ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Андижон муҳандислик-иқтисодиёт институти

«Информатика ва ахборот технологиялари» кафедраси

А.Абдуллаев, М.Юсупов,
С.Жамолдинов, Б.Абдулхаев

«АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ»

фанидан

ЛЕКЦИЯЛАР КУРСИ

Андижон – 2005 йил

Ушбу лекциялар курси Институт услубий кенгашида кўриб чиқилган ва фойдаланишга тавсия этилган «___»_____200__й.

Тақризчилар: Андижон Давлат тиллар педагогика институти
«Информатика» кафедраси мудири
ф-м.ф.н., доц. Б.Мирзакаримов

Курбонов Ё. техника фанлари номзоди, доцент.

Ушбу лекциялар курси «Информатика ва ахборот технологиялари» кафедраси йи\илишида кўриб чиқилган ва фойдаланишга тавсия этилган «___»_____200__й.
Баённома №_____

Кафедра мудири: проф. А.Абдуллаев

СЎЗ БОШИ

Тез ривожланиб бораётган компьютер ахборот технологиялари бизнинг кундалик хаётимизнинг барча жабхаларида сезиларли узгаришларни олиб кирмокда. Хозирда “ахборот тушунчаси” сотиб олиш, сотиш, бирор бошка товарга алмаштириш мумкин булган махсус товар белгиси сифатида тез-тез ишлатилмокда. Шу билан бирга ахборотнинг бахоси куп холларда унинг узи жойлашган компьютер тизимининг бахосида бир неча юз ва минг баробарга ошиб кетмокда. Шунинг учун тамомила табиий холда ахборотни унга рухсат этилмаган холда киришдан, касддан узгартиришдан, уни угирлашдан, йукотишдан ва бошка жиноий характерлардан химоя килишга кучли зарурат тугилади.

Компьютер тизимлари ва тармокларида ахборотни химоя остига олиш деганда, берилаётган, сакланаётган ва кайта ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш максадида турли восита ва усулларни куллаш, чораларни куриш ва тадбирларни амалга оширишни тушуниш кабул килинган.

Ахборотни химоя килиш деганда:

- Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йук килинишига йул куймаслик;
- Ахборотнинг бутунлигини саклаб колган холда, уни элементларини калбакилаштиришга (узгартиришга) йул куймаслик;
- Ахборотни тегишли хукукуларга эга булмаган шахслар ёки жараёнлар оркали тармокдан рухсат этилмаган холда олишга йул куймаслик;
- Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар факат томонлар уртасида келишилган шартномалар асосида кулланилишига ишониш кабилар тушунилади.

Юкорида таъкидлаб утилганларнинг барчаси асосида компьютер тармоклари ва тизимларида ахборот хавфсизлиги муаммосининг долзарблиги ва мухимлиги келиб чикади. Шунинг учун хозирги курс Республикамизнинг олий ва урта махсус укув муассасалари укув режаларида муносиб урин эгаллайди.

Ушбу курснинг вазифалари:

- Талабаларда компьютер тармоклари ва тизимларида ахборот хавфсизлиги тугрисидаги билимларни шакллантириш;
- Ахборотни химоя килишнинг назарий, амалий ва услубий асосларини бериш;

- Талабаларга компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллашни амалий жихатдан ургатиш;
- Талабаларни ахборотни химоя килиш буйича ишлаб чикарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

Курсни узлаштириш натижасида талаба куйидагиларнибилиши шарт;

- компьютер тармоклари ва тизимларидаги ахборот хавфсизлигига тахдид солиши кутилаётган хавф хатарнинг мохиятини ва окибатларини тушуниши;
- компьютер тармоклари ва тизимларида ахборотни химоя килиш буйича куйиладиган асосий талаблар ва асосларни узлаштириш;
- компьютер тармоклари ва тизимларида ахборот хавфсизлагини таъминлашда кулланиладиган замонавий усуллар ва воситаларни билиш;
- тизимларда ахборот бутунлиги ва ишочлигини бузувчи вируслар ва бошка манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлаштириш буйича чораларни куриш;

ахборотни химоя килишда кулланиладиган замонавий амалий тизимлар ва дастурий махсулотларни ишлата олиш;

1 - МАВЗУ: АХБОРОТЛАРГА НИСБАТАН МАВЖУД ХАВФСИЗЛИКЛАРНИНГ АСОСИЙ ТУШУНЧАЛАРИ ВА УНИНГ ТАСНИФИ

1. Ахборот хавфсизлигига кири;
2. Предметнинг асосий тушунчалари ва мақсади;
3. Ахборотларга нисбатан хавф-хатарлар таснифи;
4. Тармок хавфсизлигини назорат килиш воситалари

Ахборот хавфсизлигига кириш

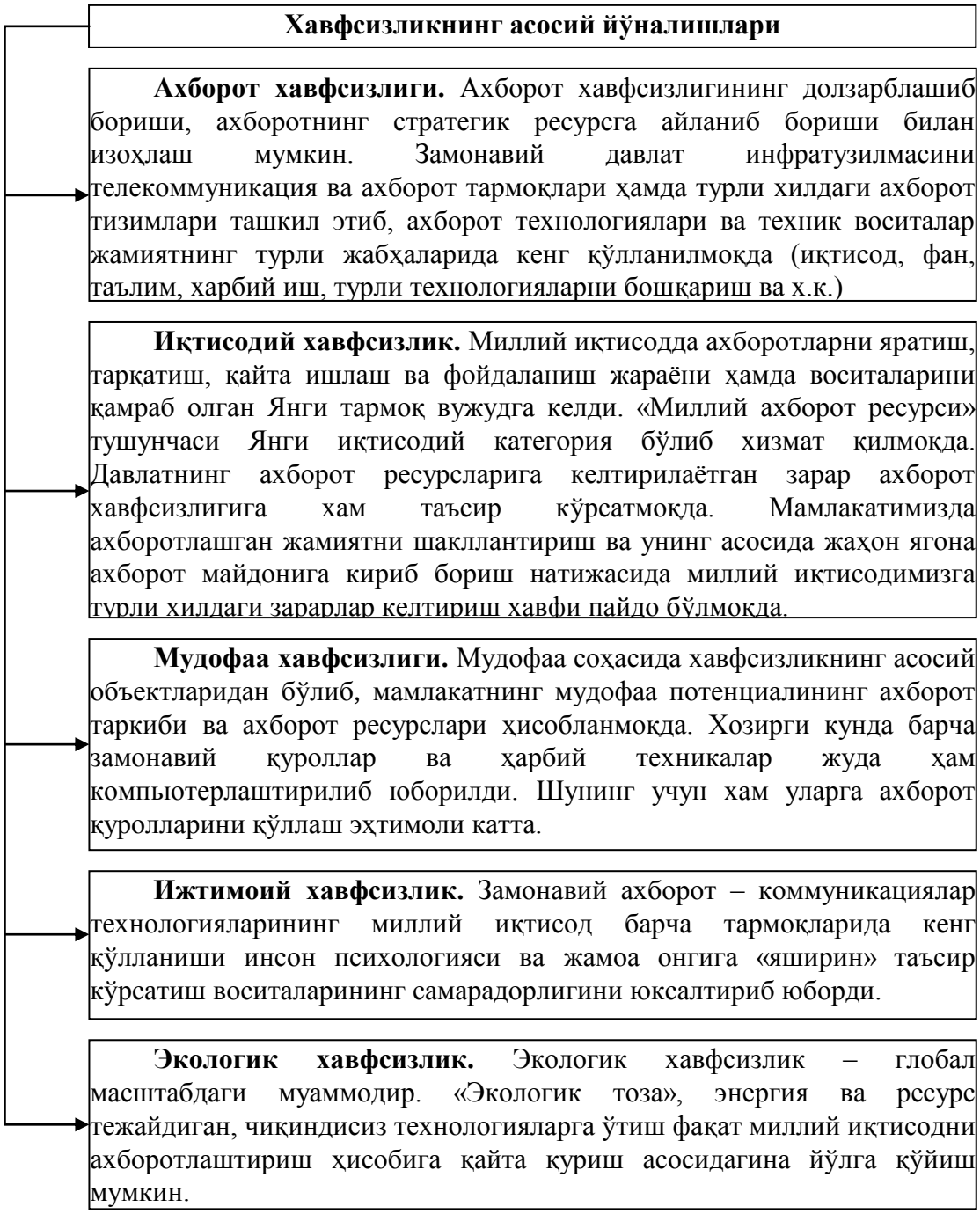
Мамлакатимиз миллий иқтисодининг ҳеч бир тармоғи самарали ва мўътадил ташкил қилинган ахборот инфратузилмасисиз фаолият кўрсатиши мумкин эмас. Ҳозирги кунда миллий ахборот ресурслари хар бир давлатнинг иқтисодий ва харбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат килмокда. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот – коммуникациялар технологияларини қўллаш кенгаяди. Турли хилдаги ахборотлар худудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга Internet ҳалқаро компьютер тармоғи орқали кириб келди. Ахборотлашган жамият шу компьютер тармоғи орқали тезлик билан шаклланиб бормокда. Ахборотлар дунёсига саёҳат қилишда давлат чегаралари деган тушунча йўқолиб бормокда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмокда, яъни давлат ахборотларнинг тарқалиши механизмини бошқара олмай қолмокда. Шунинг учун хам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Буларнинг бари шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмокда. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборот ҳимояси эса давлатнинг бирламчи масалаларига айланмокда.

Ҳозирги кунда хавфсизликнинг бир қанча йўналишларини қайд этиш мумкин. (1- расм)

Предметнинг асосий тушунчалари ва мақсади

Ахборотнинг мухимлик даражаси қадим замонлардан маълум. Шунинг учун хам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири – сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат – сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденциялари ва разведка миссияларидан ташқарига чиқмаган. Фақат бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар,

сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни ўғирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади. Ахборотни қайта ишлаш саноатининг пайдо бўлиши ахборотни ҳимоялаш саноатининг пайдо бўлишига олиб келади.



1-расм.

Автоматлаштирилтан ахборот тизимларида ахборотлар ўзининг ҳаётий даврига эга бўлади. Бу давр уни яратиш, ундан фойдаланиш ва керак бўлмаганда йўқотишдан иборатдир (2-расм).

Ахборотлар хаётий даврининг хар бир босқичида уларнинг ҳимояланганлик даражаси турлича баҳоланади.

Махфий ва қимматбаҳо ахборотларга рухсатсиз киришдан ҳимоялаш энг мухим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулки ҳуқуқларини ҳимоялаш - бу ишлаб чиқарилаётган ахборотларни жиддий иқтисодий ва бошҳа моддий ҳамда номоддий зарарлар келтириши мумкин бўлган турли киришлар ва ўғирлашлардан ҳимоялашдир.

2-расм

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва хужжатларни ўғирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компьютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир. Булардан ташқари, бу харакатлардан моддий фойда олишга интилиш ҳам ривожланди.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Ахборотнинг эгасига, фойдаланувчисига ва бошка шахсга зарар етказмокчи бўлган ноҳуқуқий муомаладан хар қандай х**ужжатлаштирилган,**

яъни идентификация қилиш имконини берувчи реквизитлари қўйилган холда моддий жисмда қайд этилган **ахборот** химояланиши керак.

Ахборот хавфсизлиги нуктаи назаридан ахборотни қуйидагича туркумлаш мумкин:

• **махфийлик** — аниқ бир ахборотга факат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши қонуний хужжатларга мувофик чеклаб қўйилиб, хужжатлаштирилганлиги кафолати. Бу банднинг бузилиши **ўғирлик** ёки **ахборотни ошкор қилиш,** дейилади;

• **конфиденциаллик** — иншончлилиги, тарқатилиши мумкин эмаслиги, махфийлиги кафолати;

• **яхлитлик** — ахборот бошланғич кўринишда эканлиги, яъни уни сақлаш ва узатишда рухсат этилмаган ўзгаришлар қилинмаганлиги кафолати; бу банднинг бузилиши **ахборотни сохталаштириш** дейилади;

• **аутентификация** — ахборот захираси эгаси деб эълон қилинган шахс хақиқатан хам ахборотнинг эгаси эканлигига бериладиган кафолат; бу банднинг бузилиши **хабар муаллифини сохталаштириш** дейилади;

• **апелляция килишлик** — етарлича мураккаб категория, лекин электрон бизнесда кенг қўлланилади. Керак бўлганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги кафолати.

Юкоридагидек, ахборот тизимига нисбатан қуйидагича таснифни келтириш мумкин:

• **ишончлилик** — тизим меьёрий ва ғайри табиий холларда режалаштирилганидек ўзини тутишлик кафолати;

• **аниқлилик** — хамма буйруқларни аниқ ва тўлиқ бажариш кафолати;

• **тизимга киришни назорат килиш —** турли шахс гурухлари ахборот манбаларига хар хил киришга эгалиги ва бундай киришга чеклашлар доим бажарилишлик кафолати;

• **назорат килиниши** — исталган пайтда дастур мажмуасининг хохлаган кисмини тулик текшириш мумкинлиги кафолати;

• **идентификациялашни назорат килиш** — хозир тизимга уланган мижоз аниқ ўзини ким деб атаган булса, аниқ ўша эканлигининг кафолати;

• **қасддан бузилишларга тўсқинлик** — олдиндан келишилган меъёрлар чегарасида қасддан хато киритилган маълумотларга нисбатан тизимнинг олдиндан келишилган холда ўзини тутиши.

Ахборотни химоялашнинг мақсадлари куйидагилардан иборат:

- ахборотнинг келишувсиз чикиб кетиши, угирланиши, йукотилиши, узгартирилиши, сохталаштирилишларнинг олдини олиш;

- шахс, жамият, давлат хавфсизлилигига булган хавф – хатарнинг олдини олиш;

- ахборотни йук килиш, узгартириш, сохталаштириш, нусха кучириш, тусиклаш буйича рухсат этилмаган харакатларнинг олдини олиш;

- хужжатлаштирилган ахборотнинг микдори сифатида хукукий тартибини таъминловчи, ахборот захираси ва ахборот тизимига хар кандай ноконуний аралашувларнинг куринишларининг олдини олиш;

- ахборот тизимида мавжуд булган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сакловчи фукароларнинг конституцион хукукларини химоялаш;

- давлат сирини, конунчиликка мос хужжатлаштирилган ахборотнинг конфиденциаллигини саклаш;

- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чикиш ва куллашда субъектларнинг хукукларини таъминлаш.

Ахборотларга нисбатан хавф-хатарлар таснифи

Илмий ва Амалий текширишлар натижаларини умумлаштириш натижасида ахборотларга нисбатан хавф хатарларни куйидагича таснифлаш мумкин.

Хавфсизлик сиёсатининг энг асосий вазифаларидан бири химоя тизимида потенциал хавфли жойларни кидириб топиш ва уларни бартараф этиш хисобланади.

Текширишлар шуни курсатадики, тармокдаги энг катта хавфлар — бу рухсатсиз киришга мулжалланган махсус дастурлар, компьютер вируслари ва дастурнинг ичига жойлаштирилган махсус кодлар булиб, улар компьютер тармокларининг барча объектлари учун катта хавф тугдиради.

Тармок хавфсизлигини назорат килиш воситалари

Замонавий ахборот - коммуникациялар технологияларининг ютуклари химоя услубларининг бир катор зарурий инструментал воситаларини яратиш имконини берди.

Ахборотларни химояловчи инструментал воситалар деганда дастурлаш, дастурий - аппаратли ва аппаратли воситалар тушунилади. Уларнинг функционал тулдирилиши хавфсизлик хизматлари олдига куйилган ахборотларни химоялаш масалаларини ечишда самаралидир. Хозирги кунда тармок хавфсизлигини назорат килиш техник воситаларининг жуда кенг спектри ишлаб чикарилган.

2 – МАВЗУ: АВТОМАТЛАШТИРИЛГАН АХБОРОТ ТИЗИМЛАРИДА МАЪЛУМОТЛАРГА НИСБАТАН ХАВФЛАР

1. Автоматлаштирилган ахборот тизимларида химоялаш зарурияти;

2. Ахборотни химоялаш тизими;

3. Ташкилотлардаги ахборотларни химоялаш;

4. Химоялаш тизимининг комплекслилиги;

5. Ахборотларни ташкилий ҳимоялаш элементлари;

6. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар.

Автоматлаштирилган ахборот тизимларида химоялаш зарурияти

Ахборот - коммуникациялар технологияларининг оммавий равишда когозсиз автоматлаштирилган асосда бошкарилиши сабабли ахборот хавфсизлигини таъминлаш мураккаблашиб ва мухимлашиб бормокда. Шунинг учун хам автоматлаштирилган ахборот тизимларида ахборотни химоялашнинг янги замонавий технологияси пайдо булмокда. DataQuest компаниясининг маълумотига кура, 1996—2000 йилларда ахборот химояси воситаларининг сотувдаги хажми 13 млрд. АКШ долларига тенг булган.

Ахборотни химоялаш тизими

Ахборотнинг заиф томонларини камайтирувчи ахборотга рухсат этилмаган киришга, унинг чикиб кетишига ва йукатилишига тускинлик килувчи ташкилий, техник, дастурий, технологик ва бошка восита, усул ва чораларнинг комплекси — **ахборотни химоялаш тизими** дейилади.

Ахборот эгалари хамда ваколатли давлат органлари шахсан ахборотнинг кимматлилиги, унинг йукотилишидан келадиган зарар ва химоялаш механизмининг нархидан келиб чиккан холда ахборотни химоялашнинг зарурий даражаси хамда тизимнинг турини, химоялаш усуллар ва воситаларини аниклашлари зарур. Ахборотнинг кимматлилиги ва талаб килинадиган химоянинг ишончлилиги бир-бири билан бевосита боглик.

Химоялаш тизими узлуксиз, режали, марказлаштирилган, максадли, аник, ишончли, комплексли, осон мукаммаллаштириладиган ва куриниши

тез узгартириладиган булиши керак. У одатда барча экстремал шароитларда самарали булиши зарур.

Ташкилотлардаги ахборотларни химоялаш

Ахборот хажми кичик булган ташкилотларда ахборотларни химоялашда оддий усулларни куллаш максадга мувофик ва самаралидир. Масалан, укиладиган кимматбохо когозларни ва электрон хужжатларни алохида гурухларга ажратиш ва никоблаш, ушбу хужжатлар билан ишлайдиган ходимни тайинлаш ва ургатиш, бинони куриклашни ташкил этиш, хизматчиларга кимматли ахборотларни таркатмаслик мажбуриятини юклаш, ташкаридан келувчилар устидан назорат килиш, компьютерни химоялашнинг энг оддий усулларини куллаш ва хоказо. Одатда, химоялашнинг энг оддий усулларини куллаш сезиларли самара беради.

Мураккаб таркибли, куп сонли автоматлаштирилган ахборот тизими ва ахборот хажми катга булган ташкилотларда ахборотни химоялаш учун химоялашнинг мажмуали тизими ташкил килинади. Лекин ушбу усул хамда химоялашнинг оддий усуллари хизматчиларнинг ишига хаддан ташкари халакит бермаслиги керак.

Химоялаш тизимининг комплекслилиги

Ҳимоя тизимининг комплекслилигига унда хукукий, ташкилий, муҳандис – техник ва дастурий – математик элементларнинг мавжудлиги билан эришилади. Элементлар нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни ҳимоялаш тизимининг ўзига хослигини ва унинг такрорланмаслигини ҳамда бузиш қийинлигини таъминлайди.

Аниқ тизимни кўп турли элементлардан иборат, деб тасаввур қилиш мумкин. Тизим элементларининг мазмуни нафақат унинг узига хослигини, балки ахборотнинг қимматлилигини ва тизимнинг қийматини ҳисобга олган ҳолда белгиланган ҳимоя даражасини аниқлайди.

Ахборотни ҳуқуқий ҳимоялаш элементи ҳимоялаш чораларининг ҳақли эканлиги маъносида ташкилот ва давлатларнинг узаро муносабатларини юридик мустаҳкамлаш хамла персоналнинг ташкилот қимматли ахборотини ҳимоялаш тартибига риоя қилиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур қилинади.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характерига эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошка барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади. Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50—60 % ни ташкил қилади. Бу ҳол кўп омилларга боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда

химоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ургатиш ҳисобланади.

Ахбортларни ҳимоялашнинг ташкилий чора – тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида уз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг ягана номи — ахборотни ташкилий - ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис – техиик ҳимоялаш элементи — техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни қуриқлашни ташкил қилиш ҳамда техник текшириш воситаларига карши суст ва фаол кураш учун мулжалланган. Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий – математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

Компьютер тизими (тармоги)га зиён етказиши мумкин бўлган шароит, харакат ва жараёнлар **компьютер тизими (тармоги)** учун хавф - хатарлар, деб ҳисобланади.

Автоматлаштирилган ахборот тизимларига тасодифий таъсир курсатиш сабаблари таркибига куйидагилар киради.

Маълумки, компьютер тизим (тармоғ)ининг асосий компонентлари — техник воситалари, дастурий - математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тўрт турдаги хавфлар мавжуд, яъни **узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш:**

— узилиш — қандайдир ташқи ҳаракатлар (ишлар, жараёнлар)ни бажариш учун ҳозирги ишларни вақтинча марказий процессор қурилмаси ёрдамида тухтатишдир, уларни бажаргандан сўнг процессор олдинги ҳолатга қайтади ва тўхтатиб қуйилган ишни давом эттиради. Ҳар бир узилиш тартиб рақамига эга, унга асосан марказий процессор қурилмаси қайта ишлаш учун қисм – дастурни қидириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник. Бирор қурилма фавқулодда хизмат кўрсатилишига муҳтож бўлса, унда техник

узилишлар пайдо бўлади. Одатда бундай узилиш марказий процессор учун кутилмаган ҳодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйруқлари ёрдамида бажарилади. Дастурий узилишда дастур ўз – ўзини вактинча тўхтатиб, узилишга тааллуқли жараённи бажаради.

— тутиб олиш — жараёни оқибатида ғаразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни қулга киритади. Дастур ва маълумотлардан ноқонуний нусха олиш, компьютер тармоклари алоқа каналларидан номуаллифлик ўқишлар ва ҳоказо ҳаракатлар тутиб олиш жараёнларига мисол бўла олади.

— ўзгартириш — ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тупламлари, дастурлар, техник элементлари) киришни қулга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам килади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман копьютер тизими файлларини ўзгартириши, ёки кандайдир қўшимча ноқонуний кайта ишлашни амалга ошириш максадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилали;

— сохталаштириш — хам жараён саналиб, унинг ёрдамида ғаразли шахслар тизимда ҳисобга олинмаган вазиятларни ўрганиб, ундаги камчиликларни аниклаб, кейинчалик ўзига керакли ҳаракатларни бажариш мақсадида тизимга қандайдир сохта жараённи ёки тизим ва бошқа фойдаланувчиларга сохта ёзувларни юборади.

3 – МАВЗУ: ВИРУС ВА АНТИВИРУСЛАР ТАСНИФИ

1. Вирус ва унинг турлари;

2. Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш;

3. Антивирус дастурлари;

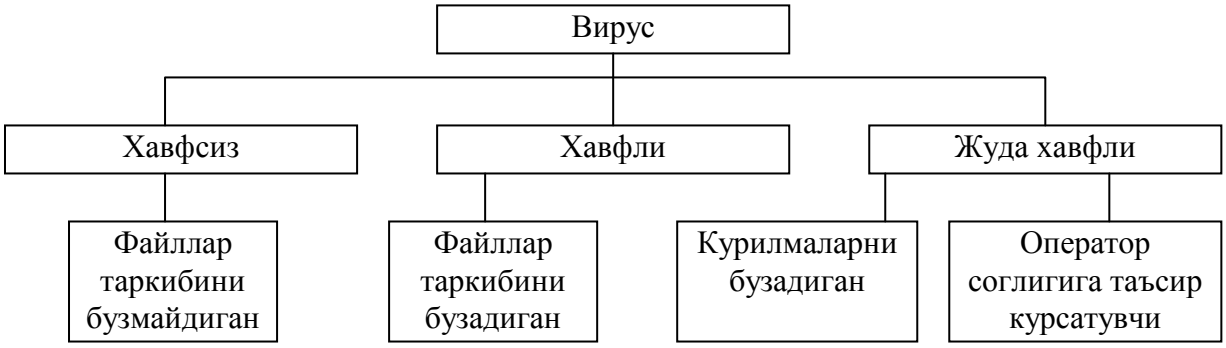
4. Вирусларга қарши чора-тадбирлар.

Вирус ва унинг турлари

Ҳозирги кунда компьютер вируслари ғаразли мақсадларда ишлатилувчи турли хил дастурларни олиб келиб татбиқ этишда энг самарали воситалардан бири ҳисобланади. Компьютер вирусларини **дастурли вируслар** деб аташ тугрироқ бўлади.

Дастурли вирус деб автоном равишда ишлаш, бошқа дастур таркибига ўз – ўзидан қушилувчи, ишга кодир ва компьютер тармоқлари ва алоҳида компьютерларда уз – узидан таркалиш хусусиятига эга булган дастурга айтилади.

Вируслар билан зарарланган дастурлар **вирус ташувчи** ёки **зарарланган дастурлар** дейилади.



Зарарланган диск – бу ишга тушириш секторида вирус дастур жойлашиб олган дискдир.

Хозирги пайтда компьютерлар учун купгина нокулайликлар тугдираётган хар хил турлардаги компьютер вируслари кенг таркалган. Шунинг учун хам улардан сакланиш усулларини ишлаб чикиш мухим масалалардан бири хисобланади. Хозирги вактда 65000 дан куп булган вирус дастурлари борлиги аникланган. Бу вирусларнинг катта гурухини компъютернинг иш бажариш тартибини бузмайдиган, яъни «таъсирчан булмаган» вируслар гурухи ташкил этадиди.

Вирусларнинг бошка гурухига компьютернинг иш тартибини бузувчи вируслар киради. Бу вирусларни куйидаги турларга булиш мумкин: **хавфсиз вируслар** (файллар таркибини бузмайдиган), **хавфли вируслар** (файллар таркибини бузувчи) хамда **жуда хавфли вируслар** (компьютер курилмаларини бузувчи ва оператор соглигига таъсир этувчи). Бу каби вируслар одатда профессионал дастурчилар томонидан тузилади.

Компьютер вируси – бу махсус ёзилган дастур булиб, бошка дастурлар таркибига ёзилади, яъни зарарлайди ва компьютерларда узининг гаразли максадларини амалга оширади.

Компьютер вируси оркали зарарланиш окибатида компьютерларда куйидаги узгаришлар пайдо булади:

• айрим дастурлар ишламайди ёки хато ишлай бошлайди;

• бажарилувчи файлнинг хажми ва унинг яратилган вакти узгаради;

• экранда англаб булмайдиган белгилар, турли хил тасвир ва товушлар пайдо булади;

• компьютернинг ишлаши секинлашади ва тезкор хотирадаги буш жой хажми камаяди;

• диск ёки дискдаги бир неча файллар зарарланади (баъзи холларда диск ва файлларни тиклаб булмайди):

• винчестер оркали компьютернинг ишга тушиши йуколади.

Вируслар асосан дискларнинг юкланувчи секторларини ва exe, com, sys ва bat кенгайтмали файлларни зараралайди. Хозирги кунда булар каторига офис дастурлари яратадиган файларни хам киритиш мумкин. Оддий матнли файлларни зараралайдиган вируслар камдан – кам учрайди.

Файллар таркибини бузмайдиган вируслар

Тезкор хотира курилмасида купаювчи	Операторни таъсирлантирувчи	Тармок вируслари

Операторни таъсирлантирувчи			
Курилмаларни ишдан чикарувчи	**Терминалда хабар чикарувчи**	**Товушли эффектларни хосил килувчи**	**Иш тартибини узгартирувчи**
- процессор			- клавиатура
- хотира	- матнли	- оханг	
- МД, винчестер			- дисплей
- принтер	- графикли	- нутк синтези	
- порт PS-232			принтер
Дисплей		- махсус эффектлар	
- клавиатура			- порт PS-232

Компьютернинг вируслар билан зарарланиш йуллари куйидагилардир:
1. Дискетлар оркали.
2. Компьютер тармоклари оркали.
3. Бошка йуллар йук.

Файл таркибини бузувчи вируслар

Фойдаланувчининг маълумотлари ва дастурларни бузувчи		Тизим маълумотларини бузувчи		
Дастурларни бузувчи	Маълумотларни бузувчи	Диск сохасини бузувчи	Форматлаш	Тезкор тизим файлларини бузувчи
Дастурнинг бошлангич ёзувларини бузувчи	Маълумотлар базаларини бузувчи	Дискнинг мантикий таркибини бузиш		
Бажарилувчи дастурларни бузувчи	Матнли хужжатларни бузувчи	Маълумот ташувчиларнинг таркибини бузувчи		
Компиляторларнинг кисм дастурлар тупламини бузувчи	График тасвирларни бузувчи			
	Электрон жадвални бузувчи			

Оператор ва курилмаларга таъсир этувчи вируслар

Курилмаларни бузувчи			Операторга таъсир этувчи	
Дисплейнинг Люминафор катламини куйдирувчи	Компьютерларнинг микросхемасини ишдан чикарувчи	Принтерни ишдан чикарувчи	МДни бузувчи	Оператор техникасига таъсир этувчи

Хозирги пайтда хазил шаклидаги вируслардан тортиб то компьютер курилмаларини ишдан чикарувчи вирусларнинг турлари мавжуд.

Масалан. Win 95.CIH вируси доимий саклаш курилмаси (Flash BIOS) микросхемасини бузади. Афсуски, бу каби вирусларни йук килиш учун, факат улар уз гаразли ишини бажариб булгандан сунггина, карши чоралар ишлаб чикилади. Win 95.CIH вирусига карши чораларни куриш имконияти Dr.Web дастурида мавжуд.

Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш

Шуни айтиб утиш лозимки, хозирги пайтда хар-хил турдаги ахборот ва дастурларни угирлаб олиш ниятида компьютер вирусларидан фойдаланиш энг самарали усуллардан бири хисобланади.

Дастурли вируслар компьютер тизимларининг хавфсизлигига тахдид солишнинг энг самарали воситаларидан биридир. Шунинг учун хам дастурли вирусларнинг имкониятларини тахлил килиш масаласи хамда бу вирусларга карши курашиш хозирги пайтнинг долзарб масалаларидан бири булиб колди.

Вируслардан ташкари файллар таркибини бузувчи **троян дастурлари** мавжуд. Вирус купинча компьютерга сездирмасдан киради. Фойдаланувчининт узи троян дастурини фойдали дастур сифатида дискка ёзади. Маълум бир вакт утгандан кейин бузгунчи дастур уз таъсирини курсатади.

Уз-узидан пайдо буладиган вируслар мавжуд эмас. Вирус дастурлари инсон томонидан компьютернинг дастурий таъминотини, унинг курилмаларини зараралаш ва бошка максадлар учун ёзилади. Вирусларнинг хажми бир неча байтдан то унлаб килобайтгача булиши мумкин.

Троян дастурлари фойдаланувчига зарар келтирувчи булиб, улар буйруклар (модуллар) кетма – кетлигидан ташкил топган, омма орасида жуда кенг таркалган дастурлар (тахрирловчилар, ўйинлар, трансляторлар) ичига ўрнатилган бўлиб, бир қанча ҳодисалар бажарилиши билан ишга тушадиган «мантиқий бомба» деб аталадиган дастурдир. Ўз навбатида, «мантикий бомба»нинг турли кўринишларидан бири «соат механизмли бомба» ҳисобланади.

Шуни таъкидлаб ўтиш керакки, троян дастурлари ўз-ўзидан кўпаймасдан, компьютер тизими бўйича дастурловчилар томонидан тарқатилади.

Троян дастурлардан вирусларнинг фарқи шундаки, вируслар компьютер тизимлари буйлаб таркатилганда, улар мустақил равишда ҳосил бўлиб, ўз иш фаолиятида дастурларга ўз матнларини ёзган ҳолда уларга зарар кўрсатади.

Зарарланган дастурда дастур бажарилмасдан олдин вирус ўзининг буйруқлари бажарилишига имконият яратиб беради. Бунинг учун хам вирус дастурнинг бош қисмида жойлашади ёки дастурнинг биринчи буйруги унга ёзилган вирус дастурига шартсиз ўтиш бўлиб хизмат қилади. Бошқарилган вирус бошқа дастурларни зарарлайди ва шундан сўнг вирус ташувчи дастурга ишни топширади.

Вирус ҳаёти одатда қуйидаги даврларни ўз ичига олади: **қулланилиш, инкубация, репликация** (ўз-ўзидан кўпайиш) ва **ҳосил бўлиш.** Инкубация даврида вирус пассив бўлиб, уни излаб топиш ва йукотиш кийин. Ҳосил булиш даврида у ўз функциясини бажаради ва қўйилган мақсадига эришади.

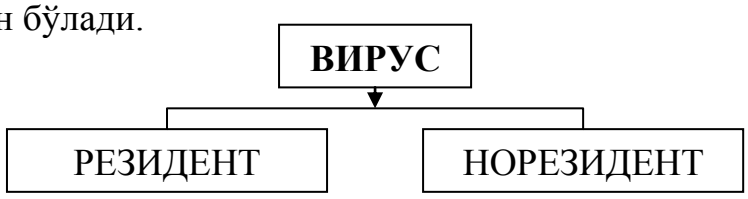
Таркиби жиҳатидан вирус жуда оддий бўлиб, бош қисм ва баьзи ҳолларда думдан иборат. Вируснинг бош қисми деб бошкарилишини биринчи бўлиб таъминловчи имкониятга эга бўлган дастурга айтилади. Вируснинг дум қисми зарарланган дастурда бўлиб, у бош кисмидан алоҳида жойда жойлашади.

Компьютер вируслари характерларига нисбатан **норезидент, резидент, бутли, гибридли ва пакетли вирусла**рга ажратилади.

Файлли **норезидент вируслар** тўлиқлигича бажарилаётган файлда жойлашади, шунинг учун ҳам у фақат вирус ташувчи дастур фаоллашгандан сўнг ишга тушади ва бажарилгандан сўнг тезкор хотирада сақланмайди.

Резидент вирус норезидент вирусдан фарқлироқ тезкор хотирада сақланади.

Резидент вирусларнинг яна бир кўриниши **бут вируслар** бўлиб, бу вируснинг вазифаси винчестер ва эгилувчан магнитли дискларнинг юкловчи секторини ишдан чиқаришдан иборат. Бут вирусларнинг боши дискнинг юкловчи бут секторида ва думи дискларнинг ихтиёрий бошка секторларида жойлашган бўлади.



Пакетли вируснинг бош қисми пакетли файлда жойлашган бўлиб, у операцион тизим топшириқларидан иборат.

Гибридли вирусларнинг боши пакетли файлда жойлашади. Бу вирус хам файлли, ҳам бут секторли бўлади.

Тармоқли вируслар компьютер тармокларида тарқалишга мослаштирилган, яъни тармоқли вируслар деб ахборот алмашишда тарқаладиган вирусларга айтилади.

Вирусларнинг турлари:

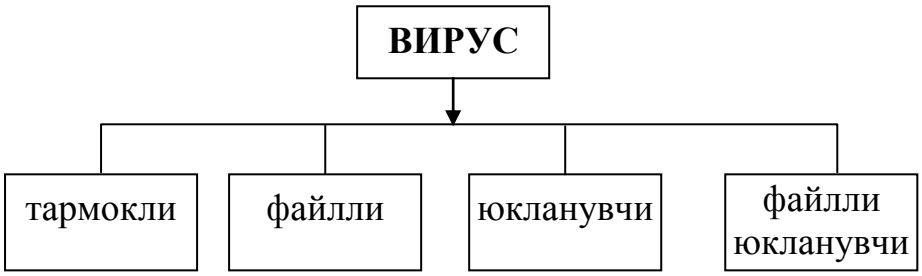
1) **файл вируслари.** Бу вируслар *сом, exe* каби турли файлларни зарарлайди;

2) **юкловчи вируслар.** Компьютерни юкловчи дастурларни зарарлайди;

3) **драйверларни зарарловчи вируслар.** Операцион тизимдаги config.sys файлни зарарлайди. Бу компьютернинг ишламаслигига сабаб бўлади;

4) **DIR вируслари.** FAT таркибини зарарлайди;

5) **стелс-вируслари.** Бу вируслар ўзининг таркибини узгартириб, тасодифий код ўзгариши бўйича тарқалади. Уни аниклаш жуда қийин, чунки файлларнинг ўзлари ўзгармайди;



6) **Windows вируслари.** Windows операцион тизимидаги дастурларни зарарлайди.

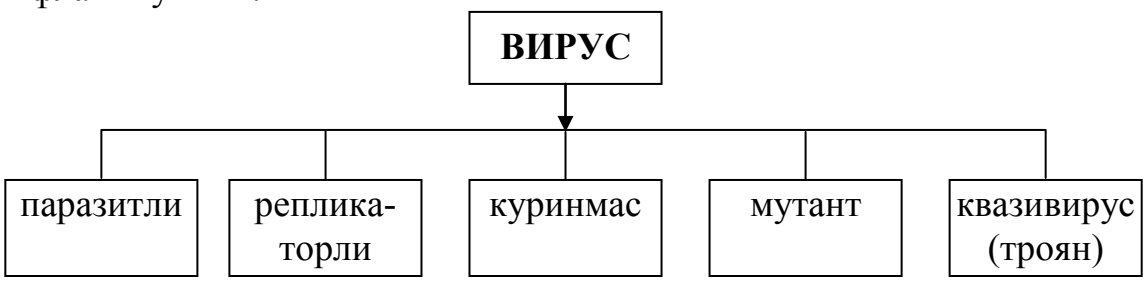
Мисол сифатида қуйидагиларни келтириш мумкин:

1) Энг хавфли вируслардан бири Internet орқали тарқатилган «Чернобиль» вируси бўлиб, у 26 апрелда таркатилган ва ҳар ойнинг 26-кунида компъютерларни зарарлаши мумкин.

2) I LOVE YOU вируси Филиппиндан 2000 йил 4 майда E-mail оркали тарқатилган. У бугун жаҳон буйича 45 млн. компьютерни зарарлаган ва ишдан чикарган. Моддий зарар 10 млрд. АҚШ долларини ташкил килган.

3) 2003 йил март ойида Швециядан злектрон почта оркали GANDA вируси тарқатилган ва у бутун дунёда минглаб компьютерларни зарарлаган. Бу вирусни тарқатган шахс ҳозир қулга олинган ва у 4 йил камоқ жазосига ҳукм этилиши мумкин.

Асосланган алгоритмлар буйича дастурли вирусларни куйидагича таснифлаш мумкин.



Паразитли вирус — файлларнинг таркибини ва дискнинг секторини узгартирувчи вирус. Бу вирус оддий вируслар туркумидан бўлиб, осонлик билан аниқланади ва ўчириб ташланади.

Репликаторли вирус — «чувалчанг» деб номланади, компьютер тармоқлари бўйича тарқалиб, комльютерларнинг тармоқдаги манзилини аниқлайди ва у ерда ўзининг нусхасини қолдиради.

Куринмас вирус — стелс-вирус деб ном олиб, зарарланган файлларга ва секторларга операцион тизим томонидан мурожаат қилинса, автоматик равишда зарарланган қисмлар ўрнига дискнинг тоза қисмини тақдим этади. Натижада ушбу вирусларни аниқлаш ва тозалаш жуда катта қийинчиликларга олиб келади.

Мутант вирус — шифрлаш ва дешифрлаш алгоритмларидан иборат бўлиб, натижада вирус нусхалари умуман бир-бирига ўхшамайди. Ушбу вирусларни аниқлаш жуда қийин муаммо.

Квазивирус вирус — «Троян» дастурлари, деб ном олган бўлиб, ушбу вируслар кўпайиш хусусиятига эга бўлмаса-да, «фойдали» қисм-дастур хисобида бўлиб, антивирус дастурлар томонидан аниқланмайди. Шу боис ҳам улар ўзларида мукаммаллаштирилган алгоритмларни тўсиқсиз бажариб, қўйилган мақсадларига эришишлари мумкин.

Антивирус дастурлари

Ҳозирги вақтда вирусларни йўқотиш учун кўпгина усуллар ишлаб чиқилган ва бу усуллар билан ишлайдиган дастурларни **антивируслар** деб аташади. Антивирусларни, кулланиш усулига кўра, қуйидагиларга ажратишимиз мумкин: ***детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар.***

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги хисобланади.

Фаглар — ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги холатига кайтаради.

Вакциналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга урнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис хам, ушбу антивирус дастурлари кенг тарқалмаган.

Прививка — файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди.

Фильтрлар — қуриқловчи дастурлар куринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради.

Ревизорлар — энг ишончли ҳимояловчи восита бўлиб, дискнинг биринчи ҳолатини хотирасида сақлаб, ундаги кейинги ўзгаришларни доимий равишда назорат қилиб боради.

Детектор дастурлар компьютер хотирасидан, файллардан вирусларни қидиради ва аниқланган вируслар хақида хабар беради.

Доктор дастурлари нафақат вирус билан касалланган файлларни топади, балки уларни даволаб, дастлабки ҳолатига қайтаради. Бундай дастурларга Aidstest, Doctor Web дастурларини мисол килиб келтириш мумкин. Янги вирусларнинг тўхтовсиз пайдо бўлиб туришини ҳисобга олиб, доктор дастурларини ҳам янги версиялари билан алмаштириб туриш лозим.

Фильтр дастурлар компьютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Бу харакатлар куйидагича бўлиши мумкин:

- файллар атрибутларининг ўзгариши;
- дискларга доимий манзилларда маълумотларни ёзиш;
- дискнинг ишга юкловчи секторларига маълумотларни ёзиб юбориш.

Текширувчи (ревизор) дастурлари вирусдан химояланишнинг энг ишончли воситаси бўлиб, компьютер зарарланмаган ҳолатидаги дастурлар, каталоглар ва дискнинг тизим майдони ҳолатини хотирада саклаб, доимий равишда ёки фойдаланувчи ихтиёри билан компьютернинг жорий ва бошлангач ҳолатларини бир-бири билан солиштиради. Бунга ADINF дастурини мисол қилиб келтириш мумкин.

Вирусларга қарши чора-тадбирлар

Компьютерни вируслар билан зарарланишидан саклаш ва ахборотларни ишончли сақлаш учун қуйидаги қоидаларга амал қилиш лозим:

- компьютерни замонавий антивирус дастурлар билан таъминлаш;
- дискеталарни ишлатишдан олдин ҳар доим вирусга қарши текшириш;
- қимматли ахборотларнинг нусхасини ҳар доим архив файл кўринишида сақлаш.

Компьютер вирусларига карши курашнинг қуйидаги турлари мавжуд:

- вируслар компьютерга кириб бузган файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компьютерга пароль билан кириш, диск юритувчиларнинг ёпиқ туриши;
- дискларни ёзишдан химоялаш;
- лицензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- компьютерга кириталаётган дастурларнинг вирусларнинг мавжудлигини текшириш;
- антивирус дастурларидан кенг фойдаланиш;

- даврий равишда компьютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Антивирус дастурларидан DrWeb, Adinf, AVP, BootCHK ва Norton Antivirus, Kaspersky Security кабилар кенг фойлаланилади.

4 – МАВЗУ: АХБОРОТЛАРНИ СТЕНОГРАФИК ХИМОЯЛАШ УСУЛЛАРИ

1. Замонавий компьютер стенографияси;
2. Компьютер стенографияси истикболлари;
3. Компьютер стенографиясининг асосий вазифалари;
4. Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш.

Замонавий компьютер стенографияси

Рухсат этилмаган киришдан ахборотни ишончли ҳимоялаш муаммоси энг илгаритдан мавжуд ва ҳозирги вақтгача ҳал қилинмаган. Махфий хабарларни яшириш усуллари қадимдан маълум, инсон фаолиятининг бу соҳаси **стенография** деган ном олган. Бу сўз грекча **Steganos** (махфий, сир) ва **Graphy** (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стенография усуллари, эҳтимол, ёзув пайдо бўлишидан олдин пайдо бўлган (дастлаб шартли белги ва белгилашлар қулланилган) бўлиши мумкин.

Ахборотни ҳимоялаш учун **кодлаштириш** ва **криптография** усуллари қўлланилади.

Кодлаштириш деб ахборотни бир тизимдан бошка тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни маьлумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тусиқ қуйиш усулига айтилади.

Стенографиянинг кринтографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни химоялаш самарадорлигини ошириш учун ишлатилиши имкони пайдо бўлади (масалан, криптографик калитларни узатиш учун).

Компьютер технологиялари стенографиянинг ривожланиши ва мукаммаллашувига янги туртки берди. Натижада ахборотни ҳимоялаш соҳасида янги йўналиш — **компьютер стеногряфия**си пайдо бўлди.

Глобал компьютер тармоқлари ва мультимедиа сохасидаги замонавий прогресс телекоммуникация каналларида маълумотларни узатиш хавфсизлигини таъминлаш учун мўлжалланган янги усулларни яратишга олиб келди. Бу усуллар шифрлаш қурилмаларининг табиий ноаниқлигидан ва аналогли видео ёки аудиосигналларнинг сероблигидан фойдаланиб

хабарларни компьютер файллари (контейнерлар)да яшириш имконини беради. Шу билан бирга криптографиядан фарқли равишда бу усуллар ахборотни узатиш фактининг ўзини ҳам яширади.

К.Шеннон сирли ёзувнинг умумий назариясини яратдики, у фан сифатида стенографиянинг базаси ҳисобланади. Замонавий компьютер стеганографиясида иккита асосий файл турлари мавжуд: яшириш учун мўлжалланган **хабар-файл**, ва **контейнер-файл**, у хабарни яшириш учун ишлатилиши мумкин. Бунда контейнерлар икки турда бўлади: **контейнер-оригинал** (ёки «бўш» контейнер) - бу контейнер яширин ахборотни сақламайди; **контейнер-натижа** (ёки «тулдирилган» контейнер) — бу контейнер яширин ахборотни сақлайди. **Калит** сифатида хабарни контейнерга киритиб куйиш тартибини аниклайдиган махфий элемент тушунилади.

Компьютер стенографияси истикболлари

Компьютер стенографияси ривожланиши тенденциясининг таҳлили шуни кўрсатадики, кейинги йилларда компьютер стенографияси усулларини ривожлантиришга қизиқиш кучайиб бормоқда. Жумладан, маълумки, ахборот хавфсизлиги муаммосининг долзарблиги доим кучайиб бормоқда ва ахборотни ҳимоялашнинг янги усулларини қидиришга рағбатлантирилаяпти. Бошка томондан, ахборот-коммуникациялар технологияларининг жадал ривожланиши ушбу ахборотни химоялашнинг янги усулларини жорий қилиш имкониятлари билан таъминлаяпти ва албатта, бу жараённинг кучли катализатори бўлиб умумфойдаланиладиган Internet компьютер тармогининг жуда кучли ривожланиши ҳисобланади.

Ҳозирги вақтда ахборотни ҳимоялаш энг кўп қулланилаётган соха бу — криптографик усуллардир. Лекин, бу йўлда компьютер вируслари, «мантиқий бомба»лар каби ахборотий қуролларнинг криптовоситаларни бузадиган таъсирига боғлиқ кўп ечилмаган муаммолар мавжуд. Бошка томондан, криптографик усулларни ишлатишда калитларни тақсимлаш муаммоси ҳам бугунги кунда охиригача ечилмай турибди. Компьютер стеганографияси ва криптографияларининг бирлаштирилиши пайдо бўлган шароитдан қутулишнинг яхши бир йўли булар эди, чунки, бу ҳолда ахборотни ҳимоялаш усулларининг заиф томонларини йўқотиш мумкин.

Шундай қилиб, компьютер стенографияси ҳозирги кунда ахборот хавфсизлиги бўйича асосий технологиялардан бири бўлиб ҳисобланади.

Компьютер стенографиясининг асосий вазифалари

Замонавий компьютер стенографиясининг асосий ҳолатлари қуйидагилардан иборат:

- яшириш усуллари файлнинг аутентификацияланишлигини ва яхлитлигини таъминлаши керак;
- ёвуз ниятли шахсларга қўлланилувчи стеганография усуллари тўлиқ маьлум деб фараз қилинади;

• усулларнинг ахборотга нисбатан хавфсизликни таъминлаши очик узаталадиган файлнинг асосий хоссаларини стенографик алмаштиришлар билан сақлашга ва бошқа шахсларга номаълум бўлган қандайдир ахборот — калитга асосланади;

• агар ёвуз ниятли шахсларга хабарни очиш вақти маълум бўлиб қолган бўлса, махфий хабарнинг ўзини чикариб олиш жараёни мураккаб хисоблаш масаласи сифатида тасаввур қилиниши лозим.

Internet компьютер тармоғининг ахборот манбаларини таҳлили қуйидаги хулосага келишга имкон берди, яъни ҳозирги вақтда стенографик тизимлар қуйидаги асосий масалаларни ечишда фаол ишлатилаяпти:

- конфиденциал ахборотни рухсат этилмаган киришдан ҳимоялаш;
- мониторинг ва тармоқ захираларини бошқариш тизимларини енгиш;
- дастурий таъминотни никоблаш;
- интеллектуал эгаликнинг баъзи бир турларида муаллифлик ҳуқуқларини ҳимоялаш.

Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш

Бу компьютер стеганографиясини ишлатиш соҳаси конфиденциал ахборотларни ҳимоялаш муаммосини ечишда энг самарали ҳисобланади. Масалан, товушнинг энг кам аҳамиятли кичик разрядлари яшириладиган хабарга алмаштирилади. Бундай узгариш купчилик томонидан товушли хабарни эшитиш пайтида сезилмайди.

Мониторинг ва тармок захираларини бошқариш тизимларини енгиш

Саноат шпионлик тизимларининг мониторинг ва тармоқ захираларини бошқариш ҳаракатларига қарши йўналтирилган стенографик усуллар локал ва глобал компьютер тармоклари серверларидан ахборотнинг ўтишида назорат ўрнатиш харакатларига карши туришга имкон беради.

Дастурий таъминотни никоблаш

Компьютер стеганографиясининг хозирги вақтда ишлатиладиган бошка бир соҳаси дастурий таъминотни ниқоблашдир. Қачонки, дастурий таъминотни кайд қилинмаган фойдаланувчилар томонидан ишлатилиши ўринсиз бўлса, у стандарт универсал дастур маҳсулотлари (масалан, матнли мухаррирлар) остида ниқобланиши ёки мультимедиа файллари (масалан, компьютер ўйинларининг мусиқий иловаси)га яширилиши мумкин.

Муаллифлик ҳуқуқларини ҳимоялаш

Стенографиядан фойдаланиладиган яна бир соҳалардан бири — бу муаллифлик ҳуқуқларини ҳимоялаш ҳисобланади. Компьютерли график тасвирларга махсус белги қуйилади ва у кузга кўринмай қатади. Лекин,

махсус дастурий таъминот билан аниқланади. Бундай дастур маҳсулоти аллакачон баъзи журналларнинг компьютер версияларида ишлатилаяпти. Стенографиянинг ушбу йўналиши нафакат тасвирларни, балки аудио ва видеоахборотни ҳам қайта ишлашга мулжалланган. Бундан ташкари унинг интеллектуал эгалигини ҳимоялашни таъминлаш вазифаси ҳам мавжуд.

Ҳозирги вақтда компьютер стенографияси усуллари икки асосий йўналиш буйича ривожланмокда:

- компьютер форматларининг махсус хоссаларини ишлатишга асосланган усуллар;
- аудио ва визуал ахборотларнинг сероблилигига асосланган усуллар.

Стенографик дастурлар тўгрисида кисқача маьлумот

Windows операцион муҳитида ишловчи дастурлар:

• Steganos for Win95 дастури ишлатишда жуда енгил бўлиб, айни пайтда файлларни шифрлаш ва уларни BMP, DIB, VOC, WAV, ASCII, HTML кен-гайтмали файллар ичига жойлаштириб яширишда жуда кудратли хисобланади;

• Contraband дастури 24-битли BMP форматдаги график файллар ичида ҳар қандай файлни яшира олиш имкониятига эга.

DOS мухитида ишловчи дастурлар:

• Jsteg дастури маълумотни JPG форматли файллар ичига яшириш учун мўлжалланган;

• FFEncode дастури маълумотларни матнли файллар ичида яшириш имкониятига эга;

• StegoDOS дастурлар пакетининг ахборотни тасвирда яшириш имконияти мавжуд;

• Winstorm дастурлар пакети PCX форматли файллар ичига хабарни шифрлаб яширади.

OS/2 операцион муҳитида ишловчи дастурлар:

- Texto дастури маълумотларни инглиз тилидаги матнга айлантиради;

- Hide4PGP v1.1 дастури BMP, WAV, VOC форматли файллар ичига маьлумотларни яшириш имкониятига эга.

Macintosh компьютерлари учун мўлжалланган дастурлар:

- Paranoid дастури маълумотларни шифрлаб, товушли форматли файл ичига яширади:

- Stego дастурининг PICT кенгайтмали файл ичига маълумотларни яшириш имконияти мавжуд.

5 – МАВЗУ: АХБОРОТЛАРНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

1. ***Криптография ҳақида асосий тушунчалар;***

2. ***Ахборотларни криптографияли ҳимоялаш тамойиллари;***

3. Симметрияли криптотизим асослари;
4. ***Уринларни алмаштириш усуллари;***
5. Алмаштириш усуллари.

Криптография ҳақида асосий тушунчалар

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб қуймоқ» маъносини билдирган. Биринчи марта у ёзув пайдо булган даврлардаёк айтиб ўтилган. Ҳозирги вақтда криптография деганда ҳар қандай шаклдаги, яъни дискда сақланадиган сонлар кўринишида ёки ҳисоблаш тармоқларида узатиладиган хабарлар кўринишидаги ахборотни яшириш тушунилади. Криптографияни рақамлар билан кодланиши мумкин бўлган ҳар қандай ахборотга нисбатан қўллаш мумкин. Махфийликни таъминлашга қаратилган криптография кенгроқ қўлланилиш доирасига эга. Аниқроқ айтганда, криптографияда қўлланиладиган усулларнинг ўзи ахборотни ҳимоялаш билан боғлиқ бўлган кўп жараёнларда ишлатилиши мумккн.

Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди. Масалан, тулов варакларини электрон почта оркали узатишда унинг ўзгартирилиши ёки сохта ёзувларнинг қушилиши мумкин. Бундай ҳолларда ахборотнинг яхлитлигини таъминлаш зарурияти пайдо бўлади. Умуман олганда компьютер тармогига рухсатсиз киришнинг мутлақо олдини олиш мумкин эмас, лекин уларни аниқлаш мумкин. Ахборотнинг яхлитлигини текширишнинг бундай жараёни, кўп ҳолларда, ахборотнинг ҳақиқийлигини таъминлаш дейилади. Криптографияда қўлланиладиган усуллар кўп бўлмаган ўзгартиришлар билан ахборотларнинг ҳақикийлигини таъминлаши мумкин.

Нафақат ахборотнинг компьютер тармогидан маъноси бузилмасдан келганлигини билиш, балки унинг муаллифдан келганлигига ишонч хосил қилиш жуда муҳим. Ахборотни узатувчи шахсларнинг ҳақиқийлигини тасдикловчи турли усуллар маълум. Энг универсал процедура пароллар билан алмашувдир, лекин бу жуда самарали бўлмаган процедура. Чунки паролни қулига киритган ҳар қандай шахс ахборотдан фойдаланиши мумкин бўлади. Агар эҳтиёткорлик чораларига риоя қилинса, у ҳолда парольларнинг самарадорлигини ошириш ва уларни криптографик усуллар билан ҳимоялаш мумкин, лекин криптография бундан кучлироқ паролни узлуксиз ўзгартириш имконини берадиган процедураларни ҳам таъминлайди.

Криптография соҳасидаги охирги ютуклардан бири — рақамли сигнатура — махсус хосса билан ахборотни тўлдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очиқ калит маълум бўлгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усулларан кўпроқ афзалликларга эга.

Криптография усулларини куллашнинг баъзи бирларини кўриб чикамиз. Узаталадиган ахборотнинг маъносини яшириш учун икки хил ўзгартиришлар қўлланилади: **кодлаштириш** ва **шифрлаш**.

Кодлаштириш учун тез-тез ишлатиладиган иборалар тўпламини ўз ичига олувчи китоб ёки жадваллардан фойдаланилади. Бу иборалардан ҳар бирига, кўп ҳалларда, рақамлар тўплами билан бериладиган ихтиёрий танланган кодли суз тўғри келади. Ахборотни кодлаш учун худди шундай китоб ёки жадвал талаб қилинади. Кодлаштирувчи китоб ёки жадвал ихтиёрий криптографик ўзгартиришга мисол бўлади. Кодлаштиришнинг ахборот технологиясига мос талаблар — каторли маълумотларни сонли маълумотларга айлантириш ва аксинча ўзгартиришларни бажара билиш. Кодлаштириш китобини тезкор ҳамда ташқи хотира қурилмаларида амалга ошириш мумкин, лекин бундай тез ва ишончли криптографик тизимни муваффакиятли деб булмайди. Агар бу китобдан бирор марта рухсатсиз фойдаланилса, кодларнинг янги китобини яратиш ва уни хамма фойдаланувчиларга таркатиш зарурияти пайдо бўлади.

Криптографик ўзгартиришнинг иккинчи тури **шифрлаш** ўз ичига — бошланғич матн белгиларини англаб олиш мумкин бўлмаган шаклга ўзгартириш алторитмларини камраб олади. Узгартиришларнинг бу тури ахборот-коммуникациялар технологияларига мос келади. Бу ерда алгоритмни ҳимоялаш муҳим аҳамият касб этади. Криптографик калитни қўллаб, шифрлаш алгоритмининг ўзида ҳимоялашга бўлган талабларни камайтариш мумкин. Энди ҳимоялаш объекти сифатада фақат калит хизмат қилади. Агар калитдан нусха олинган бўлса, уни алмаштириш мумкин ва бу кодлаштирувчи китоб ёки жадвални алмаштиришдан енгилдир. Шунинг учун ҳам кодлаштириш эмас, балки шифрлаш ахборот-коммуникациялар технологияларида кенг кўламда қулланилмоқда.

Сирли (махфий) алоқалар соҳаси **криптология** деб айтилади. Ушбу сўз юнонча «**kripto**» — сирли ва **«logus»** — хабар маъносини билдирувчи сўзлардан иборат. Криптология икки йўналиш, яъни **криптография** ва **криптотаҳлил**дан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ҳақиқийлигини таъминлашдан иборат.

Криптотаҳлилнинг вазифаси эса криптографлар томонидан ишлаб чиқилган ҳимоя тизимини очишдан иборат.

Ҳозирги кунда **криптотизим**ни икки синфга ажратиш мумкин:

• симметрияли бир калитлилик (махфий калитли);

• асимметрияли икки калитлилик (очиқ калитли).

Симметрияли тизимларда куйидаги иккита муаммо мавжуд:

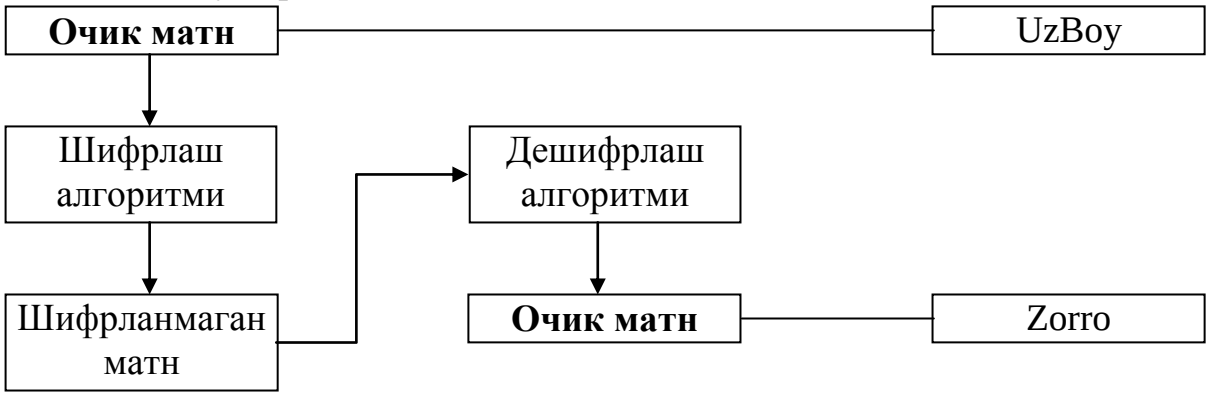
1) Ахборот алмашувида иштирок этувчилар кандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит қўлланилади. Биридан иккинчисини хисоблаш усуллари билан аниқлаб бўлмайди.

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



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қуллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо булади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

• фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниклаш:

• тармок абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентнфикациялаш.

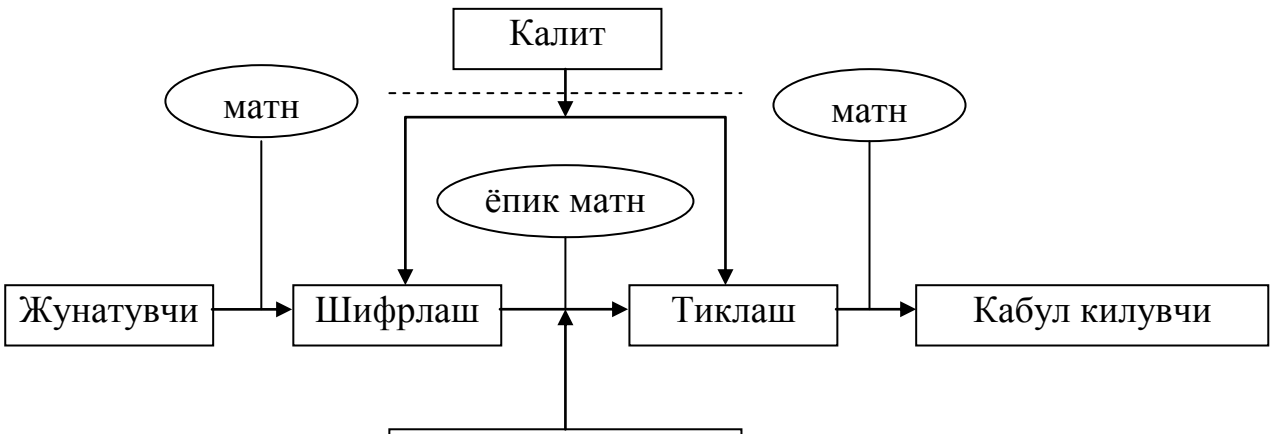
Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Internet ёрдамида амалга ошириладиган электрон савдолардир.

Ахборотларни криптографияли ҳимоялаш тамойиллари

Криптография — маълумотларни ўзгартириш усулларининг туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: **махфийлик; яхлитлилик.**

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:



Бу ерла калит кандайдир химояланган канал оркали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуклидир.

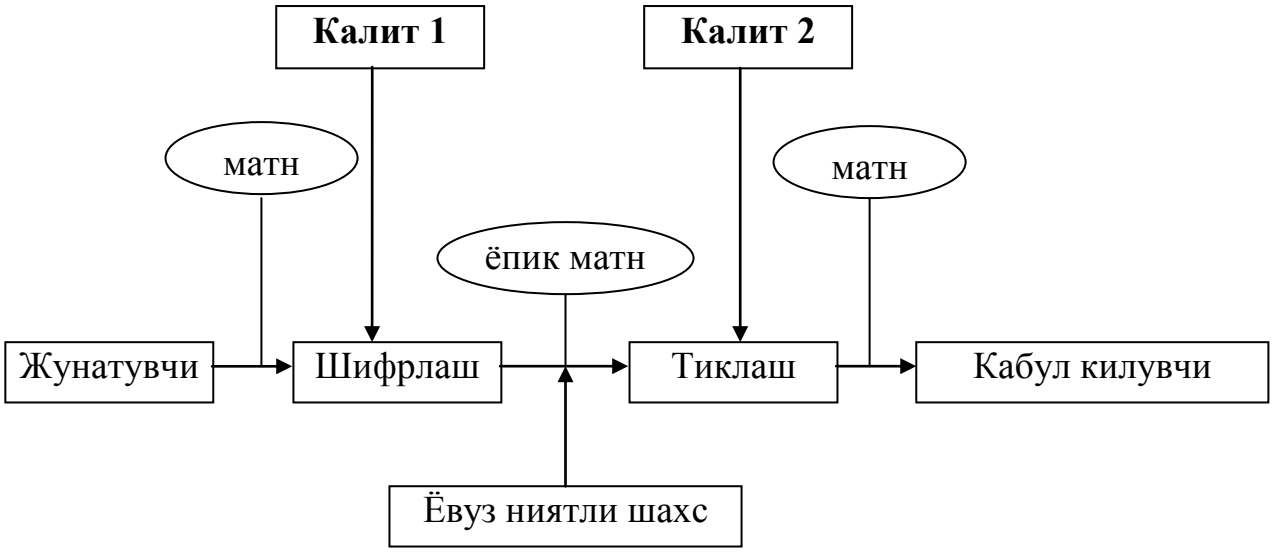
Ассимметрияли икки калитлик криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:

Бу ҳолда ҳимояланган канал бўйича очиқ калит жўнатилиб, махфий калит жўнатилмайди.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптотахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим **криптомустаҳкам тизим де**б айтилади.

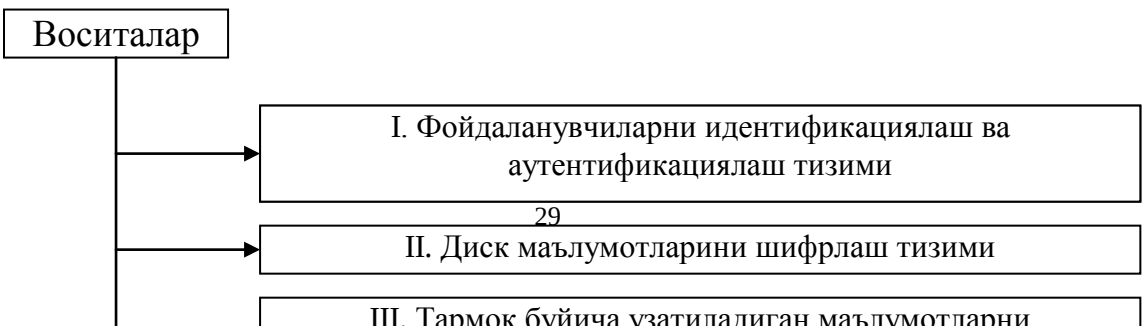
Криптотизимнинг мустахкамлиги унинг калити билан аникланади ва бу криптотаҳлилнинг асосий қоидаларидан бири бўлиб хисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим ҳисобланиб, унинг ўзгартирилиши кўп вакт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни химоялаш талаб қилинади.



Компьютер маълумотларини химоялашнинг техник-дастурий воситалари

Ушбу воситаларни куйидагича таснифлаш мумкин:



1. ***Фойдаланувччиларни идентификациялаш ва аутентификациялаш тизими.*** Ушбу тизим фойдаланувчидан олинган маълумот буйича унинг шахсини текшириш, хакикийлигини аниклаш ва шундан сунг унга тизим билан ишлашга рухсат бериш лозимлигини белгилаб беради.

Бу холда асосан фойдаланувчидан олинадиган маълумотни танлаш муаммоси мавжуд булиб, унинг куйидаги турлари мавжуд:

• фойдаланувчига маълум булган махфий ахборот, масалан, пароль, махфий калит ва бошкалар;

• шахснинг физиологик параметрлари, масалан, бармок излари, кузнинг тасвири ва бошкалар.

Биринчиси анъанавий, иккинчиси эса биометрик идентификациялаш тизими, дейилади.

II. ***Диск маълумотларини шифрлаш тизими.*** Ушбу тизимнинг асосий максади дискдаги маълумотларни химоялашдир. Бу холда мантикий ва жисмоний боскичлар ажратилади. Мантикий боскичда файл асосий объект сифатида булиб, факатгина баъзи бир файллар химояланади. Бунга мисол килиб, архиватор дастурларини келтириш мумкин. Жисмоний боскичда диск тулалигича химояланади. Бунга мисол сифатида Norton Utilities таркибидаги Diskreet шифрловчи дастурни келтириш мумкин.

III. ***Тармок буйича узатиладиган маълумотларни шифрлаш тизими.*** Ушбу тизимда икки йуналишни ажратиш мумкин:

• канал буйича, яъни алока каналлари буйича жунатиладиган барча маълумотларни шифрлаш;

• абонентлар буйича, яъни алока каналлари буйича жунатиладиган маълумотларнинг факатгина мазмуний кисми шифрланиб, колган хизматчи маълумотларни очик колдириш.

IV. ***Электрон маьлумотларни аутентификациялаш тизими.*** Ушбу тизимда тармок буйича бажариладиган электрон маълумотлар алмашувида хужжатни ва унинг муаллифини аутентификациялаш муаммоси пайдо булади.

V. ***Таянч ахборотларни бошкариш воситалари.*** Ушбу тизимда таянч ахборотлар сифатида компьютер тизими ва тармогида кулланиладиган барча

криптографик калитлар тушунилади. Бу холда калитларни генерациялаш, саклаш ва таксимлаш каби бошкарув функцияларини ажратишади.

Симметрияли криптотизим асослари

Криптография нуктаи – назаридан шифр — бу калит демакдир ва очик маълумотлар тупламини ёпик (шифрланган) маълумотларга узгартириш криптография узгартиришлар алгоритмлари мажмуаси хисобланади.

Калит — криптография узгартиришлар алгоритмининг баъзи-бир параметрларининг махфий холати булиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий курсаткич булиб **криптомустахкамлик** хисобланади.

Криптография химоясида шифрларга нисбатан куйидаги талаблар куйилади:

• етарли даражада криптомустахкамлик;

• шифрлаш ва кайтариш жараёнининг оддийлиги;

• ахборотларни шифрлаш окибатида улар хажмининг ортиб кетмаслиги;

• шифрлашдаги кичик хатоларга таьсирчан булмаслиги.

Ушбу талабларга куйидаги тизимлар жавоб беради:

• уринларини алмаштириш;

• алмаштириш;

• гаммалаштириш;

• аналитик узгартириш.

Уринларини алмаштириш шифрлаш усули буйича бошлангич матн белгиларининг матннинг маълум бир кисми доирасида махсус коидалар ёрдамида уринлари алмаштирилади.

Алмаштириш шифрлаш усули буйича бошлангич матн белгилари фойдаланилаётган ёки бошка бир алифбо белгиларига алмаштирилали.

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

Тахлилий узгартириш усули буйича бошлангич матн белгилари аналитик формулалар ёрдамида узгартирилади, масалан, векторни матрицага купайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги булса, матрица эса калит сифатида хизмат килади.

Уринларни алмаштириш усуллари

Ушбу усул энг оддии ва энг кадимий усулдир. Уринларни алмаштириш усулларига мисол сифатида куйидагиларни келтириш мумкин:

— шифрловчи жадвал;

— сехрли квадрат.

Шифрловчи жадвал усулида калит сифатида куйидагилар кулланилади:

— жадвал улчовлари;

— суз ёки сузлар кетма-кетлиги;

— жадвал таркиби хусусиятлари.

Мисол.
Куйидаги матн берилган булсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ
Ушбу ахборот устун буйича кетма – кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Натижада, 4х7 улчовли жадвал ташкил килинади.
Энди шифрланган матн каторлар буйича аникланади, яъни узимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал улчовлари хизмат килади.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал буйича сонлар йигиндиси битга сонга тенг бўлган квадрат шаклидаги жадвалга айтилали.

Сеҳрли квадратга сонлар тартиби бўйича белгилар киритилади ва бу белгилар сатрлар бўйича ўқилганда матн ҳосил бўлади.

Мисол.

4х4 улчовли сехрли квадратни оламиз, бу ерда сонларнинг 880 та хар хил комбинацияси мавжуд. Куйидагича иш юритамиз:

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

Бошлангич матн сифатида куйидаги матнни оламиз:
ДАСТУРЛАШ ТИЛЛАРИ
ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар буйича укиш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАД

Алмаштириш усуллари

Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин:

- Цезар усули;
- Аффин тизимидаги Цезар усули;
- Таянч сўзли Цезар усули ва бошқалар.

Цезар усулида алмаштирувчи харфлар k ва силжиш билан аниқланади. Юлий Цезар бевосита k қ 3 булганда ушбу усулдан фойлаланган.

k қ 3 бўлганда ва алифбодаги ҳарфлар m қ 26 та бўлганда қуйидаги жалвал ҳосил қилинади:

A → D	J → M	S → V
B → E	K → N	T → W
C → F	L → O	U → X
D → G	M → P	V → Y
E → H	N → Q	W → Z
F → I	O → R	X → A
G → J	P → S	Y → B
H → K	Q → T	Z → C
I → L	R → U	

Мисол.

Матн сифатида KOMPUTER сузини оладиган булсак, Цезар усули натижасида куйидаги шифрланган ёзув хосил булади: NRPSBXWHU.

Цезар усулининг камчилиги бу бир хил ҳарфларнинг ўз навбатида, бир хил ҳарфларга алмашишидир.

Аффин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аникланади: at+b (mod m), бу ерда a, b - бутун сонлар, 0≤a, b<m, ЭКУБ (a,m)қ1.

mқ26, ақ3, bқ5 булганда куйидаги жадвал хосил килинади:

T	0	1	2	3	4	5
3t+5	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25
13	16	19	22	25	2

Шунга мос равишда харфлар куйидагича алмашади:

A	B	C	D	E	F	G	H
F	I	L	O	R	U	X	A

I	J	K	L	M	N	O	P
D	G	J	M	P	S	V	Y

Q	R	S	T	U	V	W	X
B	E	H	K	N	Q	T	W

Y	Z
Z	C

Натижада юкорида келтирилган матн куйидагича шифрланади:

JVPYZNKRE.

Хозирги вактда компьютер тармокларида тижорат ахборотлари билан алмашишда учта асосий алгоритмлар, яъни DES, CLIPPER ва PGP алгоритмлари кулланилмокда. DES ва CLIPPER алгоритмлари интеграл схемаларда амалга оширилади. DES алгоритмининг криптомустахкамлигини куйидаги ммсол оркали хам бахолаш мумкин: 10 млн. АКШ доллари харажат килинганда DES шифрлаш очиш учун 21 минут, 100 млн, АКШ доллари харажат килинганда эса 2 минут сарфланади. CLIPPER тизими SKIPJACK шифрлаш алгоритмини уз ичига олади ва бу алгоритм DES алгоритмидан 16 млн, марта кучлирокдир.

PGP алгоритми эса 1991 йилда Филипп Циммерман (АКШ) томонидан ёзилган ва электрон почта оркали кузатиладиган хабарларни шифрлаш учун ишлатиладиган PGP дастурлар пакети ёрдамида амалга оширилади, FGP дастурий воситалари Internet тармогида электрон почта оркали ахборот жунатувчи фойдаланувчилар томонидан шифрлаш максадида кенг фойдаланилмокда.

PGP (Pretty Good Privacy) криптография дастурининг алгоритми калитли, очик ва ёпик булади.

Очик калит куйидагича куринишни олиши мумкин:

Ушбу очик калит бевосита Web сахифаларда ёки электрон почта оркали очикчасига юборилиши мумкин. Очик калитдан фойдаланган жунатилган шифрли ахборотни ахборот юборилган манзил эгасидан бошка шахс укий олмайди. PGP оркали шифрланган ахборотларни очиш учун, суперкомпьютерлар ишлатилганда бир аср хам камлик килиши мумкин.

Булардан ташкари, ахборотларни тасвирларда ва товушларда яшириш дастурлари хам мавжуд. Масалан, S-toots дастури ахборотларни BMP, GIF, WAV кенгайтмали файлларда саклаш учун кулланилади.

Кундалик жараёнда фойдаланувчилар офис дастурлари ва архиваторларни куллаб келишади. Архиваторлар, масалан PkZip дастурида маълумотларни пароль ёрдамида шифрлаш мумкин. Ушбу файлларни очганда иккита, яъни лугатли ва тугридан-тугри усулдан фойдаланишади. Лугатли усулда бевосита махсус файлдан сузлар пароль урнига куйиб текширилади, тугридан-тугри усулда эса бевосита белгилар комбинацияси тузилиб, пароль урнига куйиб текишрилади.

Офис дастурлари (Word, Excel, Access) оркали химоялаш умуман таклиф этилмайди. Бу борада мавжуд дастурлар Internet да тусиксиз таркатилади.

6 – МАВЗУ: МАЪЛУМОТЛАРНИНГ ТАРКАЛИБ КЕТИШИ ВА МАЪЛУМОТЛАРГА РУХСАТСИЗ КИРИШ

1. ***Ахборот тизимларнинг таъсирчан кисмлари;***
2. ***Электрон почтага рухсатсиз кириш;***

3. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.

Ахборот тизимларнинг таъсирчан кисмлари

Хозирги вактларда мавжуд ахборот тизимларида жуда катта хажмда махфий ахборотлар сакланади ва уларни химоялаш энг долзарб муаммолардан хисобланади.

Масалан, биргина АКШ мудофза вазирлигида айни чогда 10000 компьютер тармоклари ва 1,5 млн компьютерларга карашли ахборотларнинг аксарият кисми махфий эканлиги хаммага аён. Бу компьютерларга 1999 йили 22144 марта турлича хужумлар уюштирилган, уларнинг 600 тасида Пентагон тизимларининг вактинчалик ишдан чикишига олиб келган, 200 тасида эса махфий булмаган маълумотлар базаларига рухсатсиз кирилган ва натижада Пентагон 25 миллиард АКШ доллари микдорида иктисодий зарар курган. Бунака хужумлар 2000 йили 25000 марта амалга оширилган. Уларга карши курашиш учун Пентагон томонидан янги технологиялар яратишга 2002 йили Carnegie Mellon университетига 35,5 млн. АКШ доллари микдорида грант ажратилган.

Маълумотларга караганда, хар йили АКШ хукумати компьютерларига уртача хисобда 250—300 минг хужум уюштирилади ва улардан **65 %** и муваффакиятли амалга оширилади.

Замонавий автоматлаштирилган ахборот тизимлари — бу тараккиёт дастурий-техник мажмуасидир ва улар ахборот алмашувини талаб этадиган масалаларни ечишни таъминлайди. Кейинги йилларда фойдаланувчиларнинг ишини енгиллаштириш максадида янгиликларни таркатиш хизмати USENET-NNTP, мультимедиа маълумотларини INTERNET-HTTP тармоги оркати узатиш каби протоколлар кенг таркалди.

Бу протоколлар бир канча ижобий имкониятлари билан бирга анчагина камчиликларга хам эга ва бу камчиликлар тизимнинг захираларига рухсатсиз киришга йул куйиб бермокда.

Ахборот тизимларининг асосий таъсирчан кисмлари куйидагилар:

• INTERNET тармогидаги серверлар. Бу серверлар: дастурлар ёки маълумотлар файлларини йук, килиш оркали, серверларни хаддан ташкари куп тугалланмаган жараёнлар билан юклаш оркали: тизим журналининг кескин тулдириб юборилиши оркали; броузер — дастурларини ишламай колишига олиб келувчи файлларни нусхалаш оркали ишдан чикарилади;

• маълумотларни узатиш каналлари — бирор-бир порт оркали ахборот олиш максадида яширин канални ташкил этувчи дастурлар юборилади;

• маълумотларни тезкор узатиш каналлари — бу каналлар жуда куп микдорда хеч кимга керак булмаган файллар билан юкланади ва уларнинг маълумот узатиш тезлиги сусайиб кетади;

• янгиликларни узатиш каналлари — бу каналлар эскирган ахборот билан тулдириб ташланади ёки бу каналлар умуман йук килиб ташланади;

• ахборотларни узатиш йули — USENET тармогида янгиликлар пакетининг маршрути бузилади;

• JAVA броузерлари — SUN фирмаси яратган JAVA тили имкониятларидан фойдаланиб, апплетлар (applets) ташкил этиш оркали маълумотларга рухсатсиз кириш мумкин булади. JAVA — апплетлари тармокда автоматик равишда ишга тушиб кетади ва бунинг натижасида фойдаланувчи бирор-бир хужжатни ишлатаётгаи пайтда хакикатда нима содир этилишини хеч качон кура билмайди, масалан, тармок вирусларини ташкил этиш на JAVA-апплетлари оркали вирусларни жунатиш мумкин булади ёки фойдаланувчининг кредит карталари ракамларига эгалик килиш имконияти вужудга келади.

АКШ саноат шпионажига карши кураш ассоциациясининг текширишларига асосан компьютер тармоклари ва ахборот тизимларига хужумлар куйидагича таснифланади: 20% — аралаш хужумлар; 40% — ички хужумлар ва 40% — ташки хужумлар.

Жуда куп холларда бунака хужумлар муваффакиятли ташкил этилади. Масалан, Буюк Британия саноати, компьютер жиноятлари сабабли, хар йили 1 млрд фунт стерлинг зарар куради.

Демак, юкорида олиб борилган тахлилдан шу нарса куринадики, хозирги пайтда компьютер тармоклари жуда куп таъсирчан кисмларга эга булиб, улар оркали ахборотларга рухсатсиз киришлар амалга оширилмокда ёки маълумотлар базалари йук килиб юборилмокда ва бунинг натижасида инсоният млрд-млрд АКШ доллари микдорида иктисодий зарар курмокда.

Электрон почтага рухсатсиз кириш

Internet тизимидаги электрон почта жуда куп ишлатилаётган ахборот алмашиш каналларидан бири хисобланади. Электрон почта ёрдамида ахборот алмашуви тармокдаги ахборот алмашувининг 30%ини ташкил этади. Бунда ахборот алмашуви бор-йуги иккита протокол: SMTP (Simple Mail Transfer Protocol) ва POP-3 (Post Office Prolocol)ларни ишлатиш ёрдамида амалга оширилади. POP-3 мультимедиа технологияларининг ривожини акс эттиради, SMTP эса Appranet проекти даражасида ташкил этилган эди. Шунинг учун хам бу протоколларнинг хаммага очиклиги сабабли, электрон почта ресурсларига рухсатсиз киришга имкониятлар яратилиб берилмокда:

- SMTP сервер — дастурларининг нокоррект урнатилиши туфайли бу серверлардан рухсатсиз фойдаланилмокда ва бу технология «спама» технологияси номи билан маълум;

- электрон почта хабарларига рухсатсиз эгалик килиш учун оддийгина ва самарали усуллардан фойдаланилмокда, яъни куйи катламларда винчестердаги маълумотларни укиш, почта ресурсларига кириш паролини укиб олиш ва хоказолар.

Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари

Маълумки, хисоблаш техникаси воситалари иши электромагнит нурланиши оркали бажарилади, бу эса, уз навбатида, маълумотларни таркатиш учун зарур булган сигналларнинг захирасидир. Бундай кисмларга компьютерларнинг платалари, электрон таъминот манбалари, принтерлар, плоттерлар, алока аппаратлари ва х.к. киради. Лекин, статистик маълумотлардан асосий юкори частотали электромагнит нурланиш манбаи сифатида дисплейнинг рол уйнаши маълум булди. Бу дисплейларда электрон нурли трубкалар урнатилган булади. Дисплей экранида тасвир худди телевизордагидек ташкил этилади. Бу эса видеосигналларга эгалик килиш ва уз навбатида, ахборотларга эгалик килиш имкониятини яратади. Дисплей экранидаги курсатув нусхаси телевизорда хосил булади.

Юкорида келтирилган компьютер кисмларидан бошка ахборотларга эгалик килиш максадида тармок кабеллари хамда серверлардан хам фойдаланилмокда.

Компьютер тизимлари захираларига рухсатсиз кириш сифатида мазкур тизим маьлумотларидан фойдаланиш, уларни узгартириш ва учириб ташлаш харакатлари тушунилади.

Агар компьютер тизимлари рухсатсиз киришдан химояланиш механизмларига эга булса, у холда рухсатсиз кириш харакатлари куйидагича ташкил этилади:

- химоялаш механизмини олиб ташлаш ёки куринишини узгартириш:
- тизимга бирор-бир фойдаланувчининг номи ва пароли билан кириш.

Агар биринчи холда дастурнинг узгартирилиши ёки тизим суровларининг узтартирилиши талаб этилса, иккинчи холда эса мавжуд фойдаланувчининг паролини клавиатура оркали киритаётган пайтда куриб олиш ва ундан фойдаланиш оркали рухсатсиз кириш амалга оширилади.

Маълумотларга рухсатсиз эгалик килиш учун зарур булган дастурларни татбик этиш усуллари куйидагилардир:

• компьютер тизимлари захираларига рухсатсиз эгалик килиш;

• компьютер тармоги алока каналларидаги хабар алмашуви жараёнига рухсатсиз аралашув;

• вирус куринишидаги дастурий камчиликлар (дефектлар)ни киритиш.

Купинча компьютер тизимида мавжуд заиф кисмларни «тешик»лар, «люк»лар деб аташади. Баьзан дастурчиларнинг узи дастур тузиш пайтида бу «тушик»ларни колдиришади, масалан:

— натижавий дастурий махсулотни енгил йигиш максадида;

— дастур тайёр булгандан кейин яширинча дастурга кириш воситасига эга булиш максадида.

Мавжуд «тешик»ка зарурий буйруклар куйилади ва бу буруклар керакли пайтда уз ишини бажариб боради. Вирус куринишидаги дастурлар эса маълумотларни йукотиш ёки кисман узгартириш, иш сеансларини бузиш учун ишлатилади.

Юкорида келтирилганлардан хулоса килиб, маълумотларга рухсатсиз эгалик килиш учун дастурий мосламалар энг кучли ва самарали инструмент булиб, компьютер ахборот захираларига катта хавф тугдириши ва буларга карши кураш энг долзарб муаммолардан бири эканлигини таъкидлаш мумкин.

7 – МАВЗУ: КОМПЬЮТЕР ТАРМОКЛАРИДА МАЪЛУМОТЛАРНИНГ ТАРКАЛИШ КАНАЛЛАРИ

1. Компьютер тормокларининг заиф кисмлари. Тармок химоясини ташкил килиш асослари;

2. ***Компьютер телефониясидаги химоялаш усуллари.***

Компьютер тормокларининг заиф кисмлари. Тармок химоясини ташкил килиш асослари

Хозирги вактда локал хисоблаш тармокари (LAN) ва глобал хисоблаш тармоклари (WAN) орасидаги фарклар йуколиб бормокда. Масалан, Netware 4x ёки Vines 4.11. операцион тизимлари LANнинг фаолиятини худудий даражасига чикармокда. Бу эса, яъни LAN имкониятларининг ортиши, маълумотларни химоялаш усулларини янада такомиллаштиришни талаб килмокда.

Химоялаш воситаларини ташкил этишда куйидагиларни эътиборга олиш лозим:

• тизим билан алокада булган субъектлар сонининг куплиги, купгина холларда эса баъзи бир фойдаланувчиларнинг назоратда булмаслиги;

• фойдаланувчига зарур булган маълумотларнинг тармокда мавжудлиги:

• тармокларда турли фирмалар ишлаб чикарган шахсий компьютерларнинг ишлатилиши;

• тармок тизимида турли дастурларнинг ишлатиш имконияти;

• тармок элементлари турли мамлакатларда жойлашганлиги сабабли, бу давлатларга тортилган алока кабелларининг узунлиги ва уларни тулик, назорат килишнинг карийб мумкин эмаслиги;

• ахборот захираларидан бир вактнинг узида бир канча фойдаланувчиларнинг фойдаланиши;

• тармокка бир канча тизимларнинг кушилиши;

• тармокнинг енгилгина кенгайиши, яъни тизим чегарасининг ноаниклиги ва унда ишловчиларнинг ким эканлигининг номаълумлиги;

• хужум нукталарининг куплиги;

• тизимга киришни назорат килишнинг кийинлиги.

Тармокни химоялаш зарурлиги куйидаги холлардан келиб чикади:

• бошка фойдаланувчилар массивларини укиш;

• компьютер хотирасида колиб кетган маълумотларни укиш;

• химоя чораларини айланиб утиб, маълумот ташувчиларни нусхалаш;
• фойдаланувчи сифатида яширинча ишлаш;
• дастурий тутгичларни ишлатиш;
• дастурлаш тилларининг камчиликларидан фойлаланиш;
• химоя воситаларини билиб туриб ишдан чикариш;
• компьютер вирусларини киритиш ва ишлатиш.

Тармок, мухофазасини ташкил этишда куйидагиларни эътиборга олиш лозим:

- мухофаза тизимининг назорати;
- файлларга киришнинг назорати;
- тармокда маълумот узатишнинг назорати;
- ахборот захираларига киришнинг назорати;
- тармок билан уланган бошка тармокларга маълумот таркалишининг назорати.

Махфий ахборотни кайта ишлаш учун керакли текширувдан утган компьютерларни ишлатиш лозим булади. Мухофаза воситаларининг функционал тулик булиши мухим хисобланади. Бунда тизим администраторининг иши ва олиб бораётган назорат катта ахамиятта эгадир. Масалан, фойдаланувчиларнинг тез-тез паролларни алмаштириб туришлари ва паролларнинг жуда узунлиги уларни аниклашни кийинлаштиради. Шунинг учун хам янги фойдаланувчини кайд этишни чеклаш (масалан, факат иш вактида ёки факат ишлаётган корхонасида) мухимдир. Фойдаланувчининг хакикийлигини текшириш учун тескари алока килиб туриш лозим (масалан, модем ёрдамида). Ахборот захираларига кириш хукукини чегаралаш механизмини ишлатиш ва унинг таъсирини LAN объектларига тулалигича утказиш мумкин.

Тармок, элементлари уртасида утказилаёттан маълумотларни мухофаза этиш учун куйидаги чораларни куриш керак:
• маълумотларни аниклаб олишга йул куймаслик;
• ахборот алмашишни тахлил килишга йул куймаслик;
• хабарларни узгартиришга йул куймаслик;
• яширинча уланишга йул куймаслик ва бу холларни тезда аниклаш.

Маълумотларни тармокда узатиш пайтида криптографик химоялаш усулларидан фойдаланилади, Кайд этиш журналига рухсат этилмаган киришлар амалга оширилганлиги хакида маълумотлар ёзилиб турилиши керак. Бу журналга киришни чегаралаш хам химоя воситалари ёрдамида амалга оширилиши лозим.

Компьютер тармогида назоратни олиб бориш мураккаблигининг асосий сабаби — дастурий таъминот устидан назорат олиб боришнинг мураккаблигидир. Бундан ташкари компьютер вирусларининг куплиги хам тармокда назоратни олиб боришни кийинлаштиради.

Хозирги вакттача мухофазалаш дастурий таъминоти хилма-хил булса хам, операцион тизимлар зарурий мухофазанинг керакли даражасини

таъминламас эди. Netware 4.1, Windows NT операцион тизимлари етарли даражада мухофазани таъминлай олиши мумкин.

Компьютер телефониясидаги химоялаш усуллари

Электрон коммуникацияларнинг замонавий технологиялари кейинги пайтларда ишбилармонларга алока каналлари буйича ахборотнинг турлича куринишлари (масалан: факс, видео, компьютерли, нуткли ахборотлар)ни узатишда купгина имкониятлар яратиб бермокда.

Замонавий офис бугунги кунда алока воситалари ва ташкилий техника билан хаддан ташкари тулдириб юборилган ва уларга телефон, факс, автожавоб аппарати, модем, сканер, шахсий компьютер ва х.к. киради. Замонавий техника учун ахборот-коммуникациялар технологияси — **компьютерлар телефонияси** ривожланиши билан катта туртки берилди.

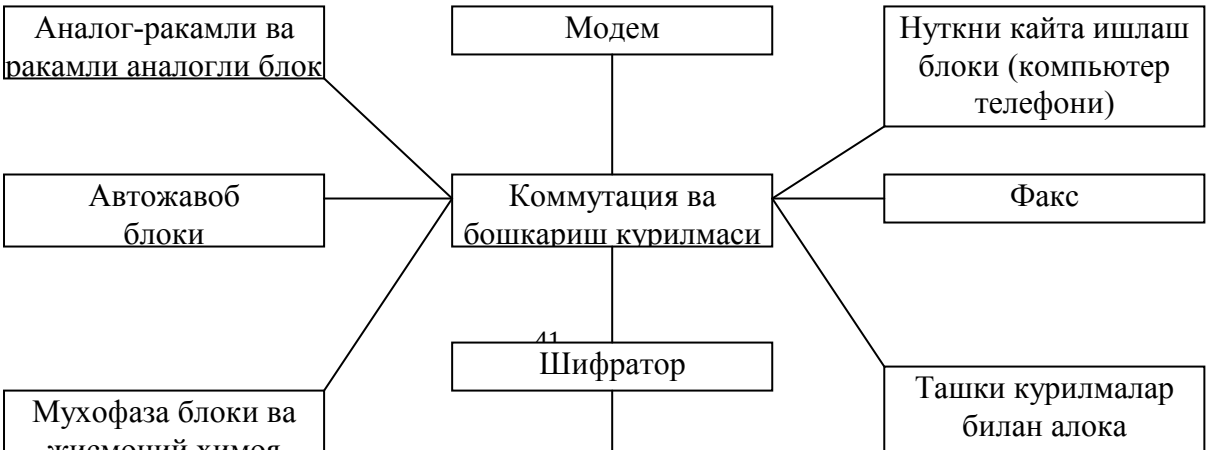
Бор-йуги ун йил илгари сотувга CANON фирмасининг нархи 6000 АКШ доллари булган «Navigator» номли махсулоти чикарилган эди ва у биринчи тизимлардан хисобланади.

Компьютер тслефонияси ун йил ичида жуда тез суръатлар билан ривожланди. Хозирги пайтда сотувда мавжуд булган «PC Phone» (Export Industries Ltd, Israel) махсулотининг нархи бор-йуги 1000 Германия маркаси туради. «Powertine-II» (Talking Technology, USA)нинг нархи эса 800 АКШ доллари туради. Кейинги пайтларда компьютер телефонияси йуналишида 70% аппарат воситаларини Dialogue (USA) фирмаси ишлаб чикармокда.

Компьютер телефониясида ахборотларнинг хавфсизлигини таъминлаш катта ахамиятга эга. Масалан, телефон хакерларининг Скотланд-Ярд АТСига кириб 1,5 млн, АКШ доллари микдорида зарар келтиришганлиги хавфсизликнинг зарурлигини исботлайди.

Компьютер телефониясида кулланилаётган нуткини аникловчи технология телефон килувчининг овозидан таниб олиш учун ахамиятга эгадир. Компьютер телефониясининг химоясини етарли даражада таъминлаш учун Pretty Good Privacy Inc. фирмасининг PC Phone 1.0 дастурий пакет ишлаб чикарилган. У компьютер телефонияси оркали узатилаёттан ахборотларни химоялаш учун ахборотларни ракамли куринишга утказади ва кабул пайтида эса дастурий-техник воситалар ёрдамида кайта ишлайди. Замонавий компьютер телефонияси воситатарининг шифрлаш тезлига хам жуда юкоридир, хато килиш эхтимоли эса жуда кичикдир (тахминан 10^{-8} – 10^{-12}).

Замонавий компьютер телефонияси курилмаси чизмаси куйидагича:



Компьютер телефонияси курилмалари куйидаги имкониятларга эга:

Курилмалар	Имкониятлар
Компьютер телефони	Нуткли хабарни ёзиб олиш ва саклаш, хабарларни кайд килиш, кодни аниклаб олиш, кайта уланиш, хабарларни узатиш
Шифратор	Маълумотларни химоялаш, маълумотларни аниклигини саклаш, маълумотларга киришни чегаралаш
Модем	Абонентни кайта текшириш, хатони тузатиш
Факс	Криптохимоя, узатилаётган ахборотни кисиш, автокайд этиш ва узатиш
Автожавоб курилмаси	Кайд этиш журналига автоматик равишда кайд килиш, абонентни тескари алока билан текшириш, тайёр килиб куйилган нуткли хабарларни узатиш, киритилаётган хабарларни ёзиб олиш
Химоя курилмаси	Ташки датчиклардан сигналлар олиш, хотирадаги ракамларни автоматик териш, рухсатсиз алокалар хакида нуткли хабар бериш, ташки курилмаларни улаб бери шва х.к.

8 – МАВЗУ: КОМПЬЮТЕР ТАРМОКЛАРИДА ЗАМОНАВИЙ ХИМОЯЛАШ УСУЛЛАРИ ВА ВОСИТАЛАРИ

1. Компьютер тармокларида химояни таъминлаш усуллари;

2. ЭХМ химоясини таъминлашнинг техник воситалари;

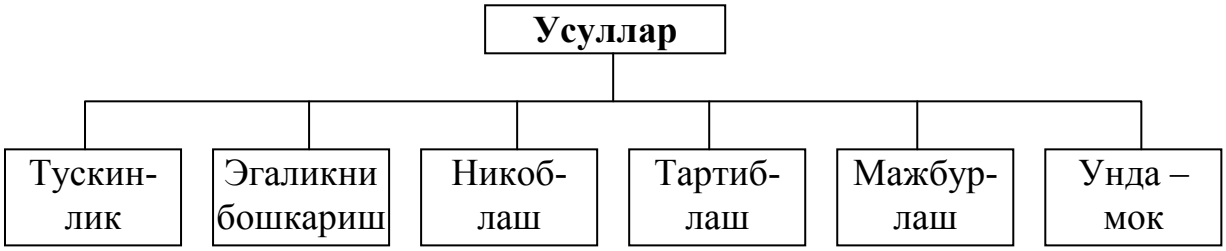
3. Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари;

4. Internet тармогида мавжуд алоканинг химоясини (хавфсизлигини) таъминлаш асослари.

Компьютер тармокларида химояни таъминлаш усуллари

Компьютер тармокларида ахборотни химоялаш деб фойдаланувчиларни рухсатсиз тармок, элементлари ва захираларига эгалик килишни ман этишдаги техник, дастурий ва криптографик усул ва воситалар, хамда ташкилий тадбирларга айтилади.

Бевосита телекоммуникация каналларида ахборот хавфсизлигини таъминлаш усул ва воситаларини куйидагича таснифлаш мумкин:



Юкорида келтирилган усулларни куйидагича таърифлаш кабул килинган.

Тускинлик аппаратларга, маьлумот ташувчиларга ва бошкаларга киришга физикавий усуллар билан **каршилик курсатиш** деб айтилади.

Эгаликни бошкариш — тизим захиралари билан ишлашни тартибга солиш усулидир. Ушбу усул куйидаги функциялардан иборат:

• тизимнинг хар бир объектини, элементини ндентификациялаш, масалан, фойдаланувчиларни;

• идентификация буйича объектни ёки субъектни хакикий, асл эканлигини аниклаш;

• ваколатларни текшириш, яъни танланган иш тартиби буйича (регламент) хафга кунини, кунлик соатни, талаб килинадиган захираларни куллаш мумкинлигини текшириш;

• кабул килинган регламент буйича ишлаш шароитларини яратиш ва ишлашга рухсат бериш;

• химояланган захираларга килинган мурожаатларни кайд килиш;

• рухсатсиз харакатларга жавоб бериш, масалан, сигнал бериш, учириб куйиш суровномани бажаришдан воз кечиш ва бошкалар.

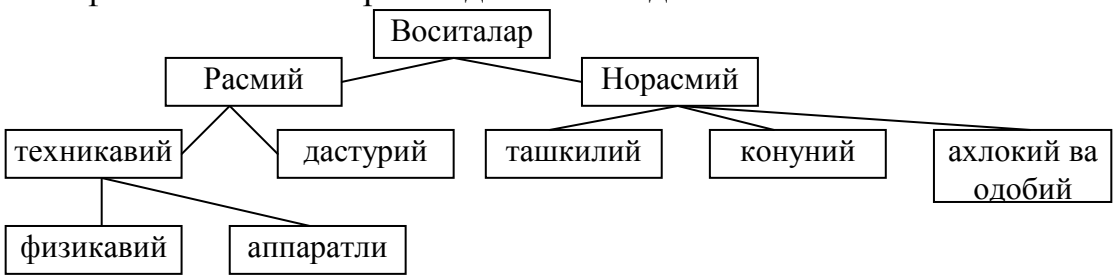
Никоблаш – маълумотларни укиб олишни кийинлаштириш максадида уларни криптография оркали кодлаш.

Тартиблаш — маълумотлар билан ишлашда шундай шарт-шароитлар яратиладики, рухсатсиз тизимга кириб олиш эхтимоли камайтирилади.

Мажбурлаш – кабул килинган коидаларга асосан маълумотларни кайта ишлаш, акс холда фойдаланувчилар моддий, маъмурий ва жиноий жазоланадилар.

Ундамок — ахлокий ва одобий коидаларга биноан кабул килинган тартибларни бажаришга йуналтирилган.

Юкорида келтирилган усулларни амалга оширишда куйидагича таснифланган воситаларни тадбик этишади.



Расмий воситалар — шахсларни иштирокисиз ахборотларни химоялаш функцияларини бажарадиган воситалардир.

Норасмий воситилар — бевосита шахсларни фаолияти ёки унинг фаолиятини аниклаб берувчи регламентлардир.

Техникавнй воситалар сифатида электр, электромеханик ва электрон курилмалар тушунилади. Техникавий воситалар уз навбатида, физикавий ва аппаратли булиши мумкин.

Аппарат-техник воситалари деб телекоммуникация курилмаларига киритилган ёки у билан интерфейс оркали уланган курилмаларга айтилади. Масалан, маълумотларни назорат килишнинг жуфтлик чизмаси, яъни жунатиладиган маълумот йулда бузиб талкин этилишини аниклашда кулланиладиган назорат булиб, автоматик равишда иш сонининг жуфтлигини (назорат разряди билан биргаликда) текширади.

Физикавий техник воситалар — бу автоном холда ишлайдиган курилма ва тизимлардир. Масалан, оддий эшик кулфлари, деразада урнатилган темир панжаралар, куриклаш электр ускуналари физикавий техник воситаларга киради.

Дастурий воситалар – бу ахборотларни химоялаш функцияларини бажариш учун мулжалланган махсус дастурий таъминотдир.

Ахборотларни химоялашда биринчи навбатда энг кенг кулланилган дастурий воситалар хозирги кунда иккинчи даражали химоя воситаси хисобланади. Бунга мисол сифатида пароль тизимини келтириш мумкин.

Ташкилий химоялаш воситалари — бу талекоммуникация ускуналарининг яратилиши ва кулланиши жараёнида кабул килинган ташкилий-техникавий ва ташкилий-хукукий тадбирлардир. Бунга бевосита мисол сифатида куйидаги жараёнларни келтириш мумкин: биноларнинг курилиши, тизимни лойихалаш, курилмаларни урнатиш, текшириш ва ишга тушириш.

Ахлокий ва одобий химоялаш воситалари — бу хисоблаш техникасини ривожланиши окибатида пайдо буладиган тартиб ва келишувлардир. Ушбу тартиблар конун даражасида булмасада, уни тан олмаслик фойдаланувчиларни обрусига зиён етказиши мумкин.

Конуний химоялаш воситалари — бу давлат томонидан ишлаб чикилган хукукий хужжатлар саналади. Улар бсвосита ахборотлардан фойдаланиш, кайта ишлаш ва узатишни тартиблаштиради ва ушбу коидаларни бузувчиларнинг масъулиятларини аниклаб беради.

Масалан, Узбекистон Республикаси Марказий банки томонидан ишлаб чикилган коидаларида ахборотни химоялаш гурузларини ташкил килиш, уларнинг ваколатлари, мажбуриятлари ва жавобгарликлари аник ёритиб берилган.

Хавфсизликни таьминлаш усуллари ва воситаларининг ривожланишини уч боскичга ажратиш мумкин: 1) дастурий воситаларни ривожлантириш; 2) барча йуналишлар буйича ривожланиши; 3) ушбу боскичда куйидаги йуналишлар буйича ривожланишлар кузатилмокда:

- химоялаш функцияларини аппаратли амалга ошириш;

- бир неча химоялаш функцияларини камраб олган воситаларни яратиш;

- алгоритм ва техникавий воситаларни умумлаштириш ва стандартлаш.

Хозирги кунда маълумотларни рухсатсиз четга чикиб кетиш йуллари куйидагилардан иборат:

• электрон нурларни четдан туриб укиб олиш;

• алока кабелларини электромагнит тулкинлар билан нурлатиш;

• яширин тинглаш курилмаларини куллаш;

• масофадан расмга тушириш;

• принтердан чикадиган акустик тулкинларни укиб олиш;

• маълумот ташувчиларни ва ишлаб чикариш чикиндиларини угирлаш;

• тизим хотирасида сакланиб колган маълумотларни укиб олиш;

• химояни енгиб маълумотларни нусхалаш;

• кайд килинган фойдаланувчи никобида тизимга кирши;

• дастурий тузокларни куллаш;

• дастурлаш тиллари ва операцион тизимларнинг камчиликларидан фойлаланиш;

• дастурларда махсус белгиланган шароитларда ишга тушиши мумкин булган кисм дастурларнинг мавжуд булиши;

• алока ва аппаратларга ноконуний уланиш;

• химоялаш воситаларини касддан ишдан чикариш;

• компьютер вирусларини тизимга киритиш ва ундан фойдаланиш.

Ушбу йуллардан деярли барчасининг олдини олиш мумкин, лекин компьютер вирусларидан хозиргача коникарли химоя воситалари ишлаб чикилмаган.

Бевосита тармок буйича узатиладиган маълумотларни химоялаш максадида куйидаги тадбирларни бажариш лозим булади:

- узатиладиган маълумотларни очиб укишдан сакланиш;

- узатиладиган маълумотларни тахтил килиҳдан сакланиш;

- узатиладиган маълумотларни узгартиришга йул куймаслик ва узгартиришга уринишларни аниклаш;

- маълумотларни узатиш максадида кулланиладиган дастурий узилишларни аниклашга йул куймаслик;

- фирибгар уланишларнинг олдини олиш.

Ушбу тадбирларни амалга оширишда асосан криптографик усуллар кулланилади.

ЭХМ химоясини таъминлашнинг техник воситалари

Компьютер оркали содир этидадиган жиноятлар окибатида факатгина АКШ хар йили 100 млрд. доллар зарар куради. Уртача хар бир жиноятда 430 минг доллар угирланади ва жиноятчини кидириб топиш эхтимоли 0,004% ни ташкил этади.

Мутахассисларнинг фикрича ушбу жиноятларни 80%и бевосита корхонада ишлайдиган ходимлар томонидан амалга оширилади.

Содир этиладиган жиноятларнинг тахлили куйидаги хулосаларни беради:

• купгина хисоблаш тармокларида фойдаланувчи исталган ишчи уриндан тармокда уланиб фаолият курсатиши мумкин. Натижада жиноятчи бажарган ишларни кайси компьютердан амалга оширилганини аниклаш кийин булади.

• угирлаш натижасида хеч нима йуколмайди, шу боис купинча жиноий иш юритилмайди;

• маълумотларга нисбатан мулкчилик хусусияти йуклиги;

• маълумотларни кайта ишлаш жараёнида йул куйилган хатолик уз вактида кузатилмайди ва тузатилмайди, натижада келгусида содир буладиган хатоларнинг олдини олиб булмайди;

• содир этиладиган компьютер жиноятлари уз вактида эълон килинмайди, бунинг сабаби хисоблаш тармокларида камчиликлар мавжудлигини бошка ходимлардан яшириш хисобланади.

Ушбу камчиликларни бартараф килишда ва компьютер жиноятларини камайтиришда куйидаги чора-тадбирларни утказиш керак булади:

• персонал масьулиятини ошириш:

• ишга кабул килинадиган ходимларни текширувдан утказиш;

• мухим вазифани бажарувчи ходимларни алмаштириб туриш;

• пароль ва фойдаланувчиларни кайд килишни яхши йулга куйиш;

• маълумотларга эгалик киилишни чеклаш;

• маълумотларни шифрлаш.

Ахборот-коммуникациялар технологияларининг ривожланиши окибатида купгина ахборотни химоялаш инструментал воситалари ишлаб чикилган. Улар дастурий, дастурий-техник ва техник воситалардир.

Хозирги кунда тармок хавфсизлигини таъминлаш максадида ишлаб чикилган техникавий воситаларни куйидагича таснифлаш мумкин:

Физикавий химоялаш воситалари — махсус электрон курилмалар ёрдамида маълумотларга эгалик килишни такиклаш воситаларидир.

Мантикий химоялаш — дастурий воситалар билан маълумотларга эгалик килишни такиклаш учун кулланилади.

Тармокларо экранлар ва шлюзлар — тизимга келадиган хамда ундан чикадиган маълумотларни маълум хужумлар билан текшириб боради ва протоколлаштиради.

Хавфсизликни аудитлаш тизимлари — жорий этилган операцион тизимдан урнатилган параметрларни заифлигини кидиришда кулланиладиган тизимдир.

Реал вактда ишлайдиган хавфсизлик тизими — доимий равишда тармокнинг хавфсизлигини тахлиллаш ва аудитлашни таъминлайди.

Стохастик тестларни ташкиллаштириш воситалари — ахборот тизимларининг сифати ва ишончлилигини текширишда кулланиладиган воситадир.

Аник йуналтирилган тестлар — ахборот-коммуникациялар технологияларининг сифати ва ишончлилигини текширишда кулланилади.

Хавфларни имитация килиш — ахборот тизимларига нисбатан хавфлар яратилади ва химоянинг самарадорлиги аникланади.

Статистик тахлилгичлар — дастурларнинг тузилиш таркибидаги камчиликларни аниклаш, дастурлар кодида аникланмаган кириш ва чикиш нукталарини топиш, дастурдаги узгарувчиларни тугри аникланганлигини ва кузда тутилмаган ишларни бажарувчи кисм дастурларини аниклашда фойдаланилади.

Динамик тахлилгичлар — бажариладиган дастурларни кузатиб бориш ва тизимда содир буладиган узгаришларни аниклашда кулланилади.

Тармокнинг заифлигини аниклаш — тармок захираларига сунъий хужумларни ташкил килиш билан мавжуд заифликларни аниклашда кулланилади.

Мисол сифитида куйидаги воситаларни келтириш мумкин:

• Dallas Lock for Administrator — мавжуд электрон Proximity ускунаси асосида яратилган дастурий-техник восита булиб, бевосита маълумотларга рухсатсиз киришни назорат килишда кулланилади;

• Security Administrator Tool for ANALYZING Networks (SATAN) — дастурий таъминот булиб, бевосита тармокнинг заиф томонларини аниклайди ва уларни бартараф этиш йулларини курсатиб беради. Ушбу йуналиш буйича бир неча дастурлар ишлаб чикилган, масалан: Internet Security Scanner, Net Scanner, Internet Scanner ва бошкалар.

• NBS тизими — дастурий-техник восита булиб, алока каналларидаги маълумотларни химоялашда кулланилади;

• Free Space Communication System — тармокда маълумотларнинг хар хил нурлар оркали, масалан лазерли нурлар оркали алмашувини таъминлайди;

• SDS тизими — ушбу дастурий тизим маълумотларини назорат килади ва кайдномада акс эттиради. Асосий вазифаси маълумотларни узатиш воситаларига рухсатсиз киришни назорат килишдир;

• Timekey — дастурий-техник ускунадир, бевосита ЭХМнинг параллел портига урнатилади ва дастурларни белгиланган вактда кенг куллалилишини такиклайди;

• IDX — дастурий-техник восита, фойдаланувчининг бармок, изларини «укиб олиш» ва уни тахлил килувчи техникалардан иборат булиб, юкори сифатли ахборот хавфсизлигини таъминлайди. Бармок изларини укиб олиш ва хотирада саклаш учун 1 минутгача, уни таккослаш учун эса 6 секундгача вакт талаб килинади.

Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари

Ахборотларни химоялашнинг мавжуд усул ва воситалари хамда компьютер тармоклари каналларидаги алоканинг хавфсизлигини таъминлаш технологияси эволюциясини солиштириш шуни курсатмокдаки, бу технология ривожланишининг биринчи боскичида дастурий воситалар афзал топилди ва ривожланишга эга булди, иккинчи боскичида химоянинг хамма асосий усуллари ва воситалари интенсив ривожланиши билан характерланди, учинчи боскичида эса куйидаги тенденциялар равшан булмокда:

- ахборотларни химоялаш асосий функцияларининг техник жихатдан амалга оширилиши;
- бир нечта хавфсизлик функцияларини бажарувчи химоялашнинг биргаликдаги воситаларини яратиш:
- алгоритм ва техник воситаларни унификация килиш ва стандартлаштириш.

Компьютер тармокларида хавфсизликни таьминлашда хужумлар юкори даражада малакага эга булган мутахассислар томонидан амалга оширилишини доим эсда тутиш лозим. Бунда уларнинг харакат моделларидан доимо устун турувчи моделлар яратиш талаб этилади. Бундан ташкари, автоматлаштирилган ахборот тизимларида персонал энг таъсирчан кисмлардан биридир. Шунинг учун, ёвуз ниятли шахсга ахборот тизими персоналидан фойдалана олмаслик чора-тадбирларини утказиб туриш хам катта ахамиятга эга.

Internet тармогида мавжуд алоканинг химоясини (хавфсизлигини) таъминлаш асослари

Маълумотларни узатиш тизимларининг ривожланиши ва улар асосида яратилган телекоммуникация хизмат курсатиш воситаларининг яратилиши бевосита фойдаланувчиларга тармок захираларидан фойдаланиш тартибларини ишлаб чикариш заруриятини пайдо килди:

• фойдаланувчининг анонимлигини таъминловчи воситалар;

• серверга киришни таъминлаш. Сервер факатгина битта фойдаланувчига эмас, балки кенг микёсдаги фойдаланувчиларга уз захираларидан фойдаланишга рухсат бериши керак;

• рухсатсиз киришдан тармокни химоялаш воситалари.

Internet тармогида рухсатсиз киришни такикловчи тармоклараро экран — Fire Wall воситалари кенг таркалган. Ушбу восита асосан UNIX операцион тизимларида кулданилиб, бевосита тармоклар орасида алока урнатиш жараёнида хавфсизликни таъминлайди. Бундан ташкари, Fire Wall тизимлари ташки мухит, масалан, Internet учун, асосий маълумотларни ва МБларини хотирасида саклаб, бевосита маьлумот алмашувини таъминлаши ва корхона тизимига киришини такиклаши мумкин.

Лекин Fire Wall тизимларининг камчиликлари хам мавжуд, масалан, E-mail оркали дастурлар жунатилиб, ички тизимга тушгандан сунг узининг кора ниятларини бажаришида ушбу химоя ожизлик килади.

Fire Wall синфидаги тизимларнинг асосий кисми ташки хужумларни кайтариш учун мулжалланган булса хам, хужумлар уларнинг 60 фоизи кучсиз эканлигини курсатди. Бундан ташкари, Fire Wall забт этилган сервернинг ишлашига каршилик курсата олмайди.

Шу боис, Internet тизимида хавфсизликни таъминлаш буиича куйидаги узгаришлар кутилмокда:

• Fire Wall тизимларининг бевосита хавфсизлик тизимларига киритилиши;

• тармок протоколлари бсвосита фойдаланувчиларни хукукларини аникловчи, хабарларнинг яхлитлигини таъминловчи ва маълумотларни шифрловчи дастурий имкониятларидан иборат булишлари. Хозирги кунда ушбу протоколларни яратиш буйича анчагина ишлар олиб борилмокда. SKIP протоколи (Simple Key management for Internet Protocol — Internet протоколлари учун криптокалитларнинг оддий бошкаруви) шунга мисол була олади.

9 – МАВЗУ: INTERNETДА АХБОРОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ АСОСЛАРИ

1. Internetda рухсатсиз кириш усулларининг таснифи;

2. ***Рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши;***

3. Тармокларапо экран ва унинг вазифалари;

4. Тармокларапо экраннинг асосий компонентлари.

Internetda рухсатсиз кириш усулларининг таснифи

Глобал тармокларнинг ривожланиши ва ахборотларни олиш, кайта ишлаш ва узатишнинг янги технологиялари пайдо булиши билан Internet тармогига хар хил шахс ва ташкилотларнинг эътибори каратилди. Куплаб ташкилотлар уз локал тармокларини глобал тармокларга улашга карор килишган ва хозирги пайтда WWW, FTP, Gophes ва бошка серверлардан фойдаланишмокда. Тижорат максадида ишлатилувчи ёки давлат сири булган ахборотларнинг глобал тармоклар буйича жойларга узатиш имкони пайдо булди ва уз навбатида, шу ахборотларни химоялаш тизимида малакали мутахассисларга эхтиёж тугилмокда.

Глобал тармоклардан фойдаланиш бу факатгина «кизикарли» ахборотларни излаш эмас, балки тижорат максадида ва бошка ахамиятга молик ишларни бажаришдан иборат. Бундай фаолият вактида ахборотларни химоялаш воситаларининг йуклиги туфайли куплаб талофотларга дуч келиш мумкин.

Хар кандай ташкилот Intenetга уланганидан сунг, хосил буладиган куйидаги муаммоларни хал этишлари шарт:

• ташкилотнинг компьютер тизимини хакерлар томонидан бузилиши:

• Internet оркали жунатилган маълумотларнинг ёвуз ниятли шахслар томонидан укиб олиниши;

• ташкилот фаолиятига зарар етказилиши.

Internet лойихалаш даврида бевосита химояланган тармок сифатида ишлаб чикилмаган. Бу сохада хозирги кунда мавжуд булган куйидаги муаммоларни келтириш мумкин:

• маълумотларни енгиллик билан кулга киритиш;

• тармокдаги компьютерлар манзилини сохталаштириш;

• TCP/IP воситаларининг заифлиги;

• купчилик сайтларнинг нотугри конфигурацияланиши;

• конфигурациялашнинг мураккаблиги.

Глобал тармокларнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб булмокда, бу эса уз навбатида ахборотлар хавфсизлигига тахдид солиш эхтимолининг ошишига олиб келмокда. Узок, масофалар билан ахборот алмашиш зарурияти ахборотларни олишнинг катъий чегараланишини талаб этади. Шу максадда тармокларнинг сегментларини хар хил даражадаги химоялаш усуллари таклиф этилган:

• эркин кириш (масалан: WWW-сервер);

• чегараланган киришлар сегменти (узок масофада жойлашган иш жойига хизматчиларнинг кириши);

• ихтиёрий киришларни ман этиш (масалан, ташкилотларнинг молиявий локал тармоклари).

Интернет глобал ахборот тармоги узида нихоятда катта хажмга эга булган ахборот ресурсларидан миллий иктисоднинг турли тармокларида самарали фойданишга имконият тугдиришига карамасдан ахборотларга булган хавфсизлик даражасини оширмокда. Шунинг учун хам Интернетга уланган хар бир корхона узининг ахборот хавфсизлигини таъминлаш масалаларига катта эътибор бериши керак. Ушбу тармокда ахборотлар хавфсизлигининг йулга куйилиши ёндашуви куйида келтирилган:

Локал тармокларнинг глобал тармокарга кушилиши учун тармоклар химояси администратори куйидаги масалаларни хал килиши лозим:

— локал тармокларга глобал тармок, томонидан мавжуд хавфларга нисбатан химоянинг яратилиши;

— глобал тармок фондаланувчиси учун ахборотларни яшириш имкониятининг яратилиши;

Бунда куйидаги усуллар мавжуд:

— кириш мумкин булмаган тармок манзили оркали;

— Ping дастури ёрдамида тармок пакетларини тулдириш;

— рухсат этилган тармок манзили билан такикланган тармок манзили буйича бирлаштириш;

— таъкикланган тармок протаколи буйича бирлаштириш;

— тармок буйича фойдаланувчига парол танлаш;

— REDIREST туридаги ICMP пакети ёрдамида маршрутлар жадвалини модификациялаш;

— RIP стандарт булмаган пакети ёрдамида маршрутлар жадвалини узгартириш;

— DNS spoofingдан фойдаланган холда уланиш.

Рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши

Ушбу хавф глобал тармокларнинг бир канча сохаларини камраб олади, жумладан:

• локал соха;

• локал-глобал тармокларнинг бирлашуви;

• мухим ахборотларни глобал тармокларда жунатиш;

• глобал тармокнинг бошкарилмайдиган кисми.

Ихтиёрий ахборот тармокларининг асосий компонентлари бу серверлар ва ишчи станциялар хисобланади. Серверда ахборотлар ёки хисоблаш ресурслари ва ишчи станцияларда хизматчилар ишлайди. Умуман

ихтиёрий компьютер хам, сервер хам ишчи станция булиши мумкин — бу холда уларга нисбатан хавфли хужумлар булиши эхтимоли бор.

Глобал тармок майдонларидаги тахдид

Тахдид	Локал майдон	ЛТ/ГТ бирлашуви	ГТ администратор майдони	ГТ бошкарилмайдиган майдони
Тармокларнинг нотугри манзили			+	+
Пакетлар билан тулдириш	+			+
Мумкин булмаган уланиш		+		+
Мумкин булган уланиш	+	+		+
Паролни танлаш	+	+		+
ICMP хужуми	+	+	+	
RIP хужуми		+	+	
Рухсатсиз узокдан бошкариш		+	+	+
Паролни узгартириш	+			+
DNS хужуми		+	+	
Мумкин булмаган вактда	+	+	+	+

Серверларнинг асосий вазифаси ахоротларни саклаш ва такдим килишдан иборат.

Ёвуз ниятли шахсларни куйидагича таснифлаш мумкин:

• ахборот олишга имконият олиш;

• хизматларга рухсат этилмаган имконият олиш;

• маълум синфдаги хизматларнинг иш режимини ишдан чикаришга уриниш;

• ахборотларни узгартиришга харакат ёки бошка турдаги хужумлар.

Уз навбатида, хозирги замонавий ривожланиш давомида сервис хизматини издан чикаришга карши кураш муаммоси мухим ахамият касб этади. Бу хилдаги хужумлар «сервисдаги бузилиш» номини олган.

Ишчи станцияларга хужумнинг асосий максади, асосан, кайта ишланаётган маълумотларни ёки локал сакланаётган ахборотларни олишдир. Бундай хужумларнинт асосий воситаси «Троян» дастурлар саналади. Бу дастур уз тузилиши буйича компьютер вирусларидан фарк килмайди ва компьютерга тушиши билан узини билинтирмасдан туради. Бошкача айтганда, бу дастурнинг асосий максади — тармок, станциясидаги химоя тизимини ички томондан бузишдан иборат.

Бу холатда масалани хал килиш маълум кийинчиликка олиб келади, яъни махсус тайёрланган мутахассис лозим ёки бошка чоралар кабул килиш керак булади. Бошка бир оддий химоя усулларидан бири хар кайси ишчи станциядаги тизимли файллар ва хизмат сохасидаги маълумотларнинг узгаришини текшириб турувчи ревизор (инг. ***advizer***— кирувчи) урнатиш саналади.

Тармоклараро экран ва унинг вазифалари

Тармокларарo экран — химоялаш воситаси булиб, ишончли тармок, ва ишончсиз тармок орасида маълумотларга киришни бошкаришда кулланилади.

Тармокларарo экран куп компонентли булиб, у Internetдан ташкилотнинг ахборот захираларини химоялаш стратегияси саналади. Яъни ташкилот тармоги ва Internet орасида куриклаш вазифасини бажаради.

Тармокларарo экраннинг асосий функцияси — маълумотларга эгалик килишни марказлаштирилган бошкарувини таъминлашдан иборат.

Тармокларарo экран куйидаги химояларни амалга оширади:

• уринсиз трафиклар, яъни тармокда узатиладиган хабарлар окимини такиклаш;

• кабул килинган трафикни ички тизимларга йуналтириш;

• ички тизимнинг заиф кисмларини яшириш билан Internet томонидан уюштириладиган хужумлардан химоялаш;

• барча трафикларни баёнлаштириш;

• ички маълумотларни, масалан тармок топологиясини, тизим номларини, тармок ускуналарини ва фойдаланувчиларнинг идентификаторларини Internetдан яшириш;

• ишончли аутентификацияни таъминлаш.

Купгина адабиётларда **тармокларарo экран** тушунчаси **брандмауэр** ёки **Fire Wall** деб юритилган. Умуман буларнинг хаммаси ягона тушунчадир.

Тармокларарo экран — бу тизим, умумий тармокни икки кисмга ажратиб, тармокларарo химоя вазифасини утайди ва маълумотлар пакетининг чегарадан утиш шартларини амалга оширадиган коидалар туплами хисобланади.

Одатда тармокларарo экран ички тармокларни глобал тармоклардан, яъни Internetдан химоя килади. Шуни айтиш керакки, тармокларарo экран нафакат Internetдан, балки корпоратив тармоклардан хам химоя килиш кобилиятига эгадир. Хар кандай тармокларарo экран ички тармокларни тулик химоя кила олади деб булмайди.

Internet хизмати ва хамма протоколларнинг амалий жихатдан ахборотларга нисбатан химоясининг тулик булмаганлиги муаммоси бор. Бу муаммолар келиб чикишининг асосий сабаби Internetнинг UNIX операцион тизим билан борликлигида.

TCP/IP (Transtnission Control Protokol/lnternet Protocol) Internetнинг глобал тармогида коммуникацияни таъминлайди ва тармокларда оммавий равишда кулланилади, лекин улар хам химояни етарлича таъминлай олмайди, чунки TCP/IP пакетининг бошида хакер хужуми учун кулай маълумот курсатилади.

Internetда электрон почтани жунатишни оддий протокол почта транспорт хизмати амалга оширади (SMTP - Simple Mail Transfer Protocol). Бу протоколда мавжуд булган химоялашнинг мухим муаммоларидан бири - фойдаланувчи жунатувчининг маизилини кура олмаслигидир. Бундан

фойдаланиб хакер катта микдорда почта хабарларини жунатиши мумкин, бу эса ишчи почта серверни хаддан ташкари банд булишига олиб келади.

Internetда оммавий тус олган дастур бу Sendmail электрон почтасидир. Sendmail томонидан жунатилган хабарлар боскинчи хакер ахборот шаклида фойдаланиши мумкин.

Тармок номлари хизмати (Domain Name System — DNS) фойдаланувчилар номи ва хост-компьютерини - манзилини курсатади. DNS компаниянинг тармок тузилиши хакида маълумотларни саклайди. DNSнинг муаммоларидан бири шундаки, бундаги маълумотлар базасини муаллифлаштирилмаган фойлаланувчилардан яшириш анча кийин. Бунинг натижасида, хакерлар DNS ни купинча хост-компьютерларнинг ишончли номлари хакида маълумотлар манбасидан фойдаланиш учун ишлатиши мумкин.

Узок, терминаллар эмуляцияси химати узок, тизимларни бир-бирига улаш учун хизмат килади. Бу сервердан фойдаланувчилар TELNET серверидан руйхатдан утиш ва уз номи ва паролини олиши лозим. TELNET серверига уланган хакер дастурни шундай урнатиши мумкинки, бунинг натижасида у фойдаланувчининг номи ва паролини ёзиб олиш имконига эга булади.

World Wide Web — WWW бу тизим Internet ёки интратармоклардаги хар хил серверлар ичидаги маълумотларни куриш учун хизмат килади. WWW нинг асосий хоссаларидан бири — Тармоклараро экран оркали аник протокол ва манзилларни фильтрлаш зарурлигини тармокнинг химоялаш сиёсати карори билан хал этилишидир.

Хар кандай ташкилотнинг **тармок хавсизлиги сиёсати** икки кисмдан иборат булади: тармок сервисларидан фойдаланиш; тармоклараро экранни куллаш.

Тармок сервисларидан фойдаланиш сиёсатига мос равишда Internetда сервислар руйхати аникланади. Бу сервисларга фойдаланувчилар чекланган кириш билан таъминланади.

Кириш усулларининг чекланилиши — фойдаланувчилар томонидан Internet сервисларига чет йуллар оркали рухсатсиз киришни такиклаш маъносини билдиради.

Тармок сервисларига кириш сиёсати, одатда, куйидаги принципларга мойил булади:

- Internetдан ички тармокка киришни такиклаш, лекин ички тармокдан Inlernetга киришга рухсат бериш;

- ваколатланган тизимларга Internetдан ички тармокка чекланилган киришга рухсат бериш.

Тармоклараро экранларга куйиладиган вазифавий талаблар куйидагилардан иборат.

• тармок даражасида фильтрлашга талаб;

• амалий даражада фильтрлашга талаб;

• администрациялаш ва фильтрлаш коидаларини урнатиш буйича талаб;

• тармокли аутентификациялаш воситаларига талаб;

• ишларни кайд килиш ва хисобни олиб бориш буйича талаб.

Тармокларарo экраннинг асосий компонентлари

Тармокларарo экранларнинг компонентлари сифатида куйидагиларни келтириш мумкин: фильтрловчи -йулловчи; тармок, даражасидаги шлюзлар; амалий даражадаги шлюзлар.

Фильтрловчи-йулловчи — йулловчи, яъни компьютер тармогида маълумотларни манзилга етказувчи дастурлар пакети ёки сервердаги дастур булиб, у кирадиган ва чикадиган пакетларни фильтрлайди. Пакетларни фильтрлаш, яъни уларни аник тупламга тегишлилигини текшириш, TCP/IP сарлавхасидаги маълумотлар буйича амалга оширилади.

Фильтрлашни аник хост-компьютер, яъни тармокдаги файл ва компьютер захираларига киришни амалга оширувчи компьютер ёки порт, яъни хабарларни жунатиш ёки кабул килиш максадида мижоз ва сервер томонидан ишлатиладиган ва одатда 16 битли сон билан номланадиган дастур билан уланишда амалга ошириш мумкин. Масалан, фойдаланувчига кераксиз ёки ишончсиз хост-компьютер ва тармоклар билан уланишда такиклаш.

Фильтрлаш коидаларини ифодалаш кийин жараён булиб, уларни тестлаш воситалари мавжуд эмас.

Биринчи коида буйича, Internetдан келадиган TCP пакети жунатувчининг порти 1023 дан катта булса, 123.4.5.6 манзилли кабул килувчига 23-портга утказилади (23-порт TELNET сервери билан богланган).

Иккинчи коида хам худди шундай булиб, факатгина 25-порт SMTP билан богланган.

Тармок даражасидаги шлюзлар ишончли мижозлардан аник хизматларга суровномасини кабул килади ва ушбу алоканинг конунийлигини текширгандан сунг уларни ташки хост-компьютер билан улайди. Шундан сунг шлюз иккала томонга хам пакетларни филътрламай жунатади.

Бундан ташкари, тармок даражасида шлюзлар бевосига **сервер-даллол** вазифасини бажаради. Яъни, ички тармокдан келадиган IP манзиллар узгартирилиб, ташкирига факатгина битта IP манзил узатилади. Натижада, ички тармокдан ташки тармок билан тугридан-тугри богламайди ва шу йул билан ички тармокни химоялаш вазифасини утайди.

Амалий даражадаги шлюзлар фильтрловчи-йулловчиларга мансуб булган камчиликларни бартараф этиш максадида ишлаб чикилган. Ушбу дастурий восита **ваколатланган сервер,** деб номланади ва у бажарилаётган хост-компьютер эса амалий даражадаги шлюз деб аталади.

Амалий даражадаги шлюзлар мижоз ва ташки хост-компьютер билан тугридан-тугри алока урнатишга йул куймайди. Шлюз келадиган ва жунатиладиган пакетларни амалий даражада фильтрлайди. Сервер-

даллоллар шлюз оркали аник сервер томонидан ишлаб чикилган маълумотларни кайтадан йуналтиради.

Амалий даражадаги шлюзлар нафакат пакетларни фильтрлаш, балки сервернинг барча ишларини кайд килиш ва тармок администраторини нохуш ишлардан хабар килиш имкониятига хам эга.

Амалий даражадаги шлюзларнинг афзалликлари куйидагилардан иборат:

• глобал тармок томонидан ички тармок таркиби куринмайди;

• ишончли аутентификация ва кайд килиш;

• фильтрлаш коидаларининг енгиллиги;

• куп тамойилли назоратларни амалга ошириш мумкинлиги.

Фильтрловчи-йулловчиларга нисбатан амалий даражадаги шлюзларнинг камчиликлари куйидагилардан иборат самарадорлигининг пастлиги; нархининг киммат булиши.

Амалий даражадаги шлюзлар сифатида куйидагиларни мисол килиб келтириш мумкин:

• Border Ware Fire Wall Server — жунатувчининг ва кабул килувчининг манзилларини, вактини ва фойдаланилган протоколларни кайд килади;

• Black Hole — сервернинг барча ишларини кайд килади ва тармок администраторига кутилаётган бузилиш хакида хабар жунатади.

Булардан ташкари куйидаги шлюзлар хам кулланилади:

Gauntlet Internel FirewaU, Alta Visla FireWali, ANS Interlock ва бошкалар.

10 – МАВЗУ: ЭЛЕКТРОН ПОЧТАДА АХБОРОТЛАРГА НИСБАТАН МАВЖУД ХАВФ-ХАТАРЛАР ВА УЛАРДАН ХИМОЯЛАНИШ АСОСЛАРИ

1. Электрон почтадан фойдаланиш;

2. E-mail асослари;

3. E-mailдаги мавжуд муаммолар;

4. Электрон почтада мавжуд хавфлар;

5. Электрон почтани химоялаш.

Электрон почтадан фойдаланиш

Электрон почта ёки E-mail хозирги кунда Internetдан фойдаланиш жараёнининг энг машхур касми хисобланади. E-mail оркали дунё буйича исталган жойга бир зумнинг узида хат юбориш ёки кабул килиш хамда ёзилган хатларни факатгина бир кишига эмас, балки манзиллар руйхати буйича жунатиш имконияти мавжуд. E-mail оркали мунозаралар утказиш имконияти мавжуд ва бу йуналишда USENET сервери кул келади.

Купгина корхоналар уз фаолиятида бевосита E-mail тизимидан фойдаланишади. Демак, корхона ва ташкилотлар рахбарлари маълум бир чора-тадбирлар оркали уз ходимларини E-mail билан ишлаш, ундан окилона

фойдаланишга ургатиши лозим. Ушбу жараённинг асосий максади мухим хужжатлар билан ишлашни тугри йулга куйиш хисобланади.

Бу ерда куйидаги йуналишлар буйича таклифларни эътиборга олиш зарур:

- E-mail тизимидан ташкилот фаолияти максадларида фойдаланиш;
- шахсий максадда фойдаланиш;
- махфий ахборотларни саклаш ва уларга кириш:
- электрон хатларни саклаш ва уларни бошкариш.

E-mail асослари

Internetда асосий почта протоколларига куйидагилар киради:

- SMTP (Simple Mail Transfer Protocol);
- POP (Post Office Protocol);
- IMAP (Internet Mail Access Protocol);
- MIME (Multi purpose Internet Mail Extensions).

Булар билан бирма-бир танишиб чикамиз:

SMTP — ушбу протокол асосида сервер бошка тизимлардан хатларни кабул килади ва уларни фойдаланувчининг почта кутисида саклайди. Почта серверига интерактив кириш хукукига эга булган фойдаланувчилар уз компьютерларидан бевосита хатларни укий оладилар. Бошка тизимдаги фойдаланувчилар эса уз хатларини POP-3 ва IMAP протоколлари оркали укиб олишлари мумкин;

POP — энг кенг таркалган протокол булиб, сервердаги хатларни, бошка серверлардан кабул килинган булса-да, бевосита фойдаланувчи томонидан укиб олинишига имконият яратади. Фойдаланувчилар барча хатларни ёки хозиргача укилмаган хатларни куриши мумкин. Хозирги кунда POP нинг 3-версияси ишлаб чикилган булиб ва аутентификациялаш усуллари билан бойитилган;

IMAP — янги ва шу боис хам кенг таркалмаган протокол саналади.

Ушбу протокол куйидаги имкониятларга эга:

- почта кутиларини яратиш, учириш ва номини узгартириш;
- янги хатларнинг келиши;
- хатларни тезкор учириш;
- хатларни кидириш;
- хатларни танлаб олиш.

IMAP саёхатда булган фойдаланувчилар учун POPга нисбатан кулай булиб хисобланади;

MIME — Internet почтасининг куп максадли кенгайтмаси сузлари кискартмаси булиб, у хатларнинг форматини аниклаш имконини беради, яъни:

- матнларни хар хил кодлаштиришда жунатиш;
- хар хил форматдаги номатн ахборотларни жунатиш;
- хабарнинг бир неча кисмдан иборат булиши;

• хат сарлавхасида хар хил кодлаштиришдаги маълумотни жойлаштириш.

Ушбу протокол ракамли электрон имзо ва маълумотларни шифрлаш воситаларидан иборат булиб, бундан ташкари унинг ёрдамида почта оркали бажарилувчи файлларни хам жунатиш мумкин. Натижада, файллар билан бирга вирусларни хам таркатиш имконияти тугилади.

E-mailдаги мавжуд муаммолар

Электрон почта билан ишлаш жараёнида куйидаги хатоларга йул куйиш мумкин:

• хатни тасодифан жунатиш;

• хатнинг нотугри манзил буйича жунатилиши;

• хатлар архивининг кескин ошиб кетиши окибатида тизимнинг ишдан чикиши;

• янгиликларга нотугри обуна булиш;

• хатни таркатиш руйхатида хатога йул куйиш.

Агар ташкилотнинг почта тизими бевосита Internetга уланган булса, йул куйилган хатолар окибати кескин ошиб кетади.

Ушбу хатоларнинг олдини олиш усулларининг баъзи бирлари куйидагилар:

- фойдаланувчиларни укитиш;
- электрон почта дастурларини тугри конфигурациялаш;
- Internetдаги протоколларга тулик амал килувчи дастурларни куллаш.

Бундан ташкари электрон почтанинг шахсий максадда ишлатилиши ташкилот рахбарияти учун баъзи бир муаммоларни келтириб чикариши мумкин, чунки E-mail манзилида ташкилот номлари акс эттирилган булиши эхтимолдан холи эмас. Натижада, шахс жунатаётган хат ташкилот номидан деб кабул килиниши мумкин. Шу боис, телефонлар каби E-mailдан шахсий ишлар учун фойдаланишни чеклаб куйиш зарур булади. Албатта, буни жорий килиш кийин масала.

Электрон почтада мавжуд хавфлар

Электрон почта билан ишлаш жараёнида куйидаги хавфлар мавжуд:

1. Жунатувчининг калбаки манзили. Кабул килинган хатни E-mail манзили аниклигига тулик ишонч хосил килиш кийин, чунки хат жунатувчи уз манзилини калбакилаштириши мумкин.

2. Хатни кулга киритиш. Электрон хат ва унинг сарлавхаси узгартирилмасдан, шифрланмасдан жунатилади. Шу боис, уни йулда кулга киритиш ва мазмунини узгартириши мумкин.

3. Почта «бомба»си. Почга тизимига куплаб электрон хатлар жунатилади, натижада тизим ишдан чикади. Почта серверининг ишдан чикиш холатлари куйидагилардир:

• диск тулиб колади ва кейинги хатлар кабул килинмайди. Агар диск тизимли булса, у холда тизим тамомила ишдан чикиши мумкин;

• киришдаги навбатда турган хатлар сонининг ошиб кетиши натижасида кейинги хатлар умуман навбатга куйилмайди;

• олинадиган хатларнинг максимал сонини узгартириш натижасида кейинги хатлар кабул килинмайди ёки учирилади;

• фойдаланувчига ажратилган дискнинг тулдирилиши натижасида кейинги хатлар кабул килинмайди ва дискни тозалаб булмайди.

4. «Куркинчли» (нохуш) хат. Internet оркали олинадиган электрон хатларнинг умуман номаълум шахслар томонидан жунатилиши ва бу хатда фойдаланувчиларнинг шахсиятига тегувчи сузлар булиши мумкин.

Электрон почтани химоялаш

Юкорида келтирилган хавфларга нисбатан куйидаги химояланиш усуллари ишлаб чикилган:

- калбаки манзилдан химояланиш, бу холда шифрланган электрон имзоларни куллаш таклиф килинади;

- хатни кулга киритишдан химояланиш, бу холда хабарни ёки жунатиш каналини шифрлаш таклиф килинади.

Ушбу химоялаш усуллари бевосита колган хавфларнинг улушини камайтиради.

11 – МАВЗУ: ЭЛЕКТРОН ТУЛОВЛАР ТИЗИМИДА АХБОРОТЛАРНИ ХИМОЯЛАШ

1. ***Электрон туловлар тизими асослари;***
2. ***Идентификацияловчн шахсий номерни химоялаш;***
3. ***POS тизими хавфсизлигини таъминлаш;***
4. ***Банкоматлар хавфсизлигини таъминлаш;***
5. ***Internetда мавжуд электрон туловлар хавфсизлигини таъминлаш;***
6. ***Ахборотларни химоялашнинг асосий восаталари.***

Электрон туловлар тизими асослари

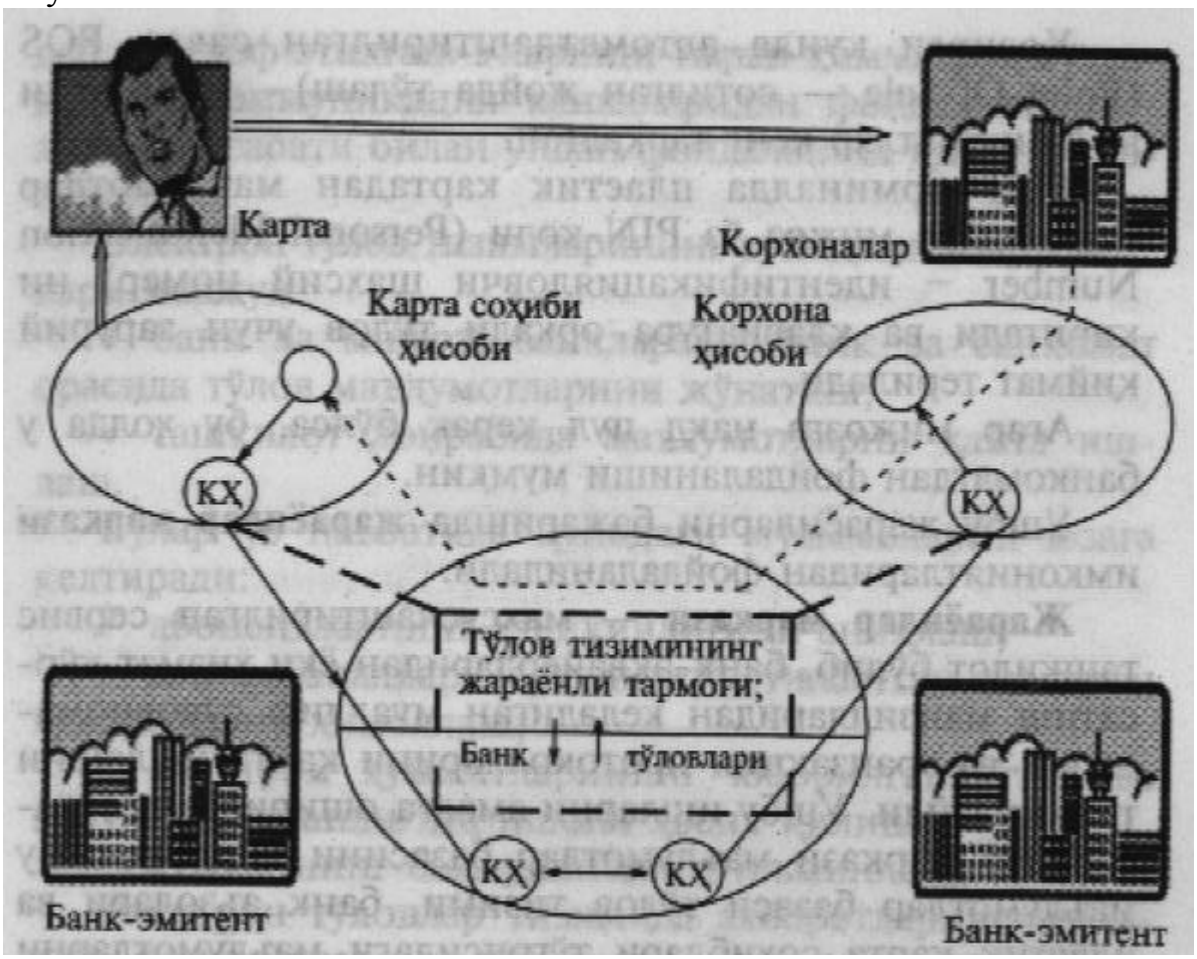
Электрон туловлар тизими деб банк пластик карталарини тулов воситаси сифатада кулланилишидаги усуллар ва уларни амалга оширувчи субъектлар мажмуасига айтилади.

Пластик карта — шахсий тулов воситаси булиб, у мазкур воситадан фойдаланадиган шахсга товар ва хизматларни накдсиз пулини тулаш, бундан ташкари банк муассасалари ва банкоматлардан накд пулни олишга имкон беради.

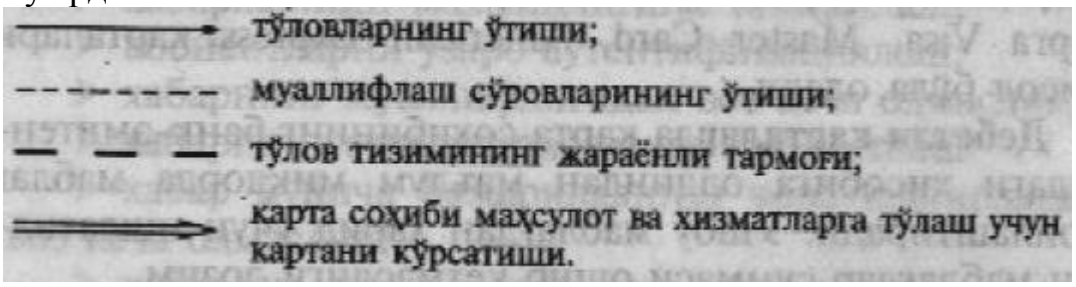
Пластик картани тулов воситаси сифатида кабул килувчилар, савдо ва хизмат курсатувчи корхоналар, банк булимлари хамда бошкалар шу пластик карталарга хизмат курсатувчи кабул килувчилар тармогини ташкил этади.

Электрон туловлар тизимини яратиҳда пластик карталарга хизмат курсатиш конун-коидаларини ишлаб чикиш ва уларга риоя килиш асосий масалалардан бири булиб хисобланади. Ушбу коидалар нафакат техникавий (маълумотларни стандартлаш, ускуналар ва бошкалар), балки молиявий масалалар (корхоналар билан хисобларни бажариш тартиби)ни хам камраб олади.

Электрон туловлар тизимининг фаолиятини куйидагидек тасаввур килиш мумкин:



Бу ерда:



Электрон туловлар тизими билан биргаликда фаолият курсатадиган банк икки, яъни **банк-эмитент ва банк-эквайер** тоифасида хизмат курсатади:

Банк-эмитент пластик карталарни ишлаб чикаради ва уларнинг тулов воситаси сифатида кулланилишига кафолат беради.

Банк-эквайер савдо ва хизмат курсатувчи ташкилотлар томонидан кабул килинган туловларни банк булимлари ёки банкоматлар оркали амалга оширади.

Хозирги кунда автоматлаштирилган савдо POS (Point-Of-Sale — сотилган жойда тулаш)— терминали ва банкоматлар кенг таркалган.

PQS-терминалда пластик картадан маълумотлар укилади ва мижоз уз PIN-коди (Personal Identification Number • идентификацияловчи шахсий номер)ни киритади ва клавиатура оркали тулов учун зарурий киймат терилади.

Агар мижозга накд пул керак булса, бу холда у банкоматдан фойдаланиши мумкин.

Ушбу жараёнларни бажаришда **жараёнлар маркази** имкониятларидан фойдаланилади.

Жараёнлар маркази – махсуслаштирилган сервис ташкилот булиб, банк-эквайерларидан ёки хизмат курсатиш манзилларидан келадиган муаллиф суровномаларни ва транзакция протоколларини кайта ишлашни таъминлайди. Ушбу ишларни амалга ошириш учун жараёнлар маркази маълумотлар базасини киритади. Бу маълумотлар базаси тулов тизими, банк аъзолари ва пластик карта сохиблари тугрисидаги маълумотларни уз таркибига олади.

Пластик карталар тулов буйича **кредитли ёки дебетли** булиши мумкин.

Кредитли карталар буйича карта сохибига купинча мухлати 25 кунгача булган вакганча карз берилади. Буларга Visa, Master Card, American Express карталари мисол була олади.

Дебетли карталарда карта сохибининг банк-эмитентидаги хисобига олдиндан маълум микдорда маблаг жойлаштиради. Ушбу маблагдан харид учун ишлатилган маблаглар суммаси ошиб кетмаслиги лозим.

Ушбу карталар факатгина шахсий эмас, балки корпоратив хам булиши мумкин.

Хозирги кунда **микропроцессорли карталар** ишлаб чикилмокда. Ушбу карталарнинг олдингиларидан асосий фарки бу мижознинг барча маълумотлари унда акс эттирилган булиб, барча **транзакциялар,** яъни маълумотлар базасини бир холатдан иккинчи холатга утказувчи суровномалар, off-line режимда амалга оширилади, шу боис, улар юкори даражада химояланган деб эътироф этилган. Уларнинг нархи кимматрок булса-да, телекоммуникация каналларидан фойдаланилмаслик муносабати билан ундан фойдаланиш киймати арзондир.

Электрон тулов тизимларининг куйидаги заиф кисмлари мавжуд:

• банк ва мижоз, банклараро, банк ва банкомат орасида тулов маълумотларини жунатиш;

• ташкилот доирасида маълумотларни кайта ишлаш.

Булар уз навбатида куйидаги муаммоларни юзага келтиради:

• абонентларнинг хакикийлигини аниклаш;

• алока каналлари оркали жунатилаётган электрон хужжатларни химоялаш;

• электрон хужжатларининг юборилганлигига ва кабул килинганлигига ишонч хосил килиш;

• хужжатнинг бажарилишини таъминлаш.

Электрон туловлар тизимида ахборотларни химоялаш функцияларини таъминлаш максадида куйидагилар амалга оширилиши керак:

- тизимнинг четки бугинларига киришни бошкариш;
- ахборотларнинг яхлитлигини назорат килиш;
- хабарларнинг махфийлигини таъминлаш;
- абонентларни узаро аутентификациялаш;
- хабарнинг муаллифлигидан воз кеча олмаслик;
- хабарнинг етказилганлигини кафолатлаш;
- хабар буйича бажариладиган чора-тадбирлардан воз кеча олмаслик;
- хабарлар кетма-кетлигини кайд килиш;
- кетма-кет хабарлар яхлитлигини таъминлаш.

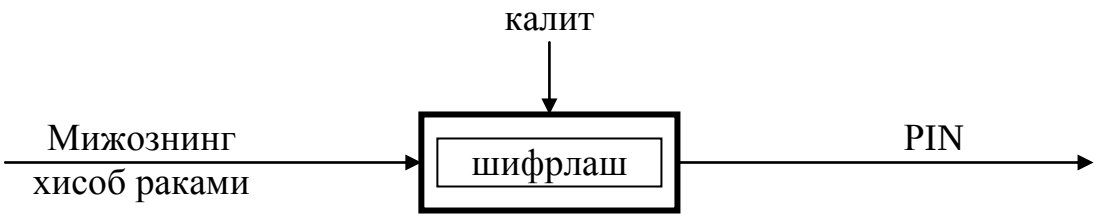
Идентификацияловчн шахсий номерни химоялаш

PIN-кодларини химоялаш тулов тизими хавфсизлигини таъминлашда асосий омилдир. Шу боис у факатгина карта сохибига маълум булиб, электрон туловлар тизимида сакланмайди ва бу тизим буйича юборилмайди.

Умуман олганда, PIN банк томонидан берилиши ёки мижоз томонидан танланиши мумкин. Банк томонидан бериладиган PIN куйидаги икки вариантдан бири буйича амалга оширилади:

1) мижоз хисоб раками буйича криптография усули билан ташкиллаштирилади;

Ушбу жараённи куйидагича тасвирлаш мумкин:



Ушбу усулнинг афзаллиги PIN коди электрон туловлар тизимида сакланиши шарт эмаслигидадир, камчилиги эса ушбу мижоз учун бошка PIN берилиши лозим булса, унга бошка хисоб раками очилиши зарурлигида, чунки банк буйича битта калит кулланилади.

2) банк ихтиёрий PIN кодни таклиф килади ва уни узида шифрлаб саклайди. PIN кодни хотирада саклаш кийинлиги ушбу усулнинг асосий камчилиги булиб хисобланади.

Мижоз томонидан танланиладиган PIN код куйидаги имкониятларга эга:

• барча максадлар учун ягона PIN кодни куллаш;

• харфлар ва ракамлардан ташкил этилган PIN кодни хотирада саклашнинг енгиллиги.

PIN коди буйича мижозни идентификациялаштиришнинг икки усули билан бажариш мумкин: **алгоритмлашган ва алгоритмлашмаган.**

Алгоритмлашмаган текшириш усулида элемент киритган PIN код маълумотлар базасидаги шифрланган код билан таккосланилади.

Алгоритмлашган текшириш усулида эса мижоз киритган PIN код, махфий калитдан фойдаланган холда, махсус алгоритм буйича узгартирилади ва картадаги ёзув билан таккосланилади.

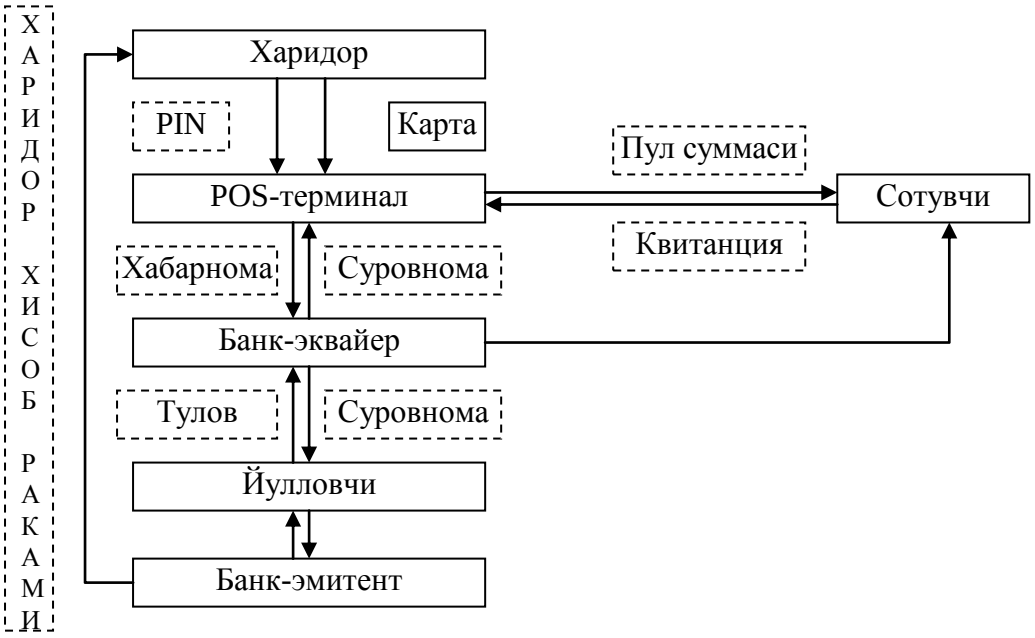
Ушбу усулнинг афзалликлари:

• асосий компьютерда PIN сакланмайди ва натижада персонал томонидан угирланмайди;

• PIN код телекоммуникация оркали жунатилмайди.

POS тизими хавфсизлигини таъминлаш

POS тизимини аник тасаввур килиш учун куйидаги чизмани келтирамиз:



Ушбу чизма буйича харидор уз пластик картасини урнатиб, PIN кодини киритади.

Сотувчи уз навбатида пул суммасини киритади. Шундан сунг, банк-эквайерга (сотувчи банки) пулни кучириш учун суровнома юборилади.

Банк-эквайер, уз навбатида, картанинг хакикийлигини аниклаш учун суровномани банк-эмитентга жунатади. Натижада, банк-эмитент пулни банк-эквайерга сотувчи хисобига кучиради. Пул кучирилгандан сунг, банк-эквайер томонидаи POS-терминалга хабарнома жунатилади. Ушбу хабарда транзакция бажарилганлиги хакида маълумот булади.

Шундан сунг, сотувчи харидорга махсулот ва квитанциясини такдим этади.

Уз-узидан куриниб турибдики, ушбу жараёнда хар хил вокеалар содир булиши мумкин.

POS тизимининг энг заиф кисми бу POS-терминалдир. Бундаги асосий хавф булиб терминалдаги махфий калитнинг угирланиши хисобланади.

Бунинг окибатлари куйидагилар булиши мумкин:

• олдинги транзакцияларда ишлатилган PIN кодни тиклаш;

• кейинги транзакцияларда кулланиладиган PIN кодни тиклаш.

Ушбу хавфлардан химояланишнинг 3 та усули таклиф этилади:

- хар бир транзакциясидан сунг калитни узгартириш;
- POS-терминал ва банк-эквайер орасидаги маълумотларни махсус калит билан шифрлаш хамда калитни хар бир транзакциядан сунг узгартириш;
- очик калитлар усули ёрдамида узатиладиган маълумотларни шифрлаш.

Банкоматлар хавфсизлигини таъминлаш

Банкоматлар накд пул олиш, хисоб ракамнинг холати ва пул кучириш имкониятларига эга.

Банкомат икки режимда ишлайди, off-line ва online.

Off-line режимда банкомат банк компьютерларидан мустакил ишлайди ва бажариладиган транзакциялар хакидаги ёзувларни уз хотирасида саклайди хамда принтерга узатиб, уларни чоп килади.

On-line режимда банкомат бевосита банк компьютерлари билан телекоммуникация оркали уланган булади. Транзакциясини амалга ошириш максадида банкомат банкдаги компьютер билан куйидаги хабарлар билан алмашади:

- банкомат суровномаси;
- банкнинг жавоб хабари;
- банкоматнинг туловни бажарганлиги хакидаги хабарни бериш.

Хозирги кунда банкоматлар тармокларидан бир неча банкларгина фойдаланади. Бу ерда мавжуд булган асосий муаммо бу банкларнинг махфий ахборотларини (масалан, махфий калит) бир-биридан химоялашдир.

Ушбу муаммонинг ечими сифатида PIN кодни, марказлаштирилган холда, хар бир банк томонидан текшириш таклиф килинади.

Бундан ташкари банкоматлар тармоги зоналарга таксимланади ва хар бир зонада ZCMK (Zone Control Master Key) калитлари, уз навбатида, компьютер тармогидаги калитларни шифрлашда кулланилади. Маьлумотларни шифрлашда эса IWK (Issuer Working Key) калитлар ишлатилади.

Internetда мавжуд электрон туловлар хавфсизлигини таъминлаш

Хозирги кунда Internetда купгина ахборот марказлари мавжуд, масалан, кутубхоналар, куп сохали маълумотлар базалари, давлат ва тижорат ташкилотлари, биржалар, банклар ва бошкалар.

Internetда бажариладиган электрон савдо катта ахамият касб этмокда. Буюртмалар тизимининг купайиши билан ушбу фаолият яна кескин ривожланади. Натижада, харидорлар бевосита уйдан ёки офисдан туриб, буюртмалар бериш имконига эга булишади. Шу боис хам, дастурий таьминотлар ва аппарат воситалар ишлаб чикарувчилар, савдо ва молиявий ташкилотлар ушбу йуналишни ривожлантиришга фаол киришишган.

Электрон савдо — глобал ахборот тармоклари оркали махсулотларни сотиш ва пулли хизматлар курсатиш демакдир.

Электрон савдонинг асосий турлари куйидагилардир:

• ахборотлар сотуви;

• электрон дуконлар;

• электрон банклар.

Ахборотлар сотуви асосан маълумотлар базасидан On-line режимда фойдаланиш учун такдим этилиши мумкин.

Электрон дуконлар Internetда Web-site оркали ташкиллаштирилади. Бунда товарлар руйхати, тулов воситалари ва бошкалар келтирилади. Харид килинган махсулотлар оддий почта оркали жунатилиши ёки агар улар электрон махсулот булса, бевосита Internetдан манзилга етказилиши мумкин.

Электрон банкларни ташкил этишдан асосий максад банкнинг доимий харажатларини камайтириш ва кенг оммани камраб олишдир. Шу боис, электрон банклар уз мижозларига юкори фоиз ставкаларини таклиф килишлари мумкин.

Ахборотларни химоялашнинг асосий восаталари

Харидор, кредит картаси сохиби, бевосита тармок оркали туловларни бажариш учун ишончли ва химояланган воситаларга эга булиши лозим.

Хозирги кунда SSL (Secure Socket Layer) ва SET (Secure Electronic Transactions) протоколлари ишлаб чикилган:

• SSL протоколи маълумотларни канал даражасида шифрлашда кулланилади;

• SET хавфсиз электрон транзакциялари протоколи якинда ишлаб чикилган булиб, факатгина молиявий маълумотларни шифрлашда кулланилади.

SET протоколининг жорий этилиши бевосита Internetда кредит карталар билан туловлар сонининг кескин ошишига олиб келади.

SET протоколи куйидагиларни таъминлашга кафолат беради:

• ахборотларнинг тулик махфийлиги, чунки фойдаланувчи тулов маълумотларининг химояланганлигига тулик ишонч хосил килиши керак;

• маълумотларнинг тулик сакланиши, яъни маълумотларни узатиш жараёнида бузилмаслигини кафолатлаш. Буни бажариш омилларидан бири ракамли имзони куллашдир;

• кредит карта сохибининг хисоб ракамини аудентификациялаш, яъни электрон (ракамли) имзо ва сертификатлар хисоб ракамини аудентификациялаш ва кредит карта сохиби ушбу хисоб ракамининг хакикий эгаси эканлигини тасдиклаш;

• тижоратчини уз фаолияти билан шугулланишини кафолатлаш, чунки кредит карта сохиби тижоратчининг хакикийлигини, яъни молиявий операциялар бажаришини билиши шарт. Бунда тижоратчининг ракамли имзосини ва сертификатини куллаш электрон туловларнинг амалга оширилишини кафолатлайди.

12 – МАВЗУ: КОМПЬЮТЕР ТИЗИМЛАРИНИНГ ХИМОЯЛАНГАНЛИК ДАРАЖАСИНИ АНИКЛАШ ВОСИТАЛАРИ

Корхоналарда жорий этилаётган автоматлаштирилган ахборот тизимининг хавфсизлигини таъминлаш, биринчи навбатда, ушбу тизимни лойихалаш боскичида кузда тутилган булиши лозим. Корхона микёсида кабул килинган хавфсизлик сиёсатининг ахборот тизимида кандай даражада акс эттирилиши мухим масалалардан бири хисобланади. Лекин, ахборот-коммуникациялар технологияларининг кескин ривожланиши, ахборот окимлари хажмининг ошиши. Internet ва intranet технологияларининг кенг микёсда кириб келиши бевосита автоматлаштирилган ахборот тизимларининг ахборот захираларини химоялашга йуналтирилган воситаларнинг мавжудлигини таъминлаш хамда тизимда мавжуд булган химоя воситаларини ривожлантиришини такозо этади.

Автоматлаштирилган ахборот тизимларига нисбатан мавжуд булган хавфларни учта йуналиш буйича ажратиш мумкин:

- амалий дастурлар;
- тармок хизматлари;
- операцион тизим хизматлари.

Амалий дастурларни текшириш буйича хозиргача ягона восита мавжуд эмас. Тармок хизматлари ва операцион тизим хизматларида кулланиладиган технологиялар умумий асосларга эга булганлиги учун уларни текшириш воситалари ишлаб чикилган.

Замонавий операцион тизимларда ахборот захираларини химоялаш воситаларининг мавжудлиги таъкидлаб келинмокда. Буларга аутентификациялаш, идентификациялаш, рухсатсиз киришни таъкиклаш, мониторинг ва аудит, криптография усулларининг мавжудлиги мисол була олади. Албатта, ушбу воситаларнинг операцион тизимларда мавжуд булганлиги корхонанинг хавфсизлик сиёсатига мос келади. Аммо, операцион тизимнинг нотугри конфигурацияланиши ва унинг дастурий таъминотидаги

мавжуд хатолар окибатида ахборот тизимларига хужумлар уюштирилиши имконияти пайдо булади.

Шу боис, операцион тизимни танлашда ундаги камчиликларни тахлил килиш, ишлаб чикарувчи фирма томонидан йул куйилган хатоларнинг тан олиниши ва уларни зудлик билан тузатишга киришилиши талаб этилади.

Операцион тизимнинг параметрларининг тугри урнатилганлигини ёки уларнинг узгармаганлигини текшириш учун «тизим хавфсизлигини сканерлаш» деб номланувчи 10 га якин махсус дастурлар ишлаб чикарилган. Масалан, Solaris операцион тизими учун мулжалланган ASET, Netware ва NT учун KSA, Unix учун SSS дастурлари мавжуд.

SSS (System Security Scanner) дастури хакида

Ушбу дастур Unix операцион тизими урнатилган компьютерларда хавфсизлик холатини текшириш ва операцион тизимнинг ташки хамда ички заиф кисмларини аниклашга йуналтирилган. Бундан ташкари у кириш хукукларини, файлларга эгалик килиш хукукларини, тармок захираларини конфигурациялашни, аутентафикациялаш дастурларини ва бошкаларни текшириши мумкин.

Дастурнинг куйидаги имкониятлари мавжуд:

- конфигурацияни текшириш, яъни рухсатсиз киришларнинг олдини олиш максадида конфигурацияни текшириш. Бунга куйидагилар киради: конфигурация файллари, операцион тизим версияси, кириш хукуклари, фойдаланувчиларнинг захиралари, пароллар;

- тизимдаги хавфли узгаришларни текшириш. Рухсатсиз киришлар окибатида тизимда содир булган узгаришларни кидиришда кулланилади. Бундай узгаришларга куйидагилар киради: файллар эгаллаган хотира хажмининг узгариши, маълумотларга кириш хукуки ёки файлдаги маълумотларнинг узгариши, фойдаланувчиларнинг захираларга кириш параметрларининг узгариши, файлларни рухсатсиз бошка бир ташки компьютерларга узатишлар;

- фойдаланувчи ннтерфейсининг кулайлиги. Бу интерфейс ёрдамида нафакат дастур билан кулай ишлаш таъминланади, балки бажарилган ишлар буйича хисоботлар хам яратилади;

- масофадан сканерлаш. Тармокдаги кампьютерларни текшириш ва алока жараёнида маълумотларни шифрлаш имконияти таъминланади;

- хисоботлар тузиш. Бажарилган ишлар буйича тулик, хисоботлар яратилади. Ушбу хисоботларда тизимнинг аникланган заиф бугинларининг изохи келтирилади ва уларни тузатиш буйича курсатмалар берилади. Хисобот HTML ёки оддий матн куринишида булиши мумкин.

SATAN дастури хакида

Тармок хизматларининг химоялганлигини тахлил килиш буйича биринчи булиб ишлаб чикарилган дастурлардан бири бу SATAN дастуридир. Бу дастур 20 га якин тармок хизматларидаги заифликларни аниклай олади.

Internet Scanner SAFEsuite дастури хакида

Агар текширувлар доимий равишда ва тулик амалга оширилиши талаб килинса, у хакда internet Scanner SAFEsuite дастурлар пакети таклиф килинади. Бу дастурлар пакети ёрдамида 140 та маълум булган заифликлар ва тармок воситалари, яъни тармоклараро экранлар, Web-серверлар, Unix, Windows 9.x, Windows NT тизимли серверлар ва ишчи станциялар, умуман TCP/IP протоколи кулланиладиган барча воситалар текширилади.

Internet Scanner SAFEsuite пакетинииг умумий имкониятлари куйидагилардан иборат:

1. Автомятлаштирилган ва конфигурацияланган сканерлаш:

• автоматлашган идентификациялаш ва заиф кисмлар буйича хисобот тузиш;

• доимий режа буйича сканерлаш;

• IP манзилларни сканерлаш;

• фойдаланувчи урнатган параметрларни сканерлаш;

• заиф бугинларни автоматик равишда тузатиш;

• ишончлилик ва такрорланувчанликни таъминлаш.

2. Хавфсизликни таъминлаш:

• тармок воситаларини инвентаризациялаш ва мавжуд асосий заиф бугинларни идентификациялаш;

• асосий хисоботларни таккослаш ва келгусида улардан фойдаланиш учун тахлил килиш.

3. Фойдаланишнинг оддийлиги:

• фойдаланувчининг график интерфейси;

• HTML туридаги тартибланган хисоботларни яратиш;

• сканерлашни марказлаштирилган холда бажариш, бошкариш ва мониторинг утказиш.

Internet Scanner SAFEsuite пакетида куйидаги дастурлар мавжуд: Web Security Scanner, FireWall Scanner ва Intranet Scanner.

Web Security Scanner бевосита Web-серверларда мавжуд заиф кисмларни аниклашга мулжалланган булиб, бу дастурнинг имкониятлари куйидагилардан иборат:

• Web-сервер урнатилган операцион тизимни аудитлаш;

• Web-серверда мавжуд дастурларни аудитлаш;

• Web-файлларда мавжуд скриптларни аудитлаш;

• Web-сервер конфигурациясини тестдан утказиш;

• асосий файллар тизимининг хавфсизлик даражасини аниклаш;

• скриптларда мавжуд хатоларни аниклаш;

• бажарилган ишлар буйича хисоботлар яратиш ва хатоларни тузатиш борасида таклифлар бериш.

FireWall Scanner дастури бевосита тармокларарo экранда мавжуд булган заиф кисмларни аниклашга мулжалланган булиб, у куйидаги амалларни бажаради:

• тармокларарo экранга хужумлар уюштириб, уни тестдан утказиш;

• тармокларарo экран оркали утадиган тармок, хизматларини сканерлаш.

Intranet Scanner дастури компьютер тармогида мавжуд камчиликларни тармокка рухсатсиз киришларини амалга ошириш оркали тестдан утказиш ёрдамида аниклашга йуналтирилган. Тармокнинг хир хил кисмлари (хост-компьютерлар, йулловчилар, Web-серверлар, Windows 9.x/NT тизимида ишлайдиган компьютерлар) ни текширишни хам амалга оширади.

Юкорида келтирилганлардан ташкари компьютер тизимларига рухсатсиз киришларни доимий равишда назорат килувчи дастурлар, масалан, Internet Security Systems компанияси томонидан ишлаб чикилган **Real Secure** дастури хам мавжуд. Бу дастур тармокда содир этилаётган ходисалар, масалан, хакерларнинг хужумларини кайд килиш билан биргаликда фаол химоя чора-тадбирларини ташкиллаштириши мумкин. Real Secure дастури йирик ташкилотлар учун мулжалланган булиб, хар куни тинимсиз ишлашга мулжалланган.

Real Secure дастури икки кисмдан иборат: **фильтрлаш** ва фойлаланувчининг **график нтерфейси.**

Фильтрлаш кисми тармокда содир этилаётган ходисаларни фаол кузатиш ва бошкариш учун хизмат килади. Дастурнинг иккинчи кисми ёрдамида фойлаланувчи руй берган ходисалар хакидаги маълумотларни кабул килади, уларни бошкаради ва тизим конфигурациясини узгартира олади. Натижада, фильтрлаш ва содир этилаётган ходисаларга нисбатан химоя тадбирларини автоматик равишда амалга ошириш мумкин булади, масалан, кайд килиш, дисплейга чикариш, ходисани ман этиш ва бошкалар.

Булардан ташкари барча кайд этилган ходисалар хакидаги маьлумотларни кейинчалик реал масштабда ёки тезкор ёки секинлашган режимларда куриб чикиш мумкин булади.

Real Secure дастури бевосита Sun OS, Solaris ва Linux операцион тизимларида ишлаш учун мулжалланган.

Axborot havfsizligi sohasida atamalar

Access - Axborotga munosabat(kirish). Axborot bilan tanishish yo u bilan biror axborot jarayonini amalga oshirish.

Access object - Munosabat (kirish) obekti. Munosabat turi va darajasi aniq qoidalar asosida cheklab qo'yilgan axborot texnologiyasi elementi va obekti.

Active attack - Tajovuz. Xavfsizlikka tah didning yuzaga chiqishi.

Active threat - Xavfsizlikka taxdid. Qasddan tizimning xolatini yomonlashtirishga qaratilgan muayyan turdagi xavf-xatarning ma'lum extimolligi.

ASCII - Armored Text - ASCII- matn. ASCII to'plamiga kiruvchi 7-bitli standart bosma simvollarda yozilib ikkili sanoq tizimida kodlangan axborot. Bu ko'rinishdagi axborot har qanday tarmoq kanali orqali uzatishga yaraydi.

Authentication information - Autentifikatsiya axboroti. Muayyan axborot manbaining yo uni egasining aslini bilib olish uchun ishlatiladigan axborot. Buknday axborot sifatida raqamli imzo, xujjat izi, manba' izi va sh.o'. bo'lishi mumkin.

Authentication- Autentifikatsiya. Muayyan axborot manbaining yo uni egasining aslini bilib olish. Bu maqsadda nosimmetrik kriptotizimdan foydalanilganda hujjatning aslini (kelib chiqishini) xujjat tuzuvchining raqamli imzosi vositasida aniqlab olinadi. Autentifikatsiya keng ma'noda qaralganda axborotning manba'idan qat'iy nazar uning faqat ichki tuzilmasi asosida butunligini aniqlashdir.

Authorized access - Ruxsatli munosabat(kirish). Axborotga va axborot texnologiyasi elementlariga nisbatan belgilab qo'yilgan cheklov qoidalariga rioya qilingan holda faol munosabatda bo'lish.

Certify - Kalitni sertifikatsiyalash. Biror kimsaning oshkora kalitini raqamli imzo bilan tasdiqlash.

Certifying Authority - Vakolatli sertifikator. Kalitni sertifikatsiyalash va buni umumiy ma'lumotlar bazasiga kiritish huquqiga ega bo'lgan ishonchga sazovor shaxs (yo shaxslar).

Confidentiality information - Axborot pinhonaligi. Axborotning u bilan bajarladigan axborot jarayonlari davomida u bilan beruhsat tanishish yo uni ko'chirib olishga yo'l qo'ymaslik xossasi.

Confidentiality information - Pinxona axborot. Xujjatlashtirilgan shunday axborotki, unga nisbatan barcha munosabatlar (ruscha, dostup) qonun bilan cheklangan.

Confidentiality mark - Maxfiylik grifi. Xujjatlashtirilgan axborotning maxfiylik darajasini ko'rsatuvchi rekvizit (masalan, o'ta maxfiy, maxfiy, pinxona, xizmatda foydalanish uchun, oshkora).

Cryptographic method - Kriptografik metod. Axborotni shifrlashga asoslangan ximoyalash usuli.

Data destruction - Axborotni yo'q qilish. Axborotni tasodifiy xato tufayli yo qasddan moddiy tashuvchidan o'chirib yuborish yokm tashuvchisi bilan birga o'g'irlab ketish.

Data falsification - Axborotni soxtalashtirish. Axborot jarayonlari davomida axborot mazmunini qastdan buzib o'zgartirish.

Data protection - Axborot ximoyasi. Axborotning pinxonaligi, butunligi va qobilligini ta'minlashga qaratilgan huquqiy, siyosiy, tashkiliy, texnikaviy va dasturiy tadbirlar majmui.

Data transmission blocking - Axborot uzatishni to'sish. Axborot uzatishni qastdan yo tasodifiy xato tufayli to'xtatib, yo'lini o'zgartirib yo kechiktirib qo'yishdan iborat bo'lgan axborot xavfsizligining buzish turi.

Decryption - Shifrni ochish. Shifrlangan axborotni tushunarli shaklga aylantirish. Buning uchun maxfiy kalitdan foydalaniladi.

Digest - raqamli iz(daydjest). Axborotning ixcham bir tomonlama xisoblanadigan funktsiyasi yoki faylning nazorat jamlamasi. Axborot o'zgarsa daydjest ham o'zgaradi.

Digital Signature - Raqamli imzo. Axborotning raqamli izi(daydjesti)ning shu axborotning xaqiqiyligini tasdiqlovchi sub'ektning maxfiy kaliti bilan shifrlangan shakli. Raqamli imzo shu sub'ektga tegishli ekaniga ishonch xosil qilish uchun axborotning raqamli izini hammaga ma'lum bo'lgan funktsiya asosida hisoblab topib, natijani raqamli imzo egasining oshkora kaliti bilan ochilgan imzosi bilan taqqoslash (verifikatsiyalash) yetarli.

Documented information - Xujjatlashtirilgan axborot. Moddiy tashuvchida aks etgan va uni belgilovchi rekvizitlarga ega bo'lgan muayyan axborot.

Encryption - Shifrlash. Axborotni undan xabardor bo'lishi lozim bo'lmagan shaxslar uchun mutlaqo tushunarsiz shaklga keltirish amali, ximoya usuli .

Enforcement - Majburlash. Foydalanuvchi yoki ijrochiga nisbatan moddiy yoki jinoiy javobgarlik taxdidi ostida axborot jarayonlari koidalarining bajarilishiga erishishga asoslangan ximoya usuli.

Identification - Identifikatsiya. Ko'rsatilgan identifikatorni uning egasiga takdim etilgan identifikator bilan takkoslash.

Identifier - Identifikator. Axborot jarayoni subekti , vositasi va obekti(axborot)ga takdim etiladigan, fakat unga biriktirilgan noyob belgi, simvollar qatori.

Information procedure - Axborot jarayoni. Axborotni yaratish, olib- yig'ish, saqlash, himoyalash, izlash, uzatish, taqsimlash, undan foydalanish yoki unga ishlov berish jarayonlaridan biri.

Information (data) integrity - Axborotning butunligi. Axborotning axborot jarayonlari davomida uni beruxsat o'zgartirish yoki yo'qotishga yo'l qo'ymaslik xossasi.

Information availability - Axborot qobilligi. Axborotning unga nisbatan ruxsat berilgan axborot jarayonlarini bajarilishiga yaroqlik va tayyorlik xossasi.

Information distortion - Axborot buzilishi. Axborotning axborot jarayonlari davomida xalal beruvchi tashqi ta'sirlar yo jarayon vositalari va ishtirokchilarining tasodifiy xatolari yo qasddan qilingan ishlar tufayli o'zgarib qolishi.

Information modification - Axborot modifikatsiyasi. Axborot mazmuni yo xmiqdorining axborot jarayonlari davomida o'zgarishi.

Information security - Axborot xavfsizligi. Axborotninig va axborot jarayonlarini amalga oshirish vositalarining ma'lum turdagi tasodifiy va qasddan qilinadigan tahdidlardan himoyalanganlik holati

Information security service - Axborot xavfsizligini ta'minlash tizimi. Axborot xavfsizligini ta'minlovchi siyosiy, huquqiy, tashkiliy, texnikaviy va dasturiy tadbirlar, vositalar va meyorlar tizimi.

Information user - Axborot foydalanuvchisi. Axborot bilan biror axborot jarayonini amalga oshiruvchi sub'ekt (shaxs, tashkilot).

Information's security - Axborotning xavfsizligi. Axborotning tasodifiy yo qasddan qilinadigan tahdidlarga qarshi pinxonalikni, butunlikni va qobillikni saqlab qolish xossasi.

Introducer - Vositachi. Ochiq kalitlarning o'z egasiga taalluqligiga kafillik berishga vakolatli shaxs yo tashkilot. PGP dasturida vositachilar ularning ochiq kalitiga ma'lum ishonch darajasi taqdim etish orqali tayinlanadilar.

Intruders (hacker) - Axborot jinoyatchisi. Axborot xavfsizligini buzgan sub'ekt (shaxs, tashkilot).

Key - Kalit. Shifrlash, shifrni ochish, raqamli imzo qo'yish va verifikatsiya(ishonib olish)da ishlatiladigan raqamli kod. Kalitlar nosimmetrik kriptotizimlarda juft(oshkora va mahfiy) xolda hosil qilinadi va bog'lamlarda saqlanadi. Simmetrik kriptotizimlarda faqat bitta(mahfiy) kalit ishlatiladi. Aralash kriptotizimlarda kalitlar juftiga qo'shimcha tarzda mahfiy seans aliti ishlatiladi.

Key Escrow - Kalitni deponirlash. Uchinchi tomonga o'z maxfiy kalitining nusxasini berish amaliyoti. Bunda uchinchi tomon shifrlangan axborotni bilib olish imkoniga ega.

Key Fingerprint - Bosma iz. Oshkora kalitni noyob tarzda ifodalovchi(belgilovchi) raqam va harflar qatori. Kalit egasidan telefon orqali Bosma izini so'rab olib o'zingizdagi uning oshkora kaliti Bosma izi nushasi bilan taqqoslab, kalit nusxasining haqiqiy yo qalbaki ekanini bilish mumkin.

Key ID - Kalit identifikatori. Kishi o'qisa bo'ladigan kalitlar juftini noyob usulda belgilovchi qator. Kalitlarning ikki jufti bir xil foydalanuvchi identifikatoriga ega bo'lishi mumkin. Lekin kalit identifikatorlari har xil bo'ladi.

Key Pair - Kalitlar jufti. Oshkora va unga mos maxfiy kalit. Oshkor kalitli tizimda har bir foydalanuvchi kamida bitta kalitlar juftiga ega.

Keyring - Bog'lam. Kalitlar to'plami. Har bir foydalanuvchi oshkora kalitlar boylamiga va maxfiy kalitlar boylamiga ega.

Masking - Niqoblash. Axborotni axborot jarayenlari davomida kriptografik usul bilan berkitish.

Obstacle - To'siq. Ximoyalanadigan axborotga axborot jinoyatchisining yo'lini fizikaviy to'sib qo'yish asosida axborotni ximoyalash usuli.

Passiv attack - Nofaol tajovuz. Xavfsizlikka nofaol taxdidning yuzaga chiqishi.

Passiv threat - Xavfsizlikka nofaol taxdid. Tizim xolatini buzmasdan turib undan axborotning begonalarga beruxsat chiqib ketish xavfi.

Password - Parol. Amaliy munosabat boshlash uchun ishlatiladigan, subektning siri xisoblanadigan identifikator. Tizimga kirish uchun klaviatura tugmalarini bosish ketma-ketligi.

Physical threat - Fizikaviy xavf. Oqibati tizimga fizikaviy xavf keltiradigan taxdid.

Plaintext - Ochiq matn. SHifrlanmagan va imzolanmagan odatdagicha o'qib-tushuniladigan matn.

Potection strategy - Himoya strategiyasi. Malum tahdidlardan ximoyalanishni taminlashga qaratilgan mezonlarning formal tarifi.

Private Key - Maxfiy kalit. Bilishi shart bo'lgan sub'ektlardan boshqa xechkimga oshkora qilinmaydigan kalit. Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun, nosimmetrik kriptotizimlarda raqamli imzo qo'yish va axborot shifrini ochish uchun ishlatiladi.

Private Keyring - Maxfiy kalitlar boylami. Boylam egasiga tegishli bir yo undan ortiq maxfiy kalitlar to'plami.

Protection model - Ximoya modeli. Axborot ximoyasi tizimini aks ettirib, uni xavfsizlik darajasini tadqiq etishga imkon beruvchi tizim.

Public Key - Oshkora kalit. Axborotni shifrlash va raqamli imzoning to'g'riligini tekshirish uchun ishlatiladigan kalit. Oshkora kalit boshqalarga erkin tarqatiladi va birov uni bilgan bilan unga mos maxfiy kalitni hisoblab topaolmaydi.

Public Keyring - Oshkora kalitlar bog'lami. Oshkora kalitlar to'plami. Uning tarkibida boylam egasining ham o'z oshkora kaliti bor.

Public-Key Cryptography - Oshkora kalitli(nosimmetrik) kriptografiya. Oshkora va maxfiy kalitlar juftidan foydalanishga asoslangan va ishlatiladigan aloqa kanalining himoyalangan bo'lishini talab qilmaydigan kriptotizimlar texnologiyasi.

Regulation - Tartibga solish. Axborotga beruxsat munosabatda bulishni minimumga keltirishga qaratilgan texnologiyaga asoslangan ximoya usuli.

Screening - Ekranlash. Tarmoklararo ekran(branmauer)ning ruxsat etilmagan tashki axborot okimlarini utkazmay ichki tarmok xavfsizligini saklash vazifasi.

Security audit - Xavfsizlikni tekshirish. Axborot tizimi va tarmog'ining hamda axborotlarning xavfsizlik xolatini tekshirib baholash.

Security model - Xavfsizlik modeli. Axborot xavfsizligi siyosatining formal ifodasi.

Security policy - Xavfsizlik siyosati. Axborot xavfsizligini taminlashga va tajovuz oqibatlarini tugatishga qaratilgan meyorlar majmui.

Signature - Imzo. Maxfiy kalit vositasida hosil qilinadigan raqamli kod. Imzo uni verifikatsiyalash jarayonida axborot aslini(manba'ini,egasini,tasdiqlovchisini) aniqlash imkonini beradi. Raqamli imzo maxfiy kalit va imzolanayotgan xujjat mazmunining funktsiyasidir.

Subject privilege - Mualliflashtirilgan kirish sub'ekti. Axborot tizimi obektlariga va axborotga amaliy munosabatda bo'lish uchun belgilab qo'yilgan xuquqlarga ega bulgan subekt.

Trojan horse - Troyan oti. Sub'ektning qonuniy vakolatlaridan foydalanib axborotga beruxsat munosabatda bo'lishga imkon beruvchi qo'shimcha pinxona vazifalarni amalga oshiruvchi dastur.

Trusted - Ishonchli. Ochiq kalit ishonchli, agar uni siz yo biror siz vakil etgan kimsa sertifikatsiyalagan bo'lsa.

Trusted computer system - Ximoyalangan kompyuter tizimi. Ximoya vositalari majmui o'rnatilgan kompyuter tizimi.

Unauthorized access - Beruxsat munosabat. Sub'ekt tomonidan axborotga va axborot vositalariga nisbatan cheklab kuyilgan qoidalarning buzilishi.

Unauthorized action - Beruhsat faoliyat. Sub'ektning axborot jarayonlarini amalga oshirish qoidalariga zid faoliyati.

User ID - Kalit foydalanuvchisi identifikatori. Kalitlar juftini belgilovchi jumla. Bunday jumla sifatida odatda kalit egasining to'la nomi va uning elektron pochtasi manzili ishlatiladi.

Verification - Ishonib olish(Verifikatsiya). Axborotga mahfiy kalit bilan qo'yilib, oshkora kalit bilan ochilgan raqamli imzoni shu axborotning raqamli izi (daydjesti) bilan taqqoslash. Verifikatsiya axborot chindan ham unda ko'rsatilgan sub'ektga tegishliligini va o'zgartirib qo'yilmaganligini isbotlashga imkon beradi.

Vulnerability - Axborot zaifligi. Axborotning uni pinxonaligi, butunligi yo qobilligiga putur yetkazuvchi ta'sirlarga dosh berolmaslik xossasi.

Адабиётлар:

1. Р.Х. Алимов, Б.Ю. Ходиев, К.А. Алимов, С.У. Усмонов, Б.А. Бегалов, Н.Р. Зайналов, А.А. Мусалиев, Ф. Файзиева, «Миллий иқтисодда ахборот тизимлари ва технологиялари», Ўқув қўлланма, Т. Шарқ, 2004 йил.
2. М.Т. Гафурова, Д.Ч. Дурсунов, В.И. Рапопорт, Б.Ю. Ходиев. Проектирование современнўх информационнўх технологий. Учебное пособие.-Тошкент, ТДИУ, 1994.-96 с.
3. Информационнўе системў в экономике: Учебник/Под ред. проф. В.В. Дика.-М.:Финансў и статистика,1996.-272 с.
4. Информатика: Учебник/Под ред. Н.В. Макаровой. -М.: Финансў и статистика, 1997.-768с.
5. /уломов С.С. ва бошқ. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
6. /уломов С.С., Шермуҳаммедов А.Т., Бегалов Б.А.; С.С. /уломовнинг умумий таҳрири остида. —Т.: «Ўзбекистон», 1999. —528 б.
7. Козўрев А.А. Информационнўе технологии в экономике и управлении: Учебник, 2-е изд. .—СПб.: Изд-во Михайлова В.А., 2001. —360 с.
8. Ходиев Б.Ю., Мусалиев А.А., Бегалов Б.А. Введение в информационнўе системў и технологии. Учебное пособие /Под ред. акад. С.С. Гулямова. — Т.:ТГЭУ, 2002. —156 с.
9. Шафрин Ю.А. Информационнўе технологии. —М.: Лаборатория Базовўх Знаний, 1998. —704 с.
10. Петров Б.Н. Информационнўе системў. – СПб.: Питер, 2003. – 688с.:ил.

+ўшимча адабиётлар:

1. Денинг В., Эссиг Г., Маас С. Диалоговўе системў "Человек-ЭВМ". Адаптация к требованиям пользователя: Пер. с англ.- М.: Мир,1984.-112 с.,ил.
2. Довгялло А.М. Диалог пользователя с ЭВМ: Основў проектирования и реализации.-Киев:Наукова думка,1981
3. Коутс Р., Влейминк И. Интерфейс "человек-компьютер": Пер. с англ.-М.: Мир, 1990.-501 с.
4. Гафурова М.Т., Дадабаева Р.А. Персонал компьютерларнинг программ системалари.- Тошкент, ТДИУ, 1992.-100 бет.
5. Р.Персон Windows 95 в подлиннике: Пер. с англ.-СПб: BHV- Санкт-Петербург, 1996.-736 с.
6. А.И. Марченко, В.П. Пасько Word 7.0 для Windows 95: К.: Торгово-издательское бюро BHX, 1996.-464 с.
7. Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникацион технологияларини жорий этиш тў\рисида \\Хабарнома. – 2002, №2.
8. Гафурова М.Т., Дурсунов Д.Ч. Стандартизация оформления дипломнўх, курсовўх проектов и лабораторнўх работ: Методические указания.—Т.: ТДИУ,1988.—80 б.

9. Острейковский В.А. Информатика. М.: Вўсшая школа, 1999.
10. IBM PC для пользователя. Фигурнов В.Э. М.: Инфра, 2001.
11. Рахмонқулова С.И. Шахсий компьютерда ишлаш. Тошкент - “Шарк”, 1998.
12. Джой Крейнак. Интернет. Санкт-Петербург, Питер, 1999.
13. www.piter.com
14. www.intuit.ru
15. www.it-study.ru
16. www.informatika.ru
17. www.edu.uz
18. www.ref.uz