқ йўқотилишига олиб келадиган тўсиқларга ёки ахборотнинг ўзгаришига йўналтирилгандир. Ахборотнинг бутунлиги нияти ёмон киши томонидан кўра била туриб, ҳамда тизимни ўраб турган мухит томонидан объектив таъсирлар натижасида бузилиши мумкин. Бу хавф айниқса ахборотни узатиш тизимлар компьютер тармоқлари ва телекоммуникация тизимлари учун долзарбдир. Ахборотнинг бутунлигини кўра била туриб, бузишга асосланган мақсадли ваколатли шахслар томонидан бажариладиган рухсат этилган ўзгариш билан адаштирмаслик керак.

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

Ресурсга мурожаат қилишни блокировкалаш доимий ва вақтинча бўлиши мумкин.

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

- тасодифий ҳолатлар (ер қимирлаши, ёнғин, довул ва б.)
- тизимнинг таркибий элементларини издан чиқиши (техник бузилишлар);
- фойдаланувчиларни ва хизмат кўрсатиш ходимларини нотўғри ҳаракатлари;
- дастур таъминотидаги хатоликлар;
- ташқи муҳит таъсири натижасидаги алоқа линиясидаги тўсиқлар ва бошқалар.

Олдиндан мўлжалланган хавфлар бузғунчининг бирор мақсадга йўналтирилган ёмон ниятли ҳаракати билан боғлангандир. Бузғунчилар сифатида хизматчилар, ташриф буюрувчилар, рақобатдошлар, ёлланма ишчилар ҳ.к. бўлиши мумкин. Бузғунчиларнинг ҳаракати турли сабаблар билан боғланган бўлиши

мумкин; хизматчининг ўзининг мансабидан норозилиги, айнан моддий қизиқиши, қизиқувчанлиги, рақобатли кураш, ҳар қандай шароитда ўзиникини маъқуллашга интилиши, мақсадга йўналтирилган ташқаридан буюртма ва ҳ.к. Бузғунчининг ҳаракатлари билан боғланган энг хавфли вазиятларини пайдо бўлиш имкониятларидан келиб чиққан ҳолда *потенциал* (бақувват кучли) бузғунчининг гипотетик моделини қуриш мумкин.

- бузғунчининг малакаси ушбу тизимни ишлаб чиқувчи даражасида бўлиши мумкин;
- бегона шахс ҳам, тизимнинг қонуний фойдаланувчиси ҳам бузғунчи бўлиши мумкин;
- тизимнинг ишлаш принципи тўғрисидаги ахборот бузғунчига маълумдир;
- бузғунчи ҳимоя қилишдаги энг кучсиз бўғинни танлайди;
- бузғунчига тизимда жойлашган ахборотнинг қимматлилиги ва муҳимлиги маълумдир.

Амалиёт шуни кўрсатмоқдаки, ҳозир жаҳонда молия-банк компьютер тармоқлари олдиндан мўлжалланган хавфларга энг юқори даражада таъқиб этилади. Бундай хавфларга тегишлидир;

- банк хизматчилари сонига тегишли бўлмаган бегона шахсларнинг тақиқланган мурожаат қилиши, ва сақланаетган махфий ахборот билан танишиши;
- банк хизматчиларининг улар мурожаат қилиши мумкин бўлмаган ахборот билан танишиб чиқиши;
- дастурларни ва маълумотларни тақиқланган нусхалаш;
- махфий ахборотни ўз ичига олган магнит ташувчиларни ўғирлаш;
- чоп қилинган банк ҳужжатларини ўғирлаш;
- ахборотни кўра била туриб йўқотиш;
- банк ходимлари томонидан молиявий ҳужжатларни, ҳисобатларни ва маълумотлар базасини рухсатсиз ўзгартириш;
- алоқа каналлари бўйича узатилаётган маълумотларни қалбақилаштириш;
- алоқа каналлари бўйича узатилаётган маълумотларининг муаллифларини рад этиш;
- маълумотни (ахборотни) олиш далилини рад этиш;
- олдин узатилган маълумотларни тўхтатиб қўйиш;
- вирусли ҳаракатлар келтириб чиқарган ахборотни бузилиши;
- магнит ташувчиларда сақланаётган архивдаги банк ахборотларини бузилиши;
- тизимнинг ташкил этувчиларини ва узелларини ўғриланиши,

2.3. Компьютер тизимларида ва тармоқларида ҳимоя қилишининг объектлари ва элементлари

Компьютер тизимларида ва тармоқларида ахборотни ишончли ҳимоя қилиш, агар хавф пайдо бўлиши мумкин бўлган тизимнинг барча объктларида ва барча элементларида ишончли бўлсагина, самарали бўлиши мумкин. Шу муносабат билан ҳимоя қилиш воситаларини яратиш учун хавф табиатини, шаклларини ва уларнинг мумкин бўлган пайдо бўлиш ва амалга ошириш йўллари, объектлар ва элементлар руйхатини аниқлаш муҳимдир, улар, бир томондан, ахборотнинг ҳимояланлигини бузиш мақсадида хавфларга дуч келиши мумкин (бевосита ва билвосита), бошқа томондан эса, ахборотни самарали ҳимоя қилишни ташкил этиш учун етарлича аниқ алоҳидалиниши мумкин.

Умуман олганда ҳимоя қилиш объекти деганда тизимнинг шундай структурали ташкил этувчиси тушуниладики, унда ҳимоя қилиниши мумкин бўлган ахборот жойлашган ёки жойлашиши мумкин, ҳимоя қилиш элементи деганда эса - ҳимоя қилиниши керак бўлган маълумотларни ўз ичига олган маълумотлар тўплами тушунилади.

Амалиёт шуни кўрсатмоқдаки, ахборот киритиш, сақлаш, қайта ишлаш, чиқариш ва узатиш жараёнида турли хил тасодифий таъсирларга дучор бўлади, уларнинг натижасида аппаратли даражада ахборотни тасвирлашни хабарли шаклларида физик ўзгаришлар бўлиб ўтади. Агар ахборотни ташиётган рақамли коднинг бирорта ёки қандайдир разрядларида рақамли кодни инверслаш (инкор этиш) бўлиб ўтган бўлса (1 дан 0 га ёки аксинча), ва у функционал назоратнинг махсус аппаратли воситалари томонидан пайқалмаган бўлса, унда ахборотни кейинчалик қайта ишлашда ёки нотўғри натижа олинади, ёки маълумот ёлғон манзил бўйича йўналтирилади, ёки бошқа кўнгилсиз ходисалар (ахборотнинг бузилиши, ўзгартирилиши, йўқотилиши ва ҳ.к.) бўлиб ўтиши мумкин.

Дастурли даражада тасодифий таъсирлар натижасида кўзда тутилмаган вақт оралиғида ахборотни қайта ишлаш алгоритмини ўзгартириш, ва бунинг оқибатида жараённинг тўхтатилиши ёки ўзгартирилиши бўлиб ўтиши мумкин, бунинг натижасида яна ахборотни бузилиши ёки йўқотилиши (масалан, манзилатни ёки операндни адаштириб юборилганда) мумкиндир.

Компьютер тизимларида ахборотни ҳимоя қилиш объектлари сифатида қуйидагиларни ажратиш мумкин:

- ✓ фойдаланувчиларнинг терминаллари (шахсий компьютерлар, тармоқнинг ишчи станциялари);
- ✓ тармоқ мажбуриятини терминали ёки гуруҳли абонентлик узели;
- ✓ алоқа узели;
- ✓ ахборотни акс эттириш воситалари
- ✓ ахборотни ҳужжатлаштириш воситалари;
- ✓ машина зали (компьютерли ёки дисплейли) ва ахборот ташувчиларини омборхонаси;
- ✓ ташқи алоқа каналлари ва тармоқдаги жиҳозлар;
- ✓ ахборотни йиғувчилари ва ташувчилари.
- ✓ Юқорида келтирилган таърифга мос равишда ҳимоя қилиш элементлари сифатида ҳимоя қилиш объектларидаги ахборот блоклари (миқдорлар, тўпламлар, оқимлар, базалар ва б.) қатнашиши мумкин, хусусан:

- ✓ компьютернинг асосий хотирасидаги маълумотлар ва дастурлар;
- ✓ ташқи машина ташувчисидаги (қаттиқ ёки эгилувчан диск-лардаги) маълумотлар ва дастурлар;
- ✓ монитор экранида акс эттирилаётган маълумотлар;
- ✓ шахсий компьютерлар автоном ёки тармоқда ишлатилганда принтерга чиқарилаётган маълумотлар;
- ✓ алоқа каналлар бўйича узатилаётган маълумотлар пакетлари;
- ✓ нусха олиш - кўпайтириш жиҳозлари ёрдамида кўпайтирилаётган (адад-ланаётган) маълумотлар;
- ✓ қоғозли ва магнит ташувчилар кўринишидаги ахборотни қайта ишлаш чиқиндилари;
- ✓ фойдаланувчи томонидан рўйхатга олинган паролларни ва устувор вазифа журналлари;
- ✓ масалалар тўплами билан ишлаш бўйича хизматга доир йўриқномалар;
- ✓ маълумотлар ва дастур таъминоти архивлари;
- ✓ тармоқли операцион тизимлар;
- ✓ тармоқли ишчи узеллар ва қисмлар станциялари.

Ахборотни ҳимоя қилиш объектларига ва элементларига мурожаат қилиш одатда фақат икки тоифадаги шахслар учун мумкиндир: қонуний фойдала-нувчилар ва бузғунчилар. Қонуний фойдаланувчи иш жойида йўқ бўлганда ёки ўзининг амалий мажбуриятларига совуққонлик билан ёндашганда, ахборот етарлича ҳимоя қилинмаганда малакали бузғунчи мос сўровларни ва буйруқларни киритиш йўли билан тақиқланган ахборотга мурожаат қилишни (АТМҚ) амалга ошириши мумкин. Компьютер тизимлари ёки компьютер тармоқлари воситалари жойлаштирилган хонага етарлича эркин мурожаат қилинганда тасвирлаш ва ҳужжатлаштириш воситаларида ахборотни кўз билан кузатиши, ҳамда ахборот ташувчиларни (дискеталар, листинглар ва б.) ўғрилаши ёки улардан нусха олиш мумкин.

Компьютер тизимига дастурларни назоратсиз юкланганда бузғунчи маълумотларни ва алгоритмларни ўзгартириши мумкин, бунинг ёрдамида кейинчалик у ўзига керакли бўлган функцияларни амалга ошириши мумкин. Ўзининг функционал мажбуриятларига мос равишда ахборотнинг маълум бир қисмига қонуний мурожаат қилиш ҳуқуқига эга бўлган, лекин бошқа қисмга ўзининг ваколатидан ташқарида мурожаат қиладиган компьютер тизимининг фойдаланувчиси бузғунчи бўлган вазият жуда ҳам хавфлидир.

2.4. Ахборот хавфсизлиги хавфи пайдо бўлишини олдиндан аниқлаб берадиган омиллар

Юқорида таъкидланганидек, компьютер тизимларини ва тармоқларини (КТ ва Т) ахборот хавфсизлигига хатарли таъсирларни тасодифий ва олдиндан мўлжалланганга ажратилади. Бунда ахборот бундай таъсирларга тизим ҳаёт даврининг ҳамма босқичларида ва ишлашида дучор бўлади.

Барча таъсирларнинг сабаблари турли омиллар бўлиши мумкин. 2.1-расмда КТ ва Т ларида ахборот ҳимояланганлигини бузадиган омилларнинг келиб чиқиши келтирилган.

Ушбу расмдан кўриниб турибдики, ахборот хавфсизлиги хавфини яратишга дестабиллаштирувчи омилларнинг манбалари ҳамда уларнинг ўзлари ҳам тўғридан тўғри таъсир кўрсатади.

Дестабиллаштирувчи омилларнинг асосий манбаларига қуйидагилар тегишлидир:

*Инсонлар, чунки компьютер тизимига мурожаат қилиш ҳуқуқига назарий ва амалий жиҳатдан фақатгина икки тоифадаги шахслар эгадирлар: хусусий мутахассис фойдаланувчилар ва бегоналар. Ёмон ниятли ахборотни бузувчиларни мутлақ кўпчилигини бегона кишилар амалга оширади, бу эса жиддий ва хавфли оқибатларга олиб келади. Ёмон ниятли киши сифатида КТ ва Тнинг ўзини кишилари бўлиши эхтимоли ҳам эътибордан четда эмас. Ҳар қандай ҳолда ҳам тақиқланган ахборотга мурожаат қилишни (АТМҚ) кишилар томонидан компьютердаги қонун бузилишларининг манбалари ҳисобланади.

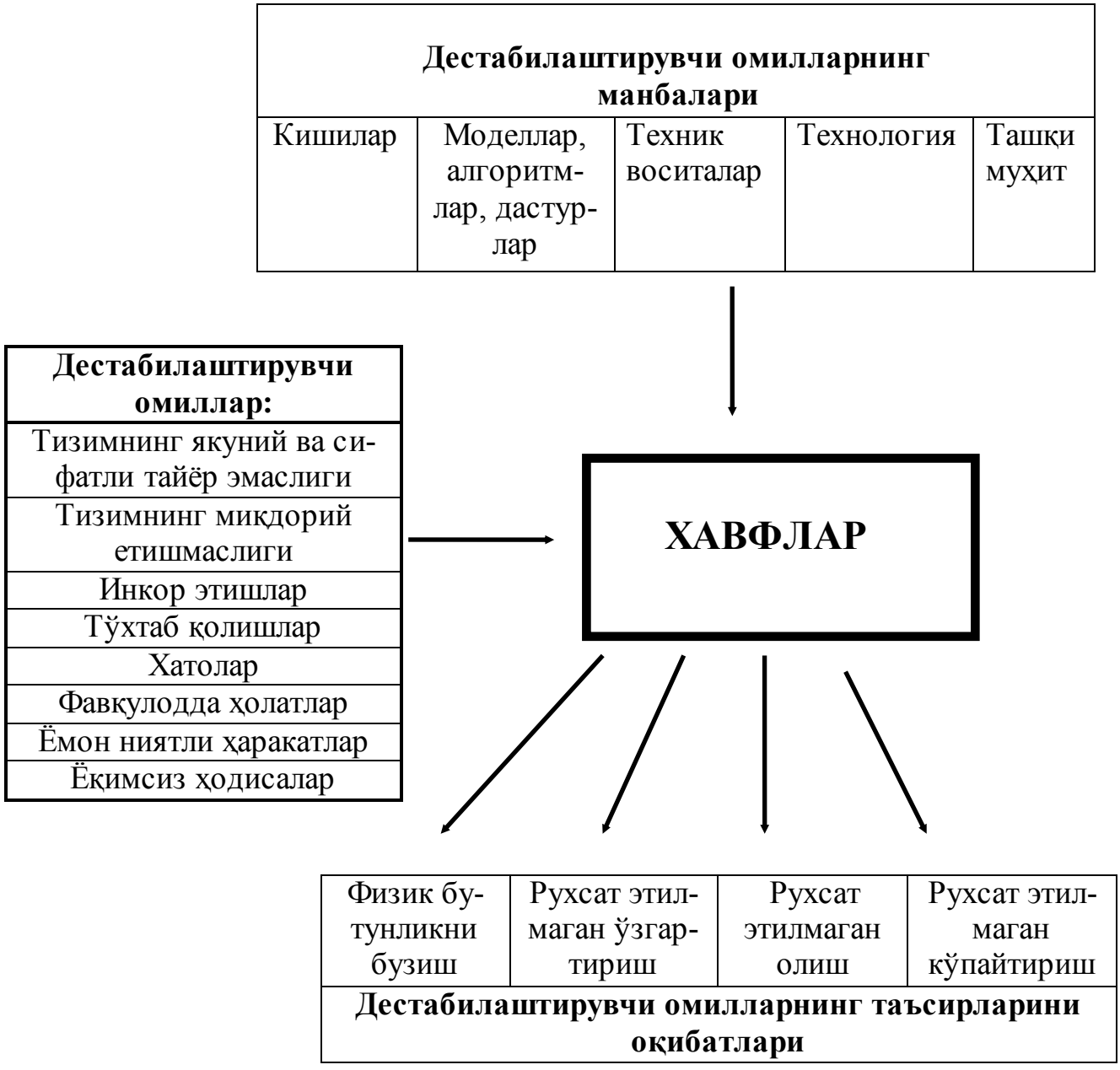
Моделлар, алгоритмлар, дастурлар, улар ахборотни ҳимоя қилиш хавфига олиб келадиган кучли манба бўлишлари мумкин, негаки ахборотни қайта ишлаш дастурларини, моделларни ва алгоритмларни мукаммал эмаслиги оқибатлари ҳисоблаш жараёнини тўхташига, кўнгилсиз натижаларга, ахборотни ўзгаришига ва чиқиб кетишига олиб келади.

Техник қурилмалар, улар ҳозир КТ ва Т ларида катта ва ўта катта интеграл, оптик-толали ва лазерли схемаларни кенг қўлланишига асосланади. Бундай схемаларни ишлашида кучланишлар, импульслар ва токларнинг даражаларини юқори частотали ўзгаришлари бўлиб ўтади. Бу, ўз навбатида, озуқа занжирларида, эфирда, яқинда жойлашган аппаратурада ва ҳ.к. турли хил электромагнит майдонларни ва йўналтиришларни пайдо бўлишига олиб келади, улар эса махсус воситалар ёрдамида (уларни шартли равишда "жосусли" деб атаймиз) қайта ишланиладиган ахборотга айлантириш мумкиндир. Шунингдек, бузғунчининг қабул қилувчиси билан КТ ва Т ларини аппарат воситалари ўртасидаги масофа камайиши билан ахборотни олишни ва қайта шифрлашни бу турдаги эҳтимоли ошади. Ахборот билан танишиш яна бузғунчи томонидан "жосуслик воситаларини" алоқа каналларига ва тармоқдаги аппарат воситаларига бевосита улаш ҳам мумкиндир

*Тизимнинг технологик ишлаши ҳам дестабиллаштирадиган омилларнинг жиддий манбаси ҳисобланади. Замонавий компьютер тизимларида ва тармоқларида ишлаш технологияси моддалаштирилган ахборотга, яъни мавжуд бўлиши физик ташувчидаги бирорта ёзув билан боғланиши мажбурий бўлмаган ахборотга асосланмаган. Шунинг учун КТ ва Т ларига нисбатан уларнинг ишлаш вақтида (билдирмасдан эшитиб олиши, ушлаб олиш, ўзгартириш, нусхалаш, режимини ўзгартириши ва ҳ.к.) турли туман ёмон ниятли таъсирлар (инсонлар томонидан ҳам, аппарат воситалари билан ҳам) мумкиндир.

*Ташқи муҳит ҳам ахборот хавфсизлигини хавфини пайдо бўлишига таъсир этадиган негатив омилларнинг манбаси бўлиши мумкин. Ташқи омил-

ларга мамлакатдаги ижтимоий-иқтисодий ва сиёсий вазиятни (қадрсизланиш, ишсизлик, рағбат, мотивация ва б.) келтириш мумкин.



2.1-расм. Ахборотнинг ҳимояланганлигини бузувчи омиллар ва уларнинг таъсирларини оқибатлари

Ўз навбатида юқорида санаб ўтилган дестабиллаштирувчи омилларнинг манбалари ахборот хавфсизлигини хавфини бевосита яратадиган бир қатор объектив-субъектив омилларни пайдо бўлишини олдиндан аниқлайди. Уларга қуйидагилар тегишлилидир:

1. Ишлашга тизимнинг якуний ва сифатли тайёр эмаслиги, лойиҳалаш ва синаб кўриш босқичларида қандайдир хатоларнинг оқибатни. Бу дастур-алгоритмик таъминлайдиган ишларнинг охирига етмаганлиги, ахборотлар ба-

засини ривожланмаганлиги, технологик бирика олмаслик, алоҳида амалларнинг ўзаро тўғри келмаслиги ва ҳ.к. бўлиши мумкин.

2. Миқдорий етишмаслик - бу бир хил воситаларнинг бошқаларига зарар келтирган ҳолда тўлиқ комплектланмаганлиги ёки ортиқча комплектланганлиги, уларнинг ўзаро бир-бири билан тўғри келмаслиги, ташқаридан мурожаат қилиш ва ҳ.к.

3. Инкор этилишлар, тўхтаб қолишлар ва хатоликлар, улар КТ ва Т ларини ишлаш жараёнини қисман кузатадилар ва тизимга хизмат кўрсатадиган мутахассисларнинг касбий малакасини пастлиги, ўзларининг вазифаларига ва ишларига нисбатан интизомсизлиги ва лоқайдлиги туфайли келиб чиқади. Табиийки, ана шу негатив омиллар моддий ва физик эскирган жиҳозлар ва воситалар уларнинг ортиқча юкланиши ва ҳ.к. оқибатида ҳам пайдо бўлиши мумкин. Бу ерда яна дастур-алгоритмик ва ахборот таъминотидаги, уларнинг тузилишли ва мантиқий элементларини бирика олмаслигидаги ва тўплаб чиқишдаги номукаммаллик ҳам муҳим ўринни эгаллайди.

4. Фавқулодда ҳолатлар (ёнғин, сув тошқини, ер қимирлаши, электрозуқани издан чиқиши ва бошқалар), улар халокатли ҳолатларни яратади ва компьютер тармоқларини ва тизимларини хавфсиз ишлашида салбий таъсир кўрсатади.

5. Ёмон ниятли ҳаракатлар - тизимнинг объектларига ва элементларига, ҳамда ундаги бўлиб ўтаётган жараёнларига турли сабаблар (моддий қизиқиш, зарар ўтказиш истаги, қизиқиш, ўзиникини маъқуллаш ва х. к.) бўйича инсоннинг фаол аралашишини натижасидир.

6. Ёқимсиз ходисалар - тизимни ва хизмат кўрсатиш ходимларини ишлаши билан бевосита боғлиқ бўлмаган омиллар.

2.5. Хавфсизлик хавфини тавсиф қилиш объекти каби компьютер тизимларини ва объектларини тавсифли хоссалари

Замонавий компьютер тизимлари ва тармоқлари мураккаб тизим кўринишига эга бўлиб, улар турли даражадаги автономликдаги ташкил этувчиларнинг катта миқдоридан ташкил топган бўлиб, улар ўзаро боғланган ва бир-бири билан маълумотлар алмашади. Деярли ҳар бир ташкил этувчи ташқи таъсирларга дучор бўлишлари ва ишдан чиқишлари мумкин. Тизимнинг ташкил этувчиларини қуйидаги гуруҳларга бўлиш мумкин:

- Аппаратли воситалар – ШЭҲМ лар ва уларнинг таркибий қисмлари (микропроцессорлар, мониторлар, терминаллар, периферия қурилмалари, алоқа линиялари, модемлар ва ҳ.к.);
- Дастур таъминоти – ҳарид қилинган ва шахсий ишлаб чиқилган дастурлар; бошланғич, объектли, юкланадиган модуллар; операцион тизимлар, утилитлар, диагностика дастурлари ва ҳ.к.;
- Маълумотлар – магнит-лазерли ташувчиларда вақтинча ва доимий сақланадиган, архивли маълумотлар базаси ва ҳ.к.;
- Ходимлар – хизмат кўрсатиш ходимлари ва фойдаланувчилар.

Компьютер тизимларини тавсифли хоссаси мурожаат қилишнинг турли кўринишларига очиқлигидир. Кутилаётган хавфсизлик хавфи нуқтаи назаридан компьютер қоида бузилишлари энг кенг тарқалган ва хавфли тури тақиқланган ахборотга мурожаат қилишдир (АТМҚ). АТМҚ нинг моҳияти ташкилотда қабул қилинган хавфсизлик сиёсатига мос равишда ўрнатилган мурожаат қилишнинг чекланиши қоидаларини бузган ҳолда фойдаланувчини (бузғунчилиги) объектга мурожаат этишга рухсат олишидадир. АТМҚ ҳимоя қилиш тизимидаги, уларни нотўғри ўрнатишдаги ва созлашдаги исталган хатоликларини ишлатади. Замонавий КТ ва Т ларини тавсифли спецификаси тақиқланган мурожаат қилишларни уларга кучсиз боғлиқлигидир. Бунда АТМҚ штатли воситалари билан ҳам, махсус яратилган аппаратли ва дастурли воситалари билан ҳам амалга оширилиши мумкин.

Бузғунчи тизим ташкил этувчиларига мурожаат қилишга эга бўлиши ва ахборотни ўғирлаши, ўзгартирилиши ёки бузиши мумкин бўлган АТМҚ нинг асосий каналларига тегишли бўлиши мумкин:

- Мурожаат қилишнинг барча штатли каналлари (тизимнинг фойдаланувчиларини, маъмуриятини терминаллари; ахборотни тасвирлаш ва ҳужжатлаштириш воситалари, алоқа канали) улар бузғунчилар, ҳамда қонуний фойдаланувчилар томонидан ўзларининг ваколатлари чегараларидан ташқарида ишлатилганда;
- Технологик ва якуний бошқариш пультлари;
- Тизимнинг аппарат воситалари ўртасидаги алоқа линиялари;
- Аппаратурадан, алоқа линиясидан, электроозуқа ва ерга уланиш тармоқларидан чиқаётган зарарли электромагнит нурланишлар.

КТ ва Т ларни ахборот хавфсизлиги учун етарлича хавфга эга бўлган, энг кенг тарқалган ва тавсифли АТМҚ нинг турли хил усулларига кирадилар:

- паролларни ушлаб олиш;
- «маскарад»;
- имтиёзларни ноқонуний ишлатиш.

Паролли ушлаб олиш махсус ишлаб чиқилган дастурлар билан амалга оширилади. Қонуний фойдаланувчи тизимга киришга ҳаракат қилганда дастур-ушлаб олувчи дисплей экранида фойдаланувчи номини ва паролини киритишни имитация қилади, улар тезда дастур-ушлаб олувчининг эгасига жўнатилади, бундан кейин экранга хато тўғрисидаги хабар чиқарилади ва бошқариш операцион тизимга қайтарилади. Фойдаланувчи паролни киритишда хатоликка йўл қўйди деб фараз қилади. У киритишни такрорлайди ва тизимга мурожаат қилишга рухсат олади. Қонуний фойдаланувчини номини ва паролини олган дастур-ушлаб олувчининг эгаси энди уларни ўзининг мақсадларида ишлатиши мумкин. Паролларни ушлаб олишни бошқача усуллари ҳам мавжуддир.

«Маскарад» − бир фойдаланувчини мос ваколатларга эга бўлган бошқа фойдаланувчи номидан бирон-бир ҳаракатларини бошқаришидир. «Маскарад»нинг мақсади бирор-бир ҳаракатларни бошқа фойдаланувчига тиркаб қўйишдир, ёки бошқа фойдаланувчини ваколатларини ва имтиёзларини тақдим этишдир. «Маскарад»ни амалга оширишга мисоллар:

- бошқа фойдаланувчининг номи ва пароли остида тизимга кириш (бу «маскарад»га олдинги кўрилган паролни ушлаб олиш киради);

- бошқа фойдаланувчи номидан тармоққа хабар жўнатиш.

«Маскарад» банк тизимидаги электрон тўловларга жуда хавфлидир, бунда ёмон ниятли кишининг «маскарад» идан мижозни нотўғри идентификациялаш банкнинг қонуний мижозига катта талофатлар келтириши мумкин.

Имтиёзларни ноқонуний ишлатиш. Ҳимоя қилишнинг кўпчилик тизимлари берилган функцияларни бажариш учун имтиёзларнинг маълум бир тўпламларни ўрнатадилар. Ҳар бир фойдаланувчи ўзининг имтиёзлар тўпламини олади: оддий фойдаланувчилар – минимал, маъмуриятлар – максимал. Тақиқланган имтиёзларни ушлаб олиш, масалан «маскарад» воситасида, бузғунчи томонидан ҳимоя қилиш тизимини айланиб ўтиб, маълум бир ҳаракатларни бажариш имкониятларига олиб келади. Шуни таъкидлаш керакки, имтиёзларни ноқонуний ушлаб олиш, ҳимоя қилиш тизимида хатоликларни борлигида, ёки тизимни бошқаришда ва имтиёзларини тайинлашда маъмуриятни совуққонлиги туфайли имкони бордир.

Компьютер тармоқлари, хавфсизлик хавфи таъсир этадиган объект каби, жиддий тавсифли хусусиятларга эгадир. Исталган компьютер тармоғининг асосий хусусияти шундаки, унинг ташкил этувчиларни бирор кенгликда тарқатиб юборилганлигидир. Тармоқнинг узеллари (объектлари) ўртасидаги алоқа тармоқли алоқа линияси ёрдамида физик ва хабарлар механизми ёрдамида дастурли амалга оширилади. Бунда тармоқнинг объектлари ўртасидаги юбориладиган бошқарадиган ҳаракатлар ва маълумотлар алмаштириш пакети кўринишида узатиладилар.

Компьютер тармоғига бостириб киришда ёмон ниятли киши бостириб киришнинг ҳам пассив, ҳам фаол усулларини ишлатилиши мумкин.

Пассив бостириб киришда (ахборотларни ушлаб олишда) бузғунчи, ахборот оқимига ҳам, узатилаётган ахборотнинг мазмунига ҳам бостириб кирмасдан, алоқа канали бўйича ахборотни ўтишини кузатади. Одатда, ёмон ниятли киши юбориш пунктларини ва идентификаторларини, ёки фақатгина хабарни ўтганлиги далилини, агар хабар мазмунини англаб бўлмаса хабарнинг узунлигини ва алмашиш частотасини аниқлаши мумкин, яъни ушбу каналдаги трафикни (хабарнинг оқимини) тахлил қилишни бажаради.

Фаол бостириб киришда бузғунчи хабарга узатилаётган ахборотни алмаштиришга интилади. У танлаб ўзгартилиши мумкин, тўғри ёки ёлғон хабарни ўзгартирилиши ёки қўшиб юбориши, хабарларни ўчириб юбориши, ушлаб туриши ёки келиш тартиби ўзгартилиши мумкин. Ёмон ниятли киши яна канал бўйича узатилаётган барча хабарларни инкор қилиши ва ушлаб қолиши мумкин. Бундай ҳаракатларни хабарларни узатишдаги рад қилиш каби қабул қилиши мумкин. Компьютер тармоқлари яна шуниси билан тавсифлики, битта тизим чегарасида амалга ошириладиган оддий локал ҳужумлардан ташқари тармоқ объектига қарши масофада туриб ҳужум деб аталадиган ҳужумлар қилинади. Бу катта кенгликдаги ахборотларни ва тармоқларни ресурсларини тақсимланганлиги билан шартлашилгандир. Ёмон ниятли киши ҳужум қилинаётган объектдан минглаб километр нарида жойлашиши мумкин, бунда ҳужумга

нафақатгина аниқ бир компьютер, балки тармоқ алоқа каналлари бўйича узатилаётган ахборот ҳам дучор бўлиши мумкин. Шундай қилиб, масофадан туриб ҳужум деганда, тақсимланган компьютер тармоғига тармоқ каналлари бўйича дастурли амалга оширилаётган, ахборотни бузадиган таъсир тушунилади.

2.6. Ахборот хавфсизлиги хавфларини амалга ошириш йўллари ва оқибатлари

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

- ***физик бутунликни бузиш*** – ахборот сифатини бузишга ёки уни тўлиқ йўқ қилишга йўналтирилган, айниқса ахборотни узатиш тизимларида ва телекоммуникацияларнинг компьютер тармоқларида;
- ***тақиқланган ўзгартириш*** – шу билан тавсифликни, у турли хил ҳужжатларда, ҳисоботларда ва маълумотлар базаларида маълумотларни қалбақилашишига ёки тўсиқларга учрашига олиб келиши мумкин;
- ***тақиқланган олиш*** – махфий ахборотни бевосита компьютер тизимларидан ва тармоқларидан уларга уланиш йўли билан ўғрилаш, ёки ахборот ташувчиларни ва ҳ.к. ўғрилаш билан тавсифлидир;
- ***тақиқланган кўпайтириш*** – дастурларни ва маълумотларни нусхалашга йўналтирган.

Ва табиийки, шунга ўхшаш хавфлардан ва уларнинг оқибат-ларини ҳимояланиш учун олдиндан уларни амалга ошириш йўлларини топиб олиш керак ва кейин эса ахборотни ҳимоя қилишни мос тизимини ишга тушириш керак.

2.1–жадвалда компьютер тизимлари ва тармоқларини хавфсизлиги хавфларини, уларни ташкил этувчиларига таъсир этилганда, амалга оширишни асосий йўллари кўрсатилган. Албатта, жадвалда юқорида баён қилинган хавфлар амалга оширилганда тизимлар билан нима бўлиб утишини энг умумий ҳолатлари берилган. Аниқ ҳолатлар ва хусусиятлар у ёки бу вазиятга боғлиқ равишда алоҳида кўриб чиқилиши керак.

2.1–жадвалдан кўриниб турибдики, хавфсизликни турли хавфлари амалга ошганда КТ ва Т ларини турли объектларига – аппарат воситалари, дастур таъминоти, маълумотлар ва ходимлар – жуда хавфли таъсир этишлари мумкин.

Агар таъсир этиш объекти аппарат воситалари бўлса, унда ахборот махфийлигини бузилиши тақиқланган уланиш, ресурсларни ишлатиш ва ташувчиларни ўғрилаш ҳисобига амалга оширилади.

Ахборот бутунлигини бузилиши тақиқланган уланиш, ресурсларни ишлатиш, маълумотларни ўзгартириш ва тизимни ишлаш режимини ўзгартириш оқибатида амалга оширилади.

Тизимни ўзининг ишлаш кобилияти эса ишлаш режимларини тақиқланган ўзгартириш, унинг алоҳида ташкил этувчиларини ишдан чиқариш ва уларни бузиш ҳисобига бузилади.

2.1– жадвал

Компьютер тизимлари ва тармоқлари учун хавфсизлик хавфини амалга ошириш йўллари

	Таъсир этиш объект-лари	Ахборот махфий-лигини бузилиши	Ахборот бутунли-гини бузилиши	Тизимни ишга лаёқатлигини бузилиши
	Аппарат воситалари	Тақиқланган улаиш; ресурс-ларни ишлатиш; ташувчиларни ўғрилаш	Тақиқланган улаиш; ресурсларни ишлатиш; ўзгартириш; ре-жимларни ўз-гартириш	Режимларни тақиқланган ўзгартириш; ишдан чиқариш; бузиш.
	Дастур таъми- ноти	Тақиқланган нусхалаш; ўғри-лаш; ушлаб олиш.	Тақиқланган мурожаат этиш; «Троян оти» ни вирусларни, «Чувалчангларни» татбиқ қилиш	Рухсат этилмаган тўсиқга учраш; ўчириш; алмаштириш
	Маълумотлар	Тақиқланган нусхалаш; ўғри-лаш; ушлаб олиш.	Тақиқланган тўсиқга учраш; ўзгартириш.	Рухсат этилмаган тўсиқга учраш; ўчириш; алмаштириш
	Ходимлар	Сирни очиб қўйиш; ахборотни ҳимоя қилиш тизими тўғрисида маълумотларни узатиш; совуқ-қонлик	«Маскарад»; шантаж қилиш; ходимни сотиб олиш.	Иш жойидан кетиш; фи- зик бартараф этиш.

Дастур таъминотига таъсир этишда ахборот махфийлиги бузилиши дастур маҳсулотларини тақиқланган нусхалаш, уларни ўғрилаш ва ушлаб олиш ҳисобига бўлиб утади.

Ахборот бутунлигини бузилиши тақиқланган мурожаат қилишда, «троян отини», «вирусларни», «чувалчангларни» татбиқ қилишда мумкиндир, тизимни ишлаш кобилиятини бузилиши эса – алоҳида файлларни ва дастур маҳсулотларни элементларини керак бўлмаган тўсиқларини, уларни ўчирилиши ёки алмаштирилишини оқибатидир.

Агар таъсир қилиш объекти сифатида маълумотлар бўлса, унда барча юқорида кўрсатилган бузилишлар тақиқланган нусхалашда, маълумотларни ўғрилашда ёки ушлаб олишда, уларни тўсиқларга учрашида ва ўзгартирилишида, ҳамда улар ўчирилганда ёки алмаштирилганда ўринлидир.

Ахборот хавфсизлиги учун ***хизмат кўрсатиш ходимларга таъсир қилиш*** энг хавфли ҳисобланади, улар тизимни ўзига бевосита мурожаат қиладилар ва ахборотларни ҳимоя қилишни мавжуд воситалар ва йўллари тўғрисида маълум бир билимларга ва маълумотларга эга бўладилар. Хизмат кўрсатиш ходимлари томонидан, уларни сотиб олиш ва шантаж қилиш оқибатида, ахборотни ҳимоя қилиш воситалари тўғрисидаги маълумотларни ва хабарларни бошқа шахсга бериш, сирни очиб қўйиш КТ ва Т ларни ахборот хавфсизлиги учун энг жиддий оқибатларга олиб келади. Юқорида баён қилинганидек, дастур таъминотига таъсир қилишда ахборотни бутунлигини бузилиши, унга «троян отини», «вирусларни», «чувалчангларни» татбиқ қилиш ҳисобига бўлиб ўтади.

«Троян оти» дастур кўринишига эга бўлиб, у, унинг ҳужжатларида ёзилган амаллар билан бир қаторда, тизимлар хавфсизлигини бузилишига ва деструктив натижаларга олиб борадиган баъзи бир бошқа амалларни ҳам бажаради. «Троян оти» атамаси аслида, фойдаланувчини яширин ички хавфли дастурини ишга туширишга чорлаш учун, алдашни ишлатади. Одатда, бундай дастур баъзи бир жуда фойдали амалларни бажариши таъкидланади. Хусусан, бундай дастурлар баъзи бир фойдали утилитлар номи остида ниқобланади.

«Троян отини» хавфлилиги, кейинчалик тизимнинг фойдаланувчиларига бериладиган бошланғич зарарсиз дастурга ўрнатилган қўшимча буйруқлар блокидир. Бу буйруқлар блоки баъзи бир шартлар амалга ошганда (сана, тизимнинг ҳолати), ёки ташқаридан бериладиган буйруқ бўйича ишга тушиши мумкин. Бундай дастурни ишга туширган фойдаланувчи ўзининг файлларини ҳам, бутун тизимни ҳам хавф остига қўяди.

Мисол тариқасида «троян оти» амалга оширадиган баъзи бир деструктив функцияларни келтирамиз:

- ахборотни йўқ қилиш. Объектларни ва йўқотиш усулларини танлаш зарар етказадиган авторнинг фантазияси билан аниқланади.
- ахборотни ушлаб олиш ва узатиш. Хусусан, клавиатурада терилаётган паролларни ушлаб олишни амалга оширадиган дастур маълумдир. [25; 103-112]
- хавфсизлик функциясини ва тизимни ҳимоя қилишни амалга оширадиган дастур матнини мақсадга йўналтирилган равишда ўзгартириш.

Умуман, «троян отлари» ахборотларни ўғрилаш ва тизимнинг дастур таъминотини очиқ - ойдин бузиш воситаси билан компьютер тизимларига талофат етказади.

«Троян оти» компьютер тизимлари хавфсизлигига таҳдид келтирувчи энг катта хавф ҳисобланади. Бундай хавфдан ҳимоя қилинишнинг радикал усули, дастурлар бажарилишини ёпиқ муҳитини ҳосил қилишдадир, улар тақиқланган мурожаат қилишдан ҳимоя қилиниши ва сақланиши керак.

«Компьютер вируси» компьютер ва ахборот технологияларини ривожланиши жараёнининг ўзида пайдо бўлган, ўзига хос ходиса кўринишига эгадир. Бу ходисанинг моҳияти шундаки, дастур вируслар тирик организмларга хос бўлган бир қатор хоссаларга эгадирлар – улар туғиладилар, кўпаядилар ва ўладилар.

«Компьютер вируси» - дастур бўлиб, у ўзининг ўзгарган нусхаларини бошқа дастурларга қўшиш йўли билан уларни ўзгартирган ҳолда шу дастур-

ларга юқади (зарарлантиради), шу билан бирга уларнинг нусхалари келгусида кўпайиш қобилиятини сақлаб колади. Компьютер вирусини таърифидаги асосий тушунчалар вируснинг ўз-ўзидан кўпайиб кетиши ва ҳисоблаш жараёнини ўзгартириш хоссасидир. Компьютер вирусининг кўрсатилган хоссалари жонли табиатда биологик вирусни паразитлашишига ўхшашдир. Вирус одатда ёмон ниятли кишилар томонидан шундай ишлаб чиқиладики, улар компьютер тизимида имкони борича узок вақт пайқалмасдан қолади. Вирусларнинг «мудрашини» бошланғич даври уларнинг яшаб кетишлик механизмидир. Вирус баъзи бир чақирув ҳодисалари, масалан, 13–сана, берилган вақт ва сана ҳ.к., бўлиб ўтган бир муайян вақтларда тўлиқ намоён бўлади. Компьютер вируслари ва вирусга қарши воситалар тўғрисида янада батафсилрок ва кенгрок маълумотлар ушбу ўқув қўлланмасининг алоҳида бўлимида баён қилинади.

«Тармоқли чувалчанг» дастур–вируснинг бир кўринишига эга бўлиб, у глобал тармоқ бўйича тарқалади ва ўзининг нусхаларини ахборот ташувчиларда қолдирмайди. Бошланишда «чувалчанглар» тақсимланган ҳисоблашларни бажариш имкониятини олиш учун бўш ресурсли бошқа компьютерларни тармоқда қидириш учун ишлаб чиқилган. «Чувалчанглар» технологияси тўғри ишлатилганда жуда фойдали бўлиши мумкин. Масалан, **World Wide Web «чувалчанги» Web** участкаларини қидириш индексини шакллантиради. Лекин, «чувалчанг» зарар келтирадиган дастурга осонгина айланади. «Чувалчанг» бузилиши мумкин бўлган узелни аниқлаш учун тармоқни қўллаб-қувватлаш механизмини ишлатади. Кейин шу механизмлар ёрдамида ўзининг танасини ўша узелга узатади фаоллашади, ёки фаоллашиш учун тўғри келадиган шароитларни кутади. Зарар етказадиган дастурлар синфининг энг маълум вакили **Моррис «чувалчанги»** дир, у UNIX тизимини буйруқли интерпретаторини кириш тилидаги ва СИ алгоритмик тилидаги 4000 та қатордан иборат дастур кўринишига эгадир. Одатда операцион тизимнинг баъзи хатоларини ёки тўхтаб қолишларини ишлатган ҳолда бу зарар етказадиган дастур ўзини бузадиган кодини машинадан машинага ўтказади, бунда у Интернетга уланган кўп сонли компьютер ва тизимларни ишдан чиқаради.

Шундай қилиб, тармоқли «чувалчанглар» дастурларга зарар етказадиган жуда хавфли кўринишидир, чунки уни ҳужум қилиш объекти сифатида Интернет глобал тармоқларига уланган миллионлаб компьютерларни исталгани бўлиши мумкин. «Чувалчанглардан» ҳимоя қилиш учун ички тармоққа ТМҚ га қарши эхтиёткорлик чораларни кўриш керак бўлади. Таъкидлаш керакки, «Троян отлари», компьютер вируслари ва тармоқли «чувалчанглар» компьютер тизимларини ва тармоқларини энг дахшатли хавфларидандир. Уларни амалга ошишига қарши туриш учун ёки улардан ҳимояланиш учун бир қатор чораларни куриш керак:

- бажариладиган файлларга тақиқланган мурожаат қилишни инкор қилиш;
- ҳарид қилинаётган воситаларни тестлаш;
- бажариладиган файлларни ва тизимли соҳаларни бутунлигини назорат қилиш;
- дастурлар бажарилишини ёпиқ муҳитини яратиш.

2.7. КТ ва Т ларини ахборот хавфсизлигини таъминлаш

Маълумки, компьютер тизимларини асосий вазифаси ахборотни қайта ишлашдир (сақлаш, узатиш, қайта ишлаш), шунинг учун ахборот хавфсизлигини таъминлаш муаммоси КТ ва Т лар учун жуда долзарбдир. Тизимларнинг ахборот хавфсизлигини таъминлаш, компьютер тармоқларини ва тизимларини ишлаш жараёнига, тақиқланган аралашиш, ҳамда уларнинг асосий элементларини ўзгартириш, нусхалаш, ўғрилаш, сафдан чиқариш ёки бузишга бўлган интилишларга қарши ҳаракатларни ташкил этишни, яъни КТ ва Т ларининг барча ташкил этувчиларини – аппарат воситаларини, дастур таъминотини, маълумотларни ва ходимларни ҳимоя қилишни кўзда тутади.

Одатда КТ ва Т ларини ахборот хавфсизлигини таъминлаш муаммосига иккита ёндашиш мавжуддир: фрагментарли ва комплекс.

Фрагментарли ёндашиш маълум берилган шароитларда аниқ аниқланган хавфларга қарши курашишга йўналтирилган. Бундай ёндашиш амалга оширишга мисоллар тариқасида мурожаат қилишни бошқаришни алоҳида воситаларини, махсуслаштирилган вирусга қарши дастурларни ва ҳ.к. кўрсатиш мумкин. Бундай ёндашишнинг афзаллиги маълум бир хавфга юқори танлашни борлигидир. Ушбу ёндашишнинг жиддий камчилиги ахборотни қайта ишлашнинг умумий ҳимоя қилинган муҳитини йўқлигидир. Ахборотни ҳимоя қилишнинг фрагментарли чоралари компьютер тизимларини ва тармоқларини конкрет объектларини фақатгина конкрет хавфлардан ҳимоя қилишни таъминлашдир. Хавфнинг кўринишини хатто унча катта бўлмаган ўзгартиришлар тизимнинг ахборот хавфсизлигини таъминлаш самарадорлигини йўқолишига олиб келади.

Комплекс ёндашиш хавфларга қарши курашишнинг турли кўринишдаги чораларини умумий комплексга бирлаштирадиган КТ ва Т ларида ахборотни қайта ишлашнинг ҳимоя қилинган муҳитини яратишга мўлжаллангандир. Ахборотни қайта ишлашни ҳимоя қилинган муҳитини ташкил этиш компьютер тизимларини хавфсизлигини маълум бир даражасини кафолатлаш имконини беради, бу комплекс ёндашишни, шубҳасиз афзаллиги ҳисоб-ланади. Бу ёндашишнинг камчиликларига қуйидагилар киради: тизим фойдаланувчиларини эркин ҳаракатларига чекланишлар, ҳимоя қилиш воситаларини ўрганиш ва созлаш хатоларига юқори сезгирлик, бошқаришнинг мураккаблиги. . [22; 157-180]

Амалга ошириш усуллари бўйича компьютер тизимларини хавфсизлигини таъминлашга бўлинади:

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

КТ ва Т ларини хавфсизлигини санаб ўтилган чораларини ахборотни ҳимоя қилишни тўсиқларини ва чораларини кетма-кетлиги каби қараш мумкин. Ҳимоя қилинаётган ахборотгача етиб бориш учун ҳимоя қилишнинг бир нечта чегараларини кетма-кет босиб ўтиш керак.

Тақиқланган ахборотга мурожаат қилишни амалга оширишга интилаётган инсон йўлида турадиган ҳимоя қилишнинг биринчи чегараси ҳуқуқийдир. Ахборотни ҳимоя қилишни бу аспекти ахборотни узатишда ва қайта ишлашда юридик меъёрларга риоя қилишни зарурлиги билан боғлангандир. Ахборотни ҳимоя қилишни ҳуқуқий меъёрларига мамлакатда ҳаракатда бўлган қонунлар, буйруқлар ва бошқа меъёрий далолатномалар тегишлидир, улар чекланган миқдорда ишлатиладиган ахборот билан мурожаат қилиш қоидаларини регламентлайди. Бу билан улар тақиқланган ахборотни ишлатишга тўсқинлик қиладилар ва ашаддий бузғунчи-ларни ушлаб турадиган омил ҳисобланади.

Ҳимоя қилишнинг иккинчи чегарасини ахлок-этикали чегаралар ташкил этади. Ҳимоя қилишнинг талабларига риоя қилишнинг этика моменти жуда катта аҳамиятга эгадир.

Компьютер тизимларига мурожаат қиладиган кишилар соғлом ахлоқ - этика муҳитида ишлашлари жуда муҳимдир. қаршилик кўрсатишнинг ахлоқ - этика чораларига, мамлакатда КТ ва Т ларини эволюцияли ривожланиб бориши билан жамиятда тўпланиб бораётган ёки анъанавий пайдо бўлган ахлокнинг барча мумкин бўлган меъёрлари тегишлидир. Бу меъёрлар кўп жиҳатдан қонунчилик томонидан тасдиқлангани каби мажбурий ҳисобланмайди, лекин уларга риоя қилмаслик одатда инсонни, шахслар гуруҳларини ёки ташкилотларни обруси пасайишга олиб келади. Ахлокий-этик меъёрлар ёзиб чиқилмагани каби (масалан, халолликни, ватанпарварликни ва ҳ.к. умумий қабул қилинган меъёрларни) ҳам, баъзи бир қоидалар ёки кўрсатмалар тўпламлари шаклида бўлишлари ҳам мумкин.

Ахборотни қонунга хилоф равишда ишлатишига тўсқинлик қиладиган учинчи чегара маъмурий усуллардир. Барча тоифали маъмуриятлар ҳуқуқий меъёрларни ва ижтимоий аспектларни ҳисобга олган ҳолда ахборотни ҳимоя қилишни маъмурий чораларини аниқлайдилар. Бу чоралар ташкилий характерли чораларга тегишли бўлади. Улар регламентлайдилар:

- КТ ва Т ларини ишлаш жараёнини;
- тизимнинг барча ресурсларини ишлатишни;
- ходимларнинг фаолиятини;
- фойдаланувчиларнинг тизим билан ўзаро таъсирлашиш тартибини, бунда хавфсизлик хавфларини амалга ошириш имкониятини юқори даражада кийинлаштириш ёки инкор қилиш кўзда тутилади.

Маъмурий чоралар ўз ичига оладилар:

- КТ ва Т ларида ахборотни қайта ишлаш қоидаларини қайта ишлаб чиқишни;
- жиҳозларни, компьютер тизимлари ва тармоқлари воситаларини лойиҳалашда ва монтаж қилишдаги ҳаракатлар тўпламини (стихияларни, ёнғинларни, ер қимирлашларни, бинoларни қўриқ-лашни ва ҳ.к. таъсирларини инобатга олиш);
- мутахассисларни ва ходимларни танлашдаги ва тайёрлашдаги ҳаракатлар тўплами (янги ходимларни текшириш, уларни махфий ахборот билан ишлаш тартиби билан таништириш, уни қайта ишлаш қоидаларини бузганлиги учун

жавобгарлик чоралари билан таништириш; ходимларни ўз мансабларидан фойдаланишдан фойда бўлмаган шароитларни яратиш ва ҳ.к.);

- ишончли ўтиш режимини ташкил этиш;

- ҳужжатларни ва махфий ахборот ташувчиларни ҳисобга олишни, сақлашни, ишлатишни ва йўқотишни ташкил этиш;

- мурожаат қилиш чекланишларини реквизитларини тақсимлаш (паролларни, калитларни, ваколатларни ва ҳ.к.);

- тизимдан фойдаланувчиларни ва ходимларни ишлаши устидан ёпиқ (билдирмасдан) назорат қилишни ташкил этиш;

- жиҳозларни ва дастур таъминотини лойиҳалашда, ишлаб чиқишда, таъмирлашда ва ўзгартиришда ҳаракатлар тўпламини (ишлаётган техник ва дастурли воситаларни сертификатлаш, барча ўзгартиришларга қатъий рухсат бериш, кўриб чиқиш ва тасдиқлаш, ҳимоя қилиш талабларига қаноатланганлигини текшириш, ўзгартиришларни ҳужжат билан қайд қилиш ва ҳ.к.).

Алоҳида таъкидлаш жоизки, тизимларни маъмурий ҳимоя қилишнинг ҳаракатдаги чоралари қайта ташкил этилмагунча, бошқа чоралар шубхасиз, самарасиз бўлади.

Ҳимоя қилишнинг маъмурий-ташкилий чоралари ахлокий-этикага нисбатан зерикарли ва машаққатли ва аппарат-дастурига нисбатан аниқликдан айрилган бўлиб кўриниши мумкин. Аммо улар ахборотни ноқонуний ишлатиш йўлидаги кучли тўсиқ ва ҳимоя қилишнинг бошқа даражалари учун ишончли база кўринишига эгадирлар.

Тўртинчи чегара ҳимоя қилишнинг физик чораларидир, уларга, ашаддий бузғунчиларни тизимнинг ташкил этувчиларига ва ҳимоя қилинаётган ахборотга кириб олишнинг мумкин бўлган йўлларида физик тўсиқларни яратиш учун махсус мўлжалланган, турли кўринишдаги механиқ, электрик ва электрон қўлланмалар ва иншоотлар тегишлидир.

Бешинчи чегара ҳимоя қилишнинг аппарат-дастурли воситаларидир. Уларга мустақил ёки бошқа воситалар билан биргаликда тизимларнинг ахборот хавфсизлигини таъминлайдиган қуйидаги усулларни амалга оширадиган турли хил электрон қурилмалар ва махсус дастурлар киради:

- тизим субъектларини идентификациялаш (англаш) ва аутентификациялаш.

- КТ ва Т ларини ресурсларига мурожаат қилишни чеклаш;

- ахборот бутунлигини назорат қилиш;

- ахборот махфийлигини таъминлаш;

- тизимларда бўлаётган ҳодисаларни қайд этиш ва тахлил қилиш;

- КТ ва Т ресурсларини ва ташкил этувчиларини захиралаш.

Олтинчи ва якуний чегара ҳимоя қилишнинг технологик чораларидир – маълумотларни қайта ишлашнинг технологик жараёнларига органиқ созланадиган тадбирлар тўпламидир. Уларга қуйидагилардан иборат:

- ахборот ташувчиларни архив нусхаларини яратиш;

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

- КТ ва Т лари фойдаланувчиларини махсус журналларда қайд этиш;

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

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

Шундай қилиб, юқорида айтиб ўтилган барча чегараларни йўналтирилган мақсадда қуриш ва юқорида кўрсатилган чораларни бажариш маълум бир даражада КТ ва Т ларини ахборот хавфсизлигини ошириш имконини беради.

2.8. КТ ва Т ларини ахборот хавфсизлигини таъминлаш сиёсатига комплекс ёндашиш

Ахборот хавфсизлигини таъминлашга комплекс ёндашиш, хавфларга қарши курашишнинг кўп даражали ва турли хил чораларини умумий комплексга бирлаштирадиган, ахборотни қайта ишлашнинг яхлит ва тизимли ҳимоя қилинган муҳитини ишлаб чиқишга ва яратишга йўналтирилгандир.

Бу ёндашиш одатда ахборот хавфсизлигини таъминлаш учун масъулиятли вазифаларни бажарадиган ёки жуда муҳим ахборотни қайта ишлаётган йирик компьютер тизимларини ва ташкилотларини ишлатадилар. Уларга ахборот хавфсизлигини бузиш ташкилот-ларини ва тизимларининг ўзига ҳам, уларнинг мижозларига ҳам катта моддий ва бошқа талофат етказиш мумкин. Шунинг учун бундай ташкилотлар ва тизимлар ахборот хавфсизлигини кафолатларига алоҳида эътибор каратишга ва комлекс ҳимоя қилишни амалга оширишга мажбурдирлар. Комплекс ёндашишга кўпчилик давлат, йирик тижорат-молия ташкилотлари ва муассасалари риоя қиладилар. Бу ёндашиш турли стандартларда ўз аксини топганлар. Ахборот хавфсизлигини таъминлашга комплекс ёндашиш маълум бир КТ ва Т учун ишлаб чиқилган хавфсизлик сиёсатига асосланган дир. [26; 141-150]

Хавфсизлик сиёсати меъёрларни, қоида ва амалий тавсиянома-ларни тўпламини ўз ичига олиб, улар асосида компьютер тизимларида ва тармоқларида ахборотни бошқариш, ҳимоя қилиш ва тақсимлаш амалга оширилади. У компьютер тизимларини ва тармоқларини ҳимоя қилиш воситаларини самарали ишлашини регламентлайди ва турли вазиятларда тизимнинг хатти-ҳаракатини аниқлаган ҳолда, ахборотни қайта ишлаш жараёнини барча хоссаларини қамраб олади.

Ахборот хавфсизлиги сиёсати юқорида айтиб ўтилган маъмурий-ташкилий чоралар, физик, аппарат-дастурли ва технологик аспектлар воситасида амалга оширилади КТ ва Т ларини ахборот хавфсизлиги тизимини умумий архитектурасини яратади. Ҳар бир маълум ташкилот учун ахборот хавфсизлиги сиёсати ахборотни қайта ишлашни аниқ технологиясини ва ишлатилаётган дастурли ва техник воситаларини ҳисобга олган ҳолда ўзининг шахсий характерига эга бўлиши керак. Ахборот хавфсизлиги сиёсати тизим объектларига мурожаат қилиш тартибини аниқлайдиган бошқариш усули билан белгиланади.

Ахборот хавфсизлиги сиёсатини икки асосий кўриниши мавжуддир:

- сайланадиган;

- ваколатли.

Ахборот хавфсизлигини сайланадиган сиёсати мурожаат қилишни бошқаришни сайланадиган усулига асосланган. Мурожаат қилишни сайланадиган бошқариш маъмурияти томонидан берилган мурожаат қилишни рухсат этилган муносабатларини тўплами (масалан, «объект-субъект-мурожаат қилиш тури» кўринишида) билан тавсифланади. Одатда мурожаат қилишни сайланадиган бошқариш хоссаларини ёзиб чиқиш учун мурожаат қилиш матрицаси асосидаги математик модель қўлланилади. Мурожаат қилиш матрицаси, устунлари тизим объектлариги, қаторлари субъектларига мос келадиган матрица кўринишига эгадир. Матрицанинг устунларини ва қаторларини кесишишида субъектни объектга рухсат этилган мурожаат қилиш тури кўрсатилади. Одатда субъектни объектга мурожаат қилишини «ўқишга мурожаат қилиш», «ёзишга мурожаат қилиш», «инкор этишга мурожаат қилиш» ва ҳ.к. каби турларни бажариш мумкин. Мурожаат қилиш матрицаси мурожаат қилишни бошқариш тизимини моделлаштиришга қулай ва оддий компьютер тизимларини ва тармоқларини янада адекватрок ёзиб чиқадиган мураккаб моделлар учун асос ҳисобланади.

Ахборот хавфсизлигини сайланадиган сиёсати тижорат секторидаги КТ ва Т ларида кенг қўлланилади, чунки уни амалга ошириш мурожаат қилишни ва ҳисоботлиликни чеклаш бўйича тижорат ташкилотларини талабларига мос келади, ҳамда мос келадиган нархга эга.

Ахборот хавфсизлигини таъминлашни ваколатли сиёсати мурожаат қилишни бошқаришни ваколатли (мандатли) усулига асосланган. Мурожаат қилишни ваколатли ёки мандатли бошқариш, субъектларни ва объектларни ахборот хавфсизлигини атрибутлари тўпламида, масалан, ахборот махфийлигини белгисига ва фойдаланувчига берилган рухсат даражасига боғлиқ равишда аниқланган мурожаат қилишга рухсат бериш қоидаларини йиғиндиси билан тавсифланади.

Мурожаат қилишни ваколатли бошқариш кўзда тутадики:

- тизимнинг барча объектлари ва субъектлари бир хил маънода идентификацияланган;

- тизимнинг ҳар бир объектига ахборот махфийлигини белгиси тақдим этилган, у ундаги мавжуд бўлган ахборотнинг аҳамиятлилигини аниқлайди;

- тизимнинг ҳар бир субъектига рухсатнинг ҳар бир даражаси тақдим этилган, у, субъект мурожаат қилиш ҳуқуқига эга бўлган объектларнинг ахборот махфийлигини белгисини энг катта қийматини аниқлайди.

Табиийки, объект қанчалик муҳим бўлса, унинг махфийлик белгиси ҳам шунчалик юқори бўлади. Шунинг учун махфийлик белгиси энг юқори бўлган объектлар энг юқори ҳимоя қилинган бўлади.

Ахборот хавфсизлигини ваколатли сиёсати асосий вазифаси турли даражали махфийликка эга бўлган объектларга субъектларни мурожаат қилишни ростлаш, юқори даражали мансабли иерархиядан пастки даражага чиқиб кетишини олдини олиш, ҳамда пастки даражадан юқори даражага мумкин бўлган кириб боришларни блокировкалашдир.

«Информатика» курсидан ҳам (ЭҲМ Ҳисоблаш комплекс –кўп машинали

ҳисоблаш комплекси, кўп процессорли ҳисоблаш комплекс; ҳисоблаш тизими, ҳисоблаш тармоғи – локал , глобал). «Компьютер тизимларида ахборотни ҳимоя қилиш» курсидан ҳам (ахборот хавфсизлиги; ахборот хавфсизлигига тахлид, ахборотга мурожаат этиш (рухсат этилган ва тақиқланган), махфийлик, объект, субъект, бутунлилик) асосий тушунчалар мавжуддир. Айниқса шуни таъкидлаш керакки, «компьютер тизимларида ахборотларни ҳимоялаш» курсида маълум бир компьютер тизими

деталида қуйидагилар тушунтирилади;

- бир синфли (авлодли) ва вазифали ЭҲМ;
- ҳисоблаш комплекслари ва тизимлвари;
- ҳисоблаш тармоқлари.

Бундай тушунчалар қуйидагича тушунтирилади. Ахборот хавфсизлигига асаосий таҳдидлардан ички ва ташқи тасодифий ва олдиндан мўлжалланган таҳдидларни таъкидлаш керакдир. Бундан ташқари ахборот махфийлигининг бузилиши ахборот бутунлигини бузилиши ва тизимини ишга лаёқатлигини бузилишларини алоҳида таъкидлаш жоиздир.

Компьютер тизимларида ахборотни ишончли ҳимоя қилиш агар у барча объектларда (фойдаланувчилар терминаллари тармоқ маъмурияти ёки гуруҳли абонентлик узели терминал алоқа узели ахборотга ишлов бериш воситалари, ахборотни акс эттириш воситалари ахборотни ҳужжатлаштириш воситалари, машина зали ташқи алоқа каналлари ва тармоқ жихозлари, ахборотни йиғувчилар ва ташувчилар) ва барча субъектларда (тезкор ва ташқи эслаб қолиш қурилмаларидаги маълумотлар ва дастурлар, монитор экранидаги ва принтерга чиқарилаётган маълумотлар алоқа канали ўйича узатилаётган маълумотлар, ахборотни қайта ишлашининг турли чиқиндилари, паролларни ва устуворларни белгилаш журналлари, хизмат кўрсатмалари, тармоқ операцион тизимлари архивлари) ишончли бўлган тақдирдагина самарали бўлиши мумкин.

Асосий атамалар

КТ ва Т ларини хавфсизлиги, ахборотга мурожаат қилиш, тақиқланган мурожаат қилиш, маълумотларнинг махфийлиги, тизим субъекти, тизим объекти, ахборот бутунлиги, тизим хавфсизлиги хавфи, хавфсизлик талофати, тизимнинг кучсиз томонлари, компьютер тизимларига ҳужум, хавфсизлик сиёсати, тақиқланган ахборотни ўзгартириш, паролларни ушлаб олиш, «маскарад», енгилликларни ноқонуний ишлатиш, сирни билдириш, ўғрилаш, қўрқитиш, сотиб олиш, алмаштириб қўйиш, бузиш, олиб ташлаш, компьютер тармоғига пассив бостириб кириш, фаол бостириб кириш, физик бутунликни бузиш, тақиқланган ахборотни олиш, тақиқланган ахборотни кўпайтириш, «троян оти», «компьютер вируси», «тармоқ чувалчанги», ахборот хавфсизлигини таъминлаш, фрагментарли ёндашиш, комплексли ёндашиш, сайланадиган сиёсат, ваколатли сиёсат.

Назорат саволлари

1. КТ ва Т лари хавфсизлиги деганда нима тушунилади?
2. Ахборотга мурожаат қилиш деганда нима тушунилади?
3. Тақиқланган ахборотга ва рухсат этилган мурожаат қилиш нимани билдиради? Мисоллар келтиринг.
4. Маълумотларни махфийлиги нимани билдиради?
5. Компьютер тизимларини субъектларини ва объектларини асосий белгилари қандай?
6. Ахборот бутунлигига таъриф беринг.
7. Тизим ташкил этувчисини бутунлигини ва мурожаат қилишлилигини асосий хоссалари қандай?
8. КТ ва Т ларини хавфсизлигини хавфи деганда нима тушунилади?
9. Тизимнинг кучсиз томонлари нима билан тавсифланади?
10. Компьютер тизимларига ва тармоқларига ҳужум деганда нима тушунилади?
11. Хавфсиз ёки ҳимоя қилинган тизим нимани билдиради?
12. Ахборот хавфсизлиги сиёсати нимани билдиради?
13. Хавфсизлик хавфлари қандай турларга бўлинади?
14. Ахборот хавфсизлигини бузишни қандай асосий сабаблари мавжуд?
15. Ахборот бутунлигини потенциал бузғунчиси тавсифларини беринг.
16. Ахборотга мурожаат қилиш қандай тоифадаги шахслар учун мумкин? Уларнинг тавсифларини беринг.
17. Хавфсизлик хавфларини пайдо бўлишини олдиндан аниқлаб борадиган асосий омиллар канака?
18. Ахборотни ҳимоя қилинганлигини бузадиган дестабиллаштирадиган омилларнинг манбаси ким ёки нима ҳисобланади?
19. Дестабиллаштирувчи омилларнинг асосий турлари қанақа?
20. Дестабиллаштирувчи омиллар қандай оқибатларга олиб келиши мумкин?
21. Хавфсизлик хавфини таъсир этиш объекти сифатида КТ ва Т ларини характерли хусусиятлари қандай?
22. Тақиқланган ахборотга мурожаат қилишни усулларини ва услубларини асосий турларини санаб утинг ва уларни таърифлаб беринг.
23. Дастур таъминотига таъсир қилганда ахборот бутунлигини бузилиши нимани ҳисобига бўлиши мумкин?
24. Ахборотни хавфсизлигин таъминлаш муаммосига қандай ёндашишлар мавжуд? Уларни таърифлаб беринг.
25. Компьютер тизимларини хавфсизлигини таъминлашни асосий чоралари ва тавсифларини келтиринг.
26. Ахборот хавфсизлигини таъминлаш сиёсатига комплекс ёндашиш нимани билдиради?
27. Ахборот хавфсизлик сиёсати, унинг асосий кўринишлари ва тавсифлари қандай?

Тавсия этиладиган адабиётлар:

1. Домашев А.В., Грунтович М.М. и др. Программирование алгоритмов защиты информации. Учеб. пособ. – М.: Издатель Молгачева С.В. Изд. «Нолидж», 2002. – 416с.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

3. Закирова Т.А., Мусаева М.А. Методические указания проведению лабораторных работ по курсу «Защита информации в компьютерных сетях" Ташкент – 2005.

4. Алимов Р.Х., Ходиев Б.Ю., Алимов Қ.А., Усмонов С.У., Бегалов Б.А., Зайналов Н.Р., Мусалиев А.А., Файзиева Ф.. Миллий иқтисодда ахборот тизимлари ва технологиялари. − Т., 2004. -319 бет.

5. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Эрматов Ш.Т., Мусаева М.А. Компьютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. −Т.: ТДИУ, 2003.

3 боб. АХБОРОТНИ ҲИМОЯ ҚИЛИШ ТИЗИМИНИНГ ШАКЛЛАНТИРИШНИ АСОСИЙ ПРИНЦИПЛАРИ

Ҳозирги замонавий босқичда ахборотнинг роли маълумдир. У халқаро ҳамжамиятининг илмий-техникавий ва ижтимоий-иқти-содий ривожланишида инсоният тараққиётининг асосий ресурси ҳисобланади. Яхши йўлга қўйилган ахборотли тармоқ жамият ҳаётидаги эволюцион ролни ўйнашга даъват қилади. Ахборот кишиларнинг барча фаолиятини биринчи асоси ҳисобланади, негаки ҳар қандай ечимнинг асосида ҳар доим олинган ва қайта ишланган ахборот ётади. Шунинг учун ахборот кишиларнинг алоҳида тоифалари томонидан жиноий ва антигуманитар мақсадларда ишлатилиши мумкин.

Бозор тизимига ўтишнинг иқтисодий жараёни (кўплаб хусусий корхоналарни пайдо бўлиши, давлат бошқаруви ролининг пасайиши ва ҳ.к.) товарларни ва хизматларни ишлаб чиқарувчилар ўртасидаги рақобатни кескин кучайишига олиб боради, бу эса умумий ҳолда ишлаб чиқариш кучларини ва жамият муносабатлари жараёнини ривожланишига, агар у ривожланган шаклларда амалга оширилаётган бўлса, имконият яратади. Лекин бу рақобатли курашда ривожланмаган, инсофсиз ва хаттоки ноқонуний воситалар ва усуллар ишлатилиши мумкин. Бизнинг Республикамизда ҳам, МДХ нинг бошқа давлатларида ҳам, бунинг учун асосий манба собиқ Иттифоқнинг иқтисодий кенглиги махсус шароитлари билан яратилмоқда: тадбиркорлик фаолиятини умумий паст маданияти, бозор муносабатларининг шакллантириш жараёнини тугалланмаганлиги, самарасиз қонуний ва меъёрий далолатномаларни йўқлиги ёки самарасизлиги, иқтисодий барқарорсизлик (кадрсизланишлар, ишсизлик,

тўламасликлар), ривожланмаган, инсофсиз ва ноқонуний рақобат билан курашиш учун давлат ва жамоа ташкилотларининг тармоқланган тизимини йўқлигидир.

Юқорида айтилганлардан инсонларни ахборот хавфсизлигини, ва умуман ахборотни ҳимоя қилиш муаммосини таъминлаш муаммолари пайдо бўлади. Бу муаммолар сифат жиҳатдан янги аҳамиятга эга ва тақиқланган ахборотни олишни усулларини барча хоссаларини ҳисобга оладиган ишончли замонавий усулларни ва воситаларни қўллашни талаб этади. [24; 218-230]

Ўтказилаётган фаол тадқиқотларга қарамасдан, ахборот хавф-сизлигини умумлашган назарияси ҳалигача яратилмаган. Амалиётда қўлланилаётган усуллар, ёндашишлар ва воситалар жиддий камчиликларга эга ва ишончли эмас. Шунинг учун, махфий ахборотлар билан ишлайдиган шахслар етарлича тайёргарликка эга бўлишлари ва ахборот хавфсизлигини таъминлаш масалаларини бутун спектрида, уларнинг комплексли ва ўзаро боғлиқлик характерини тушунган ҳолда, малакали равишда мўлжаллай олиш керак.

Ахборотни ҳимоя қилиш тизимини шакллантиришни асосий принципларини кўриб чиққунча ахборотни ҳимоя қилишни умумий муаммоларини кўриб чиқамиз. Мақсадли дунёқарашлар тизими каби ахборот хавфсизлиги концепцияси, ахборот хавфсизлигини таъминлаш усуллари ва уни ҳимоя қилиш воситалари, умумий кўринишда учта оддий саволга жавоб бериши керак: нимани, нимадан ва қандай ҳимоя қилиш керак?

«Нимани ҳимоя қилиш керак» суроғи билан ҳимоя қилиш объекти, яъни ахборотни йиғиш, узатиш, қайта ишлаш ва сақлаш учун мўлжалланган физик, аппаратли, дастурли ва ҳужжатли воситалари комплекси, тушунчаси билан боғлангандир.

«Нимадан ҳимоя қилиш керак?» суроғи билан хавф тушунчаси, яъни ахборотни йўқотишга ёки бошқалар билиб олишига олиб келадиган ҳимоя қилиш объектига ноқонуний таъсир этишни потенциал имкониятлари, билан боғлангандир. Ҳимоя қилиш объекти ва хавф тушунчалари олдин батафсил кўриб чиқилган.

«Ахборотни қандай ҳимоя қилиш керак» суроғи билан ҳимоя қилиш тизими тушунчаси, яъни ҳимоя қилиш объектини хавфсизлик хавфларини турли кўринишларини аниқлашга, акс эттиришга ва бартараф этишга йўналтирилган чора ва воситалар, ҳамда улар асосидаги фаолият комплекси билан ажралмас боғлангандир.

Компьютер тизимлари ва тармоқларида ахборотни ҳимоя қилишни комплекс тизимини ташкил этиши билан боғланган саволларни кўриб чиқамиз.

3.1 АҲҚКТ қуришни ташкилий жараёни

Ахборотни ҳимоя қилиш тизими яратилаётган компьютер тизими билан биргаликда яратилиши керак. Тизимни қуришда ҳимоя қилишнинг мавжуд воситалари ишлатилиши мумкин, ёки улар маълум бир компьютер тизими учун махсус ишлаб чиқилади. Ахборотни ҳимоя қилишни комплекс тизимини (АҲҚКТ) яратиш босқичларини кўриб чиқамиз.

Компьютер тизимини хоссаларига, унинг ишлатилиши хоссаларига ва ахборотни ҳимоя қилиш талабларига боғлиқ равишда АҲҚКТ яратиш жараёнини алоҳида босқичларини ўз ичига олмаслиги мумкин, ёки мураккаб аппарат-дастур тизимларини ишлаб чиқишда умумий қабул қилинган меъёрлардан фарқ қилиши мумкин. Лекин одатда бундай тизимларни ишлаб чиқиш қуйидаги босқичларни ўз ичига олади:

1) техник топшириқни ишлаб чиқиш;

2) эскиз лойиҳалаш;

3) техник лойиҳалаш;

4) ишчи лойиҳалаш;

5) тажрибали намунани ишлаб чиқариш.

Асосий босқичлардан биттасида – техник топшириқни ишлаб чиқиш – айнан АҲҚКТ ишлаб чиқиш учун характерли бўлган деярли барча специфик масалалар ечилади.

Техник топшириқни ишлаб чиқиш билан якунланадиган тизимларни ишлаб чиқиш жараёни илмий-тадқиқотли ишлаб чиқиш деб аталади, мураккаб тизимни яратиш бўйича ишнинг қолган қисмини эса тажриба-конструкторли ишлаб чиқиш деб аталади. Аппарат-дастурли воситаларни тажриба-конструкторли ишлаб чиқиш дастурлашнинг автоматлаштирилган тизимини қўллаган ҳолда олиб борилади, уларни лойиҳалаш алгоритмлари яхши ўрганилган ва ишлаб чиқарилгандир. Шунинг учун илмий-тадқиқотли лойиҳалаш жараёнини кўриб чиқамиз.

Техник топшириқ ишлаб чиқилаётган АҲҚКТ га асосий техник талабларни, ҳамда ишлаб чиқишнинг ижрочисини ва буюрт-мачисини келишилган ўзаро мажбуриятларини ўз ичига олади. Техник талаблар асосий техник тавсифларни қийматларини, бажариладиган функцияларини, ишлаш режимларини, ташқи тизимлар билан ўзаро таъсирини ва ҳ.к. аниқлайди.[25;43-55]

Аппарат воситалар тезкорлик, унумдорлик, эслаб қолиш қурилмасининг сиғими, разрядлилик, нархи, ишончлилик тавсифлари ва ҳоказо билан баҳоланади. Дастур воситалар тезкор ва ташқи хотиралар сиғими, бу воситалар яратилган дастурлаштириш тизими, ОТ билан ва дастур воситалари билан мос келишлиги, бажариш вақти, нархи ва ҳ.к. билан баҳоланади.

АҲҚКТ да илмий-тадқиқотли ишлаб чиқишни кетма-кетлиги ва мазмуни 3.1-расмда келтирилган.

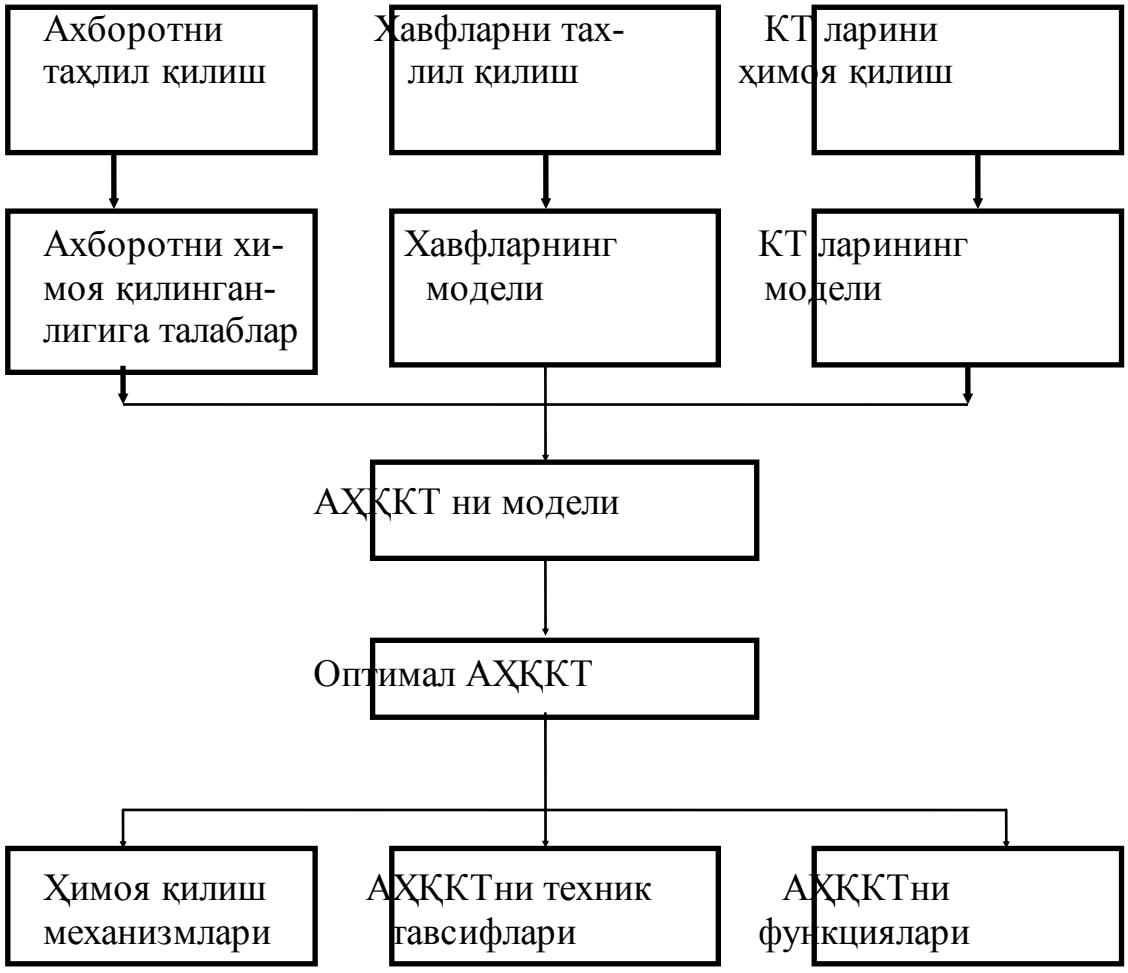
Илмий-тадқиқотли ишлаб чиқиш ахборотни махфийлигини ва муҳимлигини таҳлил қилишдан, ахборот хавфсизлигини хавфларини таҳлил қилишдан ва ҳимоя қилинаётган компьютер тизимини таҳлил қилишдан бошланади.

Ахборотни таҳлил қилиш асосида АҲҚКТни яратишни мақсадга мувофиқлиги тўғрисида хулоса чиқарилади.

Агар ахборот махфий бўлмаса ва енгил тикланадиган бўлса, унда АҲҚКТ ни яратишнинг зарурияти йўқдир. Агар ахборотнинг бутунлиги ва махфийлиги жиддий бўлмаган йўқотишлар билан боғланган бўлса ҳам КТ ва Т ларида АҲҚКТ нинг яратишни маъноси йўқдир. Бу ҳолатларда КТ ва Т ларини штатли воситаларини, ҳамда ахборотни йўқотишда суғурталашни ишлатиш етарлидир.

Ахборотни таҳлил қилишда махфий ахборотлар оқими, бу ахборот қайта

ишланаётган ва сақланаётган КТ ва Т ларини элементлари аниқланади. Шу ернинг ўзида ахборотга алоҳида фойдаланувчиларни ва КТ ва Т ларини барча сегментларини мурожаат қилишини чеклаш масалалари аниқланади, унинг ҳимоя қилин-ганлигига талаблар аниқланади.



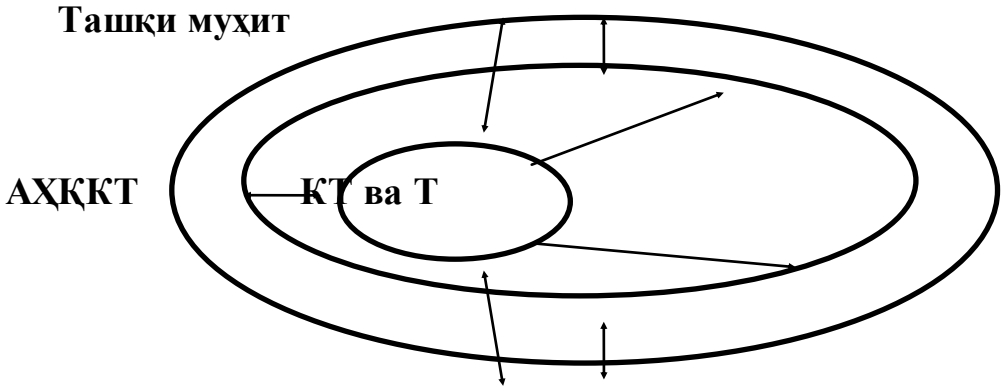
3.1 расм. АҲҚКТда илмий-тадқиқотли ишлаб чиқишни кетма-кетлиги ва мазмуни

Талаблар махфийликнинг маълум бир грифини тақдим этиш, мурожаат қилишни чеклаш қоидаларини ўрнатиш йўли билан берилади.

АҲҚКТ қуриш учун КТ ва Т ларини таҳлил қилиш натижасида олинган ахборот жуда муҳим ҳисобланади. АҲҚКТ компьютерли тизимининг қисми бўлганлиги учун, ҳимоя қилиш тизимини компьютер тизими билан ўзаро таъсирини ички ва ташқи муҳит билан аниқлаш мумкин (3.2 расм).

КТ ва Т ларини архитектураси ўзаро таъсирни ички шартларини аниқлайди, бунда КТ ва Т ларини географик жойлашиши, уларнинг турлари (тарқатилган ёки мужассамлаштирилган) ва тўзилишлари (техник, дастурий, ахборотли ва ҳ.к.), КТ ва Т ларини элементларини унумдорлиги ва ишончлилигини, ишлатилаётган аппарат ва дастурли воситаларнинг турлари ва уларнинг ишлаш режимлари, КТ ва Т нинг ички хавфлари (аппарат ва дастурли воситаларнинг ишдан чиқиши, алгоритмик хатолар) ҳисобга олинади. Ташқи шарт-

лардан ташқи тизимлар билан ўзаро таъсирлашиш ва тасодифий ва олдиндан кўзда тутилган хавфлар ҳисобга олинади.



3.2-расм. АҲҚКТ компьютер тизими ва ташқи муҳит билан ўзаро таъсири

АҲҚКТ ни қуришнинг мажбурий шарти хавфларни таҳлил қилишдир, уларнинг натижалари асосида хавфларнинг модели қурилади, бу модель маълум бир компьютер тизимида ахборот хавфсизлигини тасодифий ва олдиндан белгиланган хавфлари тўғрисидаги маълумотларни ўз ичига олади.

Тасодифий ва олдиндан белгиланган хавфларнинг моделлари хавфларнинг тўлиқ спектрини ва уларни тавсифларини олиш имконини беради. Ахборотни таҳлил қилишни бошланғич қийматлари билан биргаликда ва лойиҳаланаётган КТ архитектурасининг хоссаларини ҳисобга олган ҳолда хавфсизлик хавфларининг моделлари АҲҚКТни қуриш учун бошланғич қийматларини олиш имконини беради.

АҲҚКТни моделлаштириш реал тизимда бўлиб ўтаётган жараёнларни берилган аниқликда амалга оширадиган тизимни образини (моделини) қуришдадир. Моделни амалга ошириш реал тизимни тавсифларини олиш ва тадқиқот қилиш имкониятини беради.

3.2. АҲҚКТ куришнинг асосий принциплари

Компьютер тизимларида АҲҚКТ ни ишлаб чиқишда ва қуришда маълум бир услубий принципларига риоя қилиш керак. АҲҚКТ ни бу принциплари орасида қуйидагиларни таъкидлаш керак: очиқлиги, оддийлиги, ўчира олинишлиги, иқтисодий самарадорлиги, афзалликларни минимуми, умумий назорат, мустақиллик, ҳисоботлилик, бўлинганлик, ғаразли (душманлик) принципи, инсонга мўлжалланганлик, ортиқча ахборотнинг йўқлиги ва бошқалар.

АҲҚКТ мураккаб тизимлар синфига киради ва уларни қуриш учун ечиладиган масалаларни хоссаларини ҳисобга олган ҳолда мураккаб тизимларни қуришни асосий принциплари ишлатилиши мумкин. Бу принциплардан қуйидагиларда батафсилрок тўхталамиз:

- компьютер тизимларини ва АҲҚКТ параллел ишлаб чиқиш;
- ҳимоя қилинган компьютерли тизимларни қуришга тизимли ёндашиш;

- АҲҚКТ нинг кўп даражали тузилиши;
- ахборотни ҳимоя қилишни иерархик бошқариш тизими;
- ҳимоя қилинган компьютер тизимларини блокли архитектураси;
- АҲҚКТ нинг ривожланиш имконияти;
- ҳимоя қилинган КТ ва Т ларидан фойдаланувчилар ва хизмат кўрсатиш ходимлари билан дўстона интерфейси;

Фақатгина компьютер тизимларини ва АҲҚКТ биргаликда ишлаб чиққандагина барча бошқа принципларни амалга оширишни самарали амалга ошириш мумкин. Шу билан бирга созланган бўлинмайдиган ҳимоя қилиш механизмларини ва ҳимоя қилишнинг блокли ихчамлаштирилган воситаларини ва жараёнларини яратишда оқилона бирлаштира олишни ҳисобга олиш зарур. Фақатгина КТ ва Т ишлаб чиқиш босқичидагина хусусан, компьютер тизимларини ва ҳимоя қилиш воситаларини блокларини ва қурилмаларини ўзаро таъсир этишини тўлиқ инобатга олиш мумкин ҳамда оптимал шаклда ҳимоя қилишнинг тизимлилигига эришиш мумкин.

Ҳимоя қилинган КТ ва Т ларини яратишда тизимлилик принципи асосий концептуал ва услубий принцип ҳисобланади. Бу принцип ахборот хавфсизлигини барча мумкин бўлган хавфларини таҳлил қилишдан тортиб, компьютер тизимларини барча ҳаётий принципларида ҳам, КТ ва Т ларини барча звеноларида ҳам ҳимоя қилишнинг комплексли механизмларини таъминлашгача боғлиқ бўлган масалаларни ҳал қилади.

Ахборотни ҳимоя қилиш тизими кўп даражали бўлиши керак, яъни ҳимоя қилиш таркиби бир-бирини қоплайдиган (ичига кирадиган) даражаларга эга бўлиши керак. Берк ахборотгача етиб бориш учун ҳимоя қилишнинг барча даражаларини ўтиш зарур, масалан, ахборотни ҳимоя қилиш; дастурли воситаларни ҳимоя қилиш; аппаратли воситаларни ҳимоя қилиш; объектни хоналарини, биноларини, территориясини ҳимоя қилиш.[19; 137-145]

АҲҚКТ ҳар доим марказлашган ҳолда бошқарилиши керак. Таркатилган компьютер тизимларида ҳимоя қилишни бошқариш иерархик принцип бўйича амалга оширилиши мумкин. Бошқаришни марказлаштириш корхона, ташкилот, корпорация, вазирлик доирасида ахборот ресурсларини хавфсизлиги соҳасида умумий сиёсатини олиб боришини таъминлайди. Марказлаштирилган бошқариш масофадан назорат қилишни махсус воситалари, калитларни тақсимлаш, мурожаат қилишни чегаралаш, идентификациялаш атрибутларини тайёрлаш ва бошқалар билан таъминланади.

Блокли архитектурани ишлатиш – ҳимоя қилинган компьютер тизимларини қуришни муҳим принципларидан яна биттасидир. Бу принципнинг афзалликлари қуйидагилардир:

- қурилмаларни, дастурларни, алгоритмларни ишлаб чиқиш, соз-лаш ва назорат қилиш соддалашади;
- блокларни ишлаб чиқишни параллеллигига йўл қўйилади;
- стандарт ихчамлаштирилган блоклар ишлатилади;
- тизимларни модернизациялаш соддалашади;
- ишлатишни қулайлиги ва оддийлиги.

Мураккаб компьютер тизимини, масалан ҳисоблаш тармоғини, ишлаб

чиқишда фойдаланувчиларни сонини ошириш билан ҳам, ахборот технологияларини мукаммаллаштириш орқали кўпайтириш билан ҳам уни ривожлантиришни имкониятини кўзда тутиш керак. Бунинг учун АҲҚКТ ишлаб чиқишда ресурсларни захираларини, айниқса мураккаб тизимнинг энг танқис қисми – алоқа каналларини, кўзда тутиш лозим. Ресурсларнинг бир қисми АҲҚКТ ривожланиши билан керак бўлиб қолиши мумкин. Тизимни модернизациялаш имкониятини ҳам кўзда тутиш зарур. Мураккаб тизимлар ривожланадиган ва очиқ бўлиши керак. АҲҚКТ да ҳимоя қилиш воситаларини кўпайтириш ва халқаро стандартларни ишлатиш имкониятларини ҳам кўзда тутиш керак. Янги имкониятлар, КТ ва Т ларининг турли режимлари, янги хавфларни пайдо бўлиши – буларнинг барчаси ҳимоя қилишнинг янги механизмларини ривожланишини рағбатлантиради. Халқаро стандартларни ишлатиш ўзаро таъсирлашишнинг стандарт интерфейсларига эга бўлган турли турлардаги қисмлардаги тизимларни ишлатиш имконини беради.

Мураккаб ҳисоблаш тизимини, шу жумладан АҲҚКТ ни ҳам, ишлаб чиқишга тегишли бўлган принцип – бу фойдаланувчиларга ва хизмат кўрсатиш ходимларига нисбатан дўстона муносабатдир. Бу соҳада АҲҚКТ ни ишлаб чиқишда, имкони борича, кўзда тутиш керак:

1) АҲҚКТ максимал автоматлашган бўлиши керак;
2) фойдаланувчидан катта ишлар хажмини бажаришни талаб қилмаслиги керак;
3) фойдаланувчига ўзининг функционал вазифаларини бажаришга тўсиқ бермаслиги керак;
4) ишдан чиққан қурилмалардан уларни ишга лаёқатлилигини тиклаш учун ҳимоя қилишни олиб ташлаш имконияти.

3.3. АҲҚКТ амалга оширилиши усуллари

АҲҚКТ объектларда ахборот хавфсизлигини кўп сонли мумкин бўлган хавфлардан ҳимоя қилиш учун яратилади. У ёки бу хавфни блокировкалаш учун ҳимоя қилишнинг усулларини ва воситаларини маълум бир тўплами ишлатилади. Уларнинг баъзи бирлари ахборотни бир вақтнинг ўзида бир нечта хавфлардан ҳимоя қилади. Усулларнинг ичида универсал усуллар ҳам мавжуддир, улар исталган ҳимоя қилиш тизими учун асосий ҳисобланади. Бу ахборотни ҳимоя қилишнинг ҳуқуқий усулларидир, бу ихтиёрий вазифали ҳимоя қилиш тизимини расмий равишда куришни ва ишлатишни асоси бўлиб хизмат қилади; бу ташкилий усуллардир, улар одатда бир нечта хавфларни бартараф (қайтариш) этиш учун ишлатилади; бу техник усуллардир, улар ташкилий ва техник тадбирларга асосланган ҳолда кўпчилик хавфлардан ахборотларни ҳимоя қилади.

Ахборотни ҳимоя қилишни ҳуқуқий усулларида ҳуқуқий характерли масалалар кўриб чиқилади:

- компьютер жиноятчилиги учун жазолаш меъёрларини ишлаб чиқиш;
- дастурловчиларни муаллифлик ҳуқуқларини ҳимоя қилиш;

- жиноий ва фуқаролик қонунчилигини, ҳамда компьютер жиноятчилиги соҳасида суд ишини мукаммаллаштириш;

- компьютер тизимлари ишлаб чиқувчилар устидан жамоат назорати масалалари;

- бу масалалар бўйича мос халқаро шартномаларни қабул қилиш ва ҳ.к.

Ахборотни ҳимоя қилишни ташкилий чоралари кўриб чиқади:

- компьютер тизимларини қўриқлашни;

- ходимларни танлаб олиш;

- ўта муҳим ишларни фақат бир киши томонидан олиб борилиши ҳолатларини инкор қилиш;

- тизимни, у ишдан чиққанидан кейин, ишлаш қобилиятини тиклаш режасини борлиги;

- ахборот хавфсизлиги тизимини таъминлайдиган шахсларга жавобгарликни бериш;

- компьютер марказини жойлашган жойини танлаш ва ҳ.к.

Ҳимоя қилишни техник усуллари аппаратли, дастурли ва аппарат-дастурлига бўлинадилар. Электрон ҳисоблаш техникасига мўлжалланган хавфсизликларни таъминлашни асосий йўналишлари қуйидагилардир:

- КТ ва Т ларида тақиқланган ахборотга мурожаат қилишдан ҳимоя қилиш;

- вирусга қарши ҳимоя қилиш;

- исталмаган электромагнит ва акустик майдон ва нурланишлар орқали ушлаб олишни бартараф этиш;

- криптографик усуллар асосида хабарларни юқори тузилишли берклигини таъминлаш.

Техник усуллар (дастурли, аппаратли ва дастур-аппаратли) келгусида янада батафсил кўриб чиқилиши учун ахборотни ҳуқуқий ва ташкилий ҳимоя қилишни таъминлаш масалаларига тўхталиб утамиз.

Ахборот – ҳуқуқ объектидир. Компьютер жиноятчилиги учун асбоблар сифатида телекоммуникация ва ҳисоблаш техникаси воситалари, дастур таъминоти ва интеллектуал билимлар, уларни мукаммаллашган соҳалари нафақатгина компьютерлар, корпоратив ва глобал тармоқларгина бўлиб колмасдан, балки замонавий юқори ахборот технологиялари воситалари ишлатиладиган, катта хажмдаги ахборотлар қайта ишланадиган, масалан, статистика ва молия институтлари, фаолиятни исталган соҳаси бўлишлари мумкин.

Исталган муассасанинг фаолияти алоқа каналлари бўйича ахборотларни олиш, қайта ишлаш, қарорлар қабул қилиш, узатиш жараёнларисиз мумкин эмасдир. Бу жараёнларни таъминлайдиган барча воситалар компьютер жиноятчилиги учун асбоблар ҳисобланади ёки асбоблар сифатида ишлатилиши мумкин.

Ўзбекистонда, МДҲ барча давлатларидаги каби, яқин вақт-ларгача компьютер жиноятчиликлари билан самарали курашишни имконияти йўқ эди. Ҳозир эса вазият ўзгара бошлади. Информатика, ахборотни ҳимоя қилиш ва давлат сирлари соҳасида бевосита қонунчилик асослари 10 дан ортиқ асосий қонунларда ва Ўзбекистон Республикаси Президентини бир қатор фармойишларида акс эттирилгандир.

Асосий қонунларда ахборотни ва ахборотли ресурсларни мақсадлари, объектлари тушунчалари ва ҳуқуқий асослари аниқ-лангандир.

«Ахборот, ахборотлаштириш ва ахборотни ҳимоя қилиш тўғрисида» ги қонун фукароларни ахборотга конституцион ҳуқуқини таъминлаш, уни очиқлигини ва унга мурожаат қилишликни, фукаролар ва ташкилотлар томонидан қонунчилик, ижроия ва суд хоқимияти органлари тўғрисидаги ахборотни ва бошқа ахборотни олишни, жамоат ва шахсий манфаатга эга бўлган таъминлашга, ҳамда жамиятда ахборот билан мулокот қилишга ва ахборотлаштиришни ривожлантиришга кўмаклашиш учун даъват қилади. Унда ахборотни хужжалаштириш ва уни ахборот ресурсларини очиқ ва чекланган мурожаат қилиш тоифаларига тегишлиги, ахборотга мурожаат қилиш бўйича механизмларни ва ваколатларни аниқлаш, ахборотни ҳуқуқий ҳимоя қилиш тартиби масалалари, бу соҳада бузғунчиликлар учун жавобгарликни ўрнатиш механизмлари масалалари акс эттирилган.

Қонун билан аниқланган ахборотни ҳимоя қилиш мақсадлари:

- ўғирлашларни, бузишларни, чиқиб кетишларни, қалбақилаштиришларни бартараф этиш;
- шахсни, жамиятни, давлатни хавфсизлигини таъминлаш;
- ахборотни йўқотиш, бузиш, блокировкалаш бўйича тақиқланган ҳаракатларни бартараф этиш;
- шахсий сирни ва шахсий маълумотларни махфийлигини сақлашга фуқароларни конституциявий ҳуқуқларини ҳимоя қилиш;
- давлат сирини, ҳужжатлаштирилган ахборотни махфийлигини сақлаш.

Қонун билан **ахборот хавфсизлиги объектлари** аниқланган, уларга қуйидагилар тегишлидир:

1) ахборот ресурсларини барча кўринишлари;

2) ахборотни олишга, тарқатишга ва ишлатишга, махфий ахборотни ва интеллектуал мулкни ҳимоя қилишга фуқароларни, ҳуқуқий шахсларни ва давлатнинг ҳуқуқлари;

3) турли синфли ва вазифали ахборот тизимларини ўз ичига оладиган ахборот ресурсларини шакллантириш, тарқатиш ва ишлатиш тизими маълумотлар кутубхоналари, архивлари, тизимлари ва йирик тўпламлари ахборот технологиялари ахборотни йиғиш, қайта ишлаш, сақлаш ва узатишнинг регламентлари ва жараёнлари илмий-техникавий ва хизмат кўрсатадиган ходимлар;

4) ахборотни қайта ишлаш ва таҳлил қилиш марказларини, ахборот алмашиш ва телекоммуникация каналларини ишлашини таъминлаш механизмларини, телекоммуникацияли тизимларини ва тармоқларни, шу жумладан ахборотни ҳимоя қилишни тизимларини ва воситаларини ўз ичига олган ахборотлашган инфратузилма;

5) оммавий ахборот ва ташвикот воситаларига асосланадиган жамият онгини (дунёқараш, аҳлоқий қадр-қимматлар, одоб баҳолари, хулқни ижтимоий–йўл қўйиладиган стереотурлари ва инсонлар ўртасидаги ўзаро муносабатлар).

Қонун бўйича чегараланган мурожаат қилинадиган хабарлар ҳимоя қилинади ва ҳимоя қилиш даражасини уларнинг эгаси аниқлайди, ҳимоя чораларини жавобгарлиги эса нафақатгина эгасида эмас, балки фойдаланувчида ҳам бўлади.

Фақат ҳужжатлаштирилган ахборотгина ҳимоя қилинади. Ҳужжатлаштирилган ахборот Давлат сирига ва махфий ахборотга бўлинади.

Давлат сирига давлат томонидан ҳимоя қилинадиган унинг ҳарбий, ташқи сиёсий, иқтисодий, разведка, контрразведка ва тезкор қидирув фаолияти соҳасидаги хабарлар тегишли бўлади. Бу хабарларнинг эгаси ва фойдаланувчиси давлатнинг ўзи бўлади, шунинг учун унинг ўзи ҳимоя қилиш бўйича талабларни илгари суради ва уларнинг бошқарилишини назорат қилади. Бу талабларни бузилиши барча қатъий қонунлар билан жазоланади.

Махфий ахборот – ҳужжатлаштирилган ахборот бўлиб, унинг ҳуқуқий режими давлат, тижорат, саноат ва бошқа жамият фаолияти соҳасидаги ҳаракат қилаётган қонунчиликни махсус меъёрлари билан ўрнатилган. Эгалари – муассасалар ва ташкилотлар, улар бу ахборотларга эга бўладилар ва у билан амаллар бажарадилар, ҳамда улар ҳимоя қилиш даражасини ўрнатадилар. Махфийликни бузилган ҳолатда баъзи бир санкцияларни қўллаш қуйидаги расмиятчиликлар олдиндан бажарилган ҳоллардагина мумкиндир:

- ахборот ҳақиқатан ҳам қимматбахо бўлиши керак;
- муассаса ахборотга эркин мурожаат қилишни инкор этиш ва унинг махфийлигини қўриқлаш учун маълум бир чораларни кўриши керак;
- барча ходимлар ахборотнинг махфийлиги тўғрисида огоҳлантирилган бўлиши керак.

Махфий ахборотни тури – бу шахсий махфий маълумотлардир. Аммо бу масалада ҳуқуқий асослар етарлича ишлаб чиқилмаган бўлса ҳам, давлат шахсий ахборотни ҳимоя қилишни ўзининг шахсий назорати остига олган. Бу тоифага шахсий ва оилавий сирлар, шахсий маълумотлар, ёзишмалар сирлари, телефондаги, почтадаги, телеграфдаги ва бошқа хабарлар тегишлидир.

Умумий кўринишда махфий характерли маълумотлар таркиби қуйидаги кўринишга эга:

- шахсий маълумотлар;
- тергов ва суд иши сири;
- хизмат сири;
- касб-ҳунар сири;
- тижорат сири;
- кашфиётларни моҳияти ҳақида.

Асосий қонунларда компьютер ахбороти соҳасидаги атамалар ва тушунчалар аниқлангандир (компьютер ахбороти, ЭҲМ учун дастур, ЭҲМ (компьютер), ЭҲМ тармоғи, маълумотлар базаси ва ҳ.к.).

Компьютер жиноятчиликни кўриб чиқиладиган асосий моддаларни ўз ичига олади:

- компьютер ахборотига қонунсиз мурожаат қилиш;
- ЭҲМ учун зарар етказадиган дастурларни яратиш, ишлатиш ва тарқатиш;
- ЭҲМ, ЭҲМ тизимлари ва уларнинг тармоқларини ишлатиш қоидала-рини бузиш.

Модда бўйича компьютер ахборотига (машина ташувчисидаги, ЭҲМ даги ёки ЭҲМ тармоқларидаги) ноқонуний мурожаат қилиш учун, агар бу ахборотни йўқотишга, блокировкасига, ўзгаришига ёки нусхаланишига олиб келган бўлса,

ҳамда ҳисоблаш тармоқларида ишлашни бузганлиги учун жавобгарлик кўзда тутилган. [23; 95-112]

Тақиқланган ахборотни йўқолишига, блокировкаланишига, ўзгаришига ёки нусхаланишига, ахборот тизимларининг ишлашини бузилишига, олиб келадиган дастурларни ЭҲМ учун тузганлик учун ҳам жорий жавобгарлик кўзда тутилган.

ЭҲМ, ЭҲМ тизимлари ёки уларнинг тармоқларини, уларда ишлашга рухсати бўлган шахс томонидан, ишлатиш қоидаларини бузганлиги учун ҳам, агар бу фаолият натижасида қонун билан қўриқланадиган ахборотни йўқотишга, блокировкалашга ёки ўзгартиришга олиб келса ва жиддий зарар етказса, жавобгарлик ўрнатилган.

Компьютер ахборотини ҳимоя қилишнинг ташкилий усуллари

Компьютер ахборотини ҳимоя қилишнинг ташкилий усулларини, ҳимоя қилиш даражасини танлаш учун, мавжуд бўлган ахборотни олдиндан таҳлил қилишни ўтказишдан бошлаш керак.

Фақат ҳужжатлаштирилган ахборотгина ҳимоя қилинганлиги учун, ҳужжатлаштиришни қатъиян стандарт бўйича ўтказиш керак. Оддий ахборот учун ҳам, ҳисоблаш техникаси воситалари билан яратиладиган машинограммага ва машина ташувчиларидаги ҳужжатларга ҳуқуқий кучни бериш учун ҳам стандартлар мавжуддир.

ГОСТ ҳужжатнинг 31 та реквизитларини кўзда тутса ҳам, уларнинг ҳаммасини бўлиши шарт эмас. Асосий реквизит –матн-дир, унга маълум бир ҳуқуқий кучни бериш учун муҳим реквизитлар – сана ва имзо керакдир. Автоматлаштирилган ахборотлашган тизимнинг ҳужжатлари учун электрон имзо керакдир.

Ахборотни ҳимоя қилиш қимматга тушади, шунинг учун унинг муҳимлиги ва кимматбаҳолиги бўйича ахборотни ҳимоя қилиш принципларидан келиб чиқиш керак.

Тақиқланган мурожаат қилишни аниқлаш учун керакдир:

- файлларнинг баённомалари, айниқса, тизимга кириш баённомаларини мунтазам текшириш;
- одатдан ташқари вақтларда номаълум фойдаланувчиларни уланишини кузатиш;
- фойдаланувчиларнинг бирор-бир вақт оралиғида ишлатилмаган ва янада ҳаракатга келиб қолган идентификаторларига эътиборни қаратиш.

Тармоқда бегоналарни пайдо бўлишини аниқлашни усулларидан биттаси, алоҳида файлда тармоқ бўйича барча жараёнларни ва уланишларни қайд этувчи одатдаги жараённи (Shell тилини) ҳар 10 минутда ишга тушириш ҳисобланади. Бу дастур фойдаланувчилар рўйхатларини, барча жорий жараёнларни ва тармоқдаги уланишларни шакллантиради.

Корхоналар, ташкилотлар ва ҳ.к. тармоқларда самарали ҳимоя қилиш билан ахборот хавфсизлиги маъмурияти хизмати шуғулланиши керак, унинг вазифасига фойдаланувчиларни компьютер тармоғи ресурсларига назорат

қилинадиган мурожаат этишни, унинг ҳаёт циклини барча босқичларида ташкил этиш ва қўллаб-қувватлаш, тармоқ хавфсизлиги ҳолатини кузатиш ва ундаги бўлиб ўтаётган фойдаланувчиларнинг тақиқланган ҳаракатларига тезкор равишда муносабат билдириш керак бўлади.

Ҳимоя қилиш воситалари бозорида ҳимоя қилиш тизимининг кўпгина хилма-хили мавжуддир. Тармоқ маъмурияти уларни қўллашни зарурлигини ва тартибини аниқлаши керак. Барча компьютерлар ҳам қўшимча ҳимоя қилиш воситаларига мухтож бўлмайди. қуйидаги ҳолатларда ҳимоя қилиш воситаларини қўллаш мақсадга мувофиқдир:

- маълумотларни криптографик ҳимоя қилишни компьютер воситаларига жойлаштиришда;
- фойдаланувчилар томонидан технологияда кўзда тутилмаган ҳаракатларга йўл қўймаслик учун тармоқда фойдаланувчиларнинг ҳаракатларини регламентлаш ва баённомалаштириш керак бўлганда;
- компьютернинг локал ресурсларига (дисклар, каталоглар, файллар, ташқи қурилмалар) фойдаланувчиларнинг мурожаат қилишини чеклаш, ҳамда компьютернинг дастур воситаларини таркибини ва конфигурациясини мустақил равишда ўзгартириш имкониятини инкор қилиш керак бўлганда. Бу масалаларни хал қилиш учун маъмурият йўриқномаларида кўзда тутилган ҳаракатларни бажариш керак.

Фойдаланувчиларнинг ваколатларини ва тармоқда ахборотни ҳимоя тизимини созлашни бошқариш бўйича муаммолари тармоққа мурожаат қилишни бошқаришни марказлашган тизимини ишлатиш асосида ечилиши мумкин. Мурожаат қилишни бошқаришни махсус сервери ҳимоя қилишнинг марказий маълумотлар базасини ҳимоя қилишнинг локал маълумотлар базаси билан (маълумотларни ҳимоя қилишнинг тақсимланган базаси) автоматик синхронизациясини амалга оширади. Бу, бундан ташқари, тармоқни ёки марказий серверни ишдан чиқиши ишчи станцияларда ҳимоя қилиш воситаларини ишлашига тўсқинлик қилмаслигини кафолатлайди.

Хавфсизлик маъмурияти тармоқ ҳолатини ҳам тезкор (компьютер тармоғини ҳимоя қилинганлик ҳолатини кузатиш йўли билан), ҳам тезкор эмас (ахборотни ҳимоя қилиш тизимини ҳодисаларни қайд қилиш журналини мазмунини таҳлил қилиш йўли билан) назорат қилиши керак.

Вируслардан ҳимоя қилишни ташкилий усулларига келганда, компьютерни ёки компьютер тармоғини зарарланиш хавфини ташкилий ва профилактик тадбирлар тўпламини – «компьютер гигиенасини» қўллаш билан камайтириш мумкин, бу «гигиена» тавсия этади:

- фақатгина лицензияга эга бўлган дастур таъминотини (ДТ) ишлатиш;
- «компьютер гигиенаси» талабларига риоя қилинмаган компьютерлардан файлларни нусхалашни бажармаслик керак;
- тушуниб бўлмайдиган ёки тушунарсиз хатарли паролларни ишлатиш;
- ҳарид қилинаётган дастурлар тизими дастурчилар томонидан ўрганиб чиқилиши керак;
- янги дастурлар «карантин» муддатини ўтиши керак;

- текширилган янги ДТ « топ-тоза» компьютерда дублланиши керак, асл нусха ёзишдан ҳимоя қилинади;

- компьютерларга бегона шахсларни мурожаат қилишини чеклаш;

- вируслар симптомини аниқланганда барча фойдаланувчиларни ва тизимли дастурчиларни (вируслар бўйича мутахассисларни) огоҳлантириш.

Умуман, вируслардан ҳимоя қилиш асосланади:

1) компьютерларнинг тезкор имкониятларига;
2) дастур воситаларига;
3) тизимли дастур таъминотига;
4) ҳимоя қилишнинг тизимли дастурли воситаларига.

Ташкилий воситалар компьютерларни вируслар билан зарарланиш хавфини минималлаштириш, зарарланганда эса – тезда фойдаланувчига ахборот бериш ва вирусни ва унинг оқибатларини олдини олишни енгиллаштириш имконини беради.

Ташкилий воситалар қуйидаги тадбирларни ўз ичига олади:

1) Захиралаш:

- ОТ ва ДТ нинг барча асосий ташкил этувчиларини архивларда мавжудлиги;

- ўзгарадиган файлларни архивларини ҳар куни олиб бориш;

2) Профилактика:

- винчестернинг фаол қисмидаги маълумотларни дискеталарга доимий равишда кўчириш;

- ДТ ташкил этувчиларини ва фойдаланувчиларнинг дастурларини алоҳида сақлаш;

3) Тафтиш:

- дискеталарда янги олинадиган дастурларни вируслар борлигига тадқиқот қилиш;

- винчестернинг файлларини узунликларини доимий равишда текшириш;

- ДТ ни сақлаш ва узатишда назорат йиғиндиларини доимий равишда текшириш;

- винчестернинг ва ишлатиладиган дискеталарнинг тизимли файлларини юкланадиган секторларини мазмунини текшириш;

4) Фильтрлаш:

- винчестернинг мантиқий дискларга, уларга мурожаат қилишни турли хил имкониятлари билан, бўлиб чиқиш;

- файлли тизим устидан кузатишни резидентли дастур воситаларини ишлатиш;

5) Махсус дастур воситалари билан ҳимоя қилиш.

Бу барча тадбирлар ҳимоя қилишнинг турлича дастур воситаларини ишлатишни ўз ичига олади: дастур-архивловчиларини; файлли тизимнинг муҳим ташкил этувчиларини захиралаш дастурлари файлларни ва юкланадиган секторларнинг мазмунини кўриб чиқадиган дастурлар; назорат йиғиндиларини ва ҳимоя қилиш дастурининг ўзини ҳисобга олиш дастурлари.

Асосий атамалар

Ҳимоя қилиш сиғими, хавф, ҳимоя қилиш тизими, техник топшириқ, эс-

кизли лойиҳалаш, техник лойиҳалаш, ишчи лойиҳалаш, илмий-тадқиқотли ишлаб чиқиш, тажриба-конструкторлик ишлаб чиқиш, хавфларнинг модели, блокли архитектура, ресурсларнинг захираси, давлат сири, махфий ахборот, ахборот хавфсизлиги маъмурияти, тизимга мурожаат қилишни бошқаришнинг марказлашган тизими, захиралаш, профилактика, тафтиш, фильтрлаш, дастур-архивловчилар.

Назорат саволлари

1. Ахборотни ҳимоя қилиш тизимини шакллантириш қандай амалга оширилади?
2. АҲҚКТ қуришни ташкилий жараёнини асосий босқичларини санаб ўтинг.
3. АҲҚКТ илмий-тадқиқотли ишлаб чиқиш нимани билдиради?
4. Ички ва ташқи ўзаро таъсирлашиш нимани билдиради ва улар нимани аниқлайдилар?
5. АҲҚКТ тажриба конструкторли ишлаб чиқишда нимани билдиради?
6. АҲҚКТ яратишни асосий тамойиллари қандай?
7. КТ ва АҲҚКТ ва ҳимоя қилинган компьютер тизимларини қуришга тизимли ёндашишни параллел ишлаб чиқиш нимани билдиради?
8. АҲҚКТ кўп даражали, таркибли ва иерархик бошқариш тизими нимани билдиради?
9. АҲҚКТ мумкин бўлган ривожланишини тамойиллари ва ҳимоя қилинган КТ ларини фойдаланувчи ва хизмат кўрсатиш ходимлари билан дўстона интерфейси қандай афзалликларни кўзда тутади?
10. Ахборотни ҳимоя қилишни универсал усулларини санаб ўтинг.
11. Ахборотни ҳимоя қилишнинг ҳуқуқий усулларида ҳуқуқий характерли қандай масалалар кўриб чиқилади?
12. Ахборотни ҳимоя қилишнинг ташкилий чораларида нималар кўзда тутилган?
13. Техник усуллар билан хавфсизликни таъминлашнинг қандай асосий йўналишлари кўзда тутилган?
14. Ахборот хавфсизлигини маъмуриятининг асосий вазифалари нималардан иборат?

Тавсия этиладиган адабиётлар:

1. Завгородный В.И. Комплексная зашита информации в компьютерных системах. − М.: Логос, 2001.
2. Соколов А.В., Степанюк О.М. Методы информационной зашиты объектов и компьютернўых сетей. СПб.: Полигон, 2000.
3. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

5. Эрматов Ш.Т. Компьютер тизимларида ахборотни ҳимоялаш. Электрон дарслик. Т., – 2004.

4 боб. АХБОРОТНИ ҲИМОЯ ҚИЛИШНИНГ УСУЛЛАРИ ВА МОДЕЛЛАРИ

Ахборотни ҳимоя қилишнинг турли-туман усуллари ва моделлари мавжуддир. Ташкилий ва ий усуллар тўғрисида олдинрок қисқача баён этилган. Ахборотни ҳимоя қилишнинг техникавий усуллари масалаларида тўхталиб ўтамиз ва уни ахборотни захирали нусхалаш ёки дубллашдан бошлаймиз.

4.1. Ахборотни захиралаш усуллари

Маълумки, дубллаш ахборотни тасодифий ҳарфлардан ҳимоя қилишнинг энг самарали усулларидан биттаси ҳисобланади. Тасодифий хавфларни блокировкалаш учун бир қатор масалалар ечилади (4.1-расм).

Дубллаш билан ахборотнинг бутунлиги таъминланади. У яна олдиндан кўзда тутилган таъсирлардан ҳам ҳимоя қилишни таъминлайди.

Ахборотнинг муҳимлиги, КТ ларини қуриш хусусиятлари ва ишлаш режимлари дубллаш усулларини танлашга таъсир кўрсатади. Дубллаш усулларини таснифлаш белгилари бўлиши мумкин: ахборотни тиклаш вақти, ишлатилаётган воситалар, нусхалар сони, асосий ва дубллайдиган ахборот ташувчиларини фазовий узоқлаш-ганлик даражаси, дубллаш жараёни, дубланадиган ахборот тури.

Ахборотни тиклаш вақти бўйича тезкор ва тезкор бўлмаган усуллар мавжуддир. Дубланадиган ахборотни ҳақиқий вақт оралиғида ишлатишни таъминлайдиган усуллар тезкор усулларга тегишли бўлади. Дубланадиган ахборотни ишлатишга ўтиш, ушбу КТ лари учун ҳақиқий вақт оралиғи режимида ахборотни ишлатишга сўровларини бажариш имконини берадиган вақт ичида амалга оширилади. Бу шартни таъминламайдиган барча усуллар дубллашнинг тезкор бўлмаган усулларига тегишли бўлади.

Дубллаш мақсадлари учун ишлатилаётган воситалар бўйича дубллаш усулларини қўшимча ТаЭККларини (блокларни); олинмайдиган машина ташувчиларидаги хотиранинг махсус ажратилган соҳаларини; олинадиган ахборот ташувчиларини ишлатадиган усулларга бўлиш мумкин.

Нусхалар сони бўйича бу усуллар бир даражали ва кўп даражали бўлади (≤ 3).

Асосий ва дубллайдиган ахборот ташувчиларни фазовий узоқлашганлик даражаси бўйича жамланган ва тарқатилган усулларини таъкидлаш мумкин. Жамланган дубллаш усуллари битта хонада жойлашган асосий ва дубллайдиган ахборот ташувчиларини ишлатадилар.

Ойнали нусхалашда асосий ахборотни ҳар қандай ўзгаришлари билан эътироф этилади. Асосий ахборот ва дубль ҳар доим бир-бирига ўхшашдир.

Қисман нусхалашда маълум бир файлларнинг дубллари яратилади. Қисман нусхалашнинг кўринишларидан бири инкрементли нусхалаш ҳисобланади, унда файлларнинг дублларини яратиш охирги нусхалашни вақт бўйича ўзгариши билан амалга оширилади.

4.1-расм. Тасодифий хавфлардан ҳимоя қилиш масалалари

Аралашган нусхалаш комбинацияларга йўл қўяди (тўлиқ ва қисман нусхалашни уларни ўтказишни турли даврлари билан).

Дубланадиган ахборотни кўриниши бўйича ахборотни зичлаштириш билан ва ахборотни зичлаштирмасдан дубллаш усуллари бўлади.

Дубланадиган ахборотни сақлаш учун ташқи ЭКК сифатида қаттиқ магнит дисклардаги ва магнит ленталардаги йиғувчилар ишлатилади. Қаттиқ магнит дисклардаги йиғувчилар одатда ахборотни тезкор дубллаш учун қўлланилади.

Энг муҳим тизимли ахборот (масалан, каталоглар жадваллари ва файллар жадваллари) хотиранинг ажратилган соҳаларида ишчи дискда дубланади.

Ойнали дискларга - бу алоҳида йиғувчининг қаттиқ магнитли дискидир - ишлатиш тезкор дубллаш усули жуда ишончлидир. Ишчи дискдаги ахборот ойналига параллел ёзилади. Ишчи йиғувчи ишдан чиққанда ҳақиқий вақт оралиги режимида ойнали диск билан ишлашга автоматик ўтиш амалга оширилади, бунда ахборот тўлиқ хажмда сақланади.

Ахборотни сақланишлиги бўйича юқори талаблар қўйиладиган КТ ларида (ҳарбий тизимлар, ТЖАБС, тармоқларнинг серверлари, тармоқларнинг коммуникацияли модуллари ва бошқалар), одатда, алоҳида назоратчиларга ва озуқа манбаларига уланган икки ва ундан ортиқ захирали дисклар ишлатилади. Юқори ишончлилик аппарат воситалари билан таъминланади.

Қаттиқ дискларда ахборотни ишончли ва самарали сақлашни идеологияси RAID (Redundant Array of Independent Disks) технологиясида ўз аксини топгандир. Бу технология сўровларни параллел бажариш имкониятлари билан маълумотларни сақлашни блокли қурилмасини яратиш ва йиғувчиларнинг алоҳида блоклари ишдан чиққанда ахборотни қаттиқ магнит дискларда тиклаш концепциясини амалга оширади. Бу технологияни амалга оширадиган қурилмалар RAID қисмининг тизимлари ёки RAID дискли массивлари деб аталади.

Ахборотни дубллаш учун катта сиғимли, лекин дискларга нисбатан ахборотга мурожаат қилишни нисбатан катта вақти бўлган магнит ленталардаги йиғувчилар ҳам ишлатилади. Ҳозирги вақтда, битта ёки бир нечта лента айлантирадиган механизмлардан, кассеталарни силжитиш механизмларидан ва кассеталар учун механизмлардан ташкил топадиган, уларни (кутубхонани) автоматик алмаштирадиган лентали тизимлар ҳам ишлатилмоқда. Битта касетада 10 Г байт зичлаштирилган ёки 4 Г байт зичлаштирилмаган ахборот сақланиши мумкин. Магазинда 60 тагача кассета бўлиши мумкин. Ленталарга дублланадиган ахборот хажмлари фақатгина бўш кассеталарнинг мавжудлиги билан деярли чегаралангандир. Улар фақатгина тезкор бўлмаган дубллаш учун ишлатилади. Турли даражали нусхаларни яратиш билан тўлиқ, қисман ёки аралаштирилган нусхалаш амалга оширилиши мумкин.

Кўп даражали дубллашни ишлатганда нусхаларни яратишга ва ишлатишга қуйидаги ёндашиш амалга оширилиши мумкин. Юқори даражани эталони сифатида камдан-кам ўзгарадиган ахборот (дастурлар, доимий бошланғич қийматлар) ишлатилади. Биринчи даражали эталон фақатгина, агар ахборотни қуйироқ даражадаги эталонлардан тиклаш имконияти бўлмаса, ҳамда ахборотлар ўзгарганда, ва даврий назорат қилишда, ахборотни тиклаш учун ишлатилади. Иккинчи даражали эталон маълум даврийли (масалан, суткада бир марта) ахборотни тўлиқ нусхалаш йўли билан, ёки жиддий ва муҳим ўзгаришлардан кейин (тармоқ бўйича муҳим хабарларни ёки дастурнинг бажарилиш натижаларини олиш) олинади.

КТ ларида мумкин бўлган таркатилган нусхалаш, фавқулодда ҳолатларда ва йирик халоқатларда, ахборотни бутунлигини ва мурожаат қилиш мумкинлигини деярли ягона усули ҳисобланади.

Таснифлашнинг турли хил белгилари бўйича дубллаш усулларининг таснифланишни схематик кўриниши 4.2 расмда кўрсатилган.

Малакали маъмурий ходимлар дубллаш тизимини (захирали нусхалашни) доимо текшириб турадилар. Улар захирали нусхалашни бажарадилар, ахборотни ўчирадилар, кейин эса уларни ишлатишга уриниб кўрадилар. Бундан ташқари, маъмурият дубллашни барча маҳсулотларини доимо тестлаб бориши керак. Муҳим файлларни тезрок тиклашни кафолатлаш учун яна тиклаш жараёнларини текшириш керак.

Умумий ҳолда маъмурият дубллашнинг ҳар бир йиғувчисини иккита нусхасини олиши керак, улардан биттаси ишда, бошқаси эса хавфсиз жойда, ташкилотдан ташқарида жойлашган бўлиши керак.

Файлларни тиклашда захирали нусхалаш журналини олиб бориш жиддий ёрдам кўрсатади. Журналнинг нусхалари ишлатилаётган воситалар билан биргаликда, компьютернинг ёнида сақланиши керак. Журналда қуйидаги ахборот акс эттирилади:

- дубллашни бажарилиш санаси;
- йиғувчи номери;
- бажариладиган дубллаш тури;
- маълумотлари дублланаётган компьютер;
- сақланган файлларнинг номлари;
- амални бажараётган ходимнинг фамилияси;
- захира нусхали йиғувчининг жойлашган жойи.

Дубллаш тизимини ўрнатишда шуни билиш керакки, дубллаш йиғувчилари серверга ёки исталган компьютерга уланиши мумкин, шу билан бирга дубллаш йиғувчи уланган компьютердан бош-қарилади. Агар дубллаш бевосита серверда бажарилса, захиралаш ва тиклаш амаллари бирмунча тезроқ бўлиб ўтади, чунки тармоқ бўйича маълумотларни узатиш йўқдир.

Тармоқ орқали дубллаш кўпчилик тизимлар учун энг қулай усулдир, лекин бунда сезиларли тармоқли трафик яратилади ва тармоққа жавоб бериш вақти катталашади. Тармоқли трафик, бундан ташқари, унумдорликни камайишга олиб келади. Тармоқ орқали дубллашни амалга ошириб, захиралаш бажарилаётган компьютерни тармоқнинг ажратилган сегментига жойлаштириб, тармоқли трафикни камайтириш мумкин. Бу компьютер ҳар бир сервернинг алоҳида тармоқли платасига уланади.

4.2. Ахборотни ҳимоя қилишнинг аппарат дастури воситалари

Эслатиб ўтамизки, ҳимоя қилишнинг ташкилий-дастурли воситалари техник усулларга тегишли бўлади. Бундай усуллар ва воситалар етарлича катта миқдордадир. Бу тасодифий ҳавфлардан анъанавий жосуслик ва қўпорувчилик, электромагнит нарланишлардан ва йўналтиришлардан КТ лари таркибларини тақиқланган ўзгартиришлардан, тақиқланган мурожаат қилишдан ахборотни ҳимоя қилиш, криптографик усуллар, компьютер вируслари ва улар билан курашиш механизмларидан асраш керак.

Тасодифий ҳавфлардан ахборотни ҳимоя қилишга ахборотларни дублаш (олдинроқ батафсил кўриб чиқилган), КТ ишончлигини ошириш, ишдан чиқишларига мустахкам КТ ларини яратиш, халоқатлардан ва фавқулодда ҳолатлардан келадиган талофатларни камайтириш, нотўғри амалларни блокировкалаш билан эришилади.

Анъанавий жосусликдан ва кўпорувчиликдан ахборотни ҳимоя қилишда КТ ларида КТ лари ишлатилмайдиган бошқа объектларни ҳимоя қилиш учун ишлатиладиган воситалар ва усуллар қўлланилади. Бу тизимнинг вазифаларига объектни қўриқлаш тизиминии яратиш, КТ объектларида махфий ахборот ресурслари билан ишлашни ташкил этиш, кузатишга ва билдирмасдан эшитиб олишга, ҳамда ходимларнинг ёмон ниятли ҳаракатларга қарши курашиш киради.

Зарарли злектромагнит нурланишдан ва йўналтиришлардан (ЗЭМНЙ) ҳимоя қилиш ҳам фаол, ҳам пассив усуллар билан амалга оширилади. Ҳимоя қилишнинг фаол усуллари, ёмон ниятли киши томонидан ушлаб олинган хабарлардан фойдали ахборотларни қабул қилиш ва ажратиб олишни мураккаблаштирадиган, зарарли электромагнит нурланишлар ва йўналтирилишлар каналларида тўсиқларни яратишга қаратилгандир. Пассив усуллар хавфли хабарни даражасини камайишини ёки хабарларнинг ахборотланганлигини пасайишини таъминлайдилар.

КТ ларини таркибини тақиқланган ўзгаришлардан (СРЭУ) ҳимоя қилишнинг усуллари ва услублари КТ ларини ишлаб чиқиш ва ишлатиш босқичларида алгоритмик, дастурли ва техник структураларни ҳимоя қилиш учун мўлжалланган. Одатда, тизимни ишлаб чиқиш босқичида ва уни ўзгартиришда бажарилган КТ ларини СРЭУ қўйилмалар деб аталади.

Тақиқланган ахборотни мурожаат этишдан ҳимоя қилиш, криптографик усуллар ва вируслар билан курашиш механизмлари кейинчалик батафсил кўриб чиқилади.

4.2.1. Тақиқланган мурожаат қилишларидан КТ ларида ахборотни ҳимоя қилиш

Тақиқланган мурожаат қилишни (ТМҚ) амалга ошириш учун КТ таркибига кирмайдиган аппарат ёки дастурли воситаларни қўллаш мажбурий эмас. Бу, ахборотни ҳимоя қилиш тизими тўғрисида маълумотларга эга бўлган ҳолда, техник ва дастур воситаларни тўхтаб қолишларини ва ишдан чиқишларини ишлатган ҳолда, хизмат кўрсатиш ходимларини ва фойдаланувчиларни хатоларини, бепарволигини ишлатган ҳолда, КТ тўғрисидаги билимларни ва у билан ишлашни билишни ишлатган ҳолда бажарилади.

ТМҚ дан ҳимоя қилиш учун ахборотга мурожаат қилишни чекловчи тизим (АМҚЧТ) яратилади. АМҚЧТ мавжуд бўлганда ахборотга ТМҚ эга бўлиш фақатгина КТ ишдан чиққанда ва тўхтаб қолганда ёки АҲҚКТ ни кучсиз жойларини билган ҳолда мумкиндир.

АҲҚКТ камчиликлари тўғрисидаги ахборотга эга бўлишни йўлларидан биттаси у билан бевосита мулокатга киришиш йўли билан ҳимоя қилиш механизмларини ўрганишдир. Бошқача ёндашиш: олдин АҲҚКТ дастур воситасини нусхаси олинади, кейин эса лаборатория шароитларида уларни тадқиқот қилиш амалга оширилади. Бундан ташқари, олинадиган ташувчиларда ҳисобга олинмаган нусхаларни яратиш ахборотни ўғирлашни кенг тарқалган ва қулай усулларидан биттаси ҳисобланади. Бу дастурларни тақиқланган ададлашдир (тиражлашдир). Тадқиқот этиш учун ҳимоя қилишнинг аппарат воситаларига эга бўлиш дастурлига нисбатан мураккаброкдир, бундай хавф КТ техник таркибини бутунлигини таъминлайдиган воситалар ва усуллар билан блокировкаланади.

КТ да тақиқланган ахборотни тадқиқот қилиш ва нусхалашни блокировкалаш учун ахборотни тадқиқот қилишдан ва нусхалашдан ҳимоя қилиш воситалари ва чоралари (ТҚНХҚВ) ишлатилади.

Шундай қилиб, мурожаат қилишни чеклаш тизими ва тадқиқот қилишдан ва нусхалашдан ҳимоя қилиш тизими АТМҚ дан ҳимоя қилиш тизимининг қисмининг тизимлари каби қаралиши мумкин.

АТМҚ уч жиҳатини кўриб чиқамиз:

1. Тармоқларга ва тармоқлар ресурсларига тақиқланган мурожаат қилиш;
2. Маълумотларни ва дастурларни очиш ва ўзгартириш;
3. Графикни очиш, ўзгартириш ва алмаштириб қўйиш.

ТМҚ дан ахборотни ҳимоя қилиш муаммоси локал ва айниқса, глобал тармоқларни кенг тарқалиши билан жуда кескинлашди. Мутахасисларнинг фикрича, хакерларнинг асосий мақсади катта миқдордаги кириш номларини ва паролларини йиғиш ҳисобланади. Лекин қоидага кўра тижорат сирлари хакерларни жуда қизиқтирмасада, чидаб бўлмайдиган компьюютер жиноятлари маълумдир (В. Левин 1994 йилнинг 30 июнидан 3 октябригача Санкт Петербургда жойлашган ўзининг компьютеридан ва бегона шахсларнинг ҳисоб рақамларига АҚШ нинг «Сити банки»дан 40 дан ортиқ пул ўтказишларни амалга оширди). [26; 125-140]

Бир нечта статистик рақамлар. АҚШ да ҳар йили компьютер жиноятчилигидан келадиган йўқотишлар 100 млрд. доллардан ортиқ, ғарбий Европада эса 30 млрд. доллардан ортиқ деб баҳоланади.

Битта компьютер жиноятчилигидан келадиган ўртача ва максимал талофат мос равишда 450000 ва 1 млрд. долларни ташкил этади. АҚШ нинг 80 % дан ортиқ компаниялари ва агентликлари маълумотлар хавфсизлигини етарлича таъминламаганликлари учун молиявий зарарлар кўрмоқдалар.

4.2.1.2. Тармоқларга ва тармоқ ресурсларига рухсат этилмаган мурожаат қилиш

Ҳисоблаш тармоқларида кучсиз жойлар сифатида қуйидагиларни кўриб чиқиш мумкин:

- юклаш вақтида паролли ҳимоя қилишга эга бўлмаган компьютерларни қўллаш;

- қўшма ва енгил очиладиган паролларни ишлатиш;
- паролларни пакетли файлларда ва компьютерларнинг дискларида сақлаш;
- ҳақиқий вақт оралиғида фойдаланувчиннг ҳақиқийлигини ўрнатишни йўқлиги;
- фойдаланувчиларни идентификациялаш ва аутентификациялаш тизимини қўлланишини йўқлиги ва паст самарадорлиги;
- тармоқ қурилмалари устидан физик назоратни етарли эмаслиги;
- алоқа тармоқларини ўрнатишни кўп сонли муваффақиятсиз уринишларида ва бундай уринишларни қайд қилишда терминални ўчиб қолишини йўқлиги;
- модемларни ҳимоя қилинмаганлиги.

Тақиқланган ишлатишлардан компьютер тармоқларини ёки алоҳида компьютерларни ҳимоя қилиш учун мурожаат қилишнинг учта асосий кўриниши ишлатилади.:

1. Фойдаланувчига тегишли бўлган предметларга эга бўлишга асосланган мурожаат қилишни назорат қилиш (физик калит), англагичнинг тирқишига қўйиладиган магнитли карта, металл плас-тинка ва ҳ.к.).

2. Фойдаланувчининг шахсий тавсифларига асосланган мурожаат қилишни назорат қилиш. Биометрик асбоблар фойдаланувчининг физик хусусиятларини (имзоси, товуш йўғонлиги, бармоқ излари, кафтдаги чизиқларнинг ёки кўз қорачиғидаги расм ва ҳ.к.) таҳлил қилади ва уларни ўзининг хотирасидаги маълумотлар билан солиштиради.

3. Махсус ахборотга (одатда пароль) эга бўлишга асосланган мурожаат қилишни назорат қилиш.

Пароллар одатда, тизимга кириш учун калит сифатида ишлатилади, улар бошқа мақсадлар учун ишлатилади: дискка ёзишни блокировкалаш, маълумотларни шифрлашдаги буйруқларда, яъни мос ҳаракатлар фақатгина дастур таъминотининг қонуний эгалари ва фойдаланувчилари томонидан амалга оширилишига қатьий ишонч талаб этиладиган барча ҳолатларда.

Ишлатиладиган паролларни қуйидаги гуруҳларга ажратиш мумкин:

- фойдаланувчи томонидан ўрнатиладиган пароллар;
- тизим ишлаб чиқарадиган пароллар:
- тизим ишлаб чиқарадиган мурожаат қилишнинг тасодифий кодлари:
- яримта сўз;
- таянч иборалар;
- «савол-жавоб» туридаги интерфаол кетма-кетликлар;
- «қатъий пароллар».

Фойдаланувчи томонидан ўрнатиладиган пароллар энг кўп тарқалган гуруҳдир. Кўпчилик ҳолатларда бундай паролни фойдаланувчининг ўзи ўрнатади, пароль етарлича узун бўлиши керак. Муваффақиятсиз паролни яратишга имкон бермайдиган усуллар бор. Масалан, тизим пароль ўз ичига ёзма ва босма ҳарф-ларни рақамлар билан аралашганини олишини талаб этиши мумкин; очиқдан-очиқ пароллар тизим томонидан инкор қилинади. Турли хил ОТ ларда файлларни пароллар билан кўриб чиқадиган, уларни таҳлил қиладиган ва тўғри келмаганларини алмаштирадиган кўплаб дастурлар мавжуддир.

Тасодифий пароллар ва кодлар тизим томонидан ўрнатилади. Тизимли ДТ белгиларнинг тасодифий кетма-кетлигини тўлиқ ишлатилиши мумкин - регистрларни, рақамларни, узунликларни тасодифий танлашгача; ёки ишлаб чиқарадиган жараёнларда чекланишларнинг ишлатиш керак.

Яримта сўз қисман фойдаланувчи, қисман тасодифий жараён томонидан яратилади. Агар фойдаланувчи енгил топиладиган пароль ўйлаб топса, компьютер унга, янада мураккаб паролни ҳосил қилиб, бирорта тушунмовчиликлар билан тўлдиради (масалан, абзац-абзац 5.а32).

Таянч иборалар узун бўлиб уни топиш мураккабдир, лекин осонгина эслаб қолиш мумкин. Иборалар маънодор бўлишлари мумкин ёки умуман маънога эга бўлмаслиги мумкин. Таъкидлаш керакки, дастурлаштиришда янада кенг ишлатишга ўтиш йўналиши доимий кузатилмоқда. Таянч иборалар йўналишга кодли акроним йўналиши янада яқиндир, у бирмунча қисқадир, лекин паролнинг идеал хавфсиз шаклидир (Windows операцион тизими JCW 424 графикли интерфейсига эгадир).

«Савол-жавоб» туридаги интерфаол кетма-кетлиги фойдаланувчига, қоидага кўра шахсий режадаги бир нечта саволларга жавоб беришни таклиф этади. Компьютерда бундай саволларнинг бир нечтасига жавоблар сақланади. Фойдаланувчи тизимга кирганда компьютер олинган жавобларни «тўғрилари» билан солиштиради. «Саволлар-жавоблар» ни ишлатадиган тизимлар фойдаланувчи ишини ҳар ўн минутда тўхтатиб туради, бунда у унинг ҳуқуқини тизимдан фойдаланишини тасдиқлаш учун саволларга жавоб беришни таклиф этади.

Қатьий пароллар одатда бирорта ташқи электрон ёки механиқ қурилма билан бирга ишлатилади. Бу ҳолда компьютер таклифларнинг бир нечта вариантини таклиф этади, фойдаланувчи эса уларга тўғри келадиган жавобларни бериши керак. Паролларнинг бу кўриниши кўпинча бир марталик кодли тизимларда учрайди. Бир марталик кодлар ҳақиқий фойдаланувчи тизимга биринчи марта киришида ишлатилиши мумкин; кейин фойдаланувчи ўзининг паролини янада махфийроқ шахсий код билан алмаштирилиши керак. Тизимдан кишилар гуруҳи фойдаланган, лекин бунда махфийликни бузиш мумкин бўлмаган ҳолларда, бир марталик кодларнинг рўйхатига мурожаат қилинади. У ёки бу фойдаланувчи вақтга, санага ёки хафтанинг кунига мос келадиган код киритади.

Шундай қилиб, паролнинг ишончлиги маълум бир талабларни бажарилиши билан таъминланади:

- маълум бир узунликда бўлиши керак ;
- ўз таркибига ҳам ёзма, ҳам босма ҳарфларни олиши керак ;
- ўз таркибига битта ва ундан ортиқ рақамларни олиши керак ;
- ўз таркибига битта рақамсиз ва битта алфавитсиз белгини олиши керак.

Бу қоидалардан биттасига ёки бир нечтасига албатта риоя қилиш керак.

4.3-расмда тармоқларга ва тармоқ ресурсларига тақиқланган мурожаат қилиш схемаси кўрсатилган.

Тармоқларга тақиқланган мурожаат қилиш шу билан тавсифланадики, бирор-бир субъект, тармоқнинг кучсиз жойларини ишлатган ҳолда, «қонуний» фойдаланувчининг ҳуқуқлари билан тармоққа мурожаат этадилар.

Тақиқланган тармоқ ресурсларига мурожаат қилиш иккита сабаб бўйича бўлиши мумкин: тармоқ ресурсларига мурожаат қилиш ҳуқуқи етарлича аниқланмаган ёки мурожаат қилишларни ва ваколатларни бошқариш механизми аниқлик даражасига эга эмас. Қоидага кўра, амалиётда, етарлича кўпинча фойдаланувчиларга, тармоқ ресурсларига мурожаат қилиш бўйича янада кенгрок ваколатларни ўрнатади, бу эса ахборот хавфсизлигини зарарига олиб келади.

Ҳисоблаш тармоқларининг ресурсларига мурожаат қилишни кучсиз томонларига қуйидагиларни киритиш мумкин:

- ✓ фойдаланувчиларнинг ҳуқуқларини белгилашда ваколатларнинг йўл қўйилмайдиган кенг спектрини тизимли ўрнатишларини ишлатиш;
- ✓ тармоқ маъмуриятини ваколатларини ноқонуний ишлатиш;
- ✓ фойдаланувчи учун ваколатларни белгилаш механизмини нотўғри ишлатиш;
- ✓ файллар даражасида мурожаат қилишни назорат қилиш механизмисиз компьютерларни ишлатиш;
- ✓ маълумотларни ҳимоясиз ёки унинг етарли бўлмаган даражада сақлаш.

Компьютер жиноятчилигини амалга оширадиган шахслар учта тоифага бўлинадилар: қароқчилар-дастурларни ва маълумотларни ноқонуний версияларини яратиб муаллифлик ҳуқуқини бузадилар; хакерлар-бошқа фойдаланувчиларнинг компьютерларига ва улардаги файлларга ноқонуний мурожаат қилиш ҳуқуқига эга бўладилар, лекин улар тизим устидан ўзининг устунлигини англашдан қаноатланган ҳолда файлларни бузмайдилар ва нусхаламайдилар; кракерлар (бузувчилар)- ўзларига барча имкониятларга йўл қўядилар ва энг жиддий бузғунчилар ҳисобланадилар. Одатда хакерлар компьютер тизимига стандарт схема бўйича кириб оладилар:

Кириш осон бўлган машиналарни аниқлаш - тизимга кириш -ўзининг ҳолатларини мустахкамлаш.

Бу жараённинг оддий қисми бўлиб, кириш осон бўлган компьютерни топишдир. Улар тўғрисидаги хабарларни .zhosts ва .net25 кенгайтмали файллардан олиш мумкин. Улар олдиндан бузилган тизимларни, ёки иерахик тақсимланган маълумотлар базаси бўлган номларнинг домен тизими DNS (Domein Name System) ёрдамида исталган тизимдан исталган фойдаланувчига эркин кириш имконини беради.

DNS компьютерларнинг номерларини уларнинг Internet тармоғидаги сонли манзилларига ўзгартиришни таъминлайди. Zone transfer (зонали ахборотни сўроқлаш) ўз ичига компьютерларнинг номларини, уларнинг тармоқли манзилларини ва компьютер тўғрисидаги хизмат маълумотларини олади. DNS нинг бу хусусиятларидан хакерлар фойдаланадилар.

Тизимга кириш масаласи (бузиш) мураккаброк ечилади. Кўпчилик кўп фойдаланувчили тизимлар фойдаланувчини идентификациялаш воситаларига эга (одатда фойдаланувчи номи ва кириш пароли). Фойдаланувчиларниг номлари одатда маълум бўлади, агар номалум бўлса уларни турли хил ахборотли утилитларни ишлатган ҳолда уларни олиш мушкул эмасдир. Кириш пароллари

махфийлаштирилгандир ва мантиқдан келиб чиққан ҳолда барча мумкин бўлган вариантларни танлаб чиқиш камдан-кам ҳолларда муваффақиятли чиқади: комбинация жуда кўпдир, login дастури секин ишлайди ва одатда учта муваффақиятсиз уринишлардан кейин чизиқни узиб ташлайди. Шунинг учун янада самарали натижалар учун бузғунчилар кўпчилик тизимлар тақдим этадиган тармоқ воситаларига мурожаат этадилар.

4.3-расм. Тармоқларга ва тармоқ ресурсларига рухсат этилмаган мурожаат қилиш

Ўзининг аралашувлари изларини беркитиш учун қуйидаги усуллар ишлатилади:

- тизимнинг файл-прототурларини ўзгартириш ёки ўчириб ташлаш;
- буйруқларни масофадан туриб бажариш воситаларини ишлатган ҳолда (REXEC) масофадан туриб кириш чекланишларини четлаб ўтиш. Бу воситалар фойдаланувчига узоқда жойлашган компьютерда буйруқларни бажариш имконини беради. Бунда баённомаларнинг файлларида ёзувлар қолмайди.

Тизимга билдирмасдан татбиқ этишни умумий воситаси, баённомаларнинг файлларини нусхалаш учун буйруқларни масофадан туриб бажариш воситаларини ишлатиш ва кейинчалик масофадан кириш ёрдамида тизимга кириб олиш ҳисобланади. Ўзининг вазиятларини мустахкамлаш учун ишлатади:

- .zhosts файлларини маълум бўлган фойдаланувчиларнинг ўзларининг каталогларига ёзиш, маълумки, zhosts файллари исталган тизимдан исталган фойдаланувчига эркин мурожаат этишга рухсат беради;

- тизимнинг икқилик бажариладиган файлларини тўғриланган вариантлари билан алмаштириш. Хакер «SU» ва «newqrp» буйруқларини махсус версияларига алмаштириши мумкин, улар унга махсус пароль кўрсатилганда устун турадиган амалий қобиқни тақдим этади. Кўпинча киришга пароль сўрайдиган дастурлар алмаштирилади. Бу дастурлар оддийлари каби ишлашни давом эттиради, лекин киритилган паролларни фақатгина хакерга маълум бўлган махсус файлга ёзади.

4.2.1.3. Маълумотларни ва дастурларни очиш ва ўзгартириш

4.4- расмда маълумотларни дастурларни очиш ва ўзгартиришни шартли равишда кўрсатилган.

Маълумотларни тезкор хотирадан ёки ҳисоблаш тармоқларининг дастурларидан очиш, уларга тармоқнинг деярли исталган фойдаланувчиси мурожаат қилиши мумкин бўлгандагина мумкиндир. Бундан ташқари, сирли ахборот монитор экранини, бевосита ёки махсус қабул қилувчи қурилмаларни бирор масофадан туриб ишлатиш билан, кўриш йўли билан, ҳамда шифрланмаган маълумотларнинг ва ҳужжатларнинг ёзувларидан чиқариб олиниши мумкин.

Маълумотларни ва дастурларни очишда кучсиз жойлари сифатида таъкидлаш мумкин:

а) тармоқ маъмурияти томонидан нотўғри бошқариш ва маълумотларга бошқаришни ўрнатиш;

б) маълумотлар базасига ва дастурли таъминотга мурожаат этишни ҳи-моя қилинмаганлиги;

в) маълумотларни шифрланмаган кўринишда сақлаш;

г) бегона шахслардан ҳимоя қилинмаган жойларда мониторларни ва принтерларни ўрнатиш;

Маълумотларни ишончли ва самарали архивлаш тизимини ташкил этилиши тармоқда ахборотнинг сақланишини таъминлайди. Унча катта бўлмаган тармоқларда (1-2 серверли) серверларнинг бевосита бўш слотларига архивлаш тизимини ўрнатиш қўлланилади. Йирик корпоратив тармоқларда ажратилган махсус архивли серверни ташкил этиш мақсадга мувофиқдир.

Алоҳида муҳимлик касб этган ахборотларни сақлаш махсус қўриқланадиган хоналарда (бошқа биноларда) ташкил этилиши керак.

Ўзгартириш тақиқланган ўзгартиришларда ўринлидир. Вақт бўйича етарлича узоқ муддатларда маълумотларни сезиларсиз ўзгариши барча мавжуд бўлган ахборотни бутунлигини жиддий бузилишига келиши мумкин. Буйруқли

файллардаги, сервисли ва амалий дастурлардаги ўзгаришлар, ҳамда уларни вируслар билан зарарланиши маълумотларни уларни қайта ишлашда бузадилар ва хаттоки тизимларни ва хизматларни тармоққа мурожаат қилиш тартибини бузадилар.

Бунда энг кенг тарқалган кучсиз жойлар қуйидагилардир:

а) ДТ га киритилаётган ўзгаришларни пайқашни имкони йўқлиги;

б) Фойдаланувчиларнинг кенг оммасига ахборотга мурожаат қилишнинг асосланмаган ваколатларини, шу жумладан ёзишга, бериш;

в) Вирусларни аниқлаш ва уларни даволаш воситаларини йўқлиги;

г) Махфий маълумотларни криптографик назорат йиғиндисини йўқлиги.

4.4-расм. Маълумотларни ва дастурларни очиш ва ўзгартириш

Принципнинг моҳияти қуйидагичадир. Криптографик алгоритм ва махфий калит ёрдамида файлнинг мазмуни асосида MAC нинг бошланғич қиймати ҳисобланади, у хотира қурилмасида сақланади. Зарур бўлганда файлнинг бутунлигини текшириш ўша махфий калитни ишлатган ҳолда MAC ни қайта ҳисоблаш амалга оширилади. MAC нинг бошланғич ва такрорий қийматлари мос келган ҳолда ўзгартиришларни йўқлиги тўғрисидаги карор қўлланилади.

Тақиқланган узатилаётган ўзгаришларни пайқаш учун электрон- рақамли имзолаш (ЭРИ) тизими ишлатилиши мумкин. Бу тизимнинг ишлаш моҳияти қуйидагичадир.

ЭРИ ни шакллантириш учун очиқ ва махфий калитли криптографик алгоритмлар ишлатилади. Очиқ калитли криптографик тизимда узатилаётган хабарнинг ЭРИ жўнатувчининг махфий калити ёрдамида шакллантирилади. Олинган ЭРИ ва хабар хотира қурилмасида (ХҚ) сақланади ёки олувчига узатилади. Қабул қилувчи томонидан ЭРИ имзони яратувчининг умумий мурожаат қилинадиган, очиқ калити ёрдамида текширилиши мумкин. Агар имзо бир хил маъноли бўлса, унда қабул қилинган хабарнинг сақланганлиги тўғрисидаги қарор қабул қилинади.

Бундан ташқари, маълумотларни ва хабарларни бутунлилик механизмлари вирусларни пайқаш, фойдаланувчилар томонидан тармоққа мурожаат қилишнинг енгилликларини ва ҳуқуқларини ишлатишни қатъий назорат қилишни таъминлаш учун муҳим роль ўйнаши мумкин.

Бу механизмлар ахборотни ҳимоя қилишнинг қуйидаги восита ва жараёнларини ишлатган ҳолда амалга оширилиши мумкин:

- хабарларни аутентификациялаш кодларини ишлатиш;
- ЭРИ ни қўллаш;
- енгилликларни қабул қилинган механизмини аниқ бажариш;
- фойдаланувчи томонидан мурожаат қилишни бошқариш учун мос ҳуқуқларни белгилаш;
- вирусларни пайқаш учун ДТ ни ишлатиш;
- файлларни ва ДТ ни локал сақлашни бартараф этиш.

4.2.1.3. Трафикни очиш, ўзгартириш ва алмаштириш

Трафик - бу ҳисоблаш тармоғининг узатадиган муҳити бўйича айланадиган маълумотлар оқимига киради.

Трафикни очиш кабелли узатиш линиясига уланиш; эфирга узатилаётган ахборотни ушлаб олиш; тармоқли таҳлилаторнинг тармоғига уланиш ва ҳ.к. йўли билан амалга оширилиши мумкин. Бунда паролларни, тизимли номларни ва фойдаланувчиларнинг номларини, электрон почта хабарларини ва амалий кўринишдаги бошқа маълумотларни очиш мумкин бўлади.

Бундай хавфни тармоқли трафикка таъсир этиш самарадорлиги сақланаётган ва узатилаётган ахборотнинг ҳимоя қили-нишига адекват бўлмаган эътиборни кучига мос равишда ортади. Масалан, пароллар тизимда шифрланган кўринишда сақланади, шахсий компьютердан файлли серверга эса очиқ кўринишда узатилади. Сақланишида, мурожаат қилишга қатъий чегара қўйилган электрон почта хабарлари эса ҳисоблаш тармоғининг узатиш линиялари бўйича очиқ кўринишда узатилади.

Трафикни очишдаги энг кучсиз жойларни санаб утамиз:

а) алоқа каналлари бўйича шифрланмаган маълумотларни узатиш;

б) умумий мурожаат қилинадиган узатиш баённомаларини ишлатган ҳолда очилган маълумотларни узатиш;

в) узатиш қурилмаларини ва муҳитни етарлича физик ҳимоя қилинмаганлиги.

Фойдаланувчилар ўзаро алмашадиган маълумотлар тақиқланган ўзгаришларга дучор бўлмасалар ҳам, трафик ўзгартирилиши ёки алмаштирилиши мумкин. Хабарнинг исталган қисмини, жўнатувчининг ва олувчининг манзилли ахборотини қўшган ҳолда, маълумотларни ўзгартириш ўринлидир.

Трафикни алмаштириш, бузғунчи хабарларни жўнатувчиси ёки олувчиси остида ниқобланган ҳолда бўлиб ўтади. Агар жўнатувчиси остида бўлса - хабарнинг манзилли қисмини ҳақиқий жўнатувчининг манзили билан алмаштириш бўлиб ўтади, агар олувчиси остида бўлса - бузғунчи ўзининг манзилини ҳақиқий хабар олувчи каби тасвирлаш масаласини ҳал қилади. Иккала ҳолатда ҳам хабарларни, кейинчалик уларнинг мазмунларини алмаштириб, ушлаб олиш кўзда тутилади. Бу ҳаракат трафикни ишлатиб куриш номини олган.

Трафикни ўзгартиришдаги ёки алмаштиришдаги кучсиз жойларнинг баъзи бир турлари қуйидагилардир:

- трафикни ишлатиб кўришдан ҳимоя қилишнинг йўқлиги;
- трафикни очиқ кўринишида узатиш;
- хабарларда юборишнинг санаси ва вақти тўғрисидаги белгиларни йўқлиги;
- хабарларни ва ЭРИ ларни аутентификациялаш механизмини йўқлиги.

Хулоса қилиб, ШЭҲМ ларини АТМҚ дан ҳимоя қилишнинг замонавий тизимларида тўхталиб ўтамиз.

КТ ларини АТМҚ дан ҳимоя қилинганлигини оширадиган алоҳида дастурларга мисоллар сифатида Norton Utilities пакетларидан келтириш мумкин, буларга дискка ёзишда ахборотни шифрлаш дастури Diskreet ёки Secretdisk, дискдан ахборотни ўчириш дастури Wipcinfo, дискларга мурожаат қилишни назорат қилиш дастури DiskMonitor ва бошқа мисол бўла олади.

Россия ишлаб чиқувчилари томонидан «Снег-1.0», «Кобра» «Страж-1.1» ва бошқа ШЭҲМ ларни ҳимоя қилишнинг дастурли тизимлари таклиф этилмокда. Ҳимоя қилишнинг аппарат-дастурли воситаларига мисол сифатида «Аккорд-4», «Dallas Lock 3.1», «Редут», «ДИЗ-1» тизимларини келтириш мумкин. Ҳимоя қилишнинг аппарат-дастурли комплекслари ҳимоя қилиш механизмларининг максимал сонини амалга оширади: идентификациялаш ва аутентификациялаш; файлларга, каталогларга ва дискларга мурожаат қилишларни чеклаш; дастур воситаларини ва ахборотни бутунлигини назорат қилиш; фойдаланувчининг функционал ёпиқ муҳитини яратиш имконияти; ОТ ни юклаш жараёнини ҳимоя қилиш; фойдаланувчи йўқ вақтда ШЭҲМ ни блокировкалаш; криптографик ўзгартириш; ҳодисаларни қайд қилиш; хотирани тозалаш. Дастурли тизимлар идентификаторлар сифатида, кўпроқ, резидент дастурлар билан ушлаб олиниши мумкин бўлган паролларни ишлатадилар.

АТМҚ дан аппарат дастурли АҲҚКТ четлаб утиш мураккаброқ бўлган электрон идентификаторларни (Touch Memory) ишлатадилар. Идентификациялаш ва аутентификациялаш тизимини батафсилроқ кўриб чиқамиз.

4.3. Идентификациялаш ва аутентификациялаш

тизимлари тўғрисида тушунча

Идентификациялаш ва аунтетификациялаш тизимлари объектга мурожаат қилишда қисмининг тизимлари ёки ахборотни англаш ва мурожаат қилишни чеклаш қисмининг тизимлари ҳисобланади. Маълумки, КТ да ахборотлар жамланиб, уни ишлатишга ҳуқуқлар, шахсий ташаббускорлик тартибида ёки мансаб вазифаларига мос равишда ҳаракат қиладиган маълум бир шахсларга ёки шахслар гуруҳларига тегишлидир. Ресурсларни ахборот хавфсизлигини таъминлаш, тақиқланган мурожаат қилиш имкониятини бартараф этиш, махфий ахборотга ёки сирли ахборотга рухсат этилган мурожаат қилишни назоратини кучайтириш учун турли хил мурожаат қилишни англаш, объектни (субъектни) ҳақиқийлигини ўрнатиш ва чеклаш тизимлари татбиқ қилинади. Бундай тизимларни қуриш асосида рухсат этилган технологияларнинг мос белгилари мавжуд бўлган ахборотга фақатгина шундай мурожаат қилишларнинг принциплари ва бажарилиши ётади.

Объектга мурожаат қилишни ташкил этишда ечиладиган асосий масалалардан биттаси объектга қўйиладиган шахсларни (мурожаат қилиш субъектларини) идентификациялаш ва аутентификациялаш ҳисобланади.

Идентификациялаш - мурожаат қилиш субъектларига идентификаторларни тақдим этиш ва (ёки) кўрсатилган идентификаторларни, эгалари (ташувчилари) объектга киришга рухсат этилган, олдиндан тақдим этилган идентификаторлар рўйхати билан таққосланади.

Аутентификациялаш - мурожаат қилиш объектларини улар кўрсатган идентификаторларга тўғри келишлигини текшириш, ҳақиқийлигини тасдиқлашдир.

Инсонларни идентификациялашни атрибутив ва биометрик усуллари мавжуддир.

Атрибутив усул мурожаат қилиш субъектига ёки ноёб предметни, ёки паролни (кодни), ёки кодни ўз ичига олган предметни беришни кўзда тутади. Идентификаторлар мурожаат қилиш жараёнини автоматлаштириш имконини бермайди, шахсиятни идентификациялаш ва аутентификациялаш субъектив характерга эгадир.

КТ қурилмаларига мурожаат қилишни чекловчи тизимларда пароллар ва кодлар ишлатилади. Идентификаторлар энг истиқболли ҳисобланади, улар мурожаат қилиш субъектини идентификацияли кодини, ўзида сақлаган ахборотнинг материал ташувчили, масалан пластик картали, кўринишга эгадир. Код фақатгина махсус қурилма ёрдамида ўқилади. Карта коддан ташқари фотосуратни, эгаси тўғрисидаги маълумотларни ва ҳ.к. ўзида сақлаши мумкин.

Атрибутив идентификаторларнинг камчилиги - эгасининг шахсияти билан кучсиз алоқа ёки алоқанинг йўқлиги. Бу камчиликлардан биометрик идентификациялаш усуллари халосдир, улар инсоннинг шахсий биологик хусусиятларини ишлатишга асослангандир: бармоқларнинг капиляр нақшлари, кўз тўрининг нақшлари, қўл панжаларининг шакли, нутқ хусусиятлари, юзнинг шакллари ва ўлчамлари, имзо динамикаси, клавиатурада ишлаш ритми, тана ҳиди, тананинг термик тавсифлари.

Биометрик идентификациялаш усулларининг асосий афзалликлари тақиқланган мурожаат қилишга интилишларни пайқашни жуда юқори эҳтимоллиги ҳисобланади. Хатто энг яхши тизимларда ҳам, мурожаат қилиш ҳуқуқига эга бўлган субъектни мурожаат қилишини нотўғри инкор қилишини эҳтимоли 0,01 ни ташкил этади. Мурожаат қилишни биометрик усулларини таъминлаш ҳаражатлари атрибутив усулларни ташкил этиш ҳаражатларидан сезиларли ошади. Шунинг учун, айтиш мумкинки, ҳозирча алоҳида биометрик усуллар амалий характерга нисбатан кўпроқ реклама характерига эгадир.

Ахборот хавфсизлигини таъминлаш бўйича жадал ишлаб чиқилаётган йўналишлардан биттаси электрон-рақамли имзолаш (ЭРИ) асосида ҳужжатларни идентификациялаш ва ҳақиқийлигини ўрнатишдир.

ЭРИ криптографик ўзгартириш ёрдамида шифрлаш усули кўринишига эгадир ва у пароль ҳисобланади, бу пароль узатилаётган хабар маъзмунига, жўнатувчига ва олувчига боғликдир. Такрорий ишлатишдан огоҳлантириш учун имзо бир хабардан иккинчисига ўтганда ўзгариши керак.

Аутентификациялаш ишончлигини ошириш учун бир нечта идентификаторлар ишлатилади.

4.4. Ахборотни ҳимоя қилишнинг моделлари

Хулоса қилиб, ахборотнинг ҳимоя қилишнинг тизимини шакллан-тиришни асосий мезонларини компьютер тармоқларидаги ахборотни ҳимоя қилиш моделларида умумлаштирамиз.

Тармоқларнинг ахборот ва аппарат ресурсларини хавфсизлигини таъминлайдиган иккита модел кенг ишлатилади: пароль орқали ҳимоя қилиш, мурожаат қилиш ҳуқуқи орқали ҳимоя қилиш. Бу моделларни яна биргаликда ишлатиладиган ресурслар (resoursce level - пароль орқали ҳимоя қилиш) даражасида ҳимоя қилиш ва фойдаланувчи (user level - мурожаат қилиш ҳуқуқи орқали ҳимоя қилиш) даражасида ҳимоя қилиш деб ҳам аталади.

4.4.1. Ресурсга мурожаат қилиш пароли.

Биргаликда ишлатиладиган ресурсларни ҳимоя қилиш усулларидан биттаси - ҳар бир умумий мурожаат қилинадиган ресурсга паролларни тақдим этиш ҳисобланади. Ресурсга бундай мурожаат қилиш фақатгина паролни тўғри киритганда мумкиндир. Кўпчилик тизимларда ресурслар, мурожаат қилишнинг турли турлари билан биргаликда ишлатишда тасвирланиши мумкин. Масалан, каталогларга фақат ўқиш учун мурожаат қилиш, тўлиқ мурожаат қилиш ва паролга боғлиқ равишда мурожаат қилиш мумкиндир.

Фақат ўқиш учун (read only) **мурожаат қилишни** ишлатганда паролни биладиган ходимлар барча файлларни ўқиши, ҳужжатларни кўриб чиқиши, уларни ўз машинасига нусхалаши мумкин, лекин бошланғич ҳужжатни ўзгартира олмайдилар.

Тўлиқ мурожаат қилишда (full access) барча файлларни кўриб чиқиш, ўзгартириш ва ўчириш мумкиндир.[25; 80-84]

Паролга боғлиқ равишда мурожаат қилишда (depending on password) биргаликда ишлатиладиган каталогга икки даражали пароль тақдим этилади: фақат ўқиш учун ва тўлиқ. Фақат ўқиш учун паролни биладиган ходимлар фақатгина маълумотларни ўқишлари мумкин, тўлиқ мурожаат қилиш паролини биладиганлари эса мос равишда тўлиқ мурожаат қилишга эга бўладилар.

4.4.2. Мурожаат қилиш ҳуқуқлари

Мурожаат қилиш ҳуқуқи орқали ҳимоя қилишнинг моҳияти ҳар бир фойдаланувчига ҳуқуқларнинг маълум бир тўпламини тақдим этишдадир. Тармоққа киришда фойдаланувчи паролни киритади. Сервер хавфсизликнинг маълумотлар базасида фойдаланувчининг ҳуқуқларини текшириб, тармоқ ресурсларига мурожаат қилишни таъқиқлайди ёки рухсат беради. Мурожаат қилиш ҳуқуқини ишлатиб ҳимоя қилиш биргаликда ишлатиладиган ресурсларга мурожаат қилишни бошқаришни янада юқори даражасини, ҳамда пароль билан ҳимоя қилишга қараганда хавфсизликнинг янада қаттиқ режимини таъминлайди.

Фойдаланувчининг номини ва паролини текшириб ва тасдиқлаб, тармоқнинг хавфсизлик тизими унга мос ресурсларга мурожаат қилишга рухсат беради. Ҳуқуқларга мос равишда фойдаланувчи турли киришларга мурожаат қилиши мумкин, бу киришлар фойдаланувчига катта ёки кичик ҳуқуқларни тақдим этадилар.

Ҳар бир ажратилган ресурс ёки файл фойдаланувчилар ёки гуруҳларнинг рўйхати билан биргаликда сақланади, бу рўйхатга уларнинг ҳуқуқлари (киришлари) киритилгандир. Windows NT Server серверининг каталоглари учун баъзи бир турик ҳуқуқлари қуйидаги 4.1-жадвалда келтирилган.

Тармоқли ҳимоя қилиш даражасини қўшимча ҳимоя қилиш усулларини, масалан, аудиторлик ва дисксиз моделлар, ишлатиб ошириш мумкин.

Аудит (auditing) - бу сервернинг хавфсизлик журналига (security log) маълум бир ҳодисаларни ёзишдир. Бу жараён тармоқдаги фойдаланувчи ҳаракатини кузатиб боради. У тармоқни ҳимоя қилишнинг бир қисми каби қабул қилинади, чунки хавфсизлик журналида маълум бир ресурслар билан ишлаган ёки уларга мурожаат қилишга интилган барча фойдаланувчиларнинг номлари акс эттирилган. Бундан ташқари, баъзи бир ресурсларни ишлатгани учун тўлов ҳақидаги ахборотни хавфсизлик журналидан топиш мумкин.

4.1-жадвал

Windows NT Server серверининг каталоглари учун баъзи бир турик ҳуқуқлари

Ҳуқуқ	Мазмуни
Read	Биргаликда ишлатиладиган каталогдан файлларни ўқиш ва нусхалаш
Execute	Каталогдан дастурларни ишга тушириш (бажариш)

Write	Каталогда янги файлларни яратиш
Delete	Каталогдан файлларни ўчириш
No Access	Каталогга, файлга ёки ресурсга мурожаат қилишни таъқиқлаш

Аудит турли характердаги ҳаракатларни қайд қилади: тармоққа киришга ёринишлар, ресурсларга уланиш ва улардан езилиш, уланишларни узиб қўйиш, ҳисобот ёзувларини блокировкалаш, файлларни очиш ва ёпиш, файлларни ўзгартириш, сервердаги ҳодисаларни ўзгартириш, паролларни ўзгартириш, қайд қилиш параметрларини ўзгартириш.

Аудит тармоқнинг ишлашини кўрсатади. Журнал маъмурият томонидан ҳисоботларни тайёрлаш учун ишлатилиши мумкин, унда исталган яратилган ҳаракатлар, ҳамда уларни амалга оширилганини санаси ва вақти акс эттирилади.

Дисксиз (diskless) компьютерлар эгилувчан ёки қаттиқ диск-ларнинг юритмасига эга бўлмайди. Улар дискли компьютерлар бажарган вазифаларни бажара оладилар, лекин маълумотларни локал эгилувчан ёки қаттиқ дискларда сақлай олмайдилар. Хавфсизлик маъносида идеал ҳисобланади: фойдаланувчилар маълумотларни ташувчиларда сақлаш ва уни ўзлари билан олиш имкониятидан маҳрумдир. Бундан ташқари, улар тўлиқ жиҳозланганига нисбатан арзондир.

Дисксиз компьютер юкловчи дискларга мухтож эмаслар. Улар сервер билан боғланадилар ва тармоқ адаптери платаларида ўрнатилган махсус юкловчи ДЭҚҚ ёрдамида тармоққа кирадилар. Дисксиз компьютер манбага уланганда юкловчи ДЭҚҚ серверга компьютер ишга тушишлиги тўғрисида хабар беради. Сервер, юкловчи дастур таъминотини дисксиз компьютерни тезкор хотирасига узатиб ва фойдаланувчига тармоққа киришга таклифни автоматик жўнатиб, хабарга жавоб беради. Фойдаланувчи тармоққа кириши билан компьютер унга уланади.

Шундай қилиб, хулоса қилиш мумкинки, ахборотни ҳимоя қилишнинг таклиф этилган моделлари КТ да ҳимоя қилишнинг етарли даражасини таъминлайди.

4. 5. Ахборотни ҳимоя қилишнинг криптографик усуллари

Жамиятни компьютерлаштириш, бир қатор фойдалардан ташқари, ўзи билан бир қатор муаммоларни олиб келди. Жуда ҳам мураккаб бўлган бундай муаммолардан биттаси ахборотни қайта ишлаш ва узатиш тизимларида махфий ахборотни хавфсизлигини таъминлашдадир.

Бу муаммони хал қилиш учун **ахборотни ҳимоя қилишнинг криптографик усуллари** кенг ишлатилмоқда, бунда бошланғич ахборот шундай ўзгарти-

риладики, бунинг натижасида ахборот керакли ваколатларга эга бўлмаган шахсларга танишиш ва ишлатиш учун мумкин бўлмай қолади.

Бошланғич ахборотга таъсирни кўриниши бўйича криптографик ўзгартиришни қуйидаги усуллари мавжуд: шифрлаш, стенография, кодлаш, зичлаштириш.

Шифрлаш жараёни бошланғич ахборот устида орқага қайтадиган математик, мантиқий, комбинаторлик ва бошқа ўзгартиришларни ўтказишдир, бунинг натижасида шифрланган ахборот ҳарфларнинг, рақамларнинг, бошқа белгиларнинг ва иккилик кодларининг тартибсиз тўплами кўринишига эгадир.

Ахборотни шифрлаш учун ўзгартириш алгоритми ва калит ишлатилади. Одатда, маълум бир шифрлаш алгоритми учун ўзгартириш алгоритми ўзгармас ҳисобланади. Шифрлаш алгоритми учун бошланғич қийматлар бўлиб шифрлаш учун ахборот ва шифрлаш калити хизмат қилади. Калит бошқарувчи ахборотни ўз ичига олади, у шифрлаш алгоритмини амалга оширишда ишлатиладиган операндлар катталикларини ва алгоритмнинг маълум қадамларида ўзгартиришларни танлашни аниқлайди.

Стенография усуллари нафақатгина сақланаётган ёки узатилаётган ахборотни маъносини беркитиб қолмасдан, балки ёпиқ ахборотни сақлаш ёки узатиш омилини ҳам яшириш имконини беради. Стенографияни усулларини барчасини асосида ёпиқ ахборотни очиқ файллар ичида ниқоблаш ётади (масалан, MS DOS ОТ да EOF (ctrl Қ Z) унинг белгиси матнли файлни охирида жойлашади. ОТ нинг стандарт қурилмалари EOF белгисига етиб келганда ўқишни тўхтатадилар ва ёпиқ файлга мурожаат қилиб бўлмайди).

Стенография воситалари ёрдамида матн, тасвир, нутқ, рақамли имзо, шифрланган хабар ниқобланиши мумкин. Стенографияни ва шифрлашни комплекс ишлатиш махфий ахборотни пайқаш ва очиш масаласини ечишни мураккаблигини кўп маротаба оширади.

КТ ларида стенографияни амалий ишлатиш эндигина бошланмоқда, лекин ўтказилган тадқиқотлар унинг истиқболлигини кўрсатмоқда. КТ ларида мултимедия файлларини қайта ишлаш стенография олдида деярли чекланмаган имкониятларни очиб беради.

Ахборотни кодлаш жараёнини мазмунини бошланғич ахборотни (гаплар, сўзлар) маъновий тузилишларини кодлар билан алмаштириш ҳисобланади. Кодлар сифатида ҳарфларнинг, рақамлар-нинг, рақамлар ва ҳарфларнинг бирлашмалари ишлатиши мумкин. Кодлашда ва тескари ўзгартиришда махсус жадваллар ёки луғатлар ишлатилади. Камчилиги - кодлайдиган жадвалларни сақлашни ва тарқатишни зарурлигидир, уларни, ушлаб олинган хабарларнинг қайта ишлашнинг статистик усуллари билан кодларни очишдан сақланиш учун, тез-тез алмаштириш керакдир. Кодлаш усулини маъновий тузилишлари чекланган тўпламли тизимларда (масалан, АБТ нинг буйруқли линияларида) қўллаш мақсадга мувофиқдир.

Зичлаштириш - ахборот хажмини қисқартиришдир. Зичлаштирилган ахборот тескари ўзгартиришсиз уқилиши ёки ишлатилиши мумкин эмас. Зичлаштириш ва қайта ўзгартириш воситаларига мурожаат қила олишликни инобатга олиб, махфий ахборотни зичлаштирилган файллари кейинчалик

шифрланади. Вақтни қисқартириш учун ахборотни зичлаштириш ва шифрлаш жараёнини биргаликда ишлатиш мақсадга мувофиқдир.

4.6. Шифрлаш ва қайта шифрлаш, шифр ва калит тўғрисида тушунчалар. Уларнинг тавсифлари ва уларга қўйиладиган талаблар

Шифрлаш - криптографик ўзгартиришни асосий кўринишидир. Бу очиқ ахборотни шифрланган ахборотга (шифрматн) ўзгартириш ёки шифрланган ахборотни очиқ ахборотга тескари ўзгартириш жараёнларидир.

Очиқ ахборотни ёпиқ ахборотга ўзгартириш жараёни шифрлаш, тескариси эса - қайта шифрлаш деб аталади.

Шифрлаш усулларининг ва шифрларнинг кўплаб турлари мавжуд. Бу шифрлаш алгоритмига мос равишда очиқ ахборотни ёпиқ ахборотга орқага қайтмайдиган ўзгартиришлар тўпламидир. ЭҲМ ва КТ ларининг пайдо бўлиши ахборотни шифрлаш қайта шифрлаш учун ҳам, шифрга ҳужум қилиш учун ҳам ЭҲМ ни ишлатиш имкониятларини инобатга оладиган янги шифрларни ишлаб чиқиш жараёнини келтириб чиқарди. Шифрга ҳужум қилиш-криптотаҳлил қилиш - калитни билмасдан туриб, ва мумкинки, шифрлаш алгоритми тўғрисида маълумотлар йўқлигида, ёпиқ ахборотни қайта шифрлаш жараёнидир.

Замонавий шифрлаш усулларига қуйидаги талаблар қўйилади:

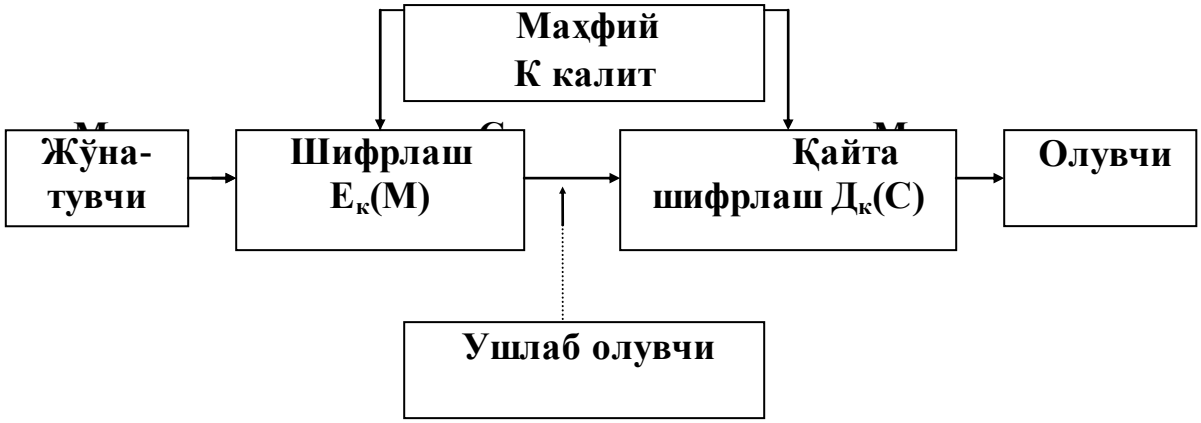
- крипточидамлилик (криптотаҳлил қилишга қарши туриш) шундай бўлиши керакки, шифрни очиш калитларини тўлиқ танлаб олиш масаласини ечиш йўли билан амалга оширилиши керак;
- крипточидамлилик шифрлаш алгоритмининг махфийлиги билан эмас, балки калитнинг махфийлиги билан таъминланади.
- шифрматн ўзи хажми бўйича бошланғич ахборотдан кўпайиб кетмаслиги керак;
- шифр хатоликлари ахборотни тўсиқларга учрашига ва йўқолишларига олиб келмаслиги керак;
- шифрлаш вақти катта бўлмаслиги керак;
- нархи беркитиладиган ахборотнинг нархи билан мослаштирилиши керак.

Криптотаҳлил қилишга сарфланадиган вақт ва восита калит узунлигига ва шифрлаш алгоритмининг мураккаблигига боғлиқ бўлади.

Кенг ишлатиладиган шифрлаш алгоритмини махфий сақлашни деярли имкони йўқдир, шунинг учун алгоритм ёпиқ кучсиз жойларга эга бўлмаслиги керак. Ахборотни ишончли яшириш учун калит узунлиги 90 битдан кам бўлмаслиги керак (масалан, 1978 йилдан буён АҚШ да давлат стандарти сифатида DES (DATA Encrypting Standard) шифри ишлатилади, алгоритм очиқ нашрда эълон қилинган. 30 млн $ турадиган супер ЭҲМ ни ишлатган ҳолда 56 битли калит 453 кунда топилиши мумкин, қўшимча 300000 $ ни сарфласа - 19 кунда, агар махсус чипни ишлаб чиқса - ҳаражатлар 300 млн. $ бўлганда 12 секундни ташкил этади).

4.7. Криптотизимнинг классик схемалари ва ишлаш моделлари

Криптотизимнинг умумлашган классик схемаси 4.6-расмда кўрсатилган.



4.6-расм. Криптотизимнинг умумлашган схемаси

Жўнатувчи бошланғич М хабарнинг очиқ матнини ишлаб чиқаради, у ҳимоя қилинмаган канал бўйича қонуний олувчига узатилиши керак. Канални, узатилаётган хабарни ушлаб олиш ва уни очиш мақсадида ушлаб олувчи кузатиб туради. Жўнатувчи орқага қайтадиган $E_к$ ўзгартириш ёрдамида М хабарни шифрлайди ва олувчига жўнатиладиган $С=E_к(М)$ шифрматни (криптограммани) олади.

Қонуний олувчи, С шифрматни қабул қилиб, тескари $Д=E_к^{-1}$ ўзгартириш ёрдамида уни қайта шифрлайди ва очиқ матн М кўринишдаги бошланғич хабарни олади:

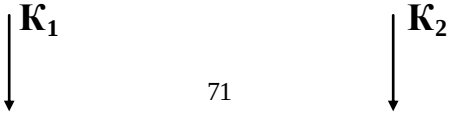
$$Д_К(С)=E_К^{-1}(М)=М$$

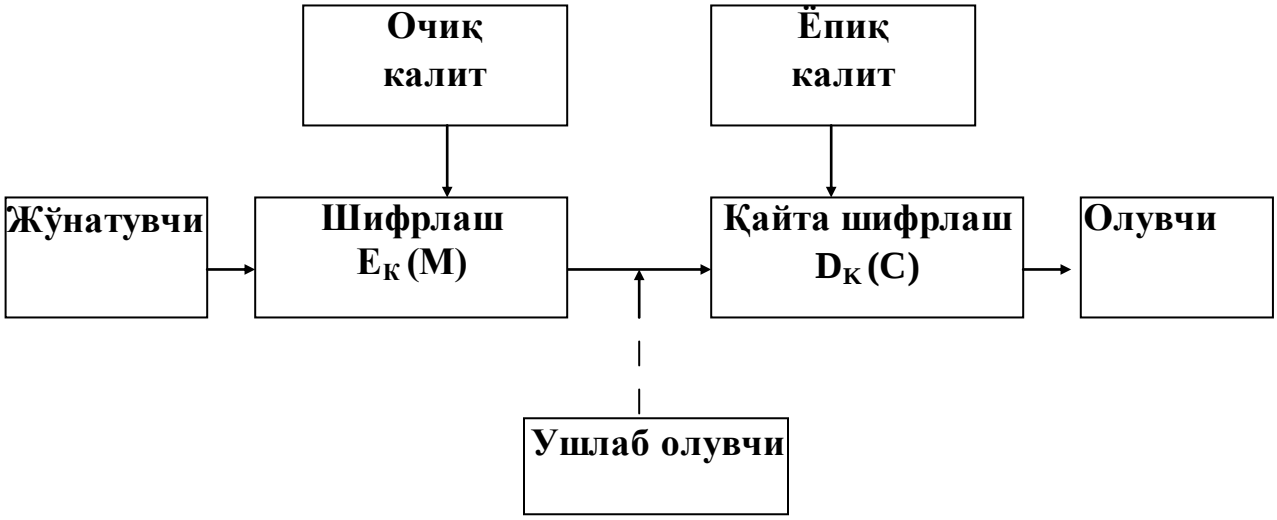
$E_К$ ўзгартириш криптографик ўзгартиришлар ёки криптоалгоритмлар тўпламидан танланади. Алоҳида ишлатиладиган ўзгартириш К калит ёрдамида танланади. Криптотизим амалга оширишнинг турли вариантларига эгадир: йўриқномалар тўплами, аппарат воситалар, компьютернинг дастурлар тупами; улар очиқ матнни шифрлаш ва очиқ шифрматнни турли усуллар билан қайта шифрлаш имконини беради, улардан биттаси аниқ бир К калит ёрдамида танланади.

Қайта шифрлашни ўзгартиришга нисбатан шифрлашни ўзгартириш симметрик ва носимметрик бўлиши мумкин Симметрикли - битта калитли, носимметрикли - иккита калитли (очиқ калитли) криптотизим синфларидир.

Битта калитли симметрик криптотизимнинг схемаси 4.7-расмда келтирилган. Унда бир хил махфий калитлар шифрлаш блокида ва қайта шифрлаш блокида ишлатилади.

Иккита калитли носимметрик криптотизимнинг умумлашган схемаси 4.8-расмда келтирилган.





4.8- расм. Очиқ калитли носимметри криптотизимнинг умумлашган схемаси

Симметрик криптотизимда махфий калит жўнатувчига ва олувчига калитлар тарқатадиган ҳимоя қилинган канал бўйича, масалан, курьер билан, узатилади. Носимметрик криптотизимда ҳимоя қилинмаган канал бўйича фақат очиқ калит узатилади, махфий калит эса уни ишлаб чиқарилган жойида сақланади.

4.8.Симметрик ва носимметрик шифрлаш усуллари, уларнинг афзалликлари ва камчиликлари. Замонавий симметрик ва носимметрик криптотизимлар

Калитларнинг белгилари ва турлари бўйича, ҳамда ўзгартириш услуби бўйича шифрлаш усулларини таснифлашни вариантларидан бирини келтирамиз (4.9- расм).

Алмаштириш (ўрнига қўйиш) усулларининг моҳияти бир алфавитда ёзилган бошланғич ахборотнинг белгиларини маълум бир қоида бўйича бошқа алфавитдаги белгилар билан алмаштиришдадир. *Тўғридан-тўғри алмаштириш усули* энг оддий ҳисобланади. Бошланғич ахборот ёзиладиган бошланғич A_o алфавитнинг S_{oi} белгилари мос равишда шифрловчи A_1 алфавитнинг S_{1i} белгиларига тўғри келтирилади. Оддий ҳолатда иккала алфавит ҳам бир белгилар тўпламидан ташкил топишлари мумкин. Масалан, иккала алфавит ҳам рус алфавити ҳарфларини ўз ичига олиши мумкин.

4.8.1. Алмаштириш усуллари

Иккала алфавитларнинг белгилари ўртасидаги мувофиқликни берилиши маълум бир алгоритм бўйича узунлиги К-та белгилардан ташкил топган

бошланғич T_o матннинг белгиларини сонли тенг кучлиларини ўзгартириш ёрдамида амалга оширилади.

Моноалфавитли ўзгартириш алгоритми қадамлар кетма - кетлиги кўринишида берилиши мумкин.

1-қадам. [1 x R] ўлчамли бошланғич A_o алфавитда тасвирланган ҳар бир S_{oi} T_o (iқ1,k) белгини A_o алфавитда S_{oi} белгини тартиб номерига мос келадиган h_{oi} (S_{oi}) сонга алмаштириш йўли билан L_{oh} сонли кортежини шакллантириш.

2-қадам. L_{oh} кортежни ҳар бир сонини L_{ih} кортежнинг қуйидаги формула бўйича ҳисобланадиган

$$\mathbf{h_{1i} \text{ к } (k_1 \text{ x } h_{0i} (S_{oi}) Қ k_2) (mod R)}$$

h_{1i} мос сонга алмаштириш йўли билан L_{ih} кортежини шакллантириш; бу ерда: k_1- ўнлик коэффициент, $к_2$ - сурилиш коэффициенти. Танланган k_1, k_2 коэффицентлар h_{oi} ва h_{1i} сонларнинг бир хил маънода мос келишини таъминлаши, h_{1i}қ0 олинганда эса h_{1i}қR алмашишини бажарилиши керак.

3-қадам. L_{1h} кортежнинг ҳар бир h_{1i} (S_{1i}) сонини ⟦1xR⟧ ўлчамли A_1 шифрлаш алфавитининг мос S_{1i} T_1 (iқ1,к) , белгиси билан алмаштириш йўли билан T_1 шифрматнни олиш.

4-қадам. Олинган шифрматн қайд қилинган b узунликдаги блокларга бўлиб чиқилади. Агар охирги блок тўлиқ бўлмаса, унда блок охирига махсус тўлдирувчи белгилар (масалан, * белгиси) жойлаштирилади. [48]

Мисол. Шифрлаш учун бошланғич қийматлар қуйидагилар:

$T_{0\ к}$ < МЕТОД - ШИФРОВАНИЯ >;

A_0 қ <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШҲЪЬЭЮЯ_>;

A_1 қ <ОРҲЬЯТЭ_ЖМЧХАВДЎФКСЕЗПИЦГНЛЪШБУЮ>;

Rқ32 ; k_1 қ 3; k_2 қ15; bқ4

Алгоритмни қадамлаб бажариш қуйидаги натижаларни олишга олиб келади;

1-қадам L_{0h} қ <12, 6, 18, 14, 5, 32, 24, 9, 20, 16, 14, 3, 1, 13, 9, 31>.

2-қадам.L_{1h} қ<19, 1, 5, 25, 30, 15, 23, 10, 11, 31, 25,24,18,22,10, 12>

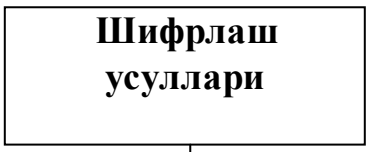
3-қадам. T_1 қ <СОЯГБДИМЧУГЦ КПМХ>.

4-қадам. T_2 қ <СОЯГ БДИМ ЧУГЦ КПМХ>.

Қайта шифрлашда олдин блокларга бўлиб чиқиш бартараф этилади. Узунлиги К та белгилардан ташкил топган T_1 шифрматн олинади. Қайта шифрлаш бутун сонли k_1h_{0i} Қ k_2 қ nR Қ h_{1i} тенгламани ечиш йўли билан амалга оширилади.

Маълум бўлган бутун k_1, k_2, h_{1i} ва R катталикларда h_{oi} катталик n ни танлаб олиш йўли билан ҳисобланади.

Бу жараённи шифрматннинг барча белгиларига кетма-кет қўлланилиши унинг қайта шифрланишига олиб келади.



Калитларнинг тури бўйича

Ўзгартириш усули билан

4.9. Шифрлаш усулларини таснифланиши

Келтирилган мисолнинг шартлари бўйича алмаштириш жадвали қурилиши мумкин, унда ўзаро алмаштириладиган белгилар битта устунда жойлашадилар (4.2 - жадвал).

4.2 - жадвал

Алмаштириш жадвали

S_{oi}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
h_{oi}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
S_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ў	С	П	Г	Ъ	У
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31

S_{oi}	С	Т	У	Ф	Х	Ц	Ч	Ш	Ҳ	Ъ	Ў	Ь	Э	Ю	Я	_
h_{oi}	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
S_{1i}	Р	Я	_	Ч	В	Ф	Е	И	Н	Ш	Ю	Ҳ	Т	Ж	Х	В
h_{1i}	2	5	8	11	14	17	20	23	26	29	32	3	6	9	12	15

Алмаштириш жадвалини ишлатиш шифрлаш жараёнини сезиларли соддалаштирилади. Шифрлашда бошланғич матн белгиси жадвалнинг S_{oi} қаторидаги белгилар билан таккосланади. Агар і-устунда мос келиш бўлса, унда бошланғич матн белгиси жадвалнинг ўша і-устунида жойлашган, S_{i}-қаторидаги белги билан алмаштирилади.

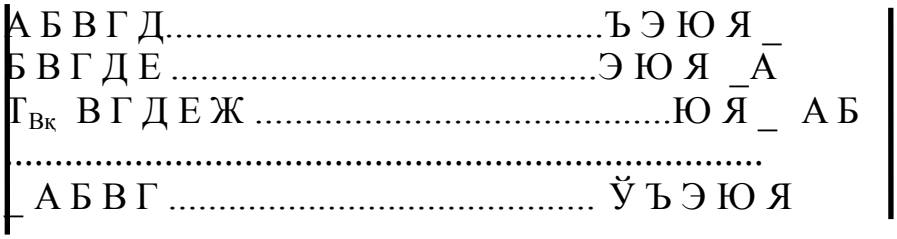
Қайта шифрлаш шунга ўхшаш амалга оширилади, лекин жадвалга кириш S_{1i} қатор бўйича амалга оширилади.

Тўғридан-тўғри алмаштириш усулининг асосий камчилиги бошланғич ва ёпиқ матнларининг бир хил статистик тавсифларини мавжудлигидадир. Бошланғич матн қайси тилда ёзилганини ва бу тилнинг алфавитларини белгиларини ишлатишни частотали тавсифини билган ҳолда криптотаҳлил қилувчи ушлаб олинган маълумотларни статистик қайта ишлаш йўли билан иккала алфавитларининг белгилари ўртасидаги мувофиқликни ўрнатиши мумкин.

Полиалфавитли алмаштириш усули янада жиддий чидамлироқ ҳисобланади. Бундай усуллар бошланғич матн белгиларини алмаштириш учун бир нечта алфавитларни ишлатишга асослангандир. Полиалфавитли алмаштиришни мавхумий қуйидагича тасвирлаш мумкин. N та алфавитли алмаштиришда бошланғич A_o алфавитдаги S_{oi} áелги A_1 алфавитдаги S_{11} белги билан алмаштирилади, S_{o2} белги A_2 алфавитдаги S_{22} белги билан алмаштирилади ва хоказо. S_{oN} белги A_N алфавитдаги S_{NN} белги билан алмаштирилгандан кейин $S_{o(NҚ1)}$ белги A_1 алфавитдаги $S_{1(Nк1)}$ белги билан ўрин алмаштирилади ва хоказо.

Вижинер жадвалини (матрицасини) $T_в$ ишлатган ҳолда полиалфавитли алмаштириш алгоритми энг кўп тарқалишга эга бўлди, бу жадвал квадрат матрица [RқR] кўринишига эгадир, бу ерда R - ишлатилаётган алфавитдаги белгилар сони. Биринчи қаторда белгилар алфавит тартибида жойлаштирилади. Иккинчи қатордан бошлаб белгилар чапга битта жойга суриш йўли билан ёзиб чиқилади. Сиқиб чиқарилаётган жойларни ўнг тарафдан тўлдирадилар (даврий суриш).

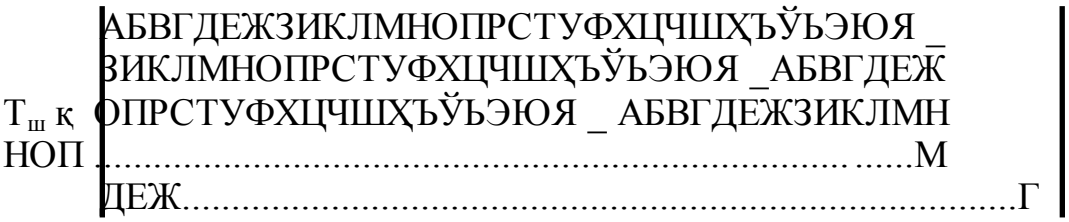
Агар рус алфавити ишлаётган бўлса, унда Вижинер матрицаси [32,32] ўлчамга эга бўлади (4.10-расм):



4.10-расм. Вижинер матрицаси

Шифрлаш М та такрорланмайдиган белгилардан ташкил топ-ган калит ёрдамида амалга оширилади. Вижинернинг тўлиқ матрицасидан [(МҚ1), R] ўлчамли шифрлаш матрицаси $T_ш$ ажратиб олинади. У биринчи қаторни ва биринчи элементларни калит белгилари билан тўғри келадиãàí қаторни ўз ичига олади.

Агар калит сифатида <ЗОНД> сўзи танланган бўлса, унда шифрлаш матрицаси бешта қатордан ташкил топади (4.11-расм):



4.11-расм. <ЗОНД > калити учун шифрлаш матрицаси

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамларнинг кетма-кетлиги кўринишига эгадир.

1-қадам. М-та белгили К калитни танлаш.

2-қадам. Танланган К калит учун [(МҚ1), R] ўлчамли шифрлаш матрицасини $T_{ш\,қ}$ (b_{ij}) қуриш.

3-қадам. І-та белги узунликка эга бўлган бошланғич матннинг ҳар бир S_{or} белгисининг тагига K_m калитнинг белгиси жойлаштирилади (4.12-расм). Калит керакли марта такрорланади.

4-қадам. Бошланғич матннинг белгилари қуйидаги қоида бўйича $T_ш$ дан танланадиган белгилар билан кетма-кет ўрин алмаштирилади:

1) ўрин алмаштирилаётган S_{or} белгига мос келган К калитнинг K_m белгиси аниқланади;

2) k_m қ b_{i1} шарт бажариладиган і-қатор $T_ш$ дан топилади;

3) $S_{orқ}b_{ij}$ шарт бажариладиган j-устун аниқланади.

4) S_{or} белги b_{ij} белги билан ўрин алмаштирилади.

5-қадам. Олинган шифрланган кетма-кетлик маълум бир узунликдаги, масалан, тўрттадан белги, блокларга бўлинади. Охирги блок, керак бўлганда, хизмат белгилари билан тўлиқ сиғимгача тўлдирилади.

Қайта шифрлаш қуйидаги кетма-кетликда амалга оширилади:

1-қадам. Шифрматн тагига калитнинг кетма-кет белгилари, шифрлаш алгоритмининг 3-қадамига мос равишда ёзилади.

2-қадам. Шифрматндан S_{1r} , белгилар ва k_m калитнинг мос белгилари кетма-кет танланади. $T_ш$ матрицада k_mқb_{i1} шарт бажариладиган элемент аниқланади. i-қаторда $b_{ijқ}S_{1r}$ элемент аниқланади. Қайта шифрланган матнда r-жойга b_{1j} белги жойлаштирилади.

3- қадам. Қайта шифрланган матн блокларга бўлинмасдан ёзилади. Хизмат белгилари олиб ташланади.

Мисол.

Кқ<ЗОНД> калити ёрдамида бошланғич Тқ<БЕЗОБЛАЧНОЕ НЕБО> матнни шифрлаш талаб этилсин. Шифрлаш ва қайта ишлаш механизмлари 4.12-расмда тасвирланган:

Бошланғич матн	БЕЗОБЛАЧНОЕ_ НЕБО
Калит	ЗОНДЗОНДЗОНДЗОНД
Алмаштирилган кейинги матн	ИУФТИШНЎФЎТГФУОТ
Шифрматн	ИУФТ ИШНЎ ФЎТГ ФУОТ
Калит	ЗОНД ЗОНД ЗОНД ЗОНД
Қайта шифрланган матн	БЕЗО БЛАЧ НОЕ_ НЕБО
Бошланғич матн	БЕЗОБЛАЧНОЕ _ НЕБО

4.12-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли

Полиалфавитли алмаштириш усулларининг крипточидамлилиги оддий алмаштириш усулларинникидан бирмунча юқорироқдир, чунки бошланғич кетма-кетликнинг бир хил белгилари турли белгилар билан алмаштирилиши мумкин. Бироқ криптотаҳлил қилишнинг статистик усулларини шифр чидамлилиги калит узунлигига боғлиқ бўлади.

Крипточидамлиликни ошириш учун шифрлашнинг ўзгартирилган матрицаси ишлатилиши мумкин. У [11,R] ўлчамли матрица кўринишига эга, бу ерда R-алфавит белгилари сони. Биринчи қаторда белгилар алфавит тартибида жойлаштирилади. Бу қаторларда белгилар тасодифий шаклда жойлаштирилади.

Калитлар сифатида, масалан, даврий бўлмаган чексиз П, е сонлари ва бошқалар, ишлатилади. Бошланғич матннинг навбатдаги n-белгиси номери чексиз соннинг n-рақами билан мос келадиган шифрлаш матрицасидаги қаторнинг мос белгиси билан алмаштирилади.

4.8.2. Қайта жойлаштириш усуллари

Қайта жойлаштириш усулларини моҳиятини бошланғич матнни маълум бир узунликдаги блокларга бўлиб чиқиш ва кейинчалик аниқ алгоритм бўйича ҳар бир блок ичида белгиларни қайта жойлаштиришни ташгил этади.

Қайта жойлаштиришлар бошланғич ахборотни ёзиш йўлларини ва шифрланган ахборотни ўқиш йўлларидан, геометрик шакл чегараларида, фарқлари ҳисобига олинадилар. Оддий қайта жойлаштириш мисол тариқасида бошланғич маълумотни блокини матрица қаторлари бўйича ёзиш, устунлари бўйича ўқишни келтириш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устунлар бўйича ўқиш кетма−кетлиги калит билан берилиши мумкин. Усулнинг крипточидамлилиги блокнинг узунлигига (матрица ўлчамлари) боғлиқ бўлади. Узунлиги 64 та белгига тенг бўлган блок учун (8х8 ўлчамли матрица) калитнинг $1,6*10^9$ та комбинацияси мумкиндир. Узунлиги 256 та белгига тенг бўлган блок учун (16х16 ўлчамли матрицалар мумкин бўлган калитлар сони $1,4*10^{26}$ тага етади. Охирги ҳолда калитларни танлаб олиш масаласини ечиш замонавий ЭҲМ лар учун жиддий қийинчиликларни келтириб чиқаради.

Қайта жойлаштиришлар яна *Гамильтон маршрутларини* ишлатишга асосланган усулда ҳам ишлатилади. Бу усул қуйидаги қадамларни бажариш йўли билан амалга ошади.

1-қадам. Бошланғич ахборот блокларга бўлиб чиқилади. Агар шифрланадиган ахборотнинг узунлиги блокнинг узунлигига каррали бўлмаса, унда охирги блокнинг бўш жойларига махсус хизмат белги - тўлдирувчилар (масалан, *) жойлаштирилади.

2-қадам. Блок белгилари билан жадвал тўлдирилади, унда белгининг ҳар бир тартиб номери учун блок жуда аниқ жой ажратилади (4.13 - расм).

3-қадам. Белгиларни жадвалдан ўқиш маршрутларни биттаси бўйича амалга оширилади. Маршрутлар сонини ошиши шифрнинг крипточидамлилигини оширади. Маршрутлар ёки кетма-кет танланади, ёки уларнинг навбати К калит билан берилади.

4-қадам. Белгиларнинг шифрланган кетма-кетлиги маълум бир L узунликдаги блокларга бўлиб чиқилади. L катталик бошланғич ахборот 1-қадамда бўлиб чиқиладиган блокларнинг узунлигидан фарқ қилиши мумкин.

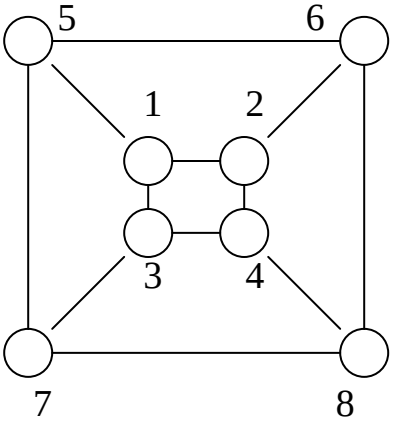
Қайта шифрлаш тескари тартибда амалга оширилади. Калитга мос равишда маршрут танланади ва бу маршрутга кўра жадвал тўлдирилади.

Жадвалдан белгилар элемент номерларини келиш тартиби бўйича ўқилади. Қуйидаги 4.13-расмда Гамильтон маршрутларини ишлатган ҳолда ахборотни шифрлаш мисоли келтирилган.

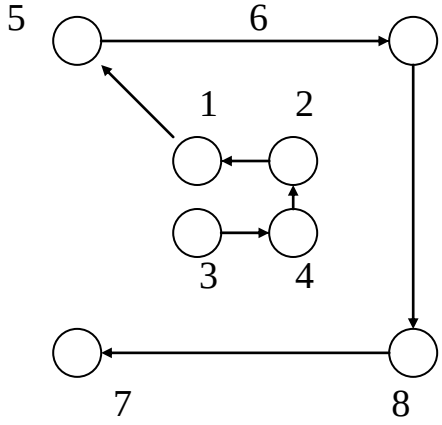
Бошланғич T_oк<МЕТОДЎ_ПЕРЕСТАНОВКИ> матнини шифрлаш талаб этилсин. Шифрланган блокларнинг узунлиги ва калит мос равишда тенг: Lқ4, Кқ<2,1,1>. Шифрлаш учун 4.13-расмда тасвирланган иккита маршрут ва жадвал ишлатилади. Берилган шартлар учун тўлдирилган матрицали маршрутлар 4.14-расмда кўрсатилган кўринишга эга бўладилар.

1-қадам. Бошланғич матн учта блокка бўлинади:

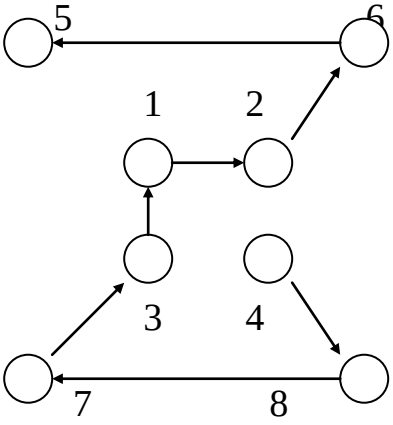
$Б_1$=<МЕТОДЫ_П>;
$Б_2$=<ЕРЕСТАНО>;
$Б_3$=<ВКИ*****>.



Жадвал



Маршрут №1



Маршрут №2

4.13-расм. Гамильтон маршрутлари ва 8 элементли жадвал варианти

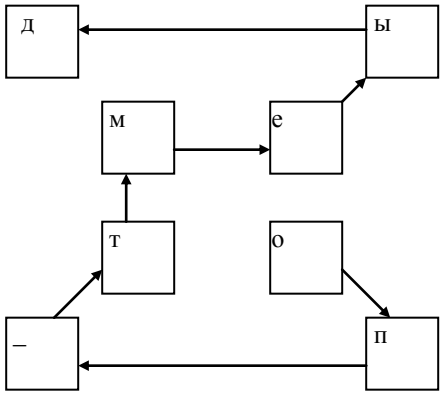
2-қадам. 2,1,1 маршрутли учта матрица тўлдирилади (4.14-расм).

3-қадам. Маршрутларга мос равишда белгиларни жойлаштириш йўли билан шифр матнни олиш.

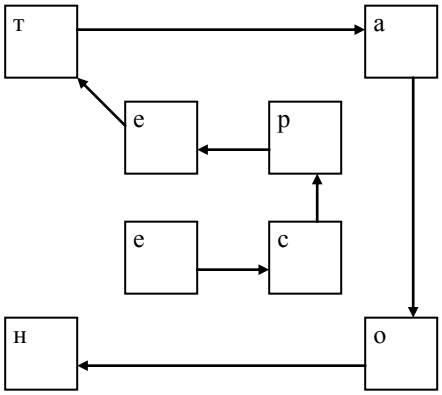
$Т_1$к<ОП_ТМЕЎДЕСРЕТАОНИ*КВ****>.

4-қадам. Шифрматнни блокларга бўлиб чиқиш.

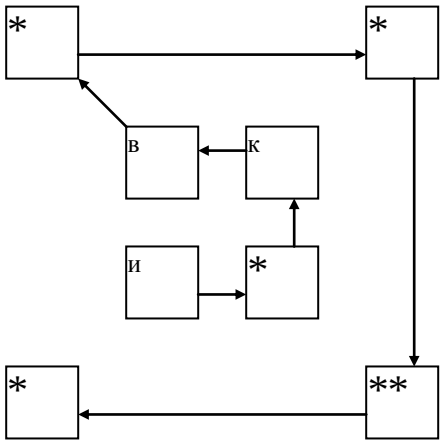
$Т_1$к<ОП_Т МЕЎД ВСРЕ ТАОН И*КВ ****>.



Маршрут №2



Маршрут №1



Маршрут №1

4.14 - расм. Гамильтон марш-рутлари ёрдамида шифрлаш мисоли

Амалиётда қайта жойлаштиришларни амалга оширадиган махсус аппаратли схемаларни ишлатиш катта аҳамиятга эгадир (4.15-расм).

Бошланғич ахборот блокининг параллел икқилик коди (масалан, икки байт) схемага берилади. Ички коммутация уланишлар ҳисобига схемада блок чегарасида битларни қайта жойлаштириш амалга оширилади. Ахборот блокини қайта шифрлаш учун схеманинг киришлари ва чиқишлари жойлари билан алмашадилар.

Қайта жойлаштиришлар усули оддийгина амалга оширилади, лекин иккита жиддий камчиликка эгадир. Биринчидан, улар шифр-матнни статистик қайта ишлаш ёрдами билан очилишига йўл қўяди. Иккинчидан, агар бошланғич матн К та белги узунликдаги блокларга бўлиб чиқилса, унда криптотаҳлил қилувчига шифрни очиш учун шифрлаш тизимига тестли ахборотнинг К-1 блокини юбориш етарлидир, бу блокда биттадан ташқари барча белгилар бир хилдир.

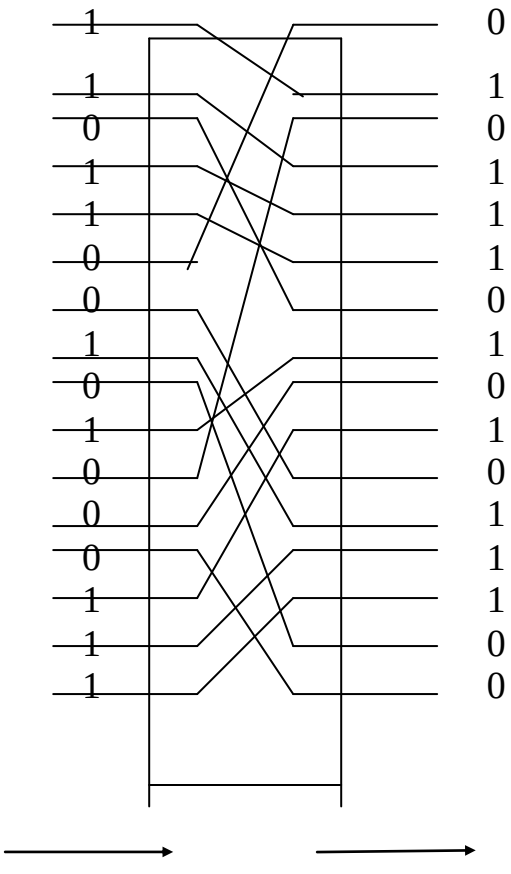
Шифрлашнинг аналитик усуллари матрицали алгебрани ишлатишга асосланган.

Шифрлашнинг аддитив усуллари (гаммалаш), кодлари бошланғич ахборотнинг рақамли кодлари билан қўшиладиган рақамли кортежнинг тасодифий кетма-кетлигини ишлатади. Гамма калит ҳисобланади. Калит қанчалик узун бўлса, крипточидамлилик шунчалик юқори бўлади.

Очиқ калитли шифрлаш тизимларида шифрлаш учун очиқ калит ва қайта шифрлаш учун махфий калит ишлатилади.

Замонавий криптотизимлардан қуйидагиларни таъкидлаш мумкин:

а) симметрик - Цезарь тизими, Трисемус жадвали, Плейфернинг биграммли шифри, Хилл криптотизими, Вижинер шифрлаш тизими ва бошқалар;



4.15- расм. қайта жойлаштириш схемаси

б) носимметрик - RSA криптотизими (Райвест Р., Шамир А. ва Адлеман А.- Rivest, Shamir ва Adleman); Полига-Хеллман, Эль-Гамаил шифрлаш тизимлари ва бошқалар.

Замонавий шифрлаш стандартларидан ахборотни шифрлашга Россия стандартини ГОСТ 28147-89, АҚШнинг DES (Data Encryption Standart) стандартини келтириш мумкин.

КТ ва Т ларида криптоҳимоя қилишни ишлатиш истиқболларига тўхталадиган бўлсак, қуйидагиларга эътиборни қаратиш керакдир:

- калитнинг узунлиги замонавий тизимлар учун > 90 бит бўлиши керак;

- жуда масъулиятли қўлланишлар учун нафақатгина калит, балки шифрлаш алгоритми ҳам махфий ҳисобланади;
- стенография криптоҳимоя қилишнинг истиқболи йўналиши ҳисобланади.

Хулоса қилиб шуни айтиш мумкинки, замонавий симметрик ва носимметрик криптотизимларни, замонавий шифрлаш стандартларини, ҳамда стенографияни ва шифрлашни комплекс ишлатиш ёпиқ ахборотнинг крипточидамлилигини бирмунча оширади.

Тасодифий таҳдидлардан ахборотни ҳимоя қилишнинг энг самарали усулларидан бири дубллаш ҳисобланади. Дубллашдан ташқари компьютер тизимини (КТ) ишончлилигини ошириш, ишдан чиқишларга мустахкам компьютер тизимларини яратиш, хато бажарилган амалларни блокировкалаш, халокатлардан фавқулодда вазиятлардан келадиган зарарларни минималлаштириш,хамда инсонни компьютер тизим билан ўзаро харакати бўйича оптималлаштириш ишларини таъкидлаш керакдир.

Захиралаш (дубллаш) усулларини

Кўриб чиқишда тезкор ва тезкор булмаган усулларга, хотира соҳасининг махсус ажратилган қисмларини ишлатадиган ташқи эслаб қолиш қурилмасининг қўшимча блокларини ишлатишга, тўлиқ ва қисман нусхалашга, зичлаштириб ва зичлаштирмасдан ойнали ва комбинацияланган нусхалашга тўхтмтилиб ўтиш керакдир.

Олдиндан кўзда тутилган таҳдидлардан анъанавий жосуслик ва қўпорувлардан ҳимоялаш ишларини ташкил этиш, зарарли электромагнит нурланишлардан ва йўналтиришлардан ҳимоя қилиш, тақиқланган мурожаат қилишдан (ТМҚ) ҳимоя қилиш усуллари (ахборотга мурожаат этишни чеклаш тизими (МЭЧТ), ахборотни тдқиқот этишдан ва нусхалашдан ҳимоя қилиш воситалари) кўриб чиқилади.

Тармоқларга ва тармоқ ресурсларига ТМҚ ларини бартараф этиш бўйича чоралардан бири паролларни ишлатишга асосланган мурожаат этишни назорат қилишдир. Ишлатиладиган пароллар қуйидагилардир: фойдаланувчи ўрнатадиган пароллар; тизим ўрнатадиган пароллар; ярим сўзлар; таянч иборалар; «савол-жавоб» интерфаол кетма-кетлиги; «қатъий» пароллар.

Объектга мурожаат этишни ташкил этишда ҳал этиладиган асосий масалалардан бири объектга киритиладиган шаклларни идентификациялаш ва аутентификациялашдир.

Ахборотни ҳимоя қилишнинг таклиф этиладиган моделлари (захираларга мурожаат этиш пароли, мурожаат этиш ҳуқуқи, аудит, дисксиз компьютерлар) компьютер тизимларини ҳимоя қилишнинг утарлича даражасини таъминлайди.

Ахборотни ҳимоя қилишнинг криптографик усулларидан шифрлашни, зичлаштиришни айтиб ўтиш жоиздир. Криптотизимларни самарадорлигини кўрсатгичларни тахлил қилиш кўрсатмоқдаки, иккита калитли тизимларни шифрлаш алгоритми очиқ калитли классик схемаларга нисбатан сезиларли даражада секинроқдир. Шу билан бир вақтда очиқ калитли шифрлаш бирмунча ишончлироқдир.

Асосий атамалар

Захирали нусхалаш (дубллаш), дубллашнинг тезкор усули, дубллашнинг тезкор бўлмаган усули, тўлиқ нусхалаш, ойнали нусхалаш RAID, захирали нусхалаш журнали, қўйилма, мурожаат қилишни чегаралаш тизими, қароқчилар, хакерлар, кракерлар, трафик, идентификация, аутентификация, электрон-рақамли имзолаш, мурожаат қилиш ҳуқуқи, аудиторли модель, дисксиз модель, криптографик усул, стенография, симметрик криптотизим, носимметрик криптотизим, очиқ калит, ёпиқ калит.

Назорат саволлари

1. Тасодифий хавфлардан КТ ларида ахборотни ҳимоя қилиш масалаларини таснифини келтиринг.
2. КТ ларида ахборотни дубллашни умумий тавсифини беринг.
3. RAID технологиясини ишлатиш афзаллиги нимада кўринади?
4. Дубллаш усулларини таснифини беринг.
5. Ахборотнинг ҳимоя қилишнинг қандай техник усуллари мавжуд?
6. Тармоқларга ва тармоқ ресурсларига тақиқланган мурожаат қилиш қандай йўналишларда кўриб чиқилади?
7. Паролларнинг турли кўринишларини, уларга қўйиладиган талабларни келтиринг.
8. Тармоқларга ва тармоқ ресурсларига тақиқланган мурожаат қилиш.
9. Маълумотларни ва дастурларни очиш ва ўзгартириш.
10. Трафикни очиш, ўзгартириш ва алмаштириш.
11. АТМҚ лардан ШЭҲМ замонавий ҳимоя қилиш тизимлари.
12. Идентификациялаш ва аутентификациялаш тизими.
13. Ахборотни ҳимоя қилишнинг моделлари.
14. Мурожаат қилиш ҳуқуқлари.
15. Ҳимоя қилишнинг қўшимча (аудиторли, дисксиз) усуллари.
16. Ахборотни ҳимоя қилишнинг криптографик усуллари.
17. Шифрлаш усуллари, уларга қўйиладиган талаблар.
18. Криптотизимларнинг ишлашини классик схемалари.
19. Симметрик ва носимметрик шифрлаш усуллари .
20. Алмаштириш (урнига қўйиш) усули.
21. Қайта ўрнатиш усули.
22. Криптотизимларни ишлатиш истиқболлари.

Тавсия этиладиган адабиётлар:

1. Романец Ю.В, Тимофеев П.А, Шаньгин В.Ф. Защита информации в КС и С. − М.: Радио и связь, 2001.

2. Домашев А.В., Грунтович М.М. и др. Программирование алгоритмов защиты информации. Учеб. пособ. – М.: Издатель Молгачева С.В. Издательство «Нолидж», 2002. – 416с.

3. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003, – 504 с.

4. Баичев С.Г. Основы современной криптографии. – М.: Горячая линия Телеком, 2001. – 1200с.

5. Эрматов Ш.Т., Шоахмедова Н.Х. Ахборотни ҳимоялашнинг криптографик усуллари. Электрон услубий қўлланма. − Т., 2005.

5 боб. КОМПЬЮТЕР ВИРУСЛАРИ ВА ВИРУСГА ҚАРШИ ВОСИТАЛАР

5.1. Компьютер вируси ҳақида тушунча. Вирусларнинг моҳияти, пайдо бўлиши ва тарқалишининг асосий белгилари

Шахсий компьютер (ШК)ларнинг оммавий қўлланилиши, бахтга қарши, компьютерларнинг меъёрда ишлашига тўсқинлик қиладиган, файлли структурани, дискларни бузадиган ва компьютерда сақланадиган ахборотга талофат етказадиган ўз-ўзидан ишлаб чиқариладиган вирус дастурларни пайдо бўлиши билан алоқадордир. Битта компьюютерга кириб олиб, компьютер вируси бошқа компьютерларга тарқалиш қобилиятига эгадир.

5.1.1. Компьютер вируси нима?

Компьютер вируси - махсус ёзилган дастур бўлиб, компьютерда ишлашда барча мумкин бўлган тўсиқларни яратиш, файлларни ва каталогларни бузиш дастурлари ишдан чиқариш мақсадида ҳисоблаш тизимларига, компьютернинг тизимли соҳаларига, файлларга татбиқ, қилинадиган, узларининг нусхаларини яратиш, бошқа дастурларга ўз-ўзидан бирикиб оладиган хоссаларга эгадирлар.

Ичида вирус жойлашган дастур “зарарланган” (“юқтирилган) деб аталади.

Бундай дастур ўз ишини бошлаганда, олдин бошқаришни вирус ўз қўлига олади. Вирус бошқа дастурларни топади ва “зарар-лантиради”, ҳамда бирор-бир зарарли ишларни бажаради (масалан, файлларни ёки дискда файлларни жойлашиш жадвалини бузади, тезкор хотирани “кирлантиради” ва ҳ.к.) Вирусни ниқоблаш учун бошқа дастурларни зарарлантириш ва зарар етказиш бўйича ишлар ҳар доим ҳам эмас, айтайлик маълум бир шартлар бажарилганда, бажарилиши мумкин. Вирус унга керакли ишларни бажаргандан кейин у бошқаришни ўзи жойлашган дастурга узатади ва у дастур одатдагидай ишлай бошлайди. Шу билан бирга ташқи кўринишдан зарарланган дастурнинг ишлаши зарарланмаган каби кўринади.

Вирусларнинг кўпгина кўринишлари шундай тузилганки, зарарлангандан дастур ишга туширилганда вирус компьютер хотирасида ҳар доим қолади ва вақти-вақти билан дастурларни зарарлантиради ва компьютерда зарарли ишларни бажаради.

Вируснинг барча ҳаракатлари етарлича тез бажарилиши мумкин ва бирор-бир хабарни бермайди, шунинг учун фойдаланувчи компьютерда бирорта одатдан ташқари ишлар бўлаётганини пайқаши жуда мушкулдир.

Компьютерда нисбатан кам дастурлар зарарланган бўлса вируснинг борлиги деярли сезиларсиз бўлади. Лекин бирор вақт ўтиши билан компьютерда қандайдир ғалати ҳодисалар рўй бера бошлайди, масалан:

- баъзи дастурлар ишлашдан тўхтайдилар ёки нотўғри ишлай бошлайдилар;
- экранга бегона хабарлар ёки белгилар чиқарилади;
- компьютерда ишлаш жиддий секинлашади;
- баъзи бир файллар бузилиб қолади ва х. к;

Бу вақтга келиб, қоидага кўра, фойдаланувчи ишлаётган етарлича кўп (ёки хатто кўпчилик) дастурлар вируслар билан зарарланган, баъзи бир файллар ёки дисклар эса ишдан чиққан ҳисобланади. Бундан ташқари, фойдаланувчи компьютеридаги зарарланган дастурлар дискеталар ёрдамида ёки локал тармоқ бўйича фойдаланувчининг ҳамкасбларини ва ўртоқларини компьютерига ўтиб кетган бўлиши мумкин.

Вирусларнинг баъзи бир кўринишлари ўзларини янада хавфлироқ тушадилар. Улар бошланишда катта миқдордаги дастурларни ёки дискларни билдирмасдан зарарлантирадилар, кейин эса жуда жиддий шикастланишларни келтириб чиқаради, масалан, компьютердаги бутун қаттиқ дискни форматлайди. Вирус-дастур сезиларсиз бўлиши учун у катта бўлмаслиги керак. Шунинг учун, қоидага кура, вируслар етарлича юқори малакали дастурловчилар томонидан Ассемблер тилида ёзилади.

Компьютер вирусларини пайдо бўлиши ва тарқатилиши сабаблари, бир томондан, инсон шаҳсиятининг психологиясида ва унинг ёмон хислатларида яширинади (ҳаваслар, қасос олишлари, тан олинмаган ижодкорларни мансабпарастлиги, ўзининг қоби-лиятларини конструктив қўллашни имконияти йўқлиги), иккинчи томондан эса, ҳимоя қилишнинг аппарат воситаларини ва шахсий компьютернинг операцион тизими томонидан қарши ҳаракатларни йўқлиги билан боғликдир.

Кўпчилик давлатларда қабул қилинган компьютер жиноятлари билан кураш ва вируслардан ҳимоя қилишнинг махсус дастур воситаларини ишлаб чиқиш тўғрисидаги қонунларга қарамасдан, янги вирус-дастурларнинг, сони доимо ошиб бормоқда. Бу шахсий компьютер фойдаланувчисидан вируслар табиати, вируслар билан зарарланиш усуллари ва улардан ҳимоя қилиш услублари тўғрисидаги билимларни талаб этади.

Вирусларни компьютерга кириб олинишини асосий йўллари олинадиган дисклар (эгилувчан ва лазерли), ҳам компьютер тармоқлари ҳисобланади. Қаттиқ дискни вируслар билан зарарланиши компьютерни вирусни ўзида сақлаган дискетадан юклаганда амалга ошиши мумкин. Бундай зарарланиш тасодифий бўлиши мумкин, масалан, дискетани А: дисководдан чиқариб олмасдан ва компьютер қайта юкланганда, дискета тизимли бўлмаслиги ҳам мумкиндир. Дискетани зарарлантириш жуда оддийроқдир. Унга вирус, ҳаттоки агар дискетани за-

рарланган компьютерни дисководига қўйилганда, унинг мундарижасини ўқилганда, тушиши мумкин.

Зарарланган диск - бу юкланиш секторида вирус-дастур жойлашган дискдан иборат.

Вирусни ўз ичига олган дастур ишга туширилгандан кейин бошқа файлларни зарарлантириш мумкин бўлиб қолади. Энг кўпроқ вируслар билан дискнинг юкланадиган сектори ва .EXE,.COM,.SYS ёки ғBAT кенгайтмасига эга бўлган бажариладиган файллар зарарланадилар. Жуда ҳам кам матнли ва графикли файллар зарарланадилар.

Зарарланган дастур - бу унга татбиқ қилинган вирус-дастурни ўз ичига олган дастурдир.

Компьютер вируси билан зарарланишда ўз вақтида уни пайқаш жуда муҳимдир. Бунинг учун вирусларни пайдо бўлишини асосий белгилари тўғрисида билимларга эга бўлиш керак. Уларга қуйидагилар тегишли бўлиши мумкин:

- олдин муваффақиятли ишлаган дастурларнинг ишлашини тўхташи ёки нотўғри ишлаши;
- компьютернинг секин ишлаши;
- операцион тизимни юклашни имкони йўқлиги;
- файлларни ва каталогларни йўқолиб қолиши ёки уларнинг мазмунини бузилиши;
- файлларни ўзгартирилганлик санасини ва вақтини ўзгариши;
- дискда файллар сони бехосдан жуда ошиб кетиши;
- бўш тезкор хотирани ўлчамини жиддий камайиши;
- экранга кўзга тутилмаган хабарларни ёки тасвирларни чиқариш;
- кўзда тутилмаган товушли хабарларни бериш;
- компьютер ишлашида тез-тез бўладиган осилиб қолишлар ва бузилишлар.

Таъкидлаш керакки, юқорида санаб ўтилган ҳодисалар вирусларни келиб чиқиши билан бўлиши мажбурий эмас, бошқа сабабларнинг оқибатлари ҳам бўлиши мумкин. Шунинг учун компьютер ҳолатини тўғри диагностикалаш ҳар доим мушкулдир.

5.1.2. Вирус билан зарарланган ва бузилган файллар

Компьютер вируси компьютерда мавжуд бўлган дисклардаги исталган файлни етарлича ўзгартириши ва бузиши мумкин. Лекин файлларнинг баъзи бир турларини вирус “зарарлантириши” мумкин. Бу билдирадики, вирус бу файлларга “татбиқ” қилиниши мумкин, яъни уларни шундай ўзгартирадики, улар вирусни ўз ичида сақлайдилар ва бу вирус баъзи бир ҳолатларда ўзининг ишини бошлаши мумкин.

Таъкидлаш лозимки, дастурларнинг ва ҳужжатларнинг матн-лари, маълумотлар базасининг ахборотли файллари, жадвалли процессорларнинг жадваллари ва бошқа шунга ўхшаш файллар вирус билан зарарланиши мумкин эмас, бу файлларни вируслар фақат бузиши мумкин.

Вирус билан “зарарланиши” мумкин бўлган файлларнинг турлари қуйидагилардир:

1. **Бажариладиган файллар**, яъни .COM ва .EXE кенгайтмали файллар, ҳамда бошқа дастурлар бажарилганда юкланадиган оверлокли (такрорланадиган) файллардир. Зарарланган бажариладиган файллардаги вирус шу вирус жойлашган дастур ишга туширилганда ўзининг ишини бошлайди. Вирус билан зарарланишнинг энг хавфлиси DOS буйруқли процессорини-COMMAND.COM дастурини зарарланишидир, чунки бу вирус DOS нинг исталган буйруғи бажарилганда ишлайди ва исталган бажариладиган дастур зарарланади (агар вирус уни зарарлантира олса). [25; 106-112]

2. **Операцион тизимни юкловчиси ва қаттиқ дискни асосий юкловчи ёзуви.** Бу соҳаларни бузадиган, қоидага кўра, икки қисмдан ташкил топган бўлади, чунки ушбу катта бўлмаган қайд қилинган диск соҳаларида вирус дастурини бутунлай жойлаштириш мушкулдир. Уларга сиғмайдиган вирус қисми, “бузилган” деб эълон қилинадиган, дискнинг бошқа қисмида жойлашади. Бундай вирус операцион тизим бошланғич юкланганда ўзининг ишини бошлайди ва резидент бўлиб қолади, яъни компьютер хотирасида доимий жойлашади.

3. Қурилмаларнинг драйверлари, яъни CONFIG.SYS файлининг Device қилишда кўрсатиладиган файллар. Уларда жойлашган вируслар ҳар сафар мос қурилмага мурожаат қилганда ўзининг ишини бошлайди.

4. DOC тизимининг тизимли файллари (MS DOS да улар IO.SYS ва MSDOS.SYS деб аталади, PS DOS да - IBMBIO.COM ва IBMDOS.COM, DR DOSда эса - DRBIOS.SYS ва DRDOS.SYS деб аталади). Бу файлларнинг зарарланиши эҳтимоли камроқдир, лекин назарий жиҳатдан мумкиндир, чунки улар дискнинг узлуксиз қисмида, файлларни жойлаштириш учун ажратилган бошланғич қисмида, жойлашиши керак. Шунинг учун бу файлларга вирусларни жойлашиши учун, IO.SYS ва MSDOS.SYS файлларидан кейин келадиган бошқа файллар банд қиладиган жойни дискда бўшатиш керак, бу эса етарлича мураккабдир. Қоидага кўра, вируснинг ҳар бир маълум тури файлларнинг фақатгина битта ёки иккита турини зарарлантириши мумкин. Кўпроқ .COM файлларни зарарлантирадиган вируслар учрайди, тарқалиши бўйича иккинчи ўринда-.EXE файлларни ҳам зарарлантирадиган вируслар учрайди. Баъзида компьютерлар дискеталарнинг юкланадиган секторлари орқали тарқатиладиган вируслар билан зарарлантирадилар.

5.2. Компьютер вирусларининг таснифланиши

Ҳозирги вақтда 60000 тадан ортиқ дастурли вируслар маълумдир. Уларни қуйидаги белгилар бўйича таснифлаш мумкин:

а) яшаш муҳити бўйича;

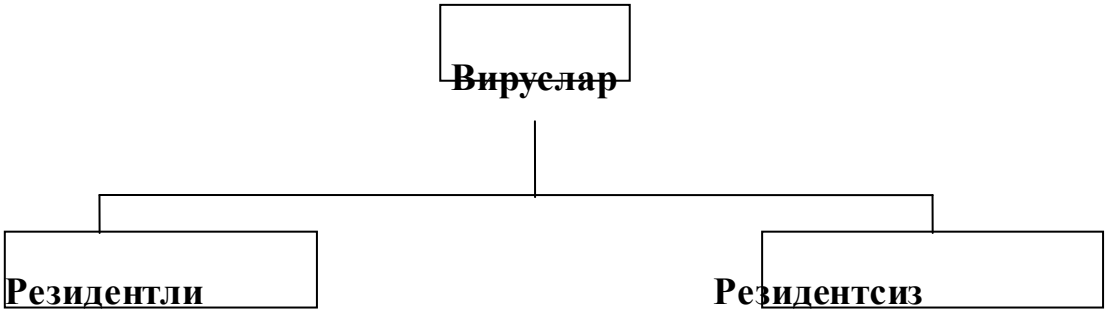
б) зарарлантириш усули бўйича;

в) таъсир этиши бўйича;

г) алгоритмнинг хусусиятлари бўйича;

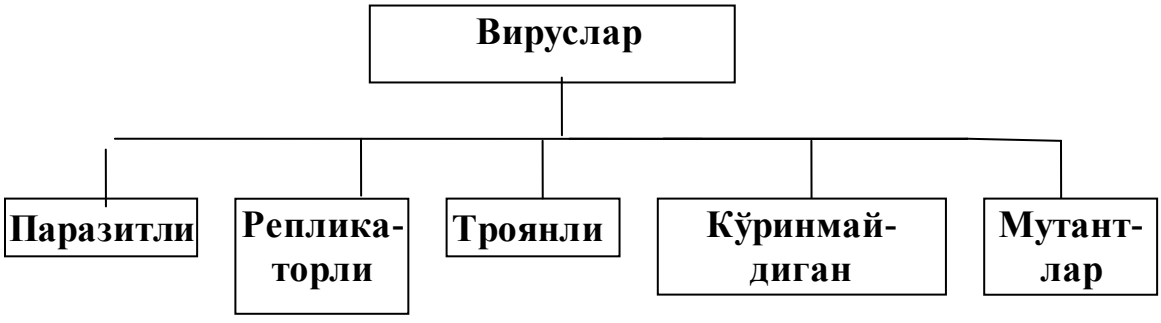
А) Яшаш муҳити бўйича вирусларнинг таснифлаши

Б) Зарарлантириш усули бўйича вирусларнинг таснифланиши



В) Таъсир этиш даражаси бўйича вирусларнинг таснифланиши

Г) Алгоритмларнинг хусусиятлари бўйича вирусларнинг таснифланиши



Яшаш муҳитига боғлиқ равишда вирусларни тармоқли, файлли, юкланадиган ва файлли-юкланадиган турларга бўлиш мумкин.

Тармоқли вируслар турли компьютер тармоқлари бўйича тарқаладилар. Дискетадан эмас, балки локал ёки глобал тармоқдан тарқатиладиган бу вируслар бажарадиган дастурларни зарарлантирмайдилар. Улар ҳимоя қилишнинг

тармоқ воситалари орқали кириб олиш учун мослашганлар ва тармоқда юқори тарқалиш тезлигига эгадир.

Тармоқли вирусларнинг энг кенг тарқалган тури компьютер “чувалчанглари” ҳисобланади, улар дастурли коднинг “бошқа жинсли” қисми бўлиб, компьютер тармоғини барча участкаларида юқори тезликда тарқаладилар.

Компьютер “чувалчанглари” тизимнинг жиддий бузилишларига олиб келмайди. Вирус “чувалчанг” сифатида Worm дастурини келтириш мумкин, у ўзининг нусхаларини тарқатиш учун ўзининг дастурли кодини Интернет тармоғи бўйича электрон хабарларга иловалар кўринишида жўнатади. Бу вирус бажариладиган HAPPУ99. EXE файлида жойлашади. [19; 150-160]

Файлли вируслар асосан бажариладиган модулларга, яъни .COM ва .EXE кенгайтмаларга эга бўлган файлларга, татбиқ қилинади. Файлли вируслар бошқа турдаги файлларга ҳам татбиқ қилиниши мумкин, лекин бунда улар бошқаришни узатадилар, ва, демак, кўпайиш қобилиятини йўқотадилар. Файлли вируслар компьютердан компьютерга файлларда кўчиб ўтадилар ва юқори зарарлантириш хоссасига эга.

Зарарланган дастурни ҳар сафар ишга туширилганда вируснинг ўз-ўзини нусхалаши бўлиб утади.

Юкланадиган вируслар- дискнинг юкланадиган секторига (Boot сектор) ёки тизимли дискни юклаш дастурини ўз ичига олган секторга (Master Boot Record) татбиқ қилинади. Улар файлли вируслардан шуниси билан фарқланадики, тизимдан тизимга юкланадиган сектор орқали кўчиб ўтади ва дискеталарни ва қаттиқ дискларни фақат Boot-секторларини зарарлантиради. Бу вирусли дастурлар кичик ўлчамларга эга (512 байтдан ошиқроқ).

Файлли юкланадиган вируслар - файлларни ҳам, дискларнинг юкланадиган секторларини ҳам зарарлантиради. Бу турдаги вирусларни яратиш учун одатда, мураккаб алгоритмлар ва технологиялар ишлатилади.

Зарарлантириш усули бўйича вируслар резидентли ва резидентли бўлмаган бўлади.

Резидентли вирус компьютерни зарарлантирганда тезкор хотирада ўзининг резидентли қисмини қолдиради, бу қисм кейин операцион тизимни зарарланган объектларга (файлларга, дискларнинг юкланадиган секторларига) мурожаатини ушлаб олади ва уларга татбиқ қилинади. Резидентли вируслар хотирада жойлашади ва компьютерни ўчиргунгача ёки қайта юклагунгача фаол ҳисобланади.

Резидентли бўлмаган вируслар компьютер хотирасини зарарлантирмайдилар ва чегараланган вақт ичида фаол ҳисобланади.

Таъсир этиш даражаси бўйича вирусларни қуйидаги кўринишларга бўлиш мумкин

1. Хавфсиз - улар компьютер ишлашига тўсиқ бермайдилар, лекин бўш тезкор хотирани ва дисклардаги хотираларни сиғимини камайтиради, бундай вирусларнинг ишлаши бирорта графикли ёки товушли самараларда намоён бўлади.

2. Хавфли - улар компьютер ишлашида турли бузилишларга олиб келиши мумкин.

3. Жуда хавфли - уларнинг таъсирида дастурлар йўқолади, маълумотлар ўчиб кетади, дискнинг тизимли соҳаларидаги ахборотлар ўчирилиб юборилади.

Алгоритмнинг хусусиятлари бўйича вирусларни уларнинг турли-туманлигини катталиги туфайли таснифлаш мушкулроқдир.

Паразитли вируслар оддийроқдир, улар файлларнинг ва диск секторларининг мазмунини ўзгартирадилар, ва етарлича енгил пайқалиши ва йўқотилиши мумкин.

Чувалчанглар деб аталадиган вирус репликаторларни таъкидлаш керакки, улар компьютер тармоқлари бўйича тарқаладилар, тармоқ компьютерларининг манзилларини ҳисоблайдилар ва бу манзиллар бўйича ўзларининг нусхаларини ёзадилар.

Стелс-вируслар деб аталадиган кўринмайдиган вируслар мавжуд бўлиб, уларни пайқаш ва зарарлантириш жуда мушкулдир, чунки улар операцион тизимни зарарланган файлларга ва дискларнинг секторларига мурожаат қилишни ушлаб оладилар ва ўзининг танасини ўрнига дискнинг зарарланмаган қисмларини қўяди.

Шифрлаш-қайта шифрлаш алгоритмларини ўз ичига олган вирус-мутантларни пайқаш жуда мушкулдир, шу алгоритмлар ҳисобига бир хил вируснинг нусхалари битта ҳам такрорланмайдиган байтлар занжирига эга эмас.

Квазивирусли ёки “троянли” дастурлар деб аталадиган вируслар ҳам мавжуддир, улар ўз-ўзидан тарқалиш хоссасига эга бўлмасада, лекин жуда хавфлидир, чунки улар фойдали дастур остида ниқобланиб, юкланадиган секторни ва дискларнинг файлли тизимини бузадилар.

5.3 Компьютер вирусларидан ҳимоя қилиш усуллари

Компьютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

- вирусларни кириб келишини бартараф этиш;
- агар вирус барибир компьютерга кирган бўлса, вирус ҳужумини бартараф этиш;
- агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф этиш.

- ҳимоя қилишни амалга оширишни учта усули мавжуддир:
- ҳимоя қилишнинг дастурли усуллари;
- ҳимоя қилишнинг аппаратли усуллари;
- ҳимоя қилишнинг ташкилий усуллари.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: “касалликни даволагандан кўра унинг олдини олган яхшироқ”. Афсуски, айнан у энг бузувчи оқибатларни келтириб чиқаради. Компьютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустахкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум - бу муҳим маълумотларни йўқотишни ягона бўлмаган ва хаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операцион тизимни ишдан

чиқариши мумкин, ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқатсиз қилиб қўйиш қобилиятига эгадирлар. Ўғирлаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда компьютерни йўқотиш эҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда "охиридан" бошлаш керак - исталган таъсирни, у вирус ҳужуми, хонада ўғрилик ёки қаттиқ дискни физик ишдан чиқиши бўлишидан қатъий назар, бузувчи оқибатларини бартараф этишдан бошлаш керак.

Маълумотлар билан ишончли ва хавфсиз ишлашга фақат шундагина эришиладики, агар исталган кутилмаган ҳодиса, шу жумладан компьютерни тўлиқ физик ишдан чиқариш ҳам, халоқатли оқибатларга олиб келмаслиги керак.

5.3.1. Вирусга қарши ҳимоя қилиш воситалари

Ахборотни ҳимоя қилишнинг асосий воситаси энг муҳим маълумотларни захирали нусхалаш ҳисобланади. Юқорида санаб ўтилган сабабларнинг исталгани бўйича ахборотни йўқотиш ҳолатида қаттиқ дисклар қайта форматланади ва янгидан ишлатишга тайёрланади. "Тоза" форматланган дискка дистрибьютив ихчам-дискдан операцион тизим ўрнатилади, кейин эса унинг бошқаруви остида барча керакли дастурли таъминот ўрнатилади, уларни ҳам дистрибьютив ташувчилардан олинади. Компьютерни тиклаш захирадаги ташувчилардан олинадиган маълумотларни тиклаш билан якунланади.

Маълумотларни захиралашда яна шуни инобатга олиш керакки, барча рўйхатдан ўтган ва паролли маълумотларни, Интернетнинг тармоқли хизматларига мурожаат қилиш учун, алоҳида сақлаш керак. Уларни компьютерда сақламаслик керак. Одатдаги сақлаш жойи - бўлим рахбарининг сейфидаги хизмат кундалигидир. Ахборотни захирали нусхалаш бўйича тадбирлар режасини тузиб олиб захирали нусхалар компьютерда алоҳида сақланиш кераклигини инобатга олиш керак. Яъни масалан, ўша компьютернинг алоҳида қаттиқ дискида ахборотни захиралаш фақатгина хавфсизлик иллюзиясини яратади.

Муҳим, лекин махфий бўлмаган маълумотларни нисбатан янги ва етарлича ишончли усули уларни Интернетда узоклашган серверларда Web-папкаларда сақлаш ҳисобланади. Фойдаланувчи маълумотларини сақлаш учун бўш жойни (бир неча Мбайтгача) текинга берадиган хизмат турлари мавжуддир.

Ахборотни ҳимоя қилишнинг ёрдамчи воситалари вирусга қарши дастурлар ва аппаратли ҳимоя қилиш воситалари ҳисобланади. Масалан, бош платада уланиш жойини оддийгина ўчириб қўйиш ДЭҚҚ сини қайта дастурланадиган (флэш - BIOS) микросхемасини ўчиришни амалга ошириш имконини бермайди, бунда бу ишни ким амалга оширишига: компьютер вирусими, ёмон ниятли кишими ёки тартибсиз фойдаланувчими бунга боғлиқ эмасдир.

Вирусга қарши ҳимоя қилишнинг етарлича кўп дастур воситалари мавжуддир.

Вирусдан ҳимоя қилиш учун ишлатиш мумкин:

- ахборотни ҳимоя қилишнинг умумий воситалари, улар магнит дискларини физик бузишдан кафолатлаш, каби, нотўғри ишлайдиган дастурлар ёки фойдаланувчиларнинг нотўғри ҳаракатлари каби фойдалидир;
- вирус билан зарарланиш эҳтимолини камайтириш имконини берадиган профилактик чоралар;
- вируслардан ҳимоя қилиш учун махсус дастурлар.

Ахборотни ҳимоя қилишни умумий воситалари вирусдан ҳимоя қилиш учун фойдали эмас. Бу воситаларнинг иккита асосий тури мавжуддир:

-ахборотни нусхалаш - файллар ва дискларнинг тизимли соҳаларини нусхаларини яратиш;

-мурожаат қилишни чеклаш -тақиқланган ахборотни ишлатишни бартараф этиш, хусусан, вируслардан дастурларни ва маълумотларни ўзгаришлардан ҳимоя қилишдан, нотўғри ишлайдиган дастурлардан ва фойдаланувчиларнинг нотўғри ҳаракатларидан ҳимоя қилишдан.

Ахборотни ҳимоя қилишни умумий воситалари вируслардан ҳимоя қилиш учун жуда муҳимлигига қарамасдан, уларнинг ўзлари етарли эмас. Вируслардан ҳимоя қилиш учун махсус дастурларни қўллаш ҳам керакдир.

Бу дастурларни бир нечта турларга бўлиш мумкин: детекторлар, вакцина (иммунизаторлар), докторлар (ораш), тафтишчилар (файлларда ва дискларнинг тизимли соҳаларида ўзгаришларни назорат қилиш дастурлари), доктор-тафтишчилар ва фильтрлар (вируслардан ҳимоя қилиш учун дастурлар).

Вируслардан компьютерларни ва маълумотларни хавфсизлигига хисса қўшиш бўйича биринчи ўринда, шубхасиз, маълумотларни нусхалаш, ҳисобланади. Вирус билан компьютер зарарланганда ҳали ҳам ҳеч бўлмаганда маълумотларнинг бир қисмини тиклаш мумкин, лекин агар компьютерда қаттиқ диск бузилса, унда нима қилмоқ керак? Бундан ташқари, нусхалари архивда мавжуд бўлган дастурлар ва маълумотлар исталганча бузилганда, қўшимча уларни турли “докторлар” билан даволашни амалга оширишга интилмасдан, архивдан тўғри нусхаларни нусхалаш мақсадга мувофиқдир.

Хавфсизликка ҳисса қўшиш бўйича иккинчи ўринга маълумотларга мурожаат қилишни чеклашни қўйиш мумкин. Агар аксарият кўпчилик ишлатиладиган дастурлар тўплами ёзишдан ҳимоя қилинган мантиқий дискда жойлашган бўлса, унда вирус билан зарарланганда бу тўпламлар бузилмайдилар ва зарарланиш оқибатларини бартараф этиш учун нисбатан кам уринишлар талаб этилади.

Тафтишчилар дастури- (вирус билан зарарланишни олдиндан пайқаш) учинчи ўринда турадилар, улар дастурларнинг ва маълумотларнинг бутунлигини аниқлайдилар. Бундай текшириш вируснинг борлигини, у ҳам кўп нарсаларни бузишга улгурмасдан олдин, энг бошланғич босқичда пайқаш имконини беради.

Фильтрлар дастури тўртинчи ўринда туради. Бу дастурлар кўплаб вирусларни (ҳаммасини бўлмаса ҳам), улар хали кўп нарсаларни бузишга ёки зарарлантиришга улгурмасдан олдин, энг бошланғич босқичда пайқаш имконини беради. Antivirus ва Flu Shot Plus туридаги дастурлар фильтрлар дастурига тегишлидир.

Детекторлар дастури - бешинчи ўринда турадилар, улар янги олинган дастур таъминотида вирусларнинг мавжудлигини текшириш учун ишлатилади.

Докторлар дастури- (фаглар) олтинчи ўринда (умуман биринчида эмас) жойлашган. Уларни, бузилган дастурни нусхаси архивда бўлмаганда, ва уни бошқа усул билан олиш қийин бўлган ҳоллардагина қўллаган маъқулроқ. Бундан ташқари, агар дастур-фаг ишлатилаётган бўлса, унда кейин тикланган файлни дастур-тафтишчи билан албатта текшириш керак бўлади (тушунарлики, агар бу файл тўғрисидаги ахборот олдиндан сақланган бўлса), лекин ҳар доим ҳам дастур-доктор тўғри даволайвермайди.

Ва ниҳоят, энг охирги ўринда **вакциналар доктори** жойлашган. Дунёда минглаб вируслар мавжуд бўлган шароитларда айнан компьютер зарарланадиган вирусдан файлни ҳимоя қилиш эҳтимоли жуда ҳам кичкинадир. Бундан ташқари, дастурни ёзувдан ҳимоя қилинган дискетага жойлаштириш янада самаралироқдир.

Жуда кўп фойдаланувчилар таъкидламоқдаларки, вируслардан ҳимоя қилиш учун вирусларни пайқайдиган ва уларни йўқотадиган дастурларни иложи борича кўпроқ (яъни детекторлар дастурини ва докторларни) йиғиш керак, ҳимоя қилишнинг бошқа чораларини инобатга олмаслик мумкин: вирус қачон пайдо бўлса, унда бу дастурлардан тўғри келадиган “дорини” танлаш балки мумкин бўлади. Шу билан бирга вирусдан келадиган зарарни камайтириш учун тиббиёт ходимлари қадимдан гапириб келаётган қоидага риоя қилиш керак: «касални даволагандан кўра унинг олдини олган яхшироқ».

5.3.2. Вирус билан зарарланишга қарши профилактика

Бу параграфда компьютерни вирус билан зарарланиш эҳтимолини камайтириш, ҳамда, агар барибир вирус билан зарарланиш бўлиб ўтган бўлса, ундан келадиган зарарни минимумга олиб келиш чоралари кўриб чиқилади. Албатта, вирус билан зарарланишга қарши профилактика учун кўриб чиқилган барча воситаларни эмас, балки фақатгина сиз керакли деб ҳисоблаган воситаларнигина ишлатиш керак.

1. Ўзгартирмайдиган файлларни ўзида сақлаган дискеталарда ёзувдан ҳимоя қилувчи кесилган жойини елимлаб қўйиш керак. Қаттиқ дискда ёзувдан ҳимоя қилинган мантиқий дискни яратиш ва унга ўзгартирилмасдан, фақат ишлатиладиган дастурларни ва файлларни жойлаштириш керак.

2. Вирусдан ҳимоя қилиш учун резидентли фильтрлар дастурини доимо, мумкин бўлган ҳамма вақтда ишлатиш мақсадга мувофиқдир.

3. Дискеталарнинг юкланадиган секторлари орқали тарқаладиган вирус билан зарарланишдан халос бўлиш учун қаттиқ дискдан компьютерни қайта юклашдан олдин А: дисководда бирорта дискета йўқлигига ишонч ҳосил қилинг. Агар у ерда дискета бор бўлса, унда қайта юклашдан олдин дисковод эшигини очиб қўйинг.

4. Агар сиз компьютерни дискетадан қайта ишлашни хохласангиз, фақатгина операцион тизимли ёзишдан ҳимоя қилинган “эталон” дискетадан фойдаланинг.

5. DOS бошланғич юкланганда бажариладиган AUTOEXEC.BAT буйруқли файлига, параметр сифатида файлларнинг унча катта бўлмаган рўйхатини кўрсатган ҳолда, файлларда ўзгаришларни текшириш учун тафтишчи-дастурни чақиришни қўйиш мақсадга мувофиқдир.

6. Сиз яратган ёки ўзгартирган файлларни даврий равишда архивлаш керак. Файлларни архивлашдан олдин, компьютерда вирус йўқлигига ишонч ҳосил қилиш ва архивга бузилган ёки зарарланган файлларни жойлашишидан халос бўлиши учун, вирус борлигини аввалроқ диагностика қилиш учун дастурни бажариш мақсадга мувофиқдир.

7. Бошқа компьютерлардан дастур таъминотини кўчириб ёзиш керак эмас, чунки у вирус билан зарарланган бўлиши мумкин.

8. Сиз бирорта дастур маҳсулотини ёки ҳужжатни олганингиздан ёки ишлаб чиққанингиздан кейин мос файлларнинг эталонли архивли нусхасини яратишингиз керак, унинг ёрдамида бу файлларни компьютер вирус билан зарарланганда енгилгина тиклаш мумкин бўлади.

9. Ташқаридан олиб келинган дискеталарни ишлатишдан олдин детектор - дастур ёрдамида вирус борлигига текшириш керак. Буни хаттоки, сиз бу дискеталарда фақатгина маълумотли файлларни ишлатишни истаган ҳолатларингизда ҳам фойдалидир - сиз вирусни қанчалик тез пайқасангиз, шунчалик яхшидир.

10. Компьютерда ишлашга бегона шахсларни, айниқса агар улар ўзларининг дискеталарига эга бўлмасалар, қаровсиз қолдирмасдан рухсат бермаслик керак. Жуда кўп ҳолларда компьютерни вирус билан зарарланиш сабаби дискетада олиб келинган, кимдир уни компьютерда 10-15 минут ўйнаган компьютер ўйини ҳисобланади. Агар компьютерга тасодифий шахсларни мурожаат қилишдан халос бўлишнинг имкони бўлмаса (масалан, ўқув марказида), компьютернинг қаттиқ дискида жойлашган барча ёки деярли барча дастурларни ёзишдан ҳимоя қилинган дискда жойлаштирилган мақсадга мувофиқдир. [21; 250-257]

11. Агар компьютер қаттиқ дискка эга бўлса, ҳар доим ишончли жойда “тизимли” дискетага, яъни DOS операцион тизимини юклаш мумкин бўлган дискетага эга бўлиш керак.

12. Турли компьютер вирусларини пайқаш ва йўқотиш учун дастурларни йиғиб бориш керак. Бу дастурларни ишончли жойда сақланиш керак бўлган дискетага жойлаштириш керак. Бу дискета билан биргаликда уни ишлатиш бўйича йўриқномани сақлаш мақсадга мувофиқдир. Дастурларни танлаб олишда “миқдор сифатни алмаштирмайди” деган қоидани ёддан чиқармаслик керак ва фақатгина:

- ўзига яхши тавсиянома берган;
- вирусларнинг кенг диапазонига ёки бошқа дастурлар билан “ушлаб олинмайдиган” вирусларга мўлжалланган;
- ўзларида вируслар йўқлигига текширилган дастурларни йиғиш керак

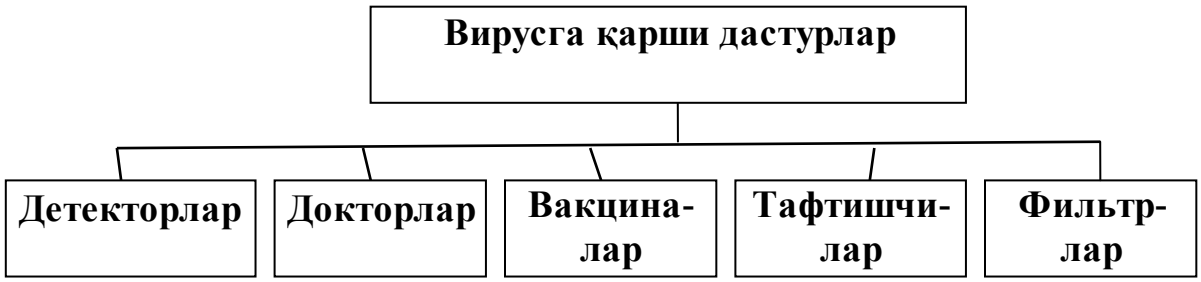
5.4 Вирусларни пайқаш ва улардан ҳимоя қилиш дастурлари ва уларнинг тавсифлари

Компьютер вирусларини пайқаш, ўчириш ва улардан ҳимоя қилиш учун махсус дастурларнинг бир нечта турлари ишлаб чиқилган, улар вирусларни пайқаш ва йўқотиш имконини беради. Бундай дастурлар **вирусга қарши** дастурлар деб аталади.

Вирусга қарши дастурларнинг қуйидаги турлари мавжуд:

1) детекторлар дастури;
2) докторлар дастури ёки фаглар;
3) тафтишчилар дастури;
4) фильтрлар дастури;
5) вакциналар дастури ёки иммунизаторлар.

Вирусга қарши дастурларнинг турлари



Детекторлар дастури маълум бир вирус учун тавсифли бўлган байтлар кетма-кетлигини (вирус сигнатуралари) тезкор хотирада ва файлларда қидиришни амалга оширилади, ва вирусни пайқаганда мос хабарни беради. Бундай вирусга қарши дастурларнинг камчилиги шундаки, улар фақат бундай дастурларнинг ишлаб чиқув-чиларига маълум бўлган вирусларнигина топа оладилар.

Докторлар дастури ёки **фаглар,** ҳамда **вакциналар дастури** нафақатгина вируслар билан зарарланган файлларни топмасдан, балки уларни “даволайди” ҳам, яъни файлдан вирус-дастур танасини ўчирадилар, файлларни бошланғич ҳолатга қайтарадилар. Фаглар ўзининг ишини бошида тезкор хотирада вирусларни қиди-ради, уларни йўқотади ва фақат кейингина файлларни “даволашга” ўтади. Фаглар орасида **ярим фагларни** ажратиш мумкин, улар катта миқдордаги вирусларни қидириш ва йўқотиш учун мўлжалланган докторлар дастуридир. **Aidstest, Scan, Norton Antivirus** ва **Doctor Web** энг машҳур полифаглар ҳисобланадилар. Янги вируслар доимо пайдо бўлиб боришини инобатга олиб, детекторлар дастури ва докторлар дастури тезда эскирадилар, ва уларнинг версияларини доимо янгилаб бориш талаб этилади.

Тафтишчилар дастури вируслардан ҳимоя қилишнинг энг ишончли усулларига тегишлидир. Тафтишчилар, компьютер вирус билан зарарланмаганда, каталогларнинг дастурларини ва дискнинг тизимли соҳаларини бошланғич қийматини эслаб қоладилар, кейин эса даврий равишда ёки фойдаланувчининг

хохиши бўйича жорий ҳолатни бошланғич ҳолат билан таққослайди. Пайқалган ўзгаришлар видеомонитор экранига чиқарилади. Қоидага кўра, ҳолатларни таққослаш опкрацион тизим юклангандан кейин бирданига амалга оширилади. Таққослашда файл узунлиги, циклик назорат қилиш коди (файлнинг назорат йиғиндиси), ўзгартириш санаси ва вақти, бошқа параметрлар текширилади. Тафтишчилар дастури етарлича ривожланган алгоритмларга эга, стелс-вирусларни пайқайдилар, ва ҳаттоки текширилаётган дастурдаги версияларини ўзгаришларини вирус томонидан киритилган ўзгаришлардан фарқини пайқайдилар.

Россияда кенг тарқалган **“Диалог-Наука”** фирмасининг **Adinf** дастури тафтишчилар дастури қаторига киради.

Фильтрлар дастури ёки “қоровуллар”- компьютер ишлашида вируслар учун тегишли бўлган шубҳали ҳаракатларни пайқаш учун мўлжалланган, унча катта бўлмаган резидентли дастурлардир. Бундай ҳаракатлар бўлиши мумкин:

1) .COM ва .EXE кенгайтмали файлларни тўғрилашга интилишлар;
2) файллар атрибутларини ўзгартириш;
3) абсолют манзил бўйича дискка тўғридан-тўғри ёзиш;
4) дискнинг юкланадиган секторларига ёзиш;
5) резидент дастурни юклаш.

Бирор дастур томонидан кўрсатилган амалларни бажаришга интилиш бўлганда “қоровул” фойдаланувчига хабар юборилади ва мос амалларни таъқиқлашни ёки рухсат беришни таклиф этади. Фильтрлар дастури жуда фойдалидир, чунки улар вирусни уни пайдо бўлишини бошланғич босқичларида, кўпайгунга кадар пайқаш қобилиятига эгадир. Аммо улар файлларни ва дискларни “даво-ламайдилар”. Вирусларни йўқотиш учун бошқа дастурларни, масалан фагларни, қўллаш талаб этилади. Дастур-қоровулларнинг камчиликларига уларнинг жонга тегишини “(масалан, улар бажарилаётган файлни нусхалашга ихтиёрий интилиш тўғрисида доимо огоҳлантириб турадилар), ҳамда бошқа дастур таъминоти билан мумкин бўлган келишмовчиликларни келтириш мумкин. Дастур-фильтрга мисол тариқасида MS DOS операцион тизимининг утилитларини тўпламини таркибига кирувчи **Vsafe** дастурини келтириш мумкин. [25; 112-119]

Вакциналар ёки иммунизаторлар - файлларни зарарланишини бартараф этувчи резидентли дастур ҳисобланади. Вакциналарни вирусни “даволайдиган” дастур докторлар йўқ бўлганда қўлланилади. Вакциналаш фақатгина маълум бўлган вируслардан мумкиндир. Вакцина дастурни ёки дискни шундай ўзгартирадики, бу уларнинг ишлашида акс эттирилмайди, вирус эса уларни зарарланган деб қабул қилади ва шунинг учун татбиқ этилмайди. Ҳозирги вақтда вакциналар дастури чекланилган қўлланишга эга.

Вируслар билан зарарланган файллар ва дискларни ўз вақтида пайқаш, ҳар бир компьютерда пайқалган вирусларни тўлиқ йўқотиш вирус эпидемиясини бошқа компьютерларга тарқалишини олдини олиш имконини беради.

5.5. Компьютер вирусларидан ҳимоя қилиш учун асосий чоралар

Компьютерни компьютер вируслари билан зарарланишини олдини олиш ва дискларда ахборотларни ишончли сақлашни таъминлаш учун қуйидаги қоидаларга риоя қилиш керак:

- компьютерни замонавий вирусга қарши дастурлар, масалан Aidstest ёки Doctor Web, билан таъминланг ва уларнинг версияларини доимо янгилаб боринг;
- бошқа компьютерларда ёзилган ахборотларни дискетадан ўқишдан олдин ўзингизни компьютердаги вирусга қарши дастурни ишга тушириб бу дискеталарни вирус борлигига доимо текширинг;
- ўзингизни компьютерингизга архивланган кўринишдаги файлларни кўчириб ўтишда, текшириш соҳасини ҳозиргина ёзилган файллар билан чеклаган ҳолда, уларни қайта архивлангандан кейин тезда қаттиқ дискда текширинг;
- олдиндан ОТ ни ёзишдан ҳимоя қилинган тизимли дискетадан юклаб, файлларни, хотираларни ва тизимли соҳаларни ёзишдан ҳимоя қилинган дискетадан вирусга қарши дастурларни ишга тушириб компьютернинг қаттиқ дисклариниви руслар борлигига даврий равишда текшириб боринг;
- бошқа компьютерда ишлаганда ўзингизни дискетани, агар уларга ахборотни ёзиш амалга оширилмаса, ёзишдан ҳар доим ҳимоя қилинг;
- Сиз учун муҳим бўлган ахборотларни архивли нусхаларини дискеталарда албатта ишлаб чиқинг;
- компьютерни юкланадиган вируслар билан зарарланишини олдини олиш учун операцион тизимни қайта юклашда ёки компьютерни улашда А: дисководда дискетани қолдирманг;
- компьютер тармоқларидан олинадиган барча бажарадиган файлларни назорат қилиш учун вирусга қарши дастурларни ишлатинг.
- Aidstest ва Doctor Web дастурларини қўллашни юқори хавф-сизлигини таъминлаш учун **Adinf** диск текширувчисини ҳар куни ишлатиб бориш керак.

5.5.1. “Диалог-наука” ҳиссадорлик жамиятини вирусга қарши тўплами

Компьютер вируслари билан курашишнинг кўплаб замонавий воситалари орасида “Диалог-наука” ҳиссадорлик жамиятини (ҲЖ) вирусга қарши тўплами устунликка эгадир, унга тўртта дастур маҳсулоти киради: **Aidstest** ва **Doctor Web** (қисқача Dr Web) полифаглари, диск тафтишчиси **Adinf** ва даволовчи **Adinf Cure Module** блоки. Бу вирусга қарши дастурларни қандай ва қачон қўлланишини қисқача кўриб чиқамиз.

A. Aidstest дастури - полифаг

Aidstest - бу жуда ҳам кенг тарқалган 1300 дан ортиқ компьютер вирусларини пайқаш ва йўқотиш имкониятига эга бўлган дастурдир. Aidstest версиялари янги вируслар тўғрисидаги ахборот билан доимий равишда янгиланиб ва тўлдирилиб бормоқда.

Aidstest ни ишга тушириш учун қуйидаги буйруқни бериш керак:

Aidstest <path>[<options>]

бу ерда: **path -** диск номи, тўлиқ ном, файл спецификацияси, файллар гуруҳининг ниқоби:

*- қаттиқ дискнинг барча бўлимлари

**- тармоқ ва CDROM дискларини қўшган ҳолда барча дисклар.

Options - қуйидаги калитларнинг исталган комбинацияси:

F- зарарланган дастурларни тўғрилаш ва бузилганларини ўчириш;

G- барча файлларни кетма-кет текшириш (фақатгина .COM, .EXE ва SYS ларни эмас);

H- бузилган вирусларни қидириш учун секин ишлаш;

X- вирус таркибида бузилишлар бўлган барча файлларни ўчириш;

Q- бузилган файлларни ўчиришга рухсат сўраш;

R- кейинги дискектани қайта ишлашни таклиф этмаслик.

Мисол 1. **AISTEST B: /F/G/Q**

B: дискни “даволаш” ва текшириш учун вирусга қарши Aidstest дастурини ишга тушириш, пайқалган зарарланган дастурлар тўғриланади. Агар файлни тўғрилашга имкон бўлмаса, унда дастур уни ўчиришга рухсат сўрайди.

5.5.2. Doctor Web полифаг дастури

Бу дастур, энг аввало, компьютер оламида нисбатан яқинда пайдо бўлган полиморфли вируслар билан курашиш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун Dr.Web ни ишлатиш Aidstest дастурига тўлиқ ўхшашдир. Бунда текширишни дубллаш деярли бўлмайди, чунки Aidstest ва Dr.Web дастурлари вирусларнинг турли тўпламлари билан ишлайди.

Dr.Web дастури Aidstest кучи етмайдиган мураккаб вируслар мутантлар билан самарали курашиши мумкин. Aidstest дан фарқли равишда Dr.Web дастури хусусий дастурли коддаги ўзгаришларни пайқаш, ҳамда “вакцинали беркитишни” енгиб ўтган ҳолда шифрланган ва ихчамлаштирилган файлларга кириб янги, ноъмалум вируслар билан зарарланган файлларни самарали аниқлаш қобилиятига эгадир. Бу кучли эвристик таҳлилчи мавжудлиги ҳисобига эришилади.

Эвристик таҳлил режимида Dr.Web дастури вируслар учун характерли бўлган янги ёки унга номаълум вирусларни пайқашга интилиб файлларни ва дискларнинг тизимли соҳаларини тадқиқот этади. Агар шундай вируслар топилса, унда объект номаълум вирус билан зарарланганлиги тўғрисида огоҳлантириш берилади.

Эвристик таҳлилни учта даражаси кўзда тутилган. Эвристик таҳлил режимида ёлғон ишлашлар, яъни зарарланмаган ҳисобланмаган файлларни детекторлаш мумкиндир. “Эвристика” даражаси ёлғон ишлаш мавжуд бўлмаган кодни таҳлил қилиш даражаси кўринишига эгадир. Эвристик таҳлилчининг ишлашини биринчи иккита даражаси тавсия этилади.

Эвристик таҳлилни учинчи даражаси файлларни яратилишини “шубхали” вақтига уларни қўшимча текширишни кўзда тутади. Файллар зарарланишида баъзи бир вируслар ушбу файлларнинг зарарганлик белгиси каби яратилишнинг нотўғри вақтини ўрнатади. Масалан, зарарланган файллар учун секундлар 62 қийматга эга бўлиши мумкин, яратилиш йили эса 100 йилга кўпайтирилиши мумкин.

Вирусга қарши Dr.Web дастурини етказиб бериш таркибига яна унинг имкониятларини кенгайтирадиган дастурнинг асосий вирусли тўпламига файл қўшимчалар ҳам кириши мумкин.

Dr.Web дастури билан икки режимда ишлаш мумкин:

- меню ва мулоқот ойнасини ишлатиб тўлиқ экранли интерфейс режимида;
- буйруқ қатори орқали бошқариш режимида.

Доимий бўлмаган бир марталик қўллаш учун биринчи режим қулайроқдир, лекин дискеталарнинг доимий киришини назорат қилиш мақсадида доимий қўллаш учун яхшиси иккинчи режимини қўллаган маъқулдир.

Иккинчи режимни ишлатганда Dr.Web нинг мос ишга тушириш буйруғи Norton Commander операцион қобиғини фойдаланувчисини менюсига ёки махсус буйруқли файлга киритилган бўлиши мумкин.

Dr.Web ни ишга тушириш учун буйруқ қатори қуйидаги кўринишга эга:

Dr.Web [диск:] [йўл] [калитлар]

бу ерда **диск: -** қаттиқ дискни мантиқий қурилмаси ёки эгилувчан дискни физик қурилмаси, масалан, F: ёки A:

*- қаттиқ дискдаги барча мантиқий қурилмалар;

йўл - бу талаб этилаётган файлларнинг йўли ёки ниқоби.

Энг муҳим калитлар:

/ AL-берилган қурилмадаги барча файлларнинг диагностикаси;

/ CU [P] - дискларни ва файлларни “даволаш”, топилган вирусларни ўчириш;

P- фойдаланувчининг тасдиқлаши билан вирусларни ўчириш;

/ DL-тўғрилаб даволашни имкони бўлмаган файлларни ўчириш;

/ HA [даража]- файлларни эвристик таҳлил қилиш ва уларда номаълум вирусларни қидириш, бу ерда [даража] 0,1,2 қийматларни қабул қилиш мумкин;

/ CL - буйруқли қатор режимида дастурни ишга тушириш, файлларни ва тизимли соҳаларни тестлашда тўлиқ экранли интерфейс ишлатилмайди;

/ QU- тестлашдан кейин тезда DOS га чиқиш.

Агар Dr.Web нинг буйруқли қаторида бирорта ҳам калит кўрсатилмаган бўлса, унда жорий сўров учун барча ахборот DRWEB. EXE жойлашган каталогда жойлашган DRWEB.INI конфигурация файлидан ўқилади. Конфигурация файли тестлаш учун зарур бўлган параметрларни сақлаш буйруғи ёрдамида Dr.Web дастури билан ишлаш жараёнида ишлатиладиМисол-2: **DrWeb B: / AL/ CUP/ HA1/QU/CL**

B: дискни текшириш ва даволаш учун Dr.Web вирусга қарши дастурини ишга тушириш.

5.5.3. Тўлиқ экранли интерфейс режимида Dr. Web дастури

билан ишлаш технологияси

Тўлиқ экранли интерфейс режимида ишга тушириш учун буйруқ қаторига фақат дастур номини киритиш етарлидир. Дастур юклангандан кейин компьютернинг тезкор хотирасини тестлаш, агар у компьютернинг олдинги ўрнатилишида ўчирилмаган бўлса, бошланади. Тестлашнинг бориши тестлаш ойнасида акс эттирилади. Хотирани унинг тугагандан кейин тўхташ амалга оширилади. Дастур ишлашини, агар экраннинг юқори қаторида жойлашган асосий менюдан фойдаланилса, давом эттириш мумкин. Менюни фаоллаштириш учун F10 клавишини босиш керак. Асосий меню қуйидаги режимларга эга:

Dr.Web ТЕСТ НАСТРОЙКИ ДОПОЛНЕНИЯ

Исталган режимни танлашда мос қисмменю очилади.

Dr.Web қисмининг менюси DOS га вақтинчалик кириш, Dr.Web дас-тури ва унинг муаллифи тўғрисида қисқача ахборотни олиш ёки дастурдан чиқиб кетиш имконини беради.

ТЕСТ қисм менюси файлларни тестлашни ва “даволашни” асосий амалларини бажариш, ҳамда бажарилган ишлар тўғрисида ҳисоботларни кўриб чиқиш имконини беради.

Настройки қисмининг менюси мулоқот ойналари ёрдамида дастурни созлаш параметрларини ўрнатиш, қидиришни йўлларини ва ниқобларини ўрнатиш ва параметрларни DRWEB.INI конфигурация файлида сақлаш учун хизмат қилади.

ДОПОЛНЕНИЯ қисмининг менюси дастурнинг асосий вирусли базасига, унинг имкониятларини кенгайтирадиган файл-қўшимчаларни қўшиш учун ишлатилади.

5.5.4. Дискнинг вирусга қарши тафтишчиси Adinf

Adinf тафтишчиси стелс-вирусларни, вирус-мутантларни ва бугунги кунгача номаълум вирусларни қўшган ҳолда исталган вирусларни пайдо бўлишини пайқаш имконини беради.

Adinf дастури эслаб қолади:

- юкланадиган секторлар тўғрисидаги ахборотни;
- бузилган кластерлар тўғрисидаги ахборотни;
- файлларнинг узунлиги ва назорат йиғиндиларини;
- файлларни яратилиш санаси ва вақтини.

Компьютерни бутун ишлаши давомида Adinf дастури бу тавсифларни сақланганлигини кузатиб боради. Ҳар кунги назорат қилиш режимида Adinf дастури компьютер биринчи марта уланганда автоматик равишда ишга туширилади. Айниқса вирусга ўхшаш ўзгаришлар кузатиб борилади, улар тўғрисида тезда огоҳлантириш берилади. Файлларнинг бутунлиги назорат қилишдан ташқари Adinf дастури қисм каталогларни яратишни ва ўчиришни, файлларни яратишни, силжитишни ва қайта номлашни, янги бузуқ кластерларни пайдо

бўлишини, юкланадиган секторларини сақлаганлигини ва кўплаб бошқа нарсаларни кузатади. Вирусни тизимга татбиқ қилиш учун мумкин бўлган барча жойлар ёпиб қўйилади. Adinf дастури, DOS ни ишлатмасдан BIOS га тўғридан-тўғри мурожаат қилиб дискни секторлари бўйича ўқиган ҳолда текширади.

5.5.5. Adinf Cure Module даволовчи блоки

Adinf Cure Module - бу компьютерни янги вирусдан "даво-лашга" ёрдам берадиган дастур бўлиб, у вирус маълум бўлган Aidstest ёки Dr.Web полифагларни янги версияларини кутиб турмайди. Adinf Cure Module дастури, вирусларни кўплаб турлари борлигига қарамасдан уларни файлларга татбиқ қилишни унчалик кўп бўлмаган турлича усуллари мавжудлиги далилини ишлатади. Меъёрий ишлаш вақтида, доимий равишда ишга туширишда Adinf тафтишчиси Adinf Cure Module дастурига охирги марта ишга туширилгандан бери қайси файллар ўзгарганлиги тўғрисида хабар беради. Adinf Cure Module дастури бу файлларни таҳлил қилади ва ўзининг жадвалларига, вирус билан зарарланганда файлларни тиклаш учун керак бўладиган, ахборотни ёзиб қўяди. Агар зарарланиш бўлиб ўтган бўлса, унда Adinf тафтишчиси ўзгаришларни пайқайди ва Adinf Cure Module дастурини яна чақиради, у зарарланган файлни таҳлил қилиш ва уни ёзиб қўйилган ахборот билан таққослаш асосида файлнинг бошланғич ҳолатини тиклашга ҳаракат қилади.

5.6. Дастур маҳсулотларини ҳимоя қилиш

Дастур маҳсулотлари бир қатор сабабларга кўра ҳимоя қилишнинг муҳим объекти ҳисобланади.

Биринчидан, улар юқори малакали мутахассисларнинг, баъзида ўнлаб ҳаттоки юзлаб кишиларнинг интеллектуал меҳнати маҳсулоти ҳисобланади.

Иккинчидан, бу маҳсулотларни лойиҳалаш жараёни моддий ва меҳнат ресурсларини сезиларли ҳаракатлари билан боғлангандир, қимматбахо компьютер жиҳозларини ва илмий-техникавий технологияларни ишлатишга асосланган.

Учинчидан, бузилган дастур таъминотини тиклаш анчагина меҳнат сарфини талаб этади, ҳисоблаш техникаси жиҳозларини ишламай туриб қолиш эса ташкилотлар ва жисмоний шахслар учун нохуш натижаларга олиб келиши мумкин.

Дастур маҳсулотларини ҳимоя қилиш қуйидаги мақсадларни кўзда тутади:

- фойдаланувчиларнинг алоҳида тоифаларини дастур маҳсулотлари билан ишлаш учун тақиқланган мурожаат қилишни чеклаш;
- маълумотларни қайта ишлашни меъёрда олиб бориш мақсадида дастурларни олдиндан режалаштирилган бузилишини инкор қилиш;
- дастур маҳсулотини ишлаб чиқарувчиларни нуфузини бузиш мақсадида дастурларни олдиндан режалаштирилган ўзгартирилишни инкор қилиш;
- дастурларни тақиқланган ададлашни (нусхалашни) инкор қилиш;

- дастурларни мазмунини, таркибини ва ишлаш механизмини тақиқланган ўрганишни инкор қилиш.

Дастур маҳсулотлари турлича объектларнинг кишини, техник воситаларни, махсус дастурларни, атроф муҳитни ва бошқаларни тақиқланган таъсирларидан ҳимоя қилиниши керак.

Кишилар дастур маҳсулотига шу дастур маҳсулотини ҳужжатларини ёки машина ташувчисининг ўзини ўғрилаш ёки физик йўқотиш, дастур воситаларини ишлаш қобилиятини бузиш йўли билан таъсир этиши мумкин.

Техник воситалар (аппаратура) компьютерга ёки узатувчи муҳитга уланиш йўли билан дастурларни ўқиш, қайта шифрлаш, ҳамда уларни физик бузишни амалга ошириши мумкин.

Махсус дастурлар ёрдамида дастур маҳсулотини вирус билан зарарлантириш, уни тақиқланган нусхалаш, унинг маъносини рухсатсиз ўрганиш ва амалга ошириши мумкин.

Ва нихоят, **атроф-муҳит** аномал ҳодисалар ёрдамида (электромагнит нурланишни кўпайиши, ёнғин, сув тошқини ва бошқалар.) дастур маҳсулотини физик бузиш амалга оширилиши мумкин.

Дастур маҳсулотларини ҳимоя қилишни энг оддий ва мумкин бўлган усули уларга қуйидаги усуллар билан мурожаат қилишни чеклаш ҳисобланади:

- дастурлар ишга тушганда уларни пароль билан ҳимоя қилиш;
- калит дискетани ишлатиш;
- компьютернинг киритиш - чиқариш портига уланадиган махсус техник қурилмани (электрон калитни) ишлатиш.
- дастурларни тақиқланган нусхалашдан сақлаш мақсадида ҳимоя қилишнинг махсус дастурли воситалари:
- дастур ишга тушириладиган муҳитни идентификациялаш;
- рухсат этилган инсталляцияларни ва нусхалашларни бажарилишини миқдорини ҳисобини олиб бориш;
- тизимларнинг ишлаш алгоритмларини ва дастурларини ўрганишга қарши туриш (хаттоки ўз-ўзини бузишгача) керак.
- дастур маҳсулотлари учун самарали ҳимоя қилиш чоралари қуйидагилар ҳисобланадилар:
- ишга туширадиган дискетани ностандарт шакллантириш;
- қаттиқ дискда дастурларни жойлашган жойини қатъий белгилаш;
- киритиш-чиқариш портига қўйиладиган электрон калитга боғланиш;
- BIOS номерига боғланиш ва бошқалар.
- Дастур маҳсулотларини ҳимоя қилиш ҳуқуқий усуллар билан ҳам албатта амалга оширилиши керак, уларнинг қаторига келишувлар ва шартномаларни, патентли ҳимоя қилишни, муаллифлик ҳуқуқини, технологик ва ишлаб чиқариш махфийлигини ва бошқаларни киритиш мумкин.

Компьютер тизимларини ривожланиши билан янада янги компьютер вируслари пайдо бўлмоқда, шунга мос равишда турли хил антивирусли тизи,млар ва воситалар ҳам пайдо бўлмоқда. Одатда вируслар компьютер тизимида сақлаётган дастур таъминотини маълумотларни ўзгартиради ёки йўқ килади. Зарар келтирадиган дастурларга биологик вирусларнинг хоссалари киради.

Компьютер вирусларини шаклларини ва турли - туманлигини кўп қирралилиги тавсифли схемаларда турли хил белгилар бўйича келтирилгандир. Айниқса «мантиқий бомбалар», «троян отлари», «чувалчанглар» каби вирусларни таъкидлаш жоиздир.

Шак-шубхасиз, махсус антивирусли воситаларни ишлаб чиқиш ва ишлатиш долзарбдир. Антивирусли воситалар вирусдан зарарланиш окибатларини аниқлаш (сканерлаш, ўзгаришларни пайқаш усули, эвриетик тахлил этиш, аппарат - дастурли антивирусли воситалар ва хакозо) ва йук килиш масалаларини ечади, шу билан бир каторда файлларни ва хотира сохаларини, юкланиш секторларини тиклайди.

Антивирусли дастурлардан детектор, ревизор (тафтишли) ва «коровул» дастурларини таъкидлаб утиш мумкин.

Компьютер вирусларидан ҳимоя қилишнинг асосий чораларидан дастур маҳсулотларини расмий йўл билан ишлатишни келтириш мумкин. Алоҳида таъкидлаш керакки, антивирусли воситалар доимо янгиланиб бориши керак, бунда ташқаридан келадиган янги дастурларга ва файлларга алоҳида эътиборни қаратиш керак.

Таъкидлаб ўтамизки, дастур маҳсулотларини вируслардан ҳимоя қилишнинг ахамияти жуда каттадир. Бундай ҳимоя, оддий вируслардан ташқари, албатта ҳуқуқий усуллар билан амалга оширилиши керакдир.

Асосий атамалар

Вирусга қарши дастур, юкланадиган вирус, компьютер вируси, вирус-мутант, кўринмайдиган вирус (стелс-вирус), хавфсиз вирус, резидент бўлмаган вирус, хавфли вирус, жуда хавфли вирус, паразит (текинхур) вирус, резидент вирус, вирус-репликатор (чувалчанг), тармоқли вирус, троян вируси, файл вируси, зарарланган дастур, зарарланган диск, дастур-вакцина, дастур-доктор (фаг), дастур-детектор, дастур-тафтишчи, дастур-фильтр (қоровул), Aidstest ва Doctor Web полифаг дастурилари.

Назорат саволлари

1. Компьютер вируси нима ва унинг табиати қандай?
2. Вирусларни компьютерга кириб боришини асосий йўллари қандай?
3. Компьютер вирусларини зарарлари нималарда намоён бўлади?
4. Сизларга компьютер вирусларини қандай асосий кўринишлари маълум?
5. Вирусларни пайқаш ва улардан ҳимоя қилиш учун дастурларнинг қандай турлари мавжуд?
6. Детекторлар дастури ва докторлар дастурининг фарқлари ва ўхшаш жойлари нимада?
7. Тафтишчилар дастурининг ва фильтрлар дастурининг афзалликлари нималарда намоён бўлади?
8. Компьютер вирусларидан ҳимоя қилиш бўйича асосий чораларни айтиб беринг.

9. “Диалог-Наука” ХЖ нинг вирусга қарши дастурлар тўпламини таркибини ва вазифасини айтиб беринг.

10. Вирусларни пайқаш ва йўқ қилиш учун Aidstest дастурини қандай қўллаш керак?

11. Dr.Web вирусга қарши дастурини Aidstest дастуридан фарқи нимада?

12. Dr.Web дастурини қандай режимларда ишлатиш мумкин?

13. Қаттиқ дискни вируслар мавжудлигига даврий равишда текшириш технологиясини айтиб беринг.

14. Дастур маҳсулотларини ҳимоя қилиш нима учун керак?

Тавсия этиладиган адабиётлар:

2. Романец Ю.В, Тимофеев П.А, Шаньгин В.Ф. Защита информации в КС и С. − М.: Радио и связь, 2001.

2. Домашев А.В., Грунтович М.М. и др. Программирование алгоритмов защиты информации. Учеб. пособ. – М.: Издатель Молгачева С.В. Издательство «Нолидж», 2002. – 416с.

3. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003, – 504 с.

4. Баичев С.Г. Основы современной криптографии. – М.: Горячая линия Телеком, 2001. – 1200с.

5. Эрматов Ш.Т., Шоахмедова Н.Х. Ахборотни ҳимоялашнинг криптографик усуллари. Электрон услубий қўлланма. − Т., 2005.

6 боб. ИНТЕРНЕТ ТАРМОҒИДА АХБОРОТНИ ҲИМОЯ ҚИЛИШ

6.1. Интернетда ахборотни ҳимоя қилишнинг объектив тахминлари ва тамойиллари

Глобал компьютер тармоқларини жадал ривожланиши, ахборотни қидиришнинг янги технологияларини пайдо бўлиши хусусий шахслар ва турли ташкилотлар томонидан Интернет тармоғига янада кўпроқ эътиборларини жалб қилмоқдалар. Кўплаб ташкилотлар ўзларининг локал ва корпоратив тармоқларини глобал тармоққа бирлаштиришга қарор қилмоқдалар. Тижорат мақсадларида, ҳамда махфий характерли хабарга эга бўлган ахборотни узатишда глобал тармоқларни ишлатиш ўз-ўзидан ахборотни ҳимоя қилишнинг самарали тизимини қуриш зарурлигини келтириб чиқаради.

Замонавий корхоналар Интернет глобал тармоғига мурожаат қилишга эга бўлган ҳолда оладиган барча афзалликларни санаб ўтишнинг хожати йўқдир. Лекин, бошқа барча технологиялар каби, Интернетни ишлатиш негатив оқибатларга олиб келиши мумкин. Глобал тармоқларнинг ривожланиши фойдаланувчилар сонининг кўп марта ошишига ва Интернет тармоғига уланган компьютерга бўладиган ҳужумларнинг сонини ошишига олиб келди. Компьютерлар

ҳимояланганлигини етарли бўлмаган даражаси билан шартлашилган талофатлари ўнлаб миллион долларлар билан баҳоланади. Локал ва корпоратив тармоқларни Интернет тармоғига улашда бу тармоқнинг ахборот хавфсизлиги тўғрисида қайғуриш керак.

Интернет глобал тармоғи очиқ тизим каби ахборотни эркин алмашиш учун мўлжалланган. Ўзининг очиқлик идеологияси нуқтаи назардан Интернет анъанавий ахборот тизимларига нисбатан ёмон ниятли кишиларга бир мунча катта имкониятларни тақдим этади. Интернет орқали бузғунчи:

- корхонанинг ички тармоғига кириб олиши ва тақиқланган махфий ахборотга мурожаат қилишга эга бўлиши;
- корхона учун муҳим ва қимматбахо ахборотни ноқонуний нусхалаши мумкин;
- паролларни, серверларнинг манзилларини, баъзида уларнинг мазмунини олиши;
- қайд қилинган фойдаланувчи номи остида корхонанинг ахборот тизимига кириши ва ҳ.к. мумкин.

Ёмон ниятли киши томонидан олинган ахборот ёрдамида корхонанинг рақобатбардошлигига ва унинг мижозларини ишончига жиддий путур етиши мумкин.

Етарли бўлмаган ахборот хавфсизлиги муаммолари Интернетнинг деярли барча баённомалари ва хизматлари учун "янги туғилган" ҳисобланади. Бу муаммоларнинг кўпчилик қисми Интернетнинг UNIX операцион тизимига тарихий боғлиқлиги билан боғлангандир. Маълумки, Arpanet тармоғи (Интернетнинг "ота-бувалари") АҚШнинг тадқиқот марказларини, илмий, ҳарбий ва давлат муассасаларини, йирик университетларини боғлайдиган тармоқ каби қурилгандир. Бу тизимлар коммуникациялар ва шахсий масалаларни ечиш учун платформа сифатида UNIX операцион тизимини ишлатганлар. Шунинг учун UNIX муҳитида дастурлаштириш услубияти ва унинг архитектураси хусусиятлари алмашиш баённомаларини ва тармоқда хавфсизлик сиёсатини амалга оширишга шароит яратди. Очиқлиги ва тарқалганлиги учун UNIX операцион тизими хакерларнинг севимли маскани бўлиб қолди. Шунинг учун шу нарса таажжуб эмаски, Интернет глобал тармоғида ва катта оммавийликка эга бўлаётган интратармоқларида коммуникацияни таъминлайдиган TCPғIP баённомаларининг тўплами ҳимоя қилишнинг "туғма" камчиликларига эгадир. Айнан шуларни Интернетнинг бир қатор хизматлари тўғрисида ҳам айтиш мумкин.

Интернетда хабарларни узатишни бошқариш баённомаларини тўплами (Transmission Control ProtocolғInternet Protocol-TCPғIP) турли турдаги компьютерлар ўртасида мос келишликни таъ-минлаган ҳолда бир жинсли бўлмаган тармоқли муҳитда коммуникацияларни ташкил этиш учун ишлатилади. Мос келишлик TCPғIP баённомаларни қўллаб-қувватлайди. Бундан ташқари, TCPғIP баённомалари Интернет глобал тармоғининг ресурсларига мурожаат қилиш имконини беради. TCPғIP пакетларни маршрутлашни (йўналтиришни) қўллаб-қувватлаганлиги учун у одатда тармоқлараро баённома сифатида ишлатилади. Ўзининг оммавийлиги туфайли TCPғIP тармоқлараро ўзаро таъсирлар учун дефакто стандарти бўлиб колди.

TCPғIP пакетларининг сарлавхаларида хакерлар ҳужум қилиши мумкин бўлган ахборот кўрсатилади. Хусусан, хакер юборувчининг манзилини ўзининг "зарарлик олиб юрадиган" пакетларида алмаштириши мумкин, бундан кейин улар муаллифлаштирилган мижоз томонидан узатилаётган пакет каби кўринишга эга бўладилар.

Интернетнинг баъзи-бир тарқалган хизматларининг "туғма" камчиликлари қуйидагилардир:

1. **Электрон почтани узатишнинг оддий баённомаси (SMTP - Simple Mail Transfer Protocol)** - Интернетнинг почта транспортли хизматини амалга ошириш имконини беради. Бу баённома билан боғлиқ хавфсизлик муаммолардан биттаси шундаки, фойдаланувчи электрон почта хабарининг сарлав=асида юборувчининг манзилини текшира олмайди. Натижада хакер ички тармоққа катта миқдордаги почта хабарларини юбориши мумкин, бу эса почта серверини ошиқча юкланишига ва ишлашини блокировкаланишига олиб келади.

2. Интернетда оммабоп бўлган **электрон почтанинг Send-mail дастури** баъзи-бир тармоқ ахборотини - юборувчининг IP манзилини ишлатади. Send-mail орқали юборилаётган хабарни ушлаб олиб хакер бу хабарни ҳужумлар учун, масалан спуфинг (манзилларни алмаштириш) учун, ишлатиши мумкин.

Файлларни узатиш баённомаси (FTP- File Transfer Protocol) матнли ва иккилик файлларни узатишни таъминлайди, шунинг учун уни кўпинча Интернетда ахборотга биргаликда мурожаат қилишни ташкил қилиш учун ишлатилади. Уни одатда дастурни, графикани ва ахборотнинг бошқа кўринишларини ишлаши усуллари каби кўриб чиқилади. Бу файлларнинг маълумотларига FTP-серверларда тўғ-ридан-тўғри мурожаат қилиш мумкин эмас. Маълумотларга мурожаат қилишни фақатгина уларни бутунлай FTP-сервердан локал серверга кўчириб ёзгандан кейингина мумкиндир. Баъзи бир FTP-серверлар фойдаланувчиларни ўзларининг маълумотлари архивига пароль ёрдамида мурожаат қилишни чеклайдилар, бошқалари эса эркин мурожаат қилишни (аноним FTP-сервер деб аталадиган) тақдим этади. Аноним FTP-сервер опцияларини (бўлакларини) ўзининг сервери учун ишлатишда фойдаланувчи уларда фақатгина эркин тарқатиш учун мўлжалланган файллар сақланаётганлигига ишонч ҳосил қилиши керак.

Тармоқ номлари хизмати (DNS-Domain Name System) тақсимланган маълумотлар базаси кўринишига эга бўлиб, у фойдаланувчиларнинг ва хост-компьютерларнинг номларини пакетларнинг сарлавхаларида кўрсатиладиган **IP**-манзилларга ва аксинча ўзгартириш учун ишлатилади. DNS яна компания тармоғи таркиби тўғрисидаги, масалан ҳар бир доменда IP-манзилли компьютерлар миқдори тўғрисидаги, ахборотни ҳам сақлайди. DNS нинг муаммоларидан бири шундаки, бу маълумотлар базасини муаллифлаштирилган фойдаланувчилардан "яшириш" жуда мушкулдир. Натижада DNS кўпинча хакерлар томонидан ишончли хост-компьютерларнинг номлари тўғрисида ахборот манбаи каби ишлатилади.[23; 124-129]

Узоқлашган терминални эмуляциялаш хизмати (TELNET) тармоққа бириктирилган узоқлашган тизимларга уланиш учун ишлатилади; терминал эмуляцияси бўйича асосий имкониятларни қўллайди. Интернетнинг бу серви-

сини ишлатишда фойдаланувчилар TELNET сервисида ўзларининг номи ва паролни киритиб рўйхатдан ўтишлари керак. Фойдаланувчини аутентификациялагандан кейин унинг ишчи станцияси ташқи хост-компьютерга уланган “ўтмас” (билимсиз) терминал режимида ишлайди. Бу терминалдан фойдаланувчи унга файлларга мурожаат қилишни ва дастурларни ишга тушириш имконини берадиган буйруқларни киритиши мумкин. TELNET серверига уланиб Хакер унинг дастурини фойдаланувчиларнинг номларини ва паролларни ёзадиган қилиб ўзгартириши мумкин.

Бутун дунё ўргимчак уяси (WWW-World Wide Web) - бу тармоқ иловаларига асосланган тизимдир, бу иловалар фойдаланувчиларга Интернетда ёки интратармоқларда турли серверларнинг мазмунини кўриб чиқиш имконини беради. WWW нинг энг фойдали хоссаси бошқа ҳужжатларга жўнатмалар созланган гиперматнли ҳужжатларни ва Web узелларни ишлатиш ҳисобланади, яъни бир узелдан бошқасига енгилгина ўтиш имкониятидир. Лекин бу хоссанинг ўзи WWW тизимининг энг заиф жойи ҳисобланади, негаки гиперматнли ҳужжатларда сақланаётган Web-узелларга жўнатмалар мос узелларга мурожаат қилиш қандай амалга оширилаётганлиги тўғрисидаги ахборотни ўзларида сақлайдилар. Бу ахборотни ишлатиб Хакерлар Web-узелни бузишлари ёки унда сақланаётган махфий ахборотга мурожаат қилишга эга бўлишлари мумкин.

Интернетнинг заиф хизматларига ва баённомаларига яна нусхалаш баённомаси UUCP, PIP баённомаси, графикли ойнали X Windovs тизими ва бошқалар тегишлидир.

Ҳар бир ташкилотнинг **тармоқ хавфсизлиги сиёсати** иккита ташкил этувчини ўз ичига олиши керак:

- ✓ тармоқ сервисларига мурожаат қилиш сиёсати;
- ✓ тармоқлараро экранларни амалга ошириш сиёсати;

Тармоқ сервисларига мурожаат қилиш сиёсатига мос равишда фойдаланувчилар мурожаат қилиши чекланиши керак бўлган Интернет сервисларининг рўйхати аниқланади. Яна мурожаат қилиш усулларига ҳам чекланишлар берилади, масалан, SLIP (Serial Line Internet Protocol) ва PPP (Point-to-Point Protocol) баённомаларини ишлатишга. Усулларни чеклаш фойдаланувчилар Интернетнинг “таъқиқланган” сервисларига ғайриоддий йўллар билан мурожаат қила олмаслиги учун керакдир. Масалан, агар Интернетга мурожаат қилишни чеклаш учун тармоқ маъмурияти фойдаланувчиларга WWW тизимида ишлаш имкониятини бермайдиган махсус шлюз ўрнатса, фойдаланувчилар коммутацияланадиган линия бўйича Web серверлар билан PPP-уланишларни ўрнатишлари мумкин эдилар

Тармоқ сервисларига мурожаат қилиш сиёсати одатда қуйидаги принципларнинг биттасига асосланади:

1) Интернетдан ички тармоққа мурожаат қилишни таъқиқлаш, лекин ички тармоқдан Интернетга мурожаат қилишга рухсат бериш;

2) фақатгина алоҳида “муаллифлаштирилган” тизимларни, масалан почта серверларини, ишлашини таъминлаган ҳолда Интернетдан ички тармоққа чекланган мурожаат қилишга рухсат бериш.

Тармоқлараро зкранларни амалга ошириш сиёсатига мос равишда ички тармоқнинг ресурсларига мурожаат қилиш қоидалари аниқланади. Энг аввало ҳимоя қилиш тизимини қанчалик даражада “ишончли” ёки “шубҳали” эканлигини ўрнатиш керакдир. Бошқача айтганда, ички ресурсларга мурожаат қилиш қоидалари қуйидаги принциплардан биттасига асосланиши керак:

1) очиқ шаклда тақиқланган барча нарсаларга рухсат бермаслик;

2) очиқ шаклда таъқиқланмаган барча нарсаларга рухсат бериш.

Тармоқлараро экранни биринчи принцип асосида амалга ошириш сезиларли ҳимоя қилинганликни таъминлайди. Лекин бу принципга мос равишда шакллантирилган мурожаат қилиш қоидалари фойдаланувчиларга катта ноқулайликлар келтириб чиқариши мумкин, бундан ташқари эса уларни амалга ошириш етарлича қимматга тушади. Иккинчи принципни амалга оширишда ички тармоқ хакерларнинг ҳужумларидан камроқ ҳимояланган бўлади. Лекин ундан фойдаланиш қулайроқдир ва кам ҳаражатларни талаб қилади.

Ички тармоқни тармоқлараро экранлар ёрдамида ҳимоя қилиш самарадорлиги нафақатгина тармоқ сервисларига ва ички тармоқнинг ресурсларига мурожаат қилишнинг танланган сиёсатига эмас, балки тармоқлараро экранни асосий ташкил этувчиларини оқилона танлаш ва ишлатишга ҳам боғлиқдир.

Тармоқлараро экранларга функционал талаблар ўз ичига олади:

- тармоқ экранида фильтрлашга талаблар;
- амалий даражада фильтрлашга талаблар;
- фильтрлаш ва маъмурийлаштириш қоидаларини созлаш бўйича талаблар;
- тармоқли аутентификациялаш воситаларига талаблар;
- журналларни ва ҳисобга олишларни татбиқ қилиш бўйича талаблар.

6.2. Интернетда ахборотни ҳимоя қилишнинг стандартлари ва усуллари.

Интернет анча вақтдан бери очиқ стандартларга тегишлилиги билан машҳурдир. Бундай қўллаб-қувватланиш ахборот алмашишнинг очиқлиги билан биргаликда “Интернет ва хавфсизлик бир-бирини ўзаро инкор қиладиган тушунчалар” деган фикрни келтириб чиқариши мумкин.

Аслида эса бундай эмас. Ўтмишда Интернетдаги ахборот хусусий VAN ёки корпоратив тармоқларга нисбатан камроқ ҳимоя қилинган бўлса ҳам, ҳозирги вақтда Интернетда трафикни ҳимоя қилиш механизмларини татбиқ қилиш учун кўп хатти-ҳаракатлар қилинмоқда.

Охирги вақтларда тармоқнинг барча даражаларини - пакетдан иловагача (6.1-жадвалга ва 6.1 расмга каранг) қамраб оладиган стандартларнинг бутун бир тўплами пайдо бўлгандан кейин Интернетда ахборотни ҳимоя қилиш масаласига хатто керагидан ортиқ эътибор берилмоқда, деган таассурот пайдо бўлмоқда. Интернет тўғрисида ахборотни ишончли ташувчиси каби фикрга қарши (кейинчалик Интернетнинг марказлаштирилмаганлиги) транзакциялар 6.1-жадвалда келтирилган баённомаларни ишлатиб яхши ҳимоя қилиниши мумкин.

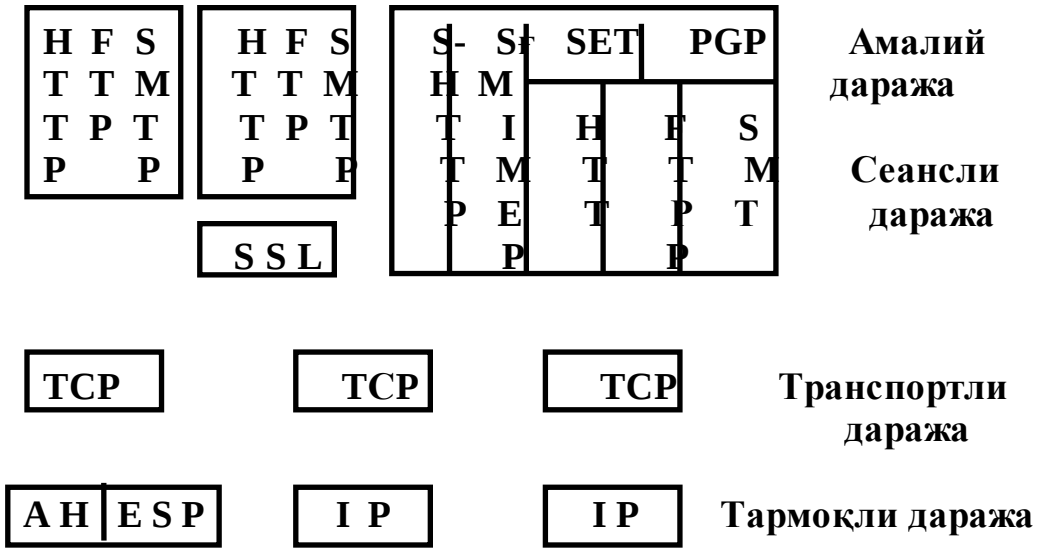
Кўриб чиқилаётган стандартларга қараб улар нимани ҳимоя қилинаётганлигига: уланишларними ёки иловаларними - қараб мос равишда таснифлаш

мумкин. **SSL** ва **SғWAN** каби стандартлар Интернетда коммуникацияларни ҳимоя қилиш учун мўлжалланган, шунга қарамай **SSL** асосан **Web-**иловалар билан ишлатилади. Бошқа томондан **SғHTTP** ва **SғMIME** махфийликни ва аутентификацияни таъминлашга йўналтирилгандир (**SғHTTP-Web-**иловалар учун, **SғMIME** эса - электрон почта учун). **SET** фақат электрон тижоратнинг транзакциясини ҳимоя қилишни таъминлайди. **SғHTTP** ва **SSL Web-** иловаларни ҳимоя қилиш учун.

6.1 - жадвал

Интернет учун маълумотларни ҳимоя қилишнинг баъзи бир стандартлари

Стандарт	**Функция**	**Ишлатилиши**
Secure HTTP (S - HTTP)	Web да транзакцияларни ҳимоя қилиш	Браузерлар, **Web**-серверлар, Интернет учун иловалар
Secure Sockets Layer (SSL)	Тармоқ даражасида маълумотлар пакетини ҳимоя қилиш	Браузерлар, **Web**-серверлар, Интернет учун иловалар
Secure MIME (S ғ MIME)	Турли платформаларда электрон жўнатмаларга киритилганларни ҳимоя қилиш	Шифрлашни ва RSA рақамли имзони қўллаб қувватлаган ҳолда почта дастурлари
Secure Wide Area Net Works(SғWAN)	Брандмауэрлар ва маршрутловчилар ўртасида бир даражадаги уланишларни шифрлаш	Виртуал хусусий тармоқлар
Securite Electronic Transaction (SET)	Кредит картали транзакцияларни ҳимоя қилиш	Смарт-карталар, транзакция серверлари, электрон тижорат



Усул 1 Усул 2 Усул 3

6.1-расм. Тармоқларда ахборотни ҳимоя қилишнинг учта усули

Web-иловалар иккита баённомалар: **Secure HTTP** ва **Secure Sockets Layer** билан ҳимоя қилингандир, улар серверлар ва браузерлар учун аутентификацияни, ҳамда Web-сервер ва браузер ўртасидаги уланишлар учун маълумотларни махфийлигини ва бутунлигини таъминлайди. Биринчи навбатда гиперматнни узатиш баённомасини (HTTP) қўллаб-қувватлаш учун мўлжалланган **SғHTTP** ҳужжатларни муаллифлаштиришни ва ҳимоя қилишни таъминлайди.

SSL ҳимоя қилишнинг ўхшаш усулларини, лекин коммуникация канали учун таклиф этади. У амалий транспортли, тармоқли даражалар TCPғIP ўртасидаги баённомаларнинг уланиш жойини пастки қисмида ҳаракат қилади (6.1-расмга қаранг).

SSL ни нафақатгина Web-серверда бўлиб ўтаётган транзакциялар учун ишлатмасдан, балки бу баённома иловалар ёки ҳужжатлар даражасида бўлиб ўтаётган аутентификация асосида хавф-сизликни таъминлаш учун мўлжаллангандир. Ҳужжатларга ва файлларга мурожаат қилишни бошқариш учун бошқа усулларни ишлатиш керак.

Электрон почтани ҳимоя қилиш: PEM, S/MIME, PGP.

Интернетда электрон почтани ҳимоя қилиш учун кўплаб турли хил баённомалар мавжуддир, лекин улардан фақат битта ёки иккитаси етарлича кенг ишлатилади. **PEM (Privaci Enhanced Mail)** - бу очиқ ёки симметрик калитларни ишлатиб электрон почтани ҳимоя қилиш учун Интернетнинг стандартидир. У камроқ қўлла-нилади, чунки у MIME қўллаб-қувватлайдиган электрон жўнатмаларнинг янги шаклини қайта ишлаш учун мўлжалланмаган ва бундан ташқари, калитларни бериш учун сертификатланган марказларнинг қатъий иерархиясини талаб этади. **S/MIME -** бу янги стандартдир. У патентланган ва лицензияланган RSA Data Security Inc. компанияларнинг кўплаб криптографик алгоритмларни ишга туширади. **S/MIME** рақамли сертификатларни ишлатади, ва натижада, аутентификацияни таъминлашда сертификацияланган марказга (корпоратив ёки глобал) асосланади.[25; 129-132]

Файлларни ва жўнатмаларни ҳимоя қилиш учун ишлаб чиқилган яна битта оммабоп иловалардан бири **PGP (Pretty Good Privacy)** иловасидир. Бу шифрлашнинг турли стандартларини ишлатадиган, Интернетда электрон почтани ҳимоя қиладиган энг кўп тарқалган иловадир. Шифрлаш-қайта шифрлашнинг **PGP** иловалари барча асосий операцион тизимлар ва электрон почтанинг жўнатмалари учун чиқарилади. Qualcomm фирмасининг Eudura Pro ва FTP Soft Ware фирмасининг On Net каби баъзи бир почта дастурлари шифрланган почтани қайта ишлаш учун махсус PGP-модулларни улаш имконини беради. PGP ишонишнинг “ўргимчак уяси” (Web of trust) принципи асосида қурилгандир ва фойдаланувчиларга узларининг калитларини сертификацияланган марказларини даллолчилигисиз тарқатиш имконини беради.

6.3. Интернетда ахборотнинг қонунийлиги ва мулклиги ҳуқуқлари.

Интернетни ишлатишни ўсиши билан тизимда жойлашган маълумотларга мулкдорликнинг ҳуқуқлари тўғрисидаги масала жуда ҳам жиддий тус олмоқда. Хавфсизликни ва ҳимоя қилишни таъминлаш бўйича чоралар ҳар доим Интернетни ташкил этадиган янги жиҳозларни ва дастур маҳсулотларни киритгандан кейингина кўрилди. Шунинг учун барчасини бутунлай эшитишга тўғри келган телефондаги сўзлашувларни билдирмасдан эшитиб олишдан фарқли равишда электрон хабарларни енгилгина ушлаб олиш, фильтрлаш, навларга ажратиш ва келгусида таҳлил қилиш учун юбориш мумкин.

Интернетни ҳимоя қилишнинг асосий сабаби шундаки АҚШ ҳукумати ҳимоя қилинган компьютер тизимларини тижорат йўлида тарқатилишига қатьиян қарши бўлиб чиққанлар. Жорий юз йиллик мобайнида АҚШ коммуникацияли тизимларда ушлаб олинган ахборотларни дустона бўлмаган кайфиятда ҳисобланган хорижий ва ички ташкилотлар билан ишлар олиб борганда асосий манба (ташкил этувчи) сифатида доимо ишлайдилар. Ким ҳам ундай уйин олиб боришда ўзининг картасини очгиси келади?

Бошқа давлатлар ҳам, шубхасиз, мамлакат сиёсатини ростлаб туриш учун ахборотни ушлаб оладилар ва билдирмасдан эшитадилар, лекин АҚШ ҳар доим компьютер тизимларини йирик ишлаб чиқарувчиси бўлиб келган. Қонунларни ишлатган ҳолда АҚШ ҳимоя қилинган компьютер жиҳозини ва дастур таъминотини чет элга олиб чиқишни чекладилар, шу билан бирга ишлаб чиқарувчиларни экспорт қилинаётган маҳсулотда шифрлаш технологиясини қўллашдан бош тортишга мажбурладилар. Натижада Интернетнинг ташкил этувчиларида хатто қуролланмаган кўз билан ҳимоя қилиш тизимидаги йирик камчиликларни кўриш мумкин.

Номаълум бўлмаган Филипп Циммерман ва унинг ҳамкасабалари фойдаланувчилар ўртасида, аббревиатурада **Pretty Good Privacy** (махфийликнинг юқори даражаси) каби қайта шифрланадиган **PGP** шифрлаш дастурини ёзиб ва тарқатиб, вазиятни тўғрилашга ҳаракат қилдилар. Ҳозир Интернетда кўпчилик компьютер платформалари учун **PGP** вариантлари мавжуддир. Нотижорат мақсаларда ушбу дастурни текинга ишлатиш мумкин.

PGP очиқ калит усули (publik Key encryption) деб аталган шифрлаш тизимини ишлатади, унда ҳар бир фойдаланувчи иккита калитга: шахсий (махфий) ва очиқ, эга бўлади. Сизга махфий хабарни жўнатмокчи бўлган ихтиёрий фойдаланувчи **PGP** дастури нусхаси шахсий махфий калитни “билган” очиқ калит усулини ишлатади. Очиқ калит сизга махфий ахборотни юборишни хохлаган ҳаммага билдирилади, шахсий калит эса қатъиян сир сақланади.

Кодланган **PGP**-хабар бузилмаслигини қатьий математик исботланганлиги хали мавжуд бўлмасада, кўпчилик фойдаланувчилар томонидан бу дастур тўғри ишлатилган тақдирда жуда кучли ҳисобланади.

Кўпчилик фойдаланувчилар Ф. Циммерманни қаҳрамон ҳисоблайдилар. Лекин АҚШ хукумати бу нуқтаи назарга қўшилмайди. Циммерманга қарши, АҚШ дан шифрловчи маҳсулотни экспортини таъқиқлайдиган қонунни бузмаганлигини ойдинлаштириш мақсадида, жиноий иш қўзғатилди. Ушбу сатрлар ёзилаётган вақтда Циммерман суднинг охирги ажримини кутмоқда. Қонунни бузганлиги учун уни бир неча йил қамоқ муддатида бўлиш хавфи қўйилмоқда. Унинг оқланишига боғлиқ бўлмаган равишда унга анчагина суд ҳаражатларини тулашга тўғри келади.

Қонунийлик масалалари

АҚШ хукумати криптографик материалларни қандайдир ҳарбий қуролланиш деб ҳисоблайди. PGP дастурини АҚШ дан ташқарига махсус лицензиясиз экспорт қилиш қонун томонидан таъқиқлангандир. ViaCrypt компанияси, агар америка фирмасига ўзининг хорижий филиаллари билан махсус ахборотларни алмашиш керак бўлса, PGP ни экспорт қилишга рухсатномаси бор деб ҳисоблайди.

PGP дастурининг 2.6 версияси RSA Data Systems Inc. (RSA DSI) фирмаси томонидан нотижорат мақсадларда ишлатиш учун лицензиялангандир. Натижада PGP 2.6 биринчи текин расмий дастур версияси бўлди (олдин ҳам текин ва расмий версия бор эди, лекин улар бунака бир вақтнинг ўзида бўлмаган эди).

Тижорат мақсадларида PGP 2.6 ни ишлатманг, Via Crypt компаниясидан PGP билан ишлаш ҳуқуқини сотиб олинг. Via Crypt компанияси RSA DSI нинг лицензиясига ва тижорат йўлида ишлатиш учун патентланган технологияларни сотишга IDEA патентини эгалигига эгадир. PGP 2.6 учун ҳеч қандай пул тўламанг, табийки, у тарқатиладиган ташувчи нархидан ташқари албатта. Ҳуқуқий нуқтаи назардан PGP 2.6 билан кодланган ахборот олдинги версиялари томонидан ўқиб бўлмайди.

Шундай бўлсада, Филипп Циммерманнинг PGP дастури ҳақиқий революцияни амалга оширди. У оддий фойдаланувчиларга ўзларининг маълумотларини ва хабарларини тақиқланган мурожаат қилишдан ҳимоя қилиш имконини берадиган дастурлардан биринчиси эди. PGP ни ишлатиб, маълумотларни ҳимоя қилиш:

- мурожаат қилса бўладиган;
- қулай;
- криптографик томондан ишончли;
- қонуний;
- ишончни оқлайдиган;
- кенг тарқалган бўлиб қолади.

Ахборот хавфсизлигини режимини шакллантириш - комплекс муаммодир. Уни хал қилиш бўйича чораларни тўртта даражага бўлиш мумкин:

- қонун чиқарувчи (қонунлар, меъёрий далолатномалар, стандартлар ва ш. ў);

- маъмурий (ташкилот рахбарияти томонидан кўриладиган умумий характерли ишлар);
- жараёнли (кишилар билан бўладиган хавфсизликнинг аниқ чоралари);
- техник-дастур (аниқ техник чоралар).

Қонун чиқарувчи даража

Ҳозирги вақтда ахборот хавфсизлиги соҳасидаги энг батафсил қонун чиқарувчи ҳужжат Жиноят кодекси, аниқроқ айтганда, 1996 йилнинг май ойида кучга кирган унинг янги таҳрири, ҳисобланади.

IX бўлимда (“Жамият хавфсизлигига қарши жиноятлар”), ”Компьютер ахбороти соҳасидаги жиноятлар” деган 28-боб бор. Унда 272-модда - “Компьютер ахборотига ҳуқуқий бўлмаган мурожаат қилиш”, 273-модда-“ЭҲМ учун зарар етказадиган дастурларни яратиш, ишлатиш ва тарқатиш”, 274-модда-“ЭҲМ, ЭҲМ тизими ёки уларнинг тармоқларини ишлатиш қоидаларини бузиш” бор.

Жиноят кодекси, ахборот хавфсизлигини барча жиҳатларини - мурожаат қила олишлик, ”ЭҲМ, ЭҲМ, тизими ёки уларнинг тармоқларини ишлашини бузиш, ахборотни йўқотиш, блокировкалаш, ўзгартириш ва нусхалаш” учун жазолашларни кўриб чиқиб, яхлитлик, махфийлик, ҳимоясида туради.

Замонавий ахборот технологиялари соҳасида жуда жиддий ишларни Давлат техника комисияси (Давтехкомиссия) олиб бормоқда. Давтехкомиссиянинг бошқарувчи ҳужжатлари (БХ) сериялари доирасида тақиқланган мурожаат қилишдан (ТМҚ) ҳимояланганликни таъминлаш даражаси бўйича БХ лойиҳаси тайёрланган. Бу Интернет ва Интранет технологиясини амалга ошириш учун керак бўлган ҳимоя қилиш воситаларини ишлатишни тартибга солишга имкон берадиган принципиал муҳим ҳужжатдир.

6.3.1. Хавфсизлик сиёсатининг тармоқли жиҳатларини ишлаб чиқиш

Хавфсизлик сиёсати ахборотни ва у билан бирлаштирилган ресурсларни ҳимоя қилишга йўналтирилган ҳужжатлаштирилган бошқарувчи карорларнинг тўплами каби аниқланади.

Хавфсизлик сиёсатини ишлаб чиқишда ва уни ҳаётга татбиқ этишда қуйидаги принципларга риоя қилиш мақсадга мувофиқдир:

- ҳимоя қилиш воситаларини четлаб ўтишнинг имкони йўқлиги;
- энг заиф звенони кучайтириш;
- хавфсиз бўлмаган ҳолатга утишнинг имкони йўқлиги;
- имтиёзларни камайтириш;
- вазифаларни бўлиб чиқиш;
- мудофаанинг кучайтирилганлиги;
- ҳимоя қилиш воситаларининг турли-туманлиги;
- ахборотли тизимнинг оддийлиги ва бошқарилувчанлиги;
- хавфсизлик чораларини умумий қўллаб-қувватлашни таъминлаш.

Санаб ўтилган принципларни маъносини тушунтириб берамиз.

Агар нияти ёмон кишида ёки норози фойдаланувчида ҳимоя қилиш воситаларини четлаб ўтиш имконияти пайдо бўлса, у, тушунарлики, шундай қилади. Тармоқлараро экранларга қўллаган ҳолда ушбу принцип билдирадики, барча ахборот оқимлари ҳимоя қилинаётган тармоққа ва ундан экран орқали ўтиши керак Экранни четлаб ўтадиган "сирли" модемли киришлар ёки тестли линиялар бўлмаслиги керак.

Ҳар қандай мудофаанинг ишончлиги энг заиф звено билан аниқланади. Нияти ёмон киши кучга қарши курашмайди, у заифлик устидан енгилгина ғалабани маъқул кўради. Кўпинча энг заиф звено компьютер ёки дастур бўлмайди, балки инсон бўлади, ва унда ахборот хавфсизлигини таъминлаш муаммоси техник бўлмаган характерга эга бўлади.

Хавфсиз бўлмаган ҳолатга ўтишнинг имкони йўқлиги принципи билдирадики, ҳар қандай, шу жумладан штатсиз, ҳолатларда ҳимоя қилиш воситаси ўзининг функциясини тўлиқ бажаради, ёки мурожаат қилишни тўлиқ блокировкалайди. Образли қилиб айтганда, агар қалъада кўтарувчи кўприк механизми бузилса, кўприк, бузғунчининг ўтишига тўсқинлик қилиб, кўтарилган ҳолатда қолиши керак.

Имтиёзларни камайтириш принципи фойдаланувчиларга ва маъмуриятларга уларга ўзларининг хизмат вазифаларини бажариш учун керак бўладиган мурожаат қилиш ҳуқуқларинигина ажратиб беришни билдиради.

Вазифаларни бўлиб чиқиш принципи ролларни ва жавобгарликни шундай тақсимланишига эгаки, унда битта киши ташкилот учун критик муҳим жараённи буза олмайди. Тизимли маъмуриятни ёмон ниятли ёки малакасиз ишларини бартараф этиш учун бу жуда муҳимдир.

Мудофаанинг кучайтирилганлиги принципи битта ҳимоя чегарасига, у қанчалик ишончли бўлишга карамасдан, ишониб қолмасликни билдиради. Физик ҳимоя қилиш воситалари устидан дастур-техника воситалари кузатишлари керак, идентификациялаш ва аутентификациялаш устидан эса - мурожаат қилишни бошқариш ва, охирги чегара каби, баённомалаштириш ва аудит кузатади. Кучайтирилган мудофаа хеч бўлмаганда ёмон ниятли кишини ушлаб олишга қодирдир, баённомалаштириш ва аудит каби чегаранинг борлиги эса ёмон ниятли ҳаракатларни билдирмасдан бажарилишини сезиларли қийинлаштиради.

Ҳимоя қилиш воситаларининг турли-туманлиги принципи потенциал ёмон ниятли кишидан турли-туман ва имкони борича бир-бирига мос келмайдиган кўникмаларга (масалан, юқори тўсиқни енгиб ўтишни билиш ва бир нечта операцион тизимларни заиф жойларини билиш) эга бўлиши талаб этилиши учун ўзининг характери бўйича турли-туман мудофаа чегараларини ташкил этиш тавсия этилади.

Ахборотли тизимни умуман ва айниқса ҳимоя қилиш воситаларини оддийлиги ва бошқарувчанлиги принципи жуда муҳимдир. Фақатгина оддий ҳимоя қилиш воситаси учун унинг корректлигини мавхум ёки мавхум бўлмаган ҳолда исботлаш мумкин. Фақатгина оддий ва бошқариладиган тизимда турли ташкил этувчиларнинг конфигурациясини мос келишлигини текшириш ва марказлашган маъмуриятни амалга ошириш мумкин. Шунинг учун хизмат кўрса-

тиладиган объектларнинг турли-туманлигини беркитадиган ва умумий, кўргазмали интерфейсни тақдим этадиган Web-сервиснинг интеграцияловчи ролини таъкидлаш муҳимдир. Мос равишда, агар баъзи бир кўринишдаги объектларга (айтайлик, маълумотлар базасининг жадваллари) Web орқали мурожаат қилинса, уларга тўғридан-тўғри мурожаат қилишни блокировкалаш керак, негаки акс ҳолда тизим мураккаб ва бошқарилиши мураккаб бўлади.

Охирги, **хавфсизлик чораларини умумий қўллаб -қувватлаш принципи** техник бўлмаган характерга эгадир. Агар фойдаланувчи ва (ёки тизим маъмуриятлари) ахборот хавфсизлигини қандайдир ошиқча ташвиш ёки хатто адоватли деб ҳисобласалар, хавфсизлик режимини умуман шакллантириб бўлмайди. Энг аввало, ходимларнинг тўғри дунёқарашини таъминлашга қаратилган чоралар тўпламини, уларнинг доимо назарий амалий ўқитилиб борилишини кўзда тутиш керак.

6.4. Интернетда ахборотни ҳимоя қилиш тизимларининг шархи

6.4.1. Тақиқланган мурожаат қилишдан ахборотни ҳимоя қилишнинг КРИПТОН - ВЕТО криптографик тизими

Бу тизим MS DOS 5.0 ва ундан юқори, Windows 3.1 ОТ лари бошқаруви остида ишлайдиган, 386 процессордан паст бўлмаган ШК ларни ҳимоя қилиш учун мўлжалланган. Бунда ШК абонентлик пункти, пакетларни коммутациялаш маркази, калитларни ишлаб чиқариш маркази сифатида ишлатиши мумкин.

Тизим шахсларни ва уларнинг ҳуқуқларини ШК даги ахборотга мурожаат қилиш ҳуқуқини чеклайди. Унинг амалга оширилиши ГОСТ 28147-89 алгоритми бўйича мантиқий дискларни “шаффоф” шифрлаш ва ГОСТ 34.10ғ11-94 бўйича электрон рақамли имзо технологияларига асосланган.

КРИПТОН-ВЕТО тизимининг асосий функциялари таркибига қуйидагилар киритилган:

- ШК ни ёки “винчестр” ни ўғрилаб кетилганда ахборот махфийлигини таъминлаш;
- компьютер ресурсларига мурожаат қилиш бўйича фойдаланувчининг ваколатларини чеклаб қўйиш;
- дастурнинг яхлитлигини уни бажаришга ишга тушириш вақтида текшириш;
- тизимда пайдо бўладиган ҳодисаларни қайд қиладиган тизимли журнални олиб бориш;
- ҳимоя қилинган дискка мурожаат қилишда ахборотни “шаффоф” шифрлашни таъминлаш;
- вируслар, фойдаланувчи хатолари, техник ишдан чиқишлар ва ёмон ниятли киши ҳаракатлари келтириб чиқарган бузилишларни пайқаш.

6.4.2.Компьютерга мурожаат қилишни чеклаш учун КРИПТОН-ЗАМОК комплекси

КРИПТОН-ЗАМОК комплекси компьютерга мурожаат қилишни чеклайдиган аппарат-дастурли воситаларни, КРИПТОН сериясидаги маълумотларни криптографик ҳимоя қилиш қурил-масини (**МКҲҚҚ**) ишлатган ҳолда, қуриш учун мўлжалланган. Комплекс ШК асосида, ундаги мавжуд бўлган ахборотга мурожаат қилишга эга бўлган шахслар доирасини чеклаган ҳолда, иш жойини ташкил қилиш имконини беради.

КРИПТОН-ЗАМОК комплексини ишлаши учун MS DOS, WINDOWS 95/98/NT, UNIX операцион тизимли, процессори 386 дан паст бўлмаган IBM PC туридаги ШК керакдир, улар учун MS DOS бошқаруви остида компьютерга ўрнатилган файлли тизим шаклини тушуниш имконини берадиган мос драйвер мавжуддир.

Комплекс **FAT 12, FAT 32, NTFS, UNIX** ва ҳ.к. шакллардаги файлли тизимли, қаттиқ дискли компьютерларни ҳимоя қилиш учун хизмат қилади. КРИПТОН-ЗАМОК комплексининг иккита кўриниши чиқарилган:

- сиғими 8 Гбайтдан камроқ қаттиқ дисклар учун;
- сиғими 8 Гбайтдан кўпроқ қаттиқ дисклар учун.

ШК га ўрнатилган, мурожаат қилишни чеклайдиган КРИПТОН -ЗАМОК комплекси қуйидаги функцияларни бажаради:

- фойдаланувчиларнинг компьютерга мурожаат қилишини, уларни идентификациялаш йўли билан, чеклаб қўяди;
- фойдаланувчиларни компьютер ресурсларига мурожаат қилишини уларнинг ваколатларига мос равишда бўлиб чиқади;
- комплексни, операцион муҳит дастурларини, амалий дастурларни ва хотира соҳаларини ўзгаришларини яхлитлигини назорат қилади;
- ҳимоя қилинган электрон журналда ҳодисаларни қайд қилади;
- бошқаришни ва фойдаланувчи параметрларини маъмурият кўрсатган дастур таъминотига (RUN -файлларга) узатади.

Бажарадиган функцияларига мос равишда КРИПТОН-ЗАМОК комплекси қуйидаги асосий қисмтизимларни ўз ичига олади:

- КРИПТОН қурилмасидан ва хизмат кўрсатадиган CRLOCK. EXE дастуридан ташкил топган мурожаат қилишни бошқарадиган қисмтизим;
- 2 та журнални ўз ичига олган қайд қилиш ва ҳисобга олиш қисмтизими **(1-журнал - аппаратли -** компьютерга, унинг ОТ ишга тушгунча, киришга интилишларни қайд қиладиган КРИПТОН қурилмасида, **2-журнал - тўлиқ -** қаттиқ дискда, унда комплексга муваффақиятли киргандан кейин барча воқеалар, шу жумладан аппаратли журнал мазмуни, акс эттирилади), журналларни бошқариш комплексга хизмат кўрсатадиган CRLOCK.EXE дастури билан амалга оширилади;
- КРИПТОН қурилмасидан ва комплекс ишлашида асосий ОТ нинг яхлитлигини текширадиган CHECKOS.EXE дастуридан ташкил топган яхлитликни таъминлайдиган қисм тизим. [25;138-141]

КРИПТОН-ЗАМОК комплекси қуйидаги вазифаларни бажаришни таъминлайди:

- компьютерга фақатгина рухсат этилган фойдаланувчи кириши мумкин.
- комплекснинг ишончли ядроси юкланади;
- ишончли ОТ юкланади;
- маъмурият томонидан кўрсатилган амалий дастур таъминотининг яхлитлиги текширилади;
- маъмурият томонидан кўрсатилган дастурларни ишга тушириш амалга оширилади.

6.4.3. Махфий ахборотни ҳимоя қиладиган Secret Disk тизими

Махфий ахборотни ҳимоя қиладиган **Secret Disk** тизими АНКАД фирмаси иштирокида Alladdin компанияси томонидан ишлаб чиқилган ва компьютерлардан фойдаланувчиларнинг кенг доираси: раҳбарлар, бошқарувчилар, бухгалтерлар, адвокатлар, яъни шахсий ёки касбий ахборотни ҳимоя қилиш тўғрисида қайғуриши керак бўлган барча учун мўлжалланган.

Secret Disk тизимини ўрнатишда компьютерда янги мантиқий дисклар яратилади, уларга ёзишда ахборот автоматик равишда шифрланади, ўқишда эса - қайта шифрланади. Махфий дисклар билан ишлаш мутлақо сезиларсиздир ва барча ишга туширилаётган иловаларга шифрлашни созлашга тенг кучлидир.

Secret Disk тизимининг муҳим хусусияти шундаки**,** ҳимоя қилинган ахборотга мурожаат қилиш учун нафақатгина фойдаланувчи киритадиган пароль, балки яна электрон идентификатор керак бўлади. Бундай идентификатор сифатида параллел порт учун оддий электрон калит, ноутбуклар учун PCMCIA карточкаси ёки смарт-карточкалар ишлатилиши мумкин.

Secret Disk тизими фақатгина фойдаланувчи пароль киритгандан ва тизим мос идентификаторни пайқагандан кейингина уланади. Шунинг учун, агар фойдаланувчи компьютердан электрон калитни чиқариб олса, ёмон ниятли кишиларга хаттоки паролни билганлиги ҳам ёрдам бермайди.

ТМҚ дан ҳимоя қилишнинг асосий усулларига тармоқ томонидан қуйидаги криптографик усуллар тегишлидир:

- абонентлик шифрлаш (АШ);
- электрон рақамли имзо (ЭРИ);
- пакетли шифрлаш (ПШ);
- абонентларни криптографик аутентификациялаш.

Абонентлик шифрлашни (АШ) ва электрон рақамли имзони (ЭРИ) амалга ошириш учун ҳужжатларни узатишга бевосита тайёрлашдан олдин ёки уни қабул қилгандан кейин ишга тушириладиган алоҳида дастур ёки дастур-аппаратли тизим қўлланилиши мумкин. АШ ва ЭРИ ни ишлатишни иккинчи варианти коммуникация дастурларига мос модулларни қўшишни кўзда тутади. Иккала вариантларда ҳам тизим тахминан бир хил функцияларни бажаради.

6.4.4. MS-DOS учун АШ ва ЭРИ дастурлари

Абонентли шифрлашнинг ва Crypton сериясидаги электрон рақамли имзонинг дастур воситаларига қуйидаги дастурлар тегишлидир:

- симметрик шифрлаш ва **Crypton Tools** калитлари билан ишлаш дастурлари;
- электрон рақамли имзонинг **Crypton Sign** дастури;
- асимметрик шифрлаш ва ЭРИ ёрдамида файллар-ҳужжатларни ҳимоя қилиш учун **Crypton Arc Mail** дастури.
- Бу дастурлардан ҳар бирининг муваффақиятли ишлаши учун компьютер қуйидаги талабларга жавоб бериши керак:
- 386 ва ундан юқори микропроцессор;
- 4.0 ва ундан юқори версияли MS DOS ОТ;
- 350 Кбайтдан кам бўлмаган тезкор хотира;
- КРИПТОН шифрлаш платаси ёки **Crypton LITE** дастури.

6.4.5. Электрон рақамли имзонинг Crypton Sign дастури

Crypton Sign дастури, электрон ҳужжатларнинг муаллифлигини ўрнатишни ва электрон ҳужжатларнинг яхлитлигини текширишни таъминлайдиган электрон ҳужжатларнинг электрон рақамли имзосини шакллантириш ва текшириш учун мўлжалланган дир.

Электрон рақамли имзо (ЭРИ) имзоланаётган ҳужжат охирига ёки алоҳида файлга жойлаштириладиган байтлар кетма-кетлиги кўринишига эгадир. **ЭРИ** ҳужжат мазмуни, махфий калит ва ҳужжатни имзолаётган шахснинг пароли асосида шакллантирилади. Ҳар бир махфий калитнинг имзосини текшириш учун очиқ калит яратилади.

Имзоланадиган электрон ҳужжат сифатида дастурда исталган файл ишлатилиши мумкин.

Crypton Sign дастурини бошқариш учун Norton Commander интерфейсига ўхшаш интерфейс фойдаланувчига керак бўлади.

Crypton Sign дастурининг асосий менюси иккита қисмга (панелга) ажратилган. Менюнинг чап қисмида дастур бажарадиган буйруқлар номлари жойлашган, ўнг қисмида эса файллар ва бу файллар жойлашган бўлимлар рўйхати жойлашгандир. Буйруқларни ва файлларни танлаш учун маркер ишлатилади.

Crypton Sign дастури ёрдамида **ЭРИ** ни яратиш ва текшириш схемаси 6.2-расмда кўрсатилган. Имзони шакллантириш ва кейинчалик текшириш учун иккита калит-имзони: махфий ва очиқ, яратиш керак. Калитлар дискетадаги оддий файллар ёки электрон карточкадаги байтлар кетма-кетлиги кўринишига эгадир.

Калитларни яратиш учун тасодифий кодни ҳосил қилиш (ишлаб чиқариш) КРИПТОН сериясидаги **МКҲҚҚ** лардан бири билан аппарат нуқтаси назардан бажарилади. Агар **МКҲҚҚ** компьютерда йўқ бўлса, тасодифий кодни **Crypt**on **LITE** дастури ёки тасодифий сонлар генератори ёрдамида дастур нуқтаи назаридан олиш мумкин.

Калитларни ишлаб чиқариш учун “Калитларни яратиш” буйруғини бажариш етарлидир. Файлни имзолаш учун имзоланадиган файлни ўзини ва махфий калитни танлаш, кейин эса “Имзони қўйиш” буйруғини бажариш керак.

“Имзони кўрсатиш” ва “Имзони текшириш” буйруқлари файлдаги имзоларни борлигини ва ҳақиқийлигини текшириш, ҳамда имзо тўғрисида қўшимча ахборотларни олиш учун ишлатилади. Бу буйруқларни бажариш учун текширилаётган файлларни танлаш ва очиқ калитли каталогларни кўрсатиш керак бўлади.

6.4.6. Windows 95/98/NT учун АШ ва ЭРИ дастурлар пакети.

Windows 95/98/NT учун КРИПТОН/Crypton сериясидаги абонентли шифрлаш ва электрон рақамли имзонинг дастур воситаларига қуйидаги дастурар пакетини келтириш мумкин:

- “КРИПТОН R Шифрлаш” пакети;
- “КРИПТОН R Имзо” пакети;
- Windows 95/98/NT 4.0 учун Crypton Ars Mail дастурлар пакети.

Бу дастурлар пакетларини муваффақиятли ишлаши учун компьютер эга бўлиши керак:

-Windows 98 ёки Windows NT 4.0 ОТ;

-1.3 ва ундан юқори версияли Windows - Crypton Emuator учун мос драйверли КРИПТОН серияли МКҲҚҚ;

-2.2 ва ундан юқори версияли Windows 95/NT учун Crypton API;

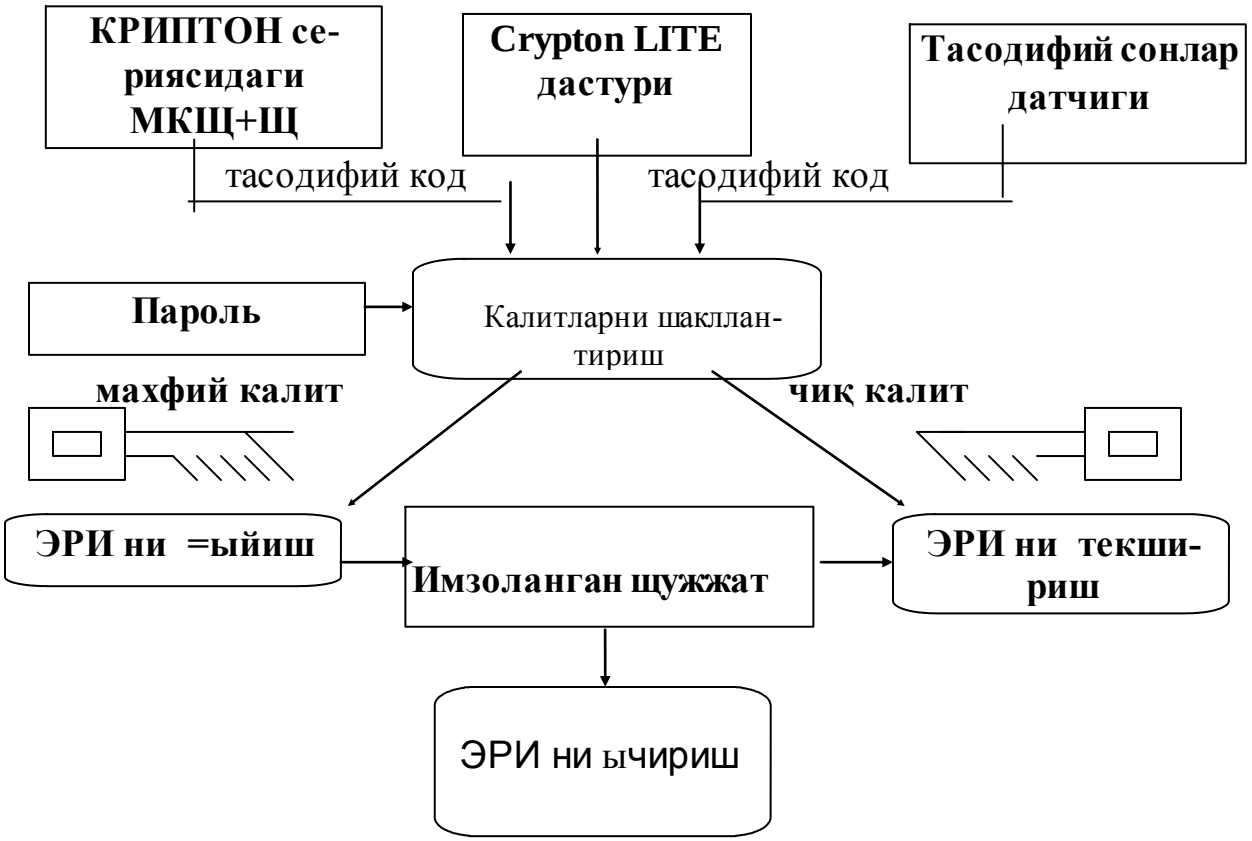
-сичқонча монипулятори.

Янада ишончлироқ ҳимоя қилишни амалга ошириш учун Crypton Emulator дастури ўрнига КРИПТОН сериясидаги МКҲҚҚ сини ишлатиш тавсия этилади.

6.5. Ҳимоя қилишнинг брандмауэрли тизимлари

Бугун кўпгина компаниялар Интернетга локал тармоққа тақиқланган мурожаат қилишга тўсқинлик қиладиган махсус дастур таъминоти билан таъминланган компьютерлар - брандмауэрлар (тармоқлараро экранлар ёки fire Wall) орқали уланмоқдалар.

Локал тармоқда брадмауэрли ўрнатилишни асосий сабаби унинг ҳар доим чақирилмаган меҳмонлардан ҳимоя қилинишидир. Ёмон ниятли киши томонидан олинган ахборот корхонанинг рақо-батбардошлигини ва унинг мижозларини ишончини жиддий бузиб қўйиши мумкин. Ички тармоқлар учун энг эҳтимолли хавфларни бартараф этиш бўйича бир қатор масалаларни брандмауэрлар хал қилиш қобилиятига эгадирлар. Компьютер муҳитидан ташқарида ёнмайдиган материаллардан ва ёнғинни тарқалишига тўсқинлик қиладиган деворни брандмауэр (ёки fire will) деб аталади. Компьютер тармоғи муҳитида тармоқлараро экран фигурали ёнғиндан-ёмон ниятли кишиларни ички тармоққа, ахборотни нусхалаш,ўзгартириш ёки ўчириш учун ёки бу тармоқда ишлаётган компьютерларнинг хотирасидан ёки ҳисоблаш қувватидан фойдаланиш учун кириб олишга интилиши тушунилади (6.3-расм).



6.2-расм. Электрон рақамли имзони яратиш ва текшириш схемаси

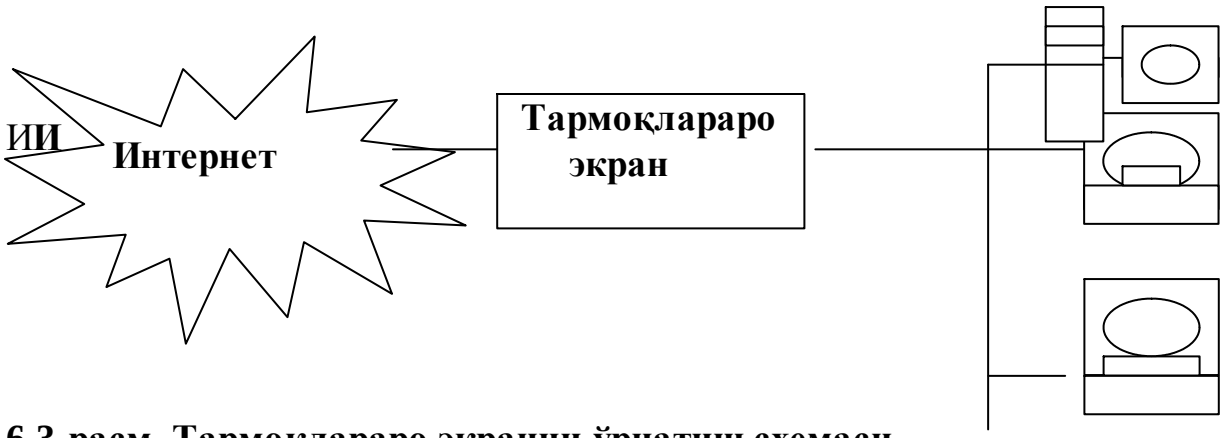
Тармоқлараро экран (ТЭ) - бу тармоқлараро ҳимоя қилиш тизими бўлиб, у умумий тармоқни икки ва ундан ортиқ қисмларга ажратишга ва маълумотлар пакетларини чегара орқали умумий тармоқнинг бир қисмидан бошқа қисмига ўтиш шартларини аниқ-лайдиган қоидалар тўпламини амалга оширишга имкон яратади. Қоидага кўра, бу чегарани корхонанинг корпоратив (локал) тармоғи ва Интернет глобал тармоғи ўртасида ўтказилади, бироқ уни корхонанинг корпоратив тармоғи ичида ҳам ўтказиш мумкин. ТЭ ўзи орқали ҳар бир ўтаётган пакет учун қарорни - уни ўтказиш керакми ёки ташлаб юбориш керакми - қабул қилган ҳолда бутун трафикни ўтказади. ТЭ буни амалга ошира олиш учун у фильтрлашнинг қоидалар тўпламини аниқлаб олиши керак. Тармоқлараро экранларнинг асосий ташкил этувчилари. Тармоқлараро экранларнинг кўпчилик ташкил этувчиларини қуйидаги учта тоифадан биттасига киритиш мумкин:

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

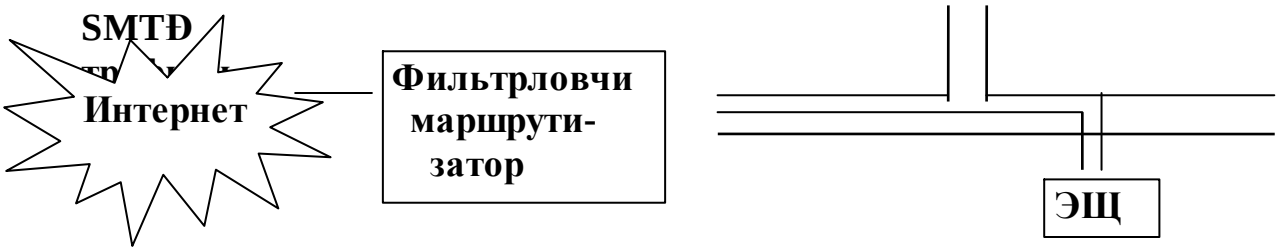
Фильтрловчи маршрутизатор маршрутизатор ёки серверда ишлайдиган дастур кўринишига эга бўлиб, у кирувчи ва чиқувчи пакетларни фильтрлайдиган қилиб тайёрланган бўлади. Пакетларни фильтрлаш пакетларнинг TCP ва IP сарлавхаларида мавжуд бўлган ахборот асосида амалга оширилади.

Фильтрлаш аниқ бир хост-компьютерлар билан ишончсиз ёки ракиб деб ҳисобланган тармоқларнинг ва хост-компьютерларнинг аниқ манзиллари алоқаларини блокировкалаш учун турли кўринишда амалга оширилиши мум-

кин. Масалан, ички тармоқ баъзи-бир тизимлардан ташқари барча хост-компьютерлар билан барча ички уланишларни блокировкалаши мумкин. Бу тизимлар учун фақатгина маълум бир сервисларгина рухсат этилиши мумкин. (SMTP битта тизим учун, TELNET ёки FTP-бошқа тизим учун) (6.4-расм).



6.3-расм. Тармоқлараро экранни ўрнатиш схемаси



6.4-расм. SMTĐ ва TELNET трафикни фильтрлаш схемаси

Фильтрловчи маршрутизаторларнинг ижобий сифатларига қуйидагиларни киритиш мумкин:

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

Фильтрловчи маршрутизаторларнинг камчиликлари қуйидагилар:

- ички тармоқ Интернет тармоғидан кўриниб туради (марш-рутланади);
- пакетларни фильтрлаш қоидаларини ёзиб чиқиш пакетларини қийин ва TCP ва UDP технологияларини жуда яхши билиш талаб этилади;
- пакетларни фильтрлашда тармоқлараро экранни ишлаш қоби-лияти бузилганда барча компьютерлар ундан кейин тўлиқ ҳимоя қилинмаган ёки мурожаат қилиб бўлмайдиган бўлиб қолади.
- ҳужум қиладиган тизим IP-манзилни ишлатиб ўзини бошқа тизим каби кўрсатади.

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

Тармоқ даражасидаги шлюз ишончга кирган мижозни аниқ бир хизматларга сўровини қабул қилади ва сўроқланган сеансни мумкин эканлигини текширгандан кейин ташқи хост-компьютер билан уланишни ўрнатади. Бундан кейин

шлюз пакетларни фильтрлашни амалга оширмасдан уларни иккала йўналишларда нусхалайди.

Пакетларни нусхалаш ва қайта йўналтириш учун тармоқ даражасидаги шлюзларда тармоқ даллоллари деб аталадиган махсус иловалар қўлланилади, чунки улар икки тармоқ ўртасида виртуал занжирни ёки канални ўрнатадилар, кейин эса TCPғIP иловалари билан ҳосил қилинаётган пакетларга бу канал бўйича ўтишга рухсат беради. Аслида эса тармоқ даражасидаги кўпчилик шлюзлар мустақил маҳсулотлар ҳисобланмайди, балки амалий даражадаги шлюзлар билан биргаликда етказиб берилади. Trusted Information System компаниясининг Gauntlet Internet Fire Wall шлюзи, Dec компаниясининг Alta Viste Fire Wall шлюзи, ANS Interlock шлюзи шундай шлюзларга мисол бўла олади.

Тармоқ даражасидаги шлюз яна ҳимоя қилишнинг битта муҳим функциясини бажаради у сервер-даллол сифатида ишлатилади. Бу сервер-даллол ички IP-манзилларни битта “ишончли” IP-манзилга ўзгартирилиши бўлиб утадиган манзилларни трансляциялаш жараёнини бажаради.

Амалий даражадаги шлюз. Фильтрловчи маршрутизаторларга хос бўлган бир қатор камчиликларни бартараф этиш учун тармоқлараро экранлар TELNET ва FTP туридаги қўшимча дастур воситаларини ишлатиши керак. Бундай дастур воситалари ваколатли сервер **(**сервер-даллоллар), улар бажариладиган хост-компью-терлар эса амалий даражасидаги шлюз деб аталади.[25; 144-149]

Амалий даражадаги шлюз муаллифлаштирилган мижоз ва ташқи хост-компьютер ўртасидаги тўғридан-тўғри ўзаро таъ-сирни инкор этади. Шлюз барча кирувчи ва чиқувчи пакетларни амалий даражада фильтрлайди. Хавфсизликни ва мослашувчанликнинг янада юқорироқ даражасига эришиш учун амалий даражадаги шлюзлар ва фильтрловчи маршрутизаторлар битта тармоқлараро экранда бирлаштирилиши мумкин. Амалий даражадаги шлюзлар амалий трафик бевосита ички хост-компьютерларга ўтказиб юбориладиган оддий режимга нисбатан бир қатор жиддий афзалликларга эга:

- Интернет глобал тармоғидан ҳимоя қилинаётган тармоқ таркибини кўринмаслиги;
- ишончли қайд қилиниш;
- нарх ва самарадорлик ўртасида оптимал нисбат;
- фильтрлашнинг оддий қоидалари;
- кўп сонли текширувларни ташкил этиш имконияти.

Амалий даражадаги шлюзларнинг камчиликларига қуйидагилар тегишлидир:

- фильтрловчи маршрутизаторларга нисбатан бирмунча паст унумдорлик;
- фильтрловчи маршрутизаторларга нисбатан бирмунча юқори нарх.

Афсуски, магнит ленталарга брандмауэрли ҳимоя қилиш тарқатилмайди (қўлланилмайди).

6.6. Электрон тўлов тизимларида ахборотни ҳал қилиш

Банк операцияларини, савдо ишларини ва ўзаро тўловларни замонавий амалиётини пластик карталарни қўллаган ҳолда ҳисоб-китобларсиз тасаввур

этишнинг имкони йўқдир. Ишончлиги, универсаллиги ва қулайлиги ҳисобига пластик карталар бошқа тўлов воситалари орасида мустахкам жойни эгалладилар.

Банкнинг пластик карталарини пластик восита сифатида тизим доирасида ишлатилишини таъминлайдиган усулларни ва уларни амалга оширадиган субъектларнинг тўпламини **электрон тўлов тизими** деб аталади.

Пластик карта - бу муаллифлаштирилган тўлов ҳужжатидир, улар бу картадан фойдаланадиган шахсга товарларга ва хизматларга нақд пулсиз тулаш имконини беради, ҳамда картани тўлов асбоби сифатида қабул қиладиган банк автоматларидан ва банкларнинг бўлимларидан нақд пул воситаларини олиш имконини беради. Банк автоматлари ва банкларнинг бўлимлари картанинг хизмат кўрсатиш нуқталарини қабул қилуви тармоғини ташкил этади.

Банк-эмитент пластик карталарни чиқаради ва бу карталарни тўлов воситаси сифатида ишлатиш билан боғланган молиявий мажбуриятларни бажарилишини кафолатлайди.

Банк-эквайер пластик карталарни тўлов воситалари сифатида қабул қилувчи савдо ва сервис корхоналарига хизмат кўрсатади, ҳамда бу тўлов воситаларини нақд пулга айлантириш учун ўзининг бўлимларида ва унга тегишли бўлган банкоматлар орқали қабул қилади.

Тўлов вақтида корхона мижознинг пластик картасини реквизитларини нусхаловчи машина - импринтер ёрдамида махсус чекка ўтказиши, ҳарид қилиш ёки кўрсатилган хизмат нархини чекка киритиши ва мижознинг имзосини олиши керак. Шундай усул билан расмийлаштирилган чекни **слип** деб аталади.

Муаллифлаштириш жараёнида корхона мижознинг ҳисоб рақамини ҳолати тўғрисида ахборотга мурожаат қилишга рухсат олади ва картани мижозга тегишлилигини ва унинг бажарилган миқдори ўлчамида тулашга қобилиятлигини ўрнатиши мумкин.

Охирги йилларда автоматлаштирилган савдо қилувчи POS -терминал (POS-Point-of-Sale-сотиш нуқтасида тўлов) ва банкоматлар кенг оммавийликка эга бўлдилар. POS-терминалларни ишлатишда слипларни тўлдиришнинг кераги йўқ. Пластик карталарнинг реквизитлари унинг магнитли йўлакчасидан POS-терминалга созланган ўқигич ёрдамида ўқиб олинади. Мижоз терминалга, фақат ўзигагина маълум бўлган, ўзининг PIN-кодини (PIN-Personal Identification Number - шахсий идентификация номери) киритади. PIN-коднинг элементлари магнит полосадаги ёзувни шифрлашнинг умумий алгоритмига киритилади ва карта эгасининг электрон имзоси бўлиб хизмат қилади.

Жараённи бажарувчи марказ маълумотлар базасини олиб боради. Махсуслаштирилган сервис хизмати кўрсатадиган ташкилот кўринишига эга бўлиб, у банк-эквайерлардан ёки бевосита хизмат кўрсатиш нуқталаридан келаётган сўровларни қайта ишлашни таъминлайди.

Кредит карталари маҳсулотлар ва хизматларга тўлаш учун савдо ва хизмат кўрсатиш корхоналарига тақдим этилади. Бундай тўловда ҳаридорнинг банки унга ҳарид суммасига тенг кредит очади, кейин эса (одатда 25 кун) почта бўйича счёт юборади. Дебет картасини ушлаб турувчи олдиндан банк-

эмитентдаги ўзининг ҳисоб рақа-мига маълум бир суммани киритиб қўйиши керак.

Ахборот хавфсизлиги нуқтаси назаридан электрон тўлов тизимларида қуйидаги боғлиқ жойлар мавжуд:

- тўлов ва бошқа хабарларни банк ва мижоз ўртасида ва банклар ўртасида жўнатиш ;
- хабарларни жўнатувчи ва олувчи ташкилотлар ичида ахборотни қайта ишлаш ;
- ҳисоб рақамларида тўпланган воситаларга мижозларнинг мурожаат қилиши.

Кредит карточкасини ҳаридор-эгаси тармоқ орқали ҳарид учун хавфсизликларсиз тўлай олиши учун электрон тўловларни узатишни ҳимоя қилишнинг ишончли, ишлатиб кўрилган механизмига эга бўлиш керак. Бундай янги принципиал ёндашишнинг моҳияти SSL ва SET схемаларини ишлатган ҳолда Интернет тармоғида молиявий ахборотни зудлик билан муаллифлаштириш ва шифрлашдадир.

SSL (Secure Socket Layer) баённомаси ахборотни каналли даражада шифрлашни кўзда тутади.

Visa ва Master Gard компаниялари ишлаб чиққан SET (Secure Electronic Transactions) хавфсиз электрон транзакциялар баённомаси фақатгина молиявий ахборотни шифрлашни кўзда тутади.

SET қоидалари тасодифий равишда ҳосил қилинган симметрик калитни ишлатган ҳолда хабарларни бошланғич шифрлашни кўзда тутади, у ўз навбатида хабарларни ҳаридорининг очиқ калити билан шифрланади. Натижада **электрон конверт** деб аталадиган тушунча ҳосил бўлади. Хабарларни олувчи, жўнатувчининг симметрик калитини олиш учун, ўзининг хусусий (махфий) калити ёрдамида электрон конвертни қайта шифрлайди. Кейин жўнатувчининг симметрик калити юборилган хабарларни қайта шифрлаш учун ишлатилади.

Бузғунчиликдан ва мансабни суистеъмол қилишдан ҳимоя қилиш учун Интернетда махсус сертификатлаш агентлиги (маркази) ташкил этилган, у электрон тижоратнинг ҳар бир иштирок-чиси ноёб электрон сертификат олишини кузатиб боради. Бу сертификатда сертификациялашнинг махсус калити ёрдамида тижорат ишининг жорий иштирокчисини очиқ калити шифрлангандир.

Сертификат маълум вақтга ишлаб чиқилади, ва уни олиш учун сертификациялаш марказига иштирокчи шахсини тасдиқлайдиган ҳужжатни (ҳуқуқий шахслар учун уларни расмий қайд қилиш) тақдим этиш кера кейин эса, “қўлда” сертификатлаш марказининг очиқ калити бўлган ҳолда, келгуси ишларда катнашиш керак.

Электрон савдони ривожланишида баъзи бир кечиқишлар ишончли ҳимоя қилиш тизимининг йўқлиги билан боғлиқдир. Энди айтиш мумкинки, бу ҳимоя қилиш тизими қандайдир даражада топилгандир. Ҳозирча тўлов ахбороти очиқ тармоқлар бўйича минимал эҳтиёткорлик билан ёки умуман уларсиз узатилмоқда. Бу автоматлаштирилган бузғунчилик учун, ҳамда баъзи бир

хакерлар учун тегишли бўлган “шумликни кўзлаб” бузғунчилик учун қулай асос ҳисобланади.

6.7. Ҳақиқийликни идентификациялаш ва текшириш

Компьютер тизимини ҳар бир объекти билан уни бир хил маънода идентификациялайдиган баъзи бир ахборот боғлангандир. Бу ушбу объектни аниқлайдиган сон, белгилар қатори, алгоритм бўлиши мумкин. Бу ахборотни **объектнинг идентификатори** деб аталади. Агар объект тармоқда қайд қилинган бирор идентификаторга эга бўлса, у қонуний (расмий) объект деб аталади, қолган объектлар эса ноқонуний (норасмий) ҳисобланади.

Объектни идентификациялаш - ҳимоя қилишнинг қисм-тизимини функцияларидан биттаси ҳисобланади. Бу функция объект тармоққа киришга интилган вақтда биринчи навбатда бажарилади. Агар идентификациялаш жараёни муваффақиятли тугалланса, ушбу объект бу тармоқ учун қонуний ҳисобланади.

Кейинги қадам - **объектни аутентификациялашдир** (объект-нинг ҳақиқийлигини текшириш). Бу жараён ушбу объект у ўзини эълон қилаётганига айнан ўхшашлигини тўғрилигини ўрнатади.

Учинчи - жараён **ваколатларни бериш** (муаллифлаштириш) объектнинг ишлаш доирасини ва у мурожаат қилиши мумкин бўлган КТ ресурсларини ўрнатади.

Ҳақиқийликни тасдиқлаш жараёни одатда сеанс бошланишида, абонентларни уланишларини ўрнатиш жараёнида, бажарилади.

Уланиш ўрнатилгандан кейин ҳимоя қилишнинг талабларини, хабарлар билан алмашишда, бажарилишини таъминлаш керак:

а) олувчи маълумотлар манбасини ҳақиқийлигига ишониши керак;

б) олувчи узатилаётган маълумотларни ҳақиқийлигига ишониши керак;

в) юборувчи олувчига маълумотларни етиб боришига ишониши керак;

г) юборувчи етказиб берилган маълумотларнинг ҳақиқийлигига ишониши керак .

а) ва б) талабларни бажариш учун рақамли имзо ҳимоя қилиш воситаси ҳисобланади. в) ва г) талабларни бажариш учун юборувчи тасдиқловчи почта (certified mail) ёрдамида топширилганлик тўғри-сидаги билдиришномани олиши керак. Бундай жараёнда ҳимоя қилиш воситаси жавоб хабарни тасдиқлайдиган рақамли имзо ҳисобланади, бу имзо ўз навбатида бошланғич хабарни юборилганлигини исботи ҳисобланади.

КТ ресурсларига мурожаат қилишга рухсат олишдан олдин фойдаланувчи КТ ни тасаввур этиш жараёнидан ўтиши керак, у иккита босқични ўз ичига олади:

- идентификациялашни - фойдаланувчи тизимига унинг сўрови бўйича ўзининг номини (идентификаторини) хабарини беради;

- аутентификациялашни - фойдаланувчи тизимига ноёб, бошқа фойдаланувчиларга номаълум бўлган ўзи тўғрисидаги хабарни (масалан, пароль) киритиб идентификациялашни тасдиқлайди.

Фойдаланувчини идентификациялаш ва аутентификациялаш жараёнларини ўтказиш учун фойдаланувчига керак:

- аутентификациялашни мос субъектини (модулни) мавжудлиги;
- фойдаланувчини аутентификациялаш учун ноёб ахборотни сақлайдиган аутентификацияловчи объектнинг мавжудлиги.

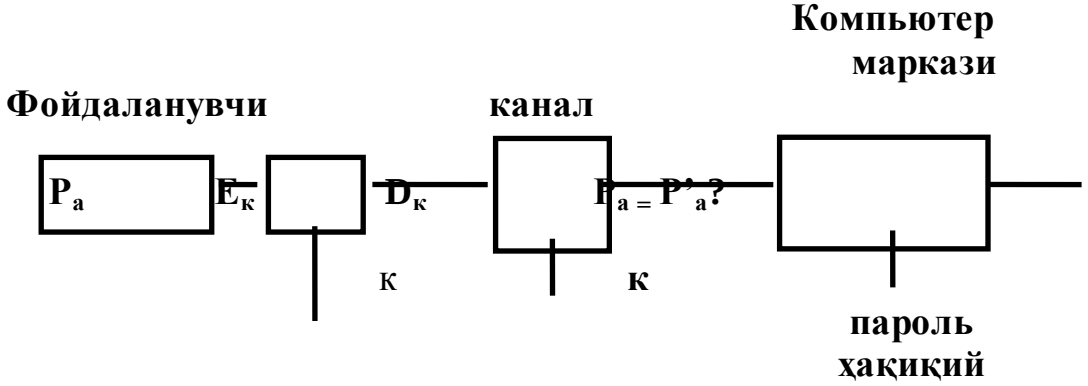
Фойдаланувчини аутентификацияловчи объектларни тасвирлашни иккита шакли мавжуд:

- тизимга тегишли бўлмаган ташқи аутентификацияловчи объект;
- тизимга тегишли бўлган ички объект, унга ташқи объектдан ахборот кўчириб ўтказилади.

Ташқи объектлар турли хил ахборот ташувчиларида - магнит дискларида, пластик карталарда ва ҳ.к. - техник нуқтаи назардан амалга оширилган бўлиши мумкин. Табиийки, аутентификацияланадиган объектларни тасаввур этишни ташқи ва ички шакллари семантиқ томондан ўхшаш бўлиши керак

Компьютер тизимининг ҳар бир қонуний фойдаланувчиси анъанавий равишда идентификатор ёки пароль олади. Ишлаш сеансининг бошланишида фойдаланувчи тизимга ўзининг идентификаторини тақдим этади (кўрсатади), тизим эса фойдаланувчидан паролни сўрайди.

Паролни ишлатган ҳолда ҳақиқийликни тасдиқлашнинг оддий усули фойдаланувчи тақдим этган P_a паролни компьютер марказида сақланадиган бошланғич P'_a қиймат билан таққослашга асосланган. Пароль сир сақланиши учун у ҳимоя қилинмаган канал бўйича юборилмасдан олдин шифрланиши керак. Агар P_a ва P'_a қийматлар мос келса, унда P_a пароль ҳақиқий, фойдаланувчи эса - қонуний ҳисобланади (6.5-расм).



6.5-расм. Пароль ёрдамида оддий аутентификациялаш схемаси

Баъзида олувчи паролнинг бошланғич очиқ шаклини олмаслиги керак. Бу ҳолда юборувчи паролнинг очиқ шакли ўрнига паролнинг бир томонлама ? **(.)** функциясини ишлатган ҳолда олинадиган паролнинг аксини (кўринишини) юбориши керак. Бу ўзгартириш рақибга паролни унинг акси бўйича очиб бўлмасликни кафолатлаши керак, чунки рақиб ечиб бўлмайдиган сонли масалага тўқнаш келади.

Масалан, ? (**.**) функцияси қуйидагича ани қланиши мумкин:

α (?) к E_p (ID),

бу ерда: Р-юборувчининг пароли, ID-юборувчининг идентификатори, E_p-пароль Р ни калит сифатида ишлатган ҳолда бажариладиган шифрлаш жараёни.

Бундай функциялар, агар паролнинг ва калитнинг узунлиги бир хил бўлса, жуда қулайдир. Бу ҳолатда пароль ёрдамида хақи-қийликни тасдиқлаш юборувчининг ?(Р) аксни юборишда ва уни олдиндан ҳисобланган ва сақланаётган ?'(Р) тенг кучлиси билан солиштиришдадир.

Қисқа пароллар барча вариантларнинг тўлиқ тўпламини ҳужумига боғликдир. Бундай ҳужумни бартараф этиш учун ?(Р) функцияни бошқача аниқланади, яъни айнан:

α (?) к Ер ⊗ к (ID),

бу ерда: К ва ID-мос равишда юборувчининг калити ва идентификатори.

Ҳақиқийликни тасдиқлаш паролнинг иккита ?(P_a) ва ?(P_a') аксларини солиштиришда ва агар бу акслар тенг бўлсалар P_a паролни тан олишдадир.

Одатда ахборот алмашинувига киритувчи томонлар бир-бир-ларининг ҳақиқийлигини ўзаро текширишга (аутентификациялашга) мухтождирлар. Бу ўзаро аутентификациялаш жараёни алоқа сеансининг бошланишида бажарилади (6.6 - расм).

Ҳақиқийликни текшириш учун қуйидаги усуллар қўлланилади:

- сўров - жавоб механизми;
- вақтни белгилаш механизми ("вақтли штемпель").

Сўров-жавоб механизмининг моҳияти қуйидагичадир. Агар "А фойдаланувчи у В фойдаланувчидан олаётган хабарларни ёлғон эканлигига ишонч ҳосил қилиши керак бўлса, у В учун юборилаётган хабарга олдиндан айтиб бўлмайдиган элементни - Х сўровни (масалан, бирорта тасодифий сонни) қўшади. Жавоб беришда В фойдаланувчи бу элемент устида бирорта амални (масалан, бирорта f (x) функцияни) бажариши керак. Буни олдиндан амалга оширишнинг имкони йўқдир, негаки В фойдаланувчига сўровда қандай тасодифий х сони келиши номаълумдир. Ишлар натижасини жавобини олиб А фойдаланувчи В фойдаланувчи ҳақиқий эканлигига ишонч ҳосил қилиши мумкин. Бу усулнинг камчилиги - сўров ва жавоб ўртасидаги қонуниятларни ўрнатиш мумкинлигидир.

Вақтни белгилаш механизми ҳар бир хабар учун вақтни қайд қилишни кўзда тутади. Бу ҳолатда тармоқнинг ҳар бир фойдаланувчиси келган хабарни қанчалик "қариганини" аниқлаши мумкин, ва уни қабул қилмаслиги мумкин, чунки у ёлғон бўлиши мумкин.

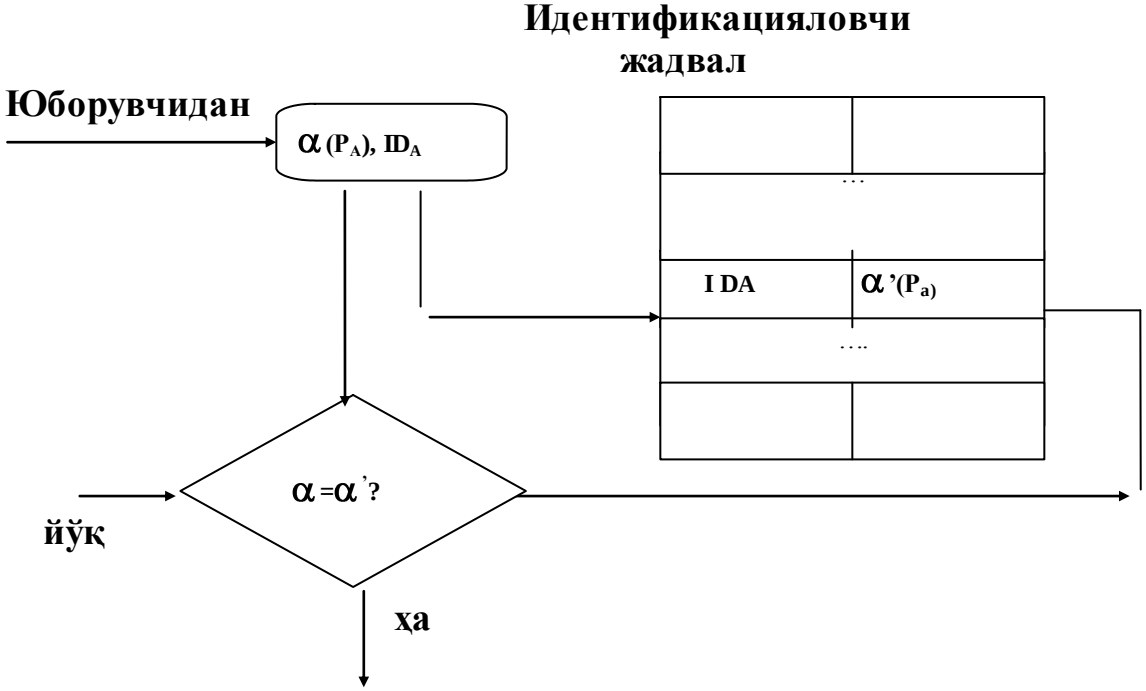
Иккала ҳолатда ҳам назорат қилиш механизмини ҳимоя қилиш учун, жавоб ёмон ниятли киши томонидан юборилмаганлигига ишонч ҳосил қилиш учун шифрлашни қўллаш тавсия этилади.

6.8. Электрон рақамли имзо

Электрон ҳужжатлар билан алмашишда алоқа тармоғи бў-йича ҳужжатларни қайта ишлашга ва сақлашга ҳаракатлар жиддий пасаяди, уларни қидириш тезлашади.

Электрон ҳужжатларни аутентификациялашни мақсади ёмон ниятли ҳаракатларнинг мумкин бўлган турларидан ҳимоя қилиш ҳисобланади, бу ҳаракатларга тегишлидир:

- **фаол ушлаб олиш** - тармоққа уланиб олган бузғунчи ҳужжатларни (файлларни) ушлаб олади ва уларни ўзгартиради;
- "**маскарад**" - С абонент ҳужжатни В абонентга А абонент номидан юборади;
- **ренегатлик** - А абонент В абонентга хабарлар юборилмаганлигини эълон қилади, аслида эса хабар юборган бўлади;



6.6-расм. Идентификацияловчи жадвални ишлатиб пароль ёрдамида аутентификациялаш схемаси

- **алмаштириб қўйиш** - В абонент янги ҳужжатни ўзгартиради ёки шакллантиради, ва уни А абонентдан олганлигини эълон қилади;
- **такрорлаш** - С абонент А абонент В абонентга олдин юборган ҳужжатни такрорлайди.

Ёмон ниятли ҳаракатларнинг бу турлари ўзининг фаолиятида компьютерли ахборот технологияларини қўллайди, банк ва тижорат структураларига, давлат корхоналари ва ташкилотларига, хусусий шахсларга жиддий талофат етказишлари мумкин.

Электрон шаклда ҳужжатларни қайта ишлашда қоғоздаги ҳужжатда қўлёзма имзоси ва мухр тамғаси бўйича ҳақиқийликни ўрнатишни анъанавий усуллари умуман яроқсиздир. **Электрон рақамли имзо (ЭРИ)** принциал янги ечим ҳисобланади. [25; 148-153]

Электрон рақамли имзо телекоммуникация каналлари бўйича узатилаётган матнларни аутентификациялаш учун ишлатилади. Функцияси жиҳатидан у оддий қўлёзма имзосига ўхшашдир ва унинг асосий афзалликларига эгадир:

- имзоланган матн имзо қўйган шахсдан келаётганини тасдиқлайди;
- шу шахснинг ўзига имзоланган матн билан боғланган мажбуриятни инкор қилишга йўл қўймайди;
- имзоланган матнни бутунлигини кафолатлайди:

Рақамли имзо имзоланадиган матн билан бирга узатиладиган қўшимча рақамли ахборотнинг нисбатан кўп бўлмаган миқдори кўринишига эгадир.

ЭРИ тизими иккита жараённи ўз ичига олади:

1) имзони қўйиш жараёни;

2) имзони текшириш жараёни.

Имзони қўйиш жараёнида хабарни юборувчининг махфий калити ишлатилади, имзони текшириш жараёнида эса юборувчининг очиқ калити ишлатилади. ЭРИ ни шакллантиришда юборувчи энг аввало имзоланаётган М матннинг ХЭШ-функциясини h(M) ҳисоблайди. ХЭШ-функ-циянинг h(M) ҳисобланган қиймати барча М матнни яхлитлигича характерловчи битта қисқа ахборот блоки m кўринишига эгадир. Кейин m сони юборувчининг махфий калити билан шифрланади. Бунда олинадиган сонлар жуфтлиги ушбу М матн учун ЭРИ кўринишига эгадир.

ЭРИ ни текширишда хабарни олувчи канал бўйича қабул қилинган М матнни ХЭШ-функциясини mқh(M) яна ҳисоблайди, бундан кейин юборувчининг очиқ калити ёрдамида олинган имзо ХЭШ-функциянинг ҳисобланган m қийматига мос келишини текширади. ЭРИ тизимида принципиал момент фойдаланувчининг ЭРИ ни унинг имзосини махфий калитини билмасдан туриб калбақилаштиришнинг имкони йўқлигидир.

Имзоланадиган ҳужжат сифатида исталган файл ишлатилиши мумкин. Имзоланган файл имзоланмаганидан унга битта ёки ундан кўпроқ электрон имзоларни қўшиш йўли билан яратилади.

Ҳар бир имзо қуйидаги имзони ўз ичига олади:

- имзони санаси;
- ушбу имзонинг калитини ҳаракатини тугаш муддати;
- файлни имзолаган шахс тўғрисида ахборот (Ф.И.Ш., мансаби, фирманинг қисқача номи);
- имзочининг идентификатори (очиқ калитнинг номи);
- шахсий рақамли имзо.

ЭРИ ни тизимини қўллаш технологияси бир-бирига имзоланган электрон ҳужжатларни юборадиган абонентлар тармоғини борлигини кўзда тутади. Ҳар бир абонент учун калитлар жуфтлиги: махфий ва очиқ ишлаб чиқарилади. Махфий калит абонент томонидан сир сақланади ва у томондан ЭРИ ни шакллантириш учун ишлатилади. Очиқ калит бошқа барча фойдаланувчиларга маълумдир ва олувчи томонидан имзоланган электрон ҳужжатни ЭРИ сини текшириш учун мўлжалланган. Бошқача айтганда, очиқ калит электрон ҳужжатни ва имзо муаллифини ҳақиқийлигини текшириш имконини берадиган ин-

струмент (ускуна) ҳисобланади. Очиқ калит махфий калитни ҳисоблаш имконини бермайди.

ЭРИ алгоритмларида калитлар жуфтлигини (махфий ва очиқ) ишлаб чиқариш учун шифрлашнинг асимметрик тизимларидаги каби, бир томонлама функцияларни ишлатишга асосланган турли хил математик схемалар ишлатилади. Бу схемалар иккита гуруҳга бўлинадилар. Бундай рухсатнинг асосида маълум бўлган мураккаб ҳисоблаш масалалари ётади:

- катта бутун сонларни факторлаш (кўпайтувчиларга ёйиб чиқиш);
- дискрет логарифмлаш масаласи.

ЭРИ нинг аниқ бир тизими АҚШ нинг Массачуссетс технологик институтида 1977 йилда математик схемаси ишлаб чиқилган **RSA** тизими бутун дунёдаги биринчи ва энг машхур тизими бўлди.

RSA рақамли имзо мультурликатив ҳужумга боғликдир. Бошқача айтганда **RSA**-рақамли имзо алгоритми ёмон ниятли кишига махфий D калитни билмасдан туриб, ХЭШ-лаш натижасини имзоланиб бўлинган ҳужжатларнинг ХЭШлаш натижаларини кўпайтмаси каби ҳисоблаш мумкин бўлган ҳужжатлар остида имзоларни шакллантириш имконини беради.

Шахсий компьютерларда амалга ошириш учун янада ишончлирок ва қулай бўлган **EGSA** рақамли имзо алгоритми 1984 йилда келиб чиқиши араб миллатига мансуб бўлган америкалик Тахир Эль Гамал томонидан ишлаб чиқилган.

Эль Гамалнинг рақамли имзо схемаси RSA рақамли имзо схемасига нисбатан бир қатор афзалликларга эга:

1. Рақамли имзо алгоритмининг берилган мустахкамлик даражасида ҳисоблашларда катнашаётган бутун сонлар 25% қисқа узунликка эгадир, бу эса ҳисоблашлар мураккаблигини деярли 2 марта камайтиради ва ишлатиладиган хотира сиғимини сезиларли қисқартириш имконини беради.

2. Эль Гамаль схемаси бўйича имзони шакллантириш жараёни махфий калитни билмасдан туриб (**RSA** даги каби) янги хабарлар остида рақамли имзоларни ҳисоблаш имконини бермайди.

Лекин Эль Гамалнинг рақамли имзо алгоритми **RSA** имзо схемасига нисбатан баъзи бир камчиликларга эга. Хусусан, рақамли имзо узунлиги 1,5 барабар катта бўлади, бу эса ўз навбатида уни ҳисоблаш вақтини катталаштиради.

Қўшимча функционал имкониятли рақамли имзо схемалари унинг асосий тизимини, масалан **RSA** алгоритми асосида, рақамли имзонинг асосий тизимига эга бўлмаган қўшимча хоссаларни таъминлаб берадиган махсус баённома билан бирлаштириш имкониятига эга.

Қўшимча хоссали рақамли имзо схемаларига киради:

-ожизона имзо (blind) схемаси;

-тортишилмайдиган имзо (undeniable) схемаси.

Рақамли имзонинг оддий схемаларидан фарқли равишда **ожизона имзо схемаси** (баъзида кўр-кўрона имзо схемаси деб аталади) юборувчи **A** ва ҳужжатни имзолайдиган **B** томон ўртасидаги икки томонлама баённома ҳисобланади.

Бу тизимларнинг асосий ғоясининг моҳияти қуйидагича**: А** юборувчи ахборот бўлагини **В** томонга жўнатади, бу бўлакни **В** имзолайди ва **А** га қайтаради. Олинган имзони ишлатиб **А** томон **В** томоннинг имзосини ўзи учун муҳимрок бўлган **m** хабарда ҳисоблаши мумкин. Бу баённома тугагандан кейин **В** томон **m** хабар тўғрисида, бу хабар остидаги имзо тўғрисида ҳеч нарса билмайди.

Ожизона имзонинг мақсади шундаки, имзолаётган **В** шахсга у имзолаётган **А** томоннинг хабари билан, ва бу хабар остидаги мос имзо билан танишишга тўсқинлик қилишдир. Шунинг учун келгусида имзоланган хабарни **А** томон билан боғлашни имкони йўқдир.

Оддий рақамли имзо каби **тортишилмайдиган имзо** имзоланган ҳужжатга ва махфий калитга боғлиқдир. Лекин оддий рақамли имзолардан фарқли равишда тортишилмайдиган имзо бу имзони қўйган шахснинг иштирокисиз верификацияланиши (тўғрилигини текшириш) мумкин эмас. Балки, бу имзолар учун янада тўғри келадигани **“қалбақилаштиришга йўл қўймайдиган имзолар”** номи бўлиши мумкин эди.

6.9. Интернет тармоғи орқали масофадан туриб ҳужумлардан ҳимоя қилиш воситалари

Глобал компьютер тармоқларини жадал ривожланиши, ахборотни қидиришнинг янги технологияларини пайдо бўлиши Интернет тармоғига хусусий шахслар ва турли ташкилотлар томонидан янада кўпроқ эътибор қаратилмоқда.

Интернет глобал тармоғи ахборотларни очиқ алмашиш учун мўлжалланган очиқ тизим каби яратилган. Ўзининг очиқлик идеологияси туфайли Интернет ёмон ниятли кишилар учун анъанавий ахборот тизимларига нисбатан анча катта имкониятлар яратиб бермоқда.

Одатда тармоқлараро экранлар корхонанинг ички тармоғини Интернет глобал тармоғидан “бостириб киришлардан” ҳимоя қилади, лекин улар корхонанинг локал тармоғи уланган корпоратив интратармоқдан “ҳужумлардан” ҳимоя қилиш учун ишлатилиши мумкин. Ҳеч бир тармоқлараро экран мумкин бўлган ҳолатларда ички тармоқни тўлиқ ҳимоя қилишни кафолатлай олмайди. Лекин кўпчилик тижорат ташкилотлари учун тармоқлараро экранни ўрнатиш ички тармоқни хавфсизлигини таъминлашнинг зарур шарти ҳисобланади. Тармоқлараро экранни қўллаш фойдасининг асосий белгиси шундаки, уларсиз ички тармоқнинг тизимлари Интернет тармоғининг кучсиз ҳимоя қилинган хизматлари томонидан хавф, ҳамда ташқи тармоқнинг бирорта бошқа хост-компьютерларининг ҳужуми хавфи келиб чиқиши мумкин.

Глобал тармоқларга корпоратив ёки локал тармоқларни улашда тармоқ хавфсизлиги маъмурияти қуйидаги масалаларни ечиши керак:

- глобал тармоқ томонидан тақиқланган масофадан туриб мурожаат қилишлардан корпоратив ёки локал тармоқларни ҳимоя қилиш;
- глобал тармоқ фойдаланувчиларидан тармоқ таркиби ва унинг ташкил этувчилари тўғрисидаги ахборотларни яшириш;
- глобал тармоқдан ҳимоя қилинаётган тармоққа ва глобал тармоққа ҳимоя қилинаётган тармоқдан мурожаат қилишларни чеклаш.

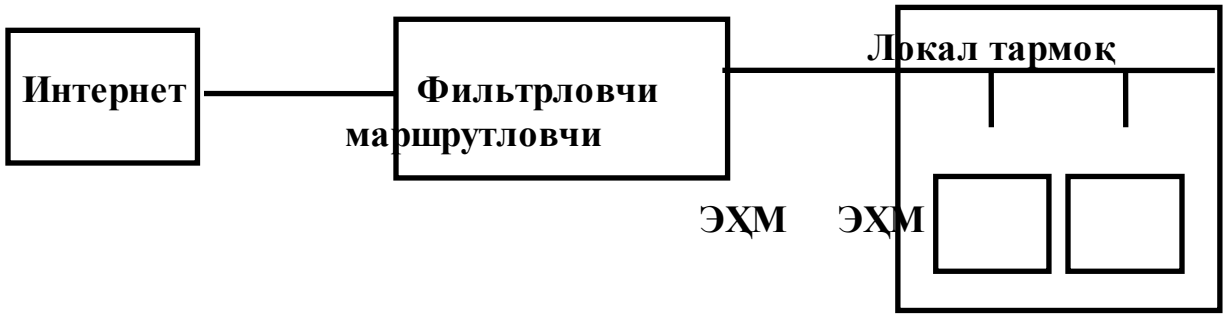
Корпоратив ёки локал тармоқни ҳимоя қилиш учун тармоқлараро экранларни ташкил этишнинг қуйидаги асосий схемалари ишлатилади:

- тармоқлараро экран - фильтрловчи маршрутизатор;
- икки портли шлюз асосидаги тармоқлараро экран;
- экранлаштирилган шлюз асосидаги тармоқлараро экран;
- тармоқлараро экран - экранлаштирилган қисм тармоғи.

Пакетларни фильтрлашга асосланган тармоқлараро экран кенг тарқалган ва амалга оширишда энг оддий ҳисобланади. У ҳимоя қилинадиган Интернет тармоқлари ўртасидаги фильтрловчи маршрутловчидан ташкил топган (6,7-расм). Фильтрловчи маршрутизатор кириш ва чиқиш пакетларини, уларнинг манзилларини ва портларини таҳлил қилиш асосида, блокировкалаш ва фильтрлаш учун мўлжалланган.

Ҳимоя қилинаётган тармоқда жойлашган компьютерлар Интернет тармоғига тўғридан-тўғри мурожаат қилади, шу билан бир вақтда Интернетдан уларга мурожаат қилишнинг катта қисми блокировкаланади.

Пакетларни фильтрлашга асосланган тармоқлараро экранлар фильтрловчи маршрутловчиларга ўхшаган камчиликларга эга, шу билан бирга бу камчиликлар ҳимоя қилинаётган тармоқнинг хавф-сизлигига талаблар кучайтирилганда янада сезиларли бўлади.

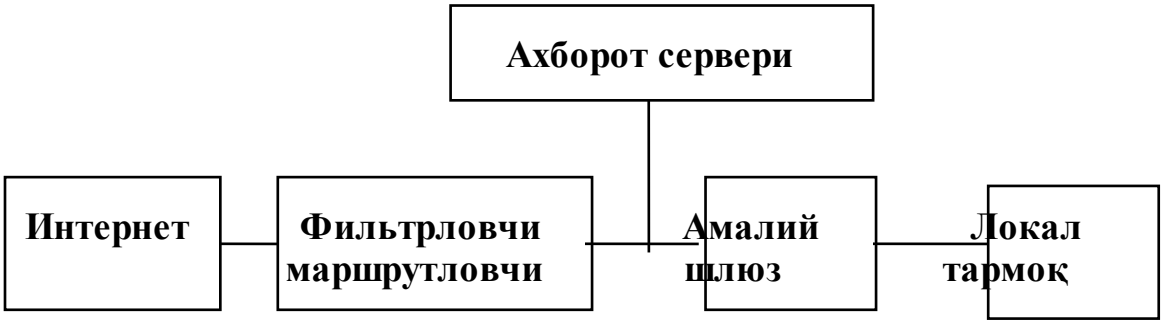


6.7-расм. Фильтрловчи маршрутловчи асосидаги тармоқлараро экран

Улардан баъзиларини таъкидлаймиз:

- фильтрлаш қоидаларини тўлиқ тестлашнинг имкони йўқлиги; бу тармоқнинг тестланмаган ҳужумлардан ҳимоя қилинмаганлигига олиб келади;
- фильтрлаш қоидаларининг мураккаблиги; баъзи бир ҳолатларда бу қоидаларнинг тўплами бошқарилмайдиган бўлиб қолиши мумкин;
- воқеаларни қайд қилиш имкониятларини деярли йўқлиги; натижада маъмурият маршрутловчига ҳужум бўлганлигини ва у ўзини билдириб қўйганлигини аниқлаши мумкин бўлади.
- Интернет тармоғи билан уланган ҳар бир хост-компьютер кучайтирилган аутентификациялашда ўзининг воситаларига мухтож бўлади. [19; 240-256]

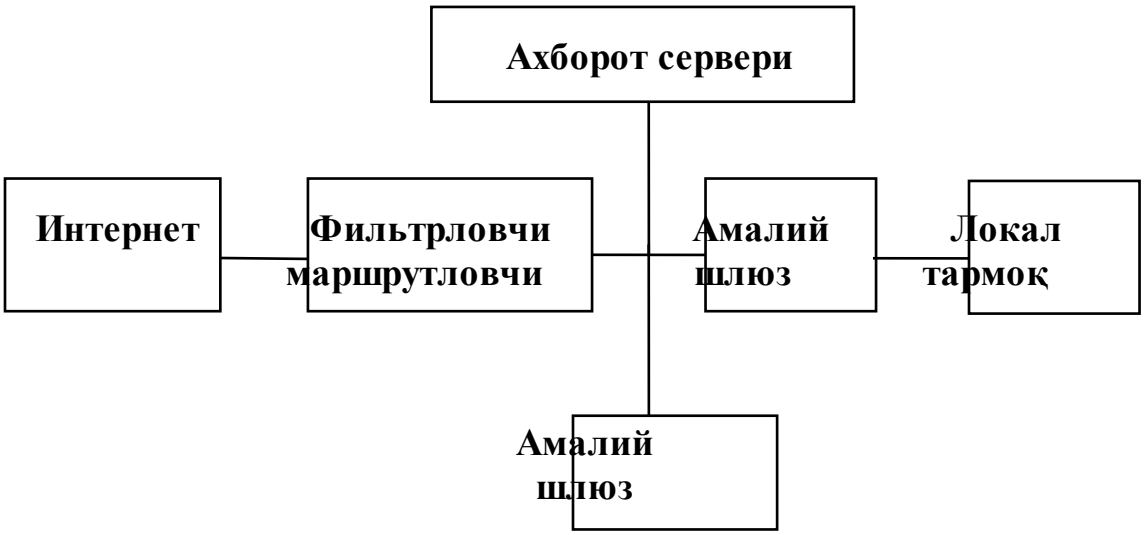
Икки портли шлюз асосидаги тармоқлараро экран иккита тармоқ интерфейсли иккита уйли хост-компьютерни ўз ичига олади. Бу интерфейслар ўртасида асосий фильтрлаш амалга оширилади. Қўшимча ҳимоялашни таъминлаш учун амалий шлюз ва Интернет тармоғи ўртасида одатда фильтрловчи маршрутловчи жойлаштирилади (6.8-расм).



6.8-расм. Амалий шлюзли ва фильтрловчи маршрутловчили тармоқлараро экран

Фильтрловчи маршрутловчили тармоқлараро экран схемасидан фарқли равишда амалий шлюз Интернет тармоғи ва ҳимоя қилинаётган тармоқ ўртасидаги IP трафикини тўлиқ блокировкалайди. Фақатгина амалий шлюзда жойлаштириладиган ваколатли сервер-даллолларгина хизматларни ва фойдаланувчига мурожаат қилишни амалга ошириши мумкин.

Экранлаштирилган шлюз асосидаги тармоқлараро экран фильтрловчи маршрутловчини ва ички тармоқ томонидан жойлаштириладиган амалий шлюзни бирлаштирилади. Амалий шлюз хост-компьютерда амалга оширилади ва фақат битта тармоқ интерфейсига эга (6.9-расм).



6.9-расм. Экранлаштирилган шлюз асосидаги тармоқлараро экран

Бу схемада бирламчи хавфсизлик фильтрловчи маршрутловчи томонидан таъминланади. Фильтрловчи маршрутловчида пакетли фильтрлаш қуйидаги усуллардан бири билан амалга оширилиши мумкин:

- ички хост-компьютерларга маълум бир сервислар учун Интернет тармоғида хост-компьютерлар билан уланишларни очиш имконини бериш;

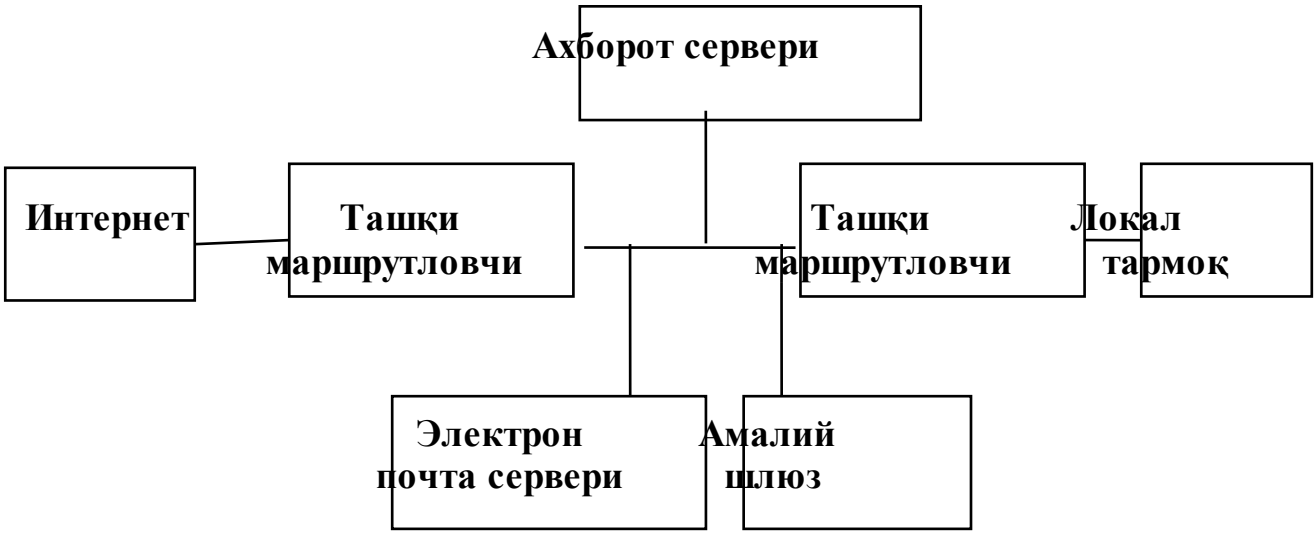
- ички хост-компьютерлардан барча уланишларни тақиқлаш (уларни амалий шлюздаги сервер-даллоллар ваколатларини ишлатишга мажбур этган ҳолда).

Экранлаштирилган шлюзли тармоқлараро экранни схемасини асосий камчилиги шундаки, агар ҳужум қилаётган бузғунчи хост-компьютерга кириб олса, унда унинг олдида ички тармоқнинг ҳимоя қилинмаган тизимлари пайдо бўлади.

Шунинг учун бугунги кунда экранлаштирилган қисм тармоқли тармоқлараро экран схемаси оммавийроқ бўлиб қолмоқда (6.10-расм).

Экранлаштирилган шлюз асосидаги тармоқлараро экран схемаси кўринишига эгадир. Экранлаштирилган қисм-тармоқни яратиш учун иккита экранловчи маршрутловчи ишлатилади.

Ташқи маршрутловчи экранлаштирилган қисм тармоқни ҳам, ички тармоқни ҳам Интернет тармоғидан ҳимоя қилади. У Интернетдан ички тармоқнинг тизимларига мурожаат қилишни тақиқлайди ва уланишларни ташаббускори бўлиши керак бўлмаган тизимлардан Интернетга келаётган барча трафикни блокировкалайди.



6.10-расм. Экранлаштирилган қисм тармоқли тармоқлараро экран схемаси

Ички маршрутловчи ички тармоқнинг тизимлар трафикни бошқаради ва улардан қуйидаги қоидаларга мос равишда:

- амалий шлюздан тармоқнинг тизимларига трафик рухсат этилади;
- тармоқ тизимларидан амалий шлюзга амалий трафик рухсат этилади;
- электрон почтанинг серверидан тармоқ тизимларига электрон почта трафики рухсат этилади;
- тармоқ тизимларидан электрон почта серверига электрон почта трафики рухсат этилади;
- тармоқ тизимларидан ахборот серверига FTP, Gopher ва ҳ.к. трафикларидан рухсат этилади;

- қолган трафиклар таъқиқланади.

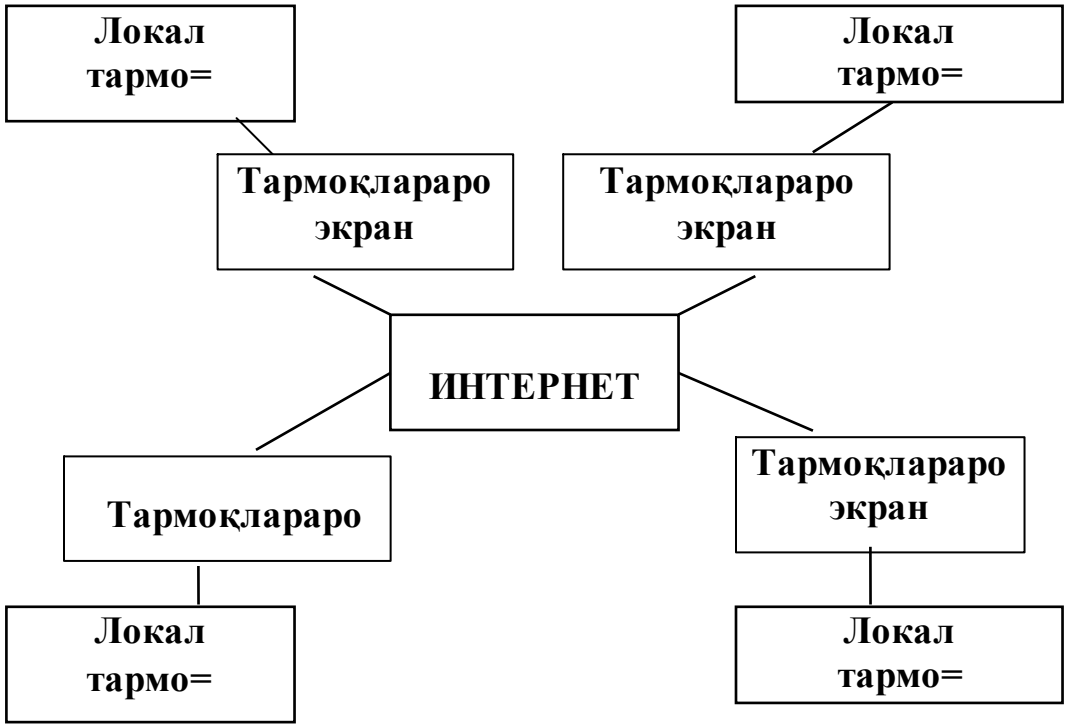
Экранлаштирилган қисм тармоқли тармоқлараро экран катта хажмдаги трафикли ёки юқори алмашиш тезлигидаги тармоқларни ҳимоя қилиш учун тўғри келади.

Экранлаштирилган қисм тармоқли тармоқлараро экран камчиликларга ҳам эга:

- фильтрловчи маршрутловчиларнинг жуфтлиги хавфсизликнинг керакли даражасини таъминлаш учун катта эътиборга мухтождир, негаки уларни конфигурациялашдаги хатолар учун бутун тармоқнинг хавфсизлигида камчиликлар пайдо бўлиши мумкин;

- амалий шлюзни айланиб утиб мурожаат қилишни принципиал имконияти мавжуддир.

Баъзи бир тармоқлараро экранлар виртуал корпоратив тармоқларни ташкил этишга имкон беради. Глобал тармоққа уланган бир нечта локал тармоқлар битта виртуал корпоратив тармоққа бирлашадилар. Виртуал корпоратив тармоқлар таркибида тармоқлараро экранларни қўллаш схемаси 6.11-расмда кўрсатилган.



6.11 - расм. Виртуал корпоратив тармоқ схемаси

Бу локал тармоқлар ўртасида маълумотлар узатиш локал тармоқларнинг фойдаланувчилари учун очиқ (шаффоф) шаклда амалга оширилади.

Узатилаётган ахборотнинг махфийлиги ва бутунлиги шифрлаш воситалари, рақамли имзоларни ишлатиш ёрдамида таъминланиши керак. Маълумотларни узатишда нафақатгина пакетнинг мазмуни, балки сарлавҳанинг баъзи бир майдонлари ҳам шифрланиши мумкин.

Интернет тармоғида ахборотни ҳимоя қилишнинг объектив жихатлари шундаки, бу бутун дунё ахборот тизими мураккаб ва очиқдир. Интернетда ҳимоя қилишни ташкил этиш Интернетнинг кўп сонли хизмат турларини хар бирини ҳимоя қилишни ташкил этишни ўз ичига олади.

Интернетда ахборотни ҳимоя қилишнинг усуллари глобал даражада қабул қилинган стандартлар асосида зарур ҳимоя қилиш билан таъкидланади, регионал ва локал даражада эса тўлиқ ҳимоя қилиш учун ҳимоя қилиш воситалари билан таъминланади

Асосий атамалар

Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Domain Name System (DNS), TELNET, World Wide Web (WWW), UNIX операцион тизими, TCPғIP, электрон почтанинг Send-mail дастури, Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP) Secure HTTP (S-HTTP), Secure Sockets Layer (SSL), Secure MIME (SғMIME), Secure Wide Area Networks (SғWAN), Secure Electronic Transaction (SET), Pretty Good Privacy (PGP), Privaci Enhanced Mail (PEM), КРИПТОН-ВЕТО криптографик ҳимоя қилиш тизими, КРИПТОН-ЗАМОК комплекси, махфий ахборотни ҳимоя қилиш тизими Secret Disk, абонентлик шифрлаш (АШ), электрон рақамли имзо (ЭРИ), пакетли шифрлаш (ПШ), абонентларни криптографик аутентификациялаш, электрон рақамли имзо дастури Crypton Sign, брандмауер (тармоқлараро экран ёки firewall), фильтрловчи маршрутловчи, электрон тўлов тизими, муаллифлаштириш жараёни, жараёнли марказ, SET (Sekure Electronic Transaction) баённомаси, объект идентификатори, тармоқлараро экран (ТЭ).

Назорат саволлари

1. Интернетда ахборотни ҳимоя қилишнинг объектив шарт-шароитлари қандай?
2. Бузғунчи Интернет орқали нималар қилиши мумкин?
3. Интернетнинг кенг тарқалган хизматлари қандай «туғма» заифликларга эга?
4. Тармоқли номлар хизмати DNS нинг муаммоси нима ҳисоблана-
5. ди?
6. Ахборот хавфсизлиги учун WWW нинг қайси хоссаси заиф буғин
7. ҳисобланади?
8. Интернетнинг тармоқ хавфсизлиги сиёсатининг моҳияти нимада?
9. Интернетнинг тармоқ сервисларига мурожаат қилиш сиёсатининг асосий принциплари қандай?
10. Интернет учун маълумотларни ҳимоя қилишнинг қайси стандартлари қўлланилади?
11. Интернетда ахборотни ҳимоя қилишнинг қайси усуллари қўлланилади?
12. Электрон почтани ҳимоя қилиш учун қайси стандартлар қўлланилади?

13. Интернетда мулкчилик ҳуқуқлари қандай?

14. Интернетнинг ахборот хавфсизлигини режимини шакллантиришнинг қонуний даражаси ўз ичига нималарни олади?

15. Интернет хавфсизлик сиёсатининг тармоқли аспектларини ишлаб чиқишда қандай принциплар ишлатилади?

16. Интернетда қайси энг кўп тарқалган ахборотни ҳимоя қилиш тизимлари ишлатилади?

17. КРИПТОН-ВЕТО тизимининг асосий функциялари қандай?

18. Мурожаат қилишни чекловчи КРИПТОН-ЗАМОК комплекси қандай функцияларни бажаради?

19. Secret Disk тизими нима?

20. Crypton Sign дастури нима учун мўлжалланган?

21. Crypton Sign ёрдамида электрон рақамли имзо қандай яратилади ва текширилади?

22. Windows 95/98/NT учун АШ ва ЭРИ нинг қайси дастурлар пакети қўлланилади?

23. Брандмауэр нима? Унинг тавсифларини келтиринг.

24. Фильтрловчи маршрутловчи нима?

25. Тармоқ даражасидаги шлюзлар тавсифларини келтиринг.

26. Электрон тўлов тизими нима?

27. Амалий даражадаги шлюзларнинг тавсифларини келтиринг.

28. Пластик картани, эмитент ва эквайер банкларини тавсифлаб беринг.

29. SSL ва SET баённомаларининг асосий функциялари ва вазифалари қандай?

30. Объектни идентификациялаш ва аутентификациялаш нима?

31. Интернетдан фойдаланувчиларни аутентификацияловчи объектларни тасвирлашни қандай шакллари бор?

32. Объектлар ҳақиқийлигини текширишни қайси усуллари ишлатилади?

33. Электрон рақамли имзо нима?

34. ЭРИ ни қўллашнинг технологияси қандай?

35. RSA ва EGSA рақамли имзо схемалари қандай ишлайди?

36. Қўшимча функционал хусусиятли рақамли имзо схемасининг хусусиятлари қандай?

37. Тармоқлараро экран-фильтрловчи машрутловчи схемаси қандай кўринишга эга?

38. Иккита портли шлюз асосидаги тармоқлараро экран схемаси қандай хоссаларга эга?

39. Экранлаштирилган шлюз асосидаги тармоқлараро экранни таърифлаб беринг.

40. Фильтрлашга асосланган тармоқлараро экран схемаси қандай кўринишга эга?

Тавсия этиладиган адабиётлар:

1. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в КС и С. – М.: “Радио и связь”, 2001.

2. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

4. Завгородный В.И. Комплексная зашита информации в компьютерных системах. – М.: Логос, 2001.

5. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Эрматов Ш.Т., Мусаева М.А. Компьютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. – Т.: ТДИУ, 2003.

ХУЛОСА

Шундай қилиб, замонавий ахборотлашган жамиятда, бозор муносабатлари жамиятда ахборот махсус товар (маҳсулот) бўлиб колмоқда, бунда кўпинча ахборотнинг нархи компьютер тизимини ўзин уни комплекс ҳимоя қилиш тизими билан бирга миқдори биргаликдаги нархидан келмоқда. Охирги вақтларда кузатилаётган компьютер тизимларининг ривожланиши қонунияти ахборотни ҳимоя килиш тизимини тўлиқ қонуний ривожлантиришни келтириб чиқаради. Компьютер тизимида етарлича ахборотни ҳимоя қилишни ташкил этиш муаммоси, шубхасиз, долбзарбдир. Мухимлилик долбзарблилик муаммосини келтириб чиқарадиган сабаблардан ташқари ахборотни ҳимоя қилишни шаклланишига ажратилаётган ва тобора ўсиб бораётган сарф – харажатларни таъкидлаш мумкин (фақатгина АҚШда ва ғарбий Европа мамлакатларида бу харажатлар 6 млрд. долларни ташкил этади.)

Компьютер тизимларида ахборотни ишончли ҳимоя қилиш, агар у барча объектларда (фойдаланувчилар терминаллари тармоқ маъмурияти ёки гуруҳли абонентлик узели терминал алоқа узели ахборотга ишлов бериш воситалари, ахборотни акс эттириш воситалари ахборотни ҳужжатлаштириш воситалари, машина зали ташқи алоқа каналлари ва тармоқ жихозлари, ахборотни йиғувчилар ва ташувчилар) ва барча субъектларда (тезкор ва ташқи эслаб қолиш қурилмаларидаги маълумотлар ва дастурлар, монитор экранидаги ва принтерга чиқарилаётган маълумотлар алоқа канали бўйича узатилаётган маълумотлар, ахборотни қайта ишлашининг турли чиқиндилари, паролларни ва устуворликларни белгилаш журналлари, хизмат кўрсатмалари, тармоқ операцион тизимлари архивлари) ишончли бўлган тақдирдагина самарали бўлиши мумкин.

Äåñòàáèëèçàòèðóþ÷è îìèëüíûé ìàíåâðè, деñòàáèëèçàòèðóþ÷è îìèëüíûé ўçè âà óëüòíîé îқèáàòëàðè ìàúëóìàëð. Óëüòíîé àðàìèўòè àðáîðîò õàâôñèçëèãèíîé ïàéäî áўëà,òãàí òàõàëëäàðèíè îëäèíäàí àíèқëàá áåðàäè. Õàâôñèçëêê òàõäëäëðèãà òàúñèð êûðñàòèø ó÷óí çàìîíàâèé êîìïüþòåð òèçèìëàðè õàðàêòåðëè õîññàëàðãà ýãà, óëàðãà òèçèìíèíã ìóðàêêàáëãè, ìóðîæàò ýòèøíèíã òóðëàðèãà óíèíã î÷èқëãè, êîìïüþòåð òèçèìíèíã òàøêèë ýòó÷èëàðè áèðîòà êåíãëêêàà æîëëàøãàí, õàìäà êîìïüþòåð òèçèìëàðèãà ìàñîôäàí òóðëá õóæòìàðíè óþøòèðèëøè ìóìêí.

Тасодифий таҳдидлардан ахборотни ҳимоя қилишнинг энг самарали усулларидан бири дублаш ҳисобланади. Дублашдан ташқари компьютер тизимини (КТ) ишончлилигини ошириш, ишдан чиқишларга мустахкам компьютер тизимларини яратиш, хато бажарилган амалларни блокировкалаш, халокатлардан фавқулодда вазиятлардан келадиган зарарларни минималлаштириш, хамда инсонни компьютер тизим билан ўзаро харакати бўйича оптималлаштириш ишларини таъкидлаш керакдир.

Олдиндан кўзда тутилган таҳдидлардан анъанавий жосуслик ва қўпорувлардан ҳимоялаш ишларини ташкил этиш, зарарли электромагнит нурланишлардан ва йўналтиришлардан ҳимоя қилиш, тақиқланган мурожаат қилишдан (ТМҚ) ҳимоя қилиш усуллари (ахборотга мурожаат этишни чеклаш тизими (МЭЧТ), ахборотни тадқиқот этишдан ва нусхалашдан ҳимоя қилиш воситалари) кўриб чиқилади.

Тармоқларга ва тармоқ ресурсларига ТМҚ ларини бартараф этиш бўйича чоралардан бири паролларни ишлатишга асосланган мурожаат этишни назорат қилишдир. Ишлатиладиган пароллар қуйидагилардир: фойдаланувчи ўрнатадиган пароллар; тизим ўрнатадиган пароллар; ярим сўзлар; таянч иборалар; «савол-жавоб» интерфаол кетма-кетлиги; «қатъий» пароллар.

Объектга мурожаат этишни ташкил этишда ҳал этиладиган асосий масалалардан бири объектга киритиладиган шаклларни идентификациялаш ва аутентификациялашдир.

Ахборотни ҳимоя қилишнинг таклиф этиладиган моделлари (захираларга мурожаат этиш пароли, мурожаат этиш ҳуқуқи, аудит, дисксиз компьютерлар) компьютер тизимларини ҳимоя қилишнинг етарлича даражасини таъминлайди.

Ахборотни ҳимоя қилишнинг криптографик усулларидан шифрлашни, зичлаштиришни айтиб ўтиш жоиздир. Криптотизимларни самарадорлигини кўрсатгичларни тахлил қилиш кўрсатмоқдаки, иккита калитли тизимларни шифрлаш алгоритми очиқ калитли классик схемаларга нисбатан сезиларли даражада секинроқдир. Шу билан бир вақтда очиқ калитли шифрлаш бирмунча ишончлироқдир.

Компьютер тизимларини ривожланиши билан янада янги компьютер вируслари пайдо бўлмоқда, шунга мос равишда турли хил антивирусли тизимлар ва воситалар ҳам пайдо бўлмоқда. Одатда вируслар компьютер тизимида сақлаётган дастур таъминотини вағёки маълумотларни ўзгартиради ёки йўқ килади. Зарар келтирадиган дастурларга биологик вирусларнинг хоссалари интилишдир.

Компьютер вирусларини шаклларини ва турли - туманлигини кўп қирралилиги тавсифли схемаларда турли хил белгилар бўйича келтирилгандир. Айниқса «мантиқий бомбалар», «троян отлари», «чувалчанглар» каби вирусларни таъкидлаш жоиздир.

Шак-шубхасиз, махсус антивирусли воситаларни ишлаб чиқиш ва ишлатиш долзарбдир. Антивирусли воситалар вирусдан зарарланиш окибатларини аниқлаш (сканерлаш, ўзгаришларни пайқаш усули, эвриетик тахлил этиш, аппарат - дастурли антивирусли воситалар ва хакозо) ва йук килиш масалаларини ечади, шу билан бир каторда файлларни ва хотира сохаларини, юкланиш секторларини тиклайди.

Антивирусли дастурлардан детектор, ревизор (тафтишли) ва «коровул» дастурларини таъкидлаб утиш мумкин.

Компьютер вирусларидан ҳимоя қилишнинг асосий чораларидан дастур маҳсулотларини расмий йўл билан ишлатишни келтириш мумкин. Алоҳида таъкидлаш керакки, антивирусли воситалар доимо янгиланиб бориши керак,

бунда ташқаридан келадиган янги дастурларга ва файлларга алоҳида эътиборни қаратиш керак.

Интернет тармоғида ахборотни ҳимоя қилишнинг объектив жихатлари шундаки, бу бутун дунё ахборот тизими мураккаб ва очиқдир. Интернетда ҳимоя қилишни ташкил этиш Интернетнинг кўп сонли хизмат турларини хар бирини ҳимоя қилишни ташкил этишни ўз ичига олади.

Интернетда ахборотни ҳимоя қилишнинг усуллари глобал даражада қабул қилинган стандартлар асосида зарур ҳимоя қилиш билан таъкидланади, регионал ва локал даражада эса тўлиқ ҳимоя қилиш учун ҳимоя қилиш воситалари билан таъминланади.

ГЛОССАРИЙ

1. **КТ ва Т -** компьютер тизимлари ва тармоқлари.

2. **Компьютер тизимлари ва тармоқларининг хавфсизлиги** – меъёрий ишлаш жараёнига тасодифий ёки олдиндан мўлжалланган аралашишдан, ўғирлашдан, ўзгартиришдан ва бузишдан ҳимоя қилиш.

3. **Ахборотга мурожаат** – ахборот билан танишув, қайта ишлаш, ўзгартириш, йўқ қилиш.

4. **Ахборотга рухсат этилган мурожаат** – бу мурожаат қилиш чекланишларига ўрнатилган қоидаларни бузмайдиган, ахборотга мурожаат қилишдир.

5. **Тақиқланган мурожаат** – чегараланган қоидаларни бузиб ахборотга мурожаат этишдир.

6. **Ахборотни ҳимоя қилиш** – узатьилаётган, сақланаётгвн ва қайта ишланаётган ахборотнинг ишончлилигини ва бутунлилигини тизимли таъминлаш мақсадида турли хил воситалданрни ва усулларни қўллаш.

7. **Пароль** – тизимга кириш учун калит сифатида ишлатиладиган мурожаат.

8. **Фойдаланувчи томонидан ўрнатиладиган пароллар** – фойдаланувчи томонидан ўрнатилади.

9. **Тасодифий пароллар ва кодлар** – тизим томонидан ўрнатилади.

10. **Ахборотнинг бутунлиги -** тизимлардаги маълумотлар тасодифан ёки олдиндан мўлжалланган халақитларга ва бузилишга учрамаганлиги тушинилади.

11. **Тизимнинг ташкил этувчисини ёки ресурсининг бутунлиги** – тизим тасодифий ёки олдиндан мўлжалланган халақитлар ёки таъсир шароитларида ишлаганда ташкитл этувчи ва ресурсининг мемантиқ маънода ўзгармай қолиши.

12. **Тизим хавфсизлигининг хавфи** – унинг хавфсизлигига тўғридан-тўғри ёки бевосита талофат етказиши мумкин бўлган таъсирлдар.

13. **Компьютер тизимларига ҳужум** – ёмон ниятли киши томонидан бажариладиган харакатдир, ҳужум хавфсизлик хавфини амалга оширишдир.

14. **Хавфсиз ёки ҳимоя қилинган тизим** – хавфсизлик хавфларига муваффақиятли ва самарали қарши турадиган, зарур ҳимоя қилиш воситаларига эга бўлган тизимдир.

15. **Ҳимоя қилиш воситалари комплекси** – компьютер тизимлари тармоқларининг ахборот хавфсизлиги таъминлаш учун яратиладиган ва қўллаб қувватланадиган дастурли ва аппарат воситалари.

16. **Хавфсизлик сиёсати** – бу ҳимоя қилиш воситаларининг ишлашни ахборот хавфсизлигининг хавфи берилган тўпламидан меъёр, қоида ва амалий тавсияномаларнинг йиғиндиси.

17. **Идентификациялаш** – мурожаат қилиш субъектларига идентификаторларни тақдим этиш ва кўрсатилган идентификаторларни объектга киришга рухсат этилган. Олдиндан тақдим этилган идентификаторлар рўйхати билан таққослаш.

18. **Аутентификациялаш** – мурожаат қилиш объектларини улар кўрсатган идентификаторларга тўғри келишлигини текшириш, ҳақиқийликни тасдиқлашдир.

19. **Шифрлаш** – криптографик ўзгартиришнинг асосий кўринишидир. Бу очиқ ахборотни шифрланган ахборотга (шифрматн) ўзгартириш.

20. **Қайта шифрлаш** - шифрланган ахборотни очиқ ахборотга тескари ўзгартириш жараёни.

21. **СРЭУ –** Компьютер тармоқларининг таркибини тақиқланган ўзгаришлардан ҳимоя қилишнинг усуллари.

22. **Қўйилмалар** - тизимни ишлаб чиқиш босқичида ва уни ўзгартиришда бажарилган КТ ларини СРЭУ.

23. **Қароқчилар** - дастурларни ва маълумотларни ноқонуний версияларини яратиб муаллифлик ҳуқуқини бузадилар

24. **Хакерлар** - бошқа фойдаланувчиларнинг компьютерларига ва улардаги файлларга ноқонуний мурожаат қилиш ҳуқуқига эга бўладилар, лекин улар тизим устидан ўзининг устунлигини англашдан қаноатланган ҳолда файлларни бузмайдилар ва нусхаламайдилар.

25. **Кракерлар** (бузувчилар) - ўзларига барча имкониятларга йўл қўядилар ва энг жиддий бузғунчилар ҳисобланадилар.

26. **MAC (Message Authentication Code)** - маълумотлар ўзгаришини пайқаш учун криптографик назорат йиғиндиси сифатида хабарларни аутентификациялаш коди.

27. **ЭРИ** - узатилаётган тақиқланган ўзгаришларни пайқаш учун электрон-рақамли имзолаш.

28. **Трафик** - бу ҳисоблаш тармоғининг узатадиган муҳити бўйича айланадиган маълумотлар оқимидир.

29. **Атрибутив усул** - мурожаат қилиш субъектига ёки ноёб предметни, ёки паролни (кодни), ёки кодни ўз ичига олган предметни бериш.

30. **Аудит (auditing)** - бу сервернинг хавфсизлик журналига (security log) маълум бир ходисаларни ёзиш.

31. **Зичлаштириш** - ахборот хажмини қисқартириш.

32. **Тармоқлараро экран** – ишончли тармоқ ва ишончсиз тармоқ орасида маълумотларга киришни бошқаришда ҳимоялаш воситаси бўлиб қўлланилади.

33. **Domain Name System (DNS) –** фойдаланувчилар номи ва хост-компьютернинг IP манзилини кўрсатади.

34. **Фильтрловчи йўлловчи** - компьютер тармоғида маълумотларни манзилга утказувчи дастурлар пакети ёки сервердаги дастурлар бўлиб, у кирағдиган ва чиқадиган пакетларни фильтрлайди.

35. **Фақат ўқиш учун** (read only) - мурожаат қилишни ишлатганда паролни биладиган ходимлар барча файлларни ўқиши, ҳужжатларни кўриб чиқиши, уларни ўз машинасига нусхалаш.

36. **Тўлиқ мурожаат қилиш** (full access) - барча файлларни кўриб чиқиш, ўзгаритириш ва ўчириш.

37. **Паролга боғлиқ равишда мурожаат қилиш** (depending on password) - биргаликда ишлатиладиган каталогга икки даражали пароль тақдим этилади: фақат ўқиш учун ва тўлиқ.

38. **Мурожаат қилиш ҳуқуқи** - ҳимоя қилишда ҳар бир фойдаланувчига ҳуқуқларнинг маълум бир тўпламини тақдим этиш.

39. **Ахборотни ҳимоя қилишнинг криптографик усуллари** - бунда бошланғич ахборот шундай ўзгартириладики, бунинг натижасида ахборот керакли ваколатларга эга бўлмаган шахсларга танишиш ва ишлатиш учун мумкин бўлмай қолади.

40. **Стенография усуллари** - нафақатгина сақланаётган ёки узатилаётган ахборотни маъносини беркитиб қолмасдан, балки ёпиқ ахборотни сақлаш ёки узатиш омилини ҳам яшириш имконини беради.

41. **Симметрик криптотизим** - махфий калит жўнатувчига ва олувчига калитлар тарқатадиган ҳимоя қилинган канал бўйича узатилади.

42. **Носимметрик криптотизим**- ҳимоя қилинмаган канал бўйича фақат очиқ калит узатилади, махфий калит эса уни ишлаб чиқарилган жойида сақланади.

43. **Алмаштириш (ўрнига қўйиш) усулли** - бир алфавитда ёзилган бошланғич ахборотнинг белгиларини маълум бир қоида бўйича бошқа алфавитдаги белгилар билан алмаштириш.

44. **Полиалфавитли алмаштириш усули** - бошланғич матн белгиларини алмаштириш учун бир нечта алфавитларни ишлатиш.

45. **Шифрлашнинг аддитив усуллари (гаммалаш)** - бошланғич ахборотнинг рақамли кодлари билан қўшиладиган рақамли кортежнинг тасодифий кетма-кетлигини ишлатади.

46. **Компьютер вируси** - махсус ёзилган дастур бўлиб, компьютерда ишлашда барча мумкин бўлган тўсиқларни яратиш, файлларни ва каталогларни бузиш дастурлари.

47. **Зарарланган диск** - бу юкланиш секторида вирус-дастур жойлашган дискдир.

48. **Зарарланган дастур** - бу унга татбиқ қилинган вирус-дастурни ўз ичига олган дастурдир.

49. **Чувалчанглар** деб аталадиган **вирус репликаторларни** - улар компьютер тармоқлари бўйича тарқаладилар, тармоқ компьютерларининг манзилларини ҳисоблайдилар ва бу манзиллар бўйича ўзларининг нусхаларини ёзадилар.

50. **Стелс-вируслар** - деб аталадиган кўринмайдиган вируслар маълумдир, уларни пайқаш ва зарарлантириш жуда мушкулдир, чунки улар операцион тизимни зарарланган файлларга ва диск-ларнинг секторларига мурожаат

қилишни ушлаб оладилар ва ўзининг танасини ўрнига дискнинг зарарланмаган қисмларини қўяди.

51. **Квазивирусли ёки "троянли" дастурлар** - улар ўз-ўзидан тарқалиш хоссасига эга бўлмасаларда, лекин жуда хавфлидир, чунки улар фойдали дастур остида ниқобланиб, юкланадиган секторни ва дискларнинг файлли тизимини бузадилар.

52. **Дастур фильтрлар** - улар хали кўп нарсаларни бузишга ёки зарар-лантиришга улгурмасдан олдин, энг бошланғич босқичда пайқаш имконини беради.

53. **Детекторлар дастури-** бешинчи ўринда турадилар, улар янги олинган дастур таъминотида вирусларнинг мавжудлигини текшириш учун ишлатилади.

54. **Докторлар дастури** (фаглар) - Уларни, бузилган дастурни нусхаси архивда бўлмаганда, ва уни бошқа усул билан олиш қийин бўлган ҳоллардагина қўллаган маъқулроқ. Бундан ташқари, агар дастур-фаг ишлатилаётган бўлса, унда кейин тикланган файлни дастур-тафтишчи билан албатта текшириш керак бўлади (тушунарлики, агар бу файл тўғрисидаги ахборот олдиндан сақланган бўлса), лекин ҳар доим ҳам дастур-доктор тўғри даволайвермайди.

55. **Тафтишчилар дастури** - компьютер вирус билан зарарланмаганда, каталогларнинг дастурларини ва дискнинг тизимли соҳаларини бошланғич қийматини эслаб қоладилар, кейин эса даврий равишда ёки фойдаланувчининг хохиши бўйича жорий ҳолатни бошланғич ҳолат билан таққослайди.

56. **Вакциналар ёки иммунизаторлар** - бу файлларни зарарланишини бартараф этувчи резидентли дастурдир.

57. **Doctor Web дастур** -компьютер оламида нисбатан яқинда пайдо бўлган полиморфли вируслар билан курашиш учун мўлжалланган дастур.

58. **Aidstest дастур полифаг** - бу жуда ҳам кенг тарқалган 1300 дан ортиқ компьютер вирусларини пайқаш ва йўқотиш имкониятига эга бўлган дастурдир.

59. **Adinf Cure Module** - бу компьютерни янги вирусдан "даво-лашга" ёрдам берадиган дастур бўлиб, у бу вирус маълум бўлган Aidstest ёки Dr.Web полифагларни янги версияларини кутиб турмайди. Adinf Cure Module дастури, вирусларни кўплаб турлари борлигига қарамасдан уларни файлларга татбиқ қилишни унчалик кўп бўлмаган турлича усуллари мавжудлиги далилини ишлатади.

60. **Бутун дунё ўргимчак уяси (WWW-World Wide Web)** - бу тармоқ иловаларига асосланган тизимдир, бу иловалар фойдаланувчиларга Интернетда ёки интратармоқларда турли серверларнинг мазмунини кўриб чиқиш имконини беради.

61. **TCPғIP (Transmission Control ProtocolғInternet Protocol)**- интернетда хабарларни узатишни бошқариш баённомаларини тўплами турли турдаги компьютерлар ўртасида мос келишликни таъ-минлаган ҳолда бир жинсли бўлмаган тармоқли муҳитда коммуникацияларни ташкил этиш учун ишлатилади.

62. **TELNET (Узоқлашган терминални эмуляциялаш хизмати)** - тармоққа бириктирилган узоқлашган тизимларга уланиш учун ишлатилади.

63. **SMTP** (**Simple Mail Transfer Protocol**) –электрон почтани узатиш-нинг оддий баённомаси**.** Интернетнинг почта транспортли хизматини амалга ошириш имконини беради.

64. **SLIP (Serial Line Internet Protocol) ва PPP (Point-to-Point Protocol)** - тармоқ сервисларига мурожаат қилиш сиёсатига мос равишда фойдаланувчилар мурожаат қилиши чекланиши керак бўлган Интернет сервислар. Интернетнинг "таъқиқланган" сервисларига ғайриоддий йўллар билан мурожаат қила олмаслиги учун керакдир.

65. **Secure HTTP (S – HTTP)** - Web да транзакцияларни ҳимоя қилиш.

66. **Secure Sockets Layer (SSL)-** тармоқ даражасида маълумотлар пакетини ҳимоя қилиш.

67. **Securite Electronic Transaction (SET)-** кредит картали транзакцияларни ҳимоя қилиш

68. **Secure MIME** (**S ғ MIME)** -турли платформаларда электрон жўнатмаларга киритилганларни ҳимоя қилиш

69. **Secure Wide Area Net Works(SғWAN)-** брандмауэрлар ва маршрутловчилар ўртасида бир даражадаги уланишларни шифрлаш

70. **PEM (Privaci Enhanced Mail)** - бу очиқ ёки симметрик калитларни ишлатиб электрон почтани ҳимоя қилиш учун Интернетнинг стандарти.

71. **Pretty Good Privacy** - аббревиатурада (махфийликнинг юқори даражаси) каби қайта шифрланадиган **PGP** шифрлаш дастури.

72. **КРИПТОН-ЗАМОК комплекси** - компьютерга мурожаат қилишни чеклайдиган аппарат-дастурли воситалари.

73. **Crypton Sign** дастури - электрон ҳужжатларнинг муаллифлигини ўрнатишни ва электрон ҳужжатларнинг яхлитлигини текширишни таъминлайди.

74. **Экранлаштирилган шлюз** - тармоқлараро экран фильтрловчи маршрутловчини ва ички тармоқ томонидан жойлаштириладиган амалий шлюзни бирлаштиради.

75. **Икки портли шлюз** - тармоқлараро экран иккита тармоқ интерфейсили иккита уйли хост-компьютерни ўз ичига олади.

V. ТАВСИЯ ЭТИЛГАН АДАБИЁТЛАР РЎЙХАТИ.

I. Ўзбекистон Республикаси Қонунлари

1. Ўзбекистон Республикаси Конституцияси. – Т., Ўзбекистон 2003.
2. Ўзбекистон Республикасининг “Ахборотлаштириш тўғрисида”ги қонуни. // Халқ сўзи. 2004 й., 11 феврал.
3. “Электрон тижорат тўғрисида”ги Ўзбекистон Республикаси қонуни. // Халқ сўзи. 2004 й., 21 май.

II. Ўзбекистон Республикаси Президенти Фармон ва Қарорлари

4. “Ахборот технологиялари соҳасида кадрлар тайёрлаш тизимини такомиллаштириш тўғрисида Ўзбекистон Республикаси Президенти Қарори. // Халқ сўзи. газетаси, 2005, 3-июн.
5. “Компьютерлаштиришни янада ривожлантириш ва ахборот-коммуникация технологияларини жорий этиш тўғрисида” Ўзбекистон Республикаси Президенти Фармони. // Халқ сўзи.. 2002 й., 6 июн.

III. Ўзбекистон Республикаси Вазирлар Маҳкамаси Қарорлари

6.“2001-2005 йилларда компьютер ва ахборот технологияларини ривожлантириш, “Интернет”нинг халқаро ахборот тизимларига кенг кириб боришини таъминлаш дастурини ишлаб чиқишни ташкил этиш чора-тадбирлари тўғрисида” Ўзбекистон Республикаси Вазирлар Маҳкамасининг Қарори. //Халқ сўзи. 24 май, 2001 й.
7. “Компьютерлаштиришни янада ривожлантириш ва ахборот-коммуникация технологияларини жорий этиш чора-тадбирлари тўғрисида” Ўзбекистон Республикаси Вазирлар Маҳкамасининг Қарори. // Халқ сўзи. 2002 й., 8 июн.
8. Электрон рақамли имзодан фойдаланиш соҳасида норматив-ҳуқуқий базани такомиллаштириш тўғрисида” Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 26 сентябрдаги 215-сон Қарори. Ўзбекистон Республикаси қонун ҳужжатлари тўплами 39-сон (175) 2005 й., сентябр.
9. “Ахборотлаштириш соҳасида норматив-ҳуқуқий базани такомиллаштириш тўғрисида” Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 22 ноябрдаги 256-сон қарори. Ўзбекистон

Республикаси қонун ҳужжатлари тўплами 47-48-сон (183-184) 2005й. ноябр-декабр.

IV. Ўзбекистон Республикаси Президенти асарлари.

10. Мамлакатимиз тараққиётини қонуний асосларини мустаҳкамлаш фаолиятимиз мезони бўлиши даркор // Президент И.А. Каримовнинг 2006 йил 24 февраль куни Тошкент шахрида Ўзбекистон Республикаси Олий Мажлиси Сенатининг бешинчи ялпи мажлисидаги маърузаси. // Халқ сўзи, 2006 йил, 25 февраль, № 39(3838).

11. Каримов И.А. Эришилган ютуқларни мустахкамлаб, янги марралар сари изчил ҳаракат қилишимсиз лозим // Президент И.А. Каримовнинг 2006 йил 10 февраль куни Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йилда мамлакатимизни ижтимоий–иқтисодий ривожлантириш якунлари ва 2006 йилда иқтисодий ислохотларни чуқурлаштиришнинг мухим устувор йўналишларига бағишланган мажлисидаги маърузаси. // Халқ сўзи.-2006 йил, 11 февраль, № 29(3828). 1-2-бет

12. Каримов И.А. Бизнинг бош мақсадимиз – жамиятни демократлаштириш ва янгилаш, мамлакатни модернизация ва ислоҳ этишдир. – Т.: Ўзбекистон, 2005.

13. Каримов И.А. Ўзбекистон демократик тараққиётининг янги босқичида. –Т.: Ўзбекистон, 2005.

14. Президент И.А.Каримовнинг Вазирлар Маҳкамасининг 2004 йилда мамлакатни ижтимоий-иқтисодий ривожлантириш якунлари ва 2005 йилда иқтисодий ислоҳотларни чуқурлаштиришнинг асосий йўналишларига бағишланган мажлисидаги маърузаси. // Халқ сўзи. – 2005, 19 январ.

15. Каримов И.А. Биз танлаган йўл – демократик тараққиёт ва маърифий дунё билан ҳамкорлик йўли. –Т.: Ўзбекистон, 2003.

V. Ўзбекистон Республикаси вазирликлари меъёрий –ҳуқуқий ҳужжатлари

16.Ўзбекистон Республикаси Президентининг «Ахборот технологиялари соҳасида кадрлар тайёрлаш тизимини такомиллаштириш тўғрисида» ги қарори, // Халқ сўзи, 2005, 3-июнь, 1-бет.

17.«Ахборот-коммуникация технологияларини янада ривожлантиришга оид қўшимча чора-тадбирлар тўғрисида» Ўзбекистон Республикаси Президентининг 2005 йил 8 июлдаги -117-сон Қарори.

18. «ZiyoNET ахборот тармоғини янада ривожлантириш тўғрисида» Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 28-декабрдаги 282-сон қарори.

VI. Дарсликлар

19. Завгородный В.И. Комплексная защита информации в компьютерных системах. – М.: Логос, 2001.

20. Домашев А.В., Грунтович М.М. и др. Программирование алгоритмов защиты информации. Учеб. пособ. 2-е изд., – М.: Издатель Молгачева С.В. Издательство «Нолидж», 2002. – 416с.

21. Хорошко В.А. Чекатков А.А. Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504 с.

22. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

23. Степанов Е.А. Корнеев И.К. Информационная безопастность и защита информации. – М.: Инфра, 2002.

24. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. “Защита информации в КС и С”. – М.: “Радио и связь”, 2001

VII. Ўқув қўлланмалар.

25. Р.Х. Алимов, Б.Ю.Ходиев, Қ.А. Алимов, С.У.Усмонов, Б.А. Бегалов, Н.Р. Зайналов, А.А. Мусалиев , Ф. Файзиева. Миллий иқтисодда ахборот тизимлари ва технологиялари. – Т., 2004. 319 бет.

26. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Эрматов Ш.Т., Мусаева М.А. Компьютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. – Т.: ТДИУ, 2003.

27. Галатенко В.А. Основы информационной безопасности - М.: ИНТУИТ РУ. 2003, - 280с.

28. Арипов М.М., Муҳаммадиев Ж.У. Информатика, Информацион технологиялар. – Т.: ТДЮИ. 2004 й.

29. Соколов А.В., Степанюк О.М. Методы информационной зашиты объектов и компьютерных сетей. – Спб.: Полигон, 2000.

VIII. Монография ва илмий мақолалари.

30. Қодиров М. Иқтисодий салоҳият ифодаси. // Солиқ тўловчининг журнали № 4, 2005, 47 – 49 бетлар

IX. Докторлик, номзодлик диссертациялари.

31. Рихсимбоев О. Ўзбекистон Республикасида кичик ва Ўрта бизнеснинг устувор йўналишларини эконометрик башоратлаш. // иқт. фан. номзод. учун ёз. дисс. -Т. ТДИУ, 2002.

32. Яхшибоев Г.К. Ўзбекистон Республикасида кичик бизнес ва хусусий тадбиркорликни молиявий таъминлаш масалалари. // иқт. фан. номзод. учун ёз. дисс. -Т. Ўзбекистон Республикаси Президент ҳузуридаги Давлат ва Жамият қурилиш академияси, 2005.

X. Илмий амалий анжуманлар маърузалар тўплами.

33."Иқтисодчи кадрлар тайёрлаш сифатини таъминлашда ахборот-коммуникациялар технологиялари". Республика илмий-амалий анжумани. -Т., 2003, 15-16 май.

34.16-е Международнўе Плехановские чтения. материалў международной научно-практической конференции. -Москва-Ташкент., 2003.

XI. Газета ва журналлар.

35. Таълим ва тарбия. Журнал. 2005 й. 304-сон.

36. Иқтисодиёт ва таълим. Журнал 1-2 сон. 2004**.**

37. Ўзбекистон иқтисодий ахборотномаси. // Журнал. 2003-2005 йил сонлари.

38. Экономическое обозрение. // Журнал. 2003-2005 йил сонлари.

XII. Статистик маълумотлар тўпламлари.

39. Промышленность Республики Ўзбекистан 2004: статистический сборник. – Т.: Госкомитет РУ по статистике, 2005.

40. Ўзбекистон Республикасининг 2004 йилдаги ижтимоий иқтисодиёт ривожлантириш бўйича якунлари. – Т.: Статистика давлат қўмитаси, 2005.

41. Инсон тараққиёти тўғрисида маъруза. Ўзбекистон. 2001-2004 йиллар.

XIII. Интернет сайтлари.

42. http://ad.cctpu.edu.ru - Томск Политехник Университетининг «Информатика ва тизимларни лойиҳалаштириш» кафедраси сайти.

43. http://diamond.stup.ac.ruғENGғF4ғDirectғ4.html - «Таълимда янги ахброт технологиялари» номли Россия таълим сайти.

44. www.search.re.uz - Ўзбекистоннинг ахборотларни излаб топиш тизими.

45. www.ictcouncil.gov.uz -Компьютерлаштиришни ривожлантириш буйича Вазирлар Махкамаси мувофиқлаштирувчи Кенгашининг сайти.

46. www.ecsoman.edu.ru - Россия Федерация олий ўқув юртларида ўқитилаётган фанлар бўйича ўқув-услубий комплекслар.

XIV. Виртуал кутубхона электрон дарслик ва ўқув қўлланмалари.

47. Зокирова Т.А., Мусаева М.А. Microsoft Office ҳужжат ва дастурларини тақиқланган мурожаат этишдан сақлаш. Электрон дарслик 2005 й.

48. Эрматов Ш.Т., Шоахмедова Н.Х. Ахборотни ҳимоя қилишнинг криптографик усуллари. Электрон дарслик 2005 й.

49. Эрматов Ш.Т. Компьютер тизимларида ахборотни ҳимоя қилиш. Электрон дарслик. – Т., 2004

XV. Битирув-малакавий ишлари.

50. Мухамедов Х.Б. Эконометрический таҳлил монетарной политики государства. // Магистерская диссертация. -Т.: ТГЭУ, 2002.

51. Абдуллаев У.А. Банк фаолияти ва банк хатарларини баҳолаш усуллари. // Магистрлик диссертацияси, Т.: ТДИУ, 2002.

52. Отабоев В.Т. Кичик бизнесни ривожлантиришда маркетинг тамойилларидан фойдаланишни такомиллаштириш Т.: ТДИУ, 2005.

53. Юлдашев А. Кичик бизнес ва тадбиркорликни ривожлантиришда маркетинг томойилларидан фойдаланиш самарадорлиги. Битирув малакавий иши. -Т.: ТДИУ, 2005.

54. Нажимов Р. Банк фаолиятидаги таваккалчилик турлари ва уларни модуллаштириш. Битирув малакавий иши. -Т.: ТДИУ, 2001.