12- мавзу. Тиббиёт тизимларининг ахборот хавфсизлигини таъминлаш. Хулоса.

Режа:

1. **Ахборот хавсизлигида химоялаш усуллари.**
2. **Идентификациялаш ва аутентификациялаш усуллари.**
3. **Компьютер вируслари ва улардан ҳимояланиш.**
4. **Электрон рақамли имзо билан ишлаш ва унинг ахамияти**

Ахборот хавсизлигида химоялаш усуллари.

Компьютер тармоқларида ахборотни ҳимоялаш деб фойдаланувчиларни рухсатсиз тармоқ, элементлари ва заҳираларига эгалик қилишни ман этишдаги техник, дастурий ва криптографик усул ва воситалар, ҳамда ташкилий тадбирларга айтилади.

Физикавий техник воситалар — бу автоном ҳолда ишлайдиган қурилма ва тизимлардир. Масалан, оддий эшик қулфлари, деразада ўрнатилган темир панжаралар, қўриқлаш электр ускуналари физикавий техник воситаларга киради.

Дастурий воситалар – бу ахборотларни ҳимоялаш функцияларини бажариш учун мўлжалланган махсус дастурий таъминотдир.

Ахборотларни ҳимоялашда биринчи навбатда энг кенг қўлланилган дастурий воситалар ҳозирги кунда иккинчи даражали ҳимоя воситаси ҳисобланади. Бунга мисол сифатида пароль тизимини келтириш мумкин.

Ташкилий ҳимоялаш воситалари — бу талекоммуникация ускуналарининг яратилиши ва қўлланиши жараёнида қабўл қилинган ташкилий-техникавий ва ташкилий-хуқуқий тадбирлардир. Бунга бевосита мисол сифатида қуйидаги жараёнларни келтириш мумкин: биноларнинг қурилиши, тизимни лойиҳалаш, қурилмаларни ўрнатиш, текшириш ва ишга тушириш.

Ахлоқий ва одобий ҳимоялаш воситалари — бу ҳисоблаш техникасини ривожланиши оқибатида пайдо бўладиган тартиб ва келишувлардир. Ушбу тартиблар қонун даражасида бўлмасада, уни тан олмаслик фойдаланувчиларни обрўсига зиён етказиши мумкин.

Қонуний ҳимоялаш воситалари — бу давлат томонидан ишлаб чиқилган хуқуқий ҳужжатлар саналади. Улар бсвосита ахборотлардан фойдаланиш, қайта ишлаш ва узатишни тартиблаштиради ва ушбу қоидаларни бузувчиларнинг масъулиятларини аниқлаб беради.

Масалан, Ўзбекистон Республикаси Марказий банки томонидан ишлаб чиқилган қоидаларида ахборотни ҳимоялаш гурухларини ташкил қилиш,

уларнинг ваколатлари, мажбуриятлари ва жавобгарликлари аниқ ёритиб берилган.

Ҳозирги кунда маълумотларни рухсатсиз четга чиқиб кетиш йўллари қуйидагилардан иборат:

- электрон нурларни четдан туриб ўқиб олиш;
- алоқа кабелларини электромагнит тўлқинлар билан нурлатиш;
- яширин тинглаш қурилмаларини қўллаш;
- масофадан расмга тушириш;
- принтердан чикадиган акустик тўлқинларни ўқиб олиш;
- маълумот ташувчиларни ва ишлаб чиқариш чиқиндиларини ўғирлаш;
- тизим хотирасида сақланиб қолган маълумотларни ўқиб олиш;
- ҳимояни енгиб маълумотларни нусхалаш;
- қайд қилинган фойдаланувчи ниқобида тизимга кирши;
- дастурий тузоқларни қўллаш;
- дастурлаш тиллари ва операцион тизимларнинг камчиликларидан фойлаланиш;
- дастурларда махсус белгиланган шароитларда ишга тушиши мумкин бўлган қисм дастурларнинг мавжуд бўлиши;
- алоқа ва аппаратларга ноқонуний уланиш;
- ҳимоялаш воситаларини қасддан ишдан чиқариш;
- компьютер вирусларини тизимга киритиш ва ундан фойдаланиш.

Ушбу йўллардан деярли барчасининг олдини олиш мумкин, лекин компьютер вирусларидан ҳозиргача қониқарли ҳимоя воситалари ишлаб чиқилмаган.

Бевосита тармоқ бўйича узатиладиган маълумотларни ҳимоялаш мақсадида қуйидаги тадбирларни бажариш лозим бўлади:

- узатиладиган маълумотларни очиб ўқишдан сақланиш;

- узатиладиган маълумотларни таҳлил қилищдан сақланиш;

- узатиладиган маълумотларни ўзгартиришга йўл қўймаслик ва ўзгартиришга уринишларни аниқлаш;

- маълумотларни узатиш мақсадида қўлланиладиган дастурий узилишларни аниқлашга йўл қўймаслик;

- фирибгар уланишларнинг олдини олиш.

Ушбу тадбирларни амалга оширишда асосан криптографик усуллар қўлланилади.

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

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

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

Стенографиянинг криптографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни ҳимоялаш 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.

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. Бошқа томондан, ахборот-коммуникациялар технологияларининг жадал ривожланиши ушбу ахборотни ҳимоялашнинг янги усулларини жорий қилиш имкониятлари билан таъминлаяпти ва албатта, бу жараённинг кучли катализатори бўлиб умумфойдаланиладиган Internet компьютер тармоғининг жуда кучли ривожланиши ҳисобланади.

Ҳозирги вақтда ахборотни ҳимоялаш энг кўп қўлланилаётган соҳабу — криптографик усуллардир. Лекин, бу йўлда компьютер вируслари, «мантиқий бомба»лар каби ахборотий қуролларнинг криптовоситаларни бузадиган таъсирига боғлиқ кўп ечилмаган муаммолар мавжуд. Бошқа 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 бўлар эди, чунки, бу ҳолда ахборотни ҳимоялаш усулларининг заиф томонларини йўқотиш мумкин.

Криптография нуқтаи – назаридан шифр — бу калит демакдир ва очиқ маълумотлар тўпламини ёпиқ (шифрланган) маълумотларга ўзгартириш криптография ўзгартиришлар алгоритмлари мажмуаси ҳисобланади.

Калит — криптография ўзгартиришлар алгоритмининг баъзи-бир параметрларининг махфий ҳолати бўлиб, барча алгоритмлардан ягона

вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий кўрсаткич бўлиб **криптомустаҳкамлик** ҳисобланади.

Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қуйилади:

- етарли даражада криптомустахкамлик;
- шифрлаш ва қайтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;
- шифрлашдаги кичик хатоларга таьсирчан бўлмаслиги.
- Ушбу талабларга қуйидаги тизимлар жавоб беради:
- ўринларини алмаштириш;
- алмаштириш;
- гаммалаштириш;
- аналитик ўзгартириш.

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

Алмаштириш шифрлаш усули бўйича бошлангич матн белгилари фойдаланилаётган ёки бошқа бир алифбо белгиларига алмаштирилали.

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

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

Ўринларни алмаштириш усуллари

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

— шифрловчи жадвал;

— сеҳрли квадрат.

Шифрловчи жадвал усулида калит сифатида қуйидагилар қўлланилади:

— жадвал ўлчовлари;

— сўз ёки сўзлар кетма-кетлиги;

— жадвал таркиби хусусиятлари.

Мисол.

Қуйидаги матн берилган бўлсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун бўйича 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 ўлчовли жадвал ташкил қилинади.

Энди шифрланган матн қаторлар бўйича аниқланади, яъни ўзимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал ўлчовлари хизмат қилади.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал бўйича сонлар йиғиндиси 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 ўлчовли сеҳрли квадратни оламиз, бу ерда сонларнинг 880 та хар хил комбинацияси мавжуд. Қуйидагича иш юритамиз:

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

Бошлангичматнсифатидақуйидагиматнниоламиз:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланганматнжадвалэлементларинисатрларбўйичаўқишнатижасида ташкилтопади:

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 kва силжиш билан аниқланади. Юлий Цезар бевосита k = 3 бўлганда ушбу усулдан фойлаланган.

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

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

Y	→	**B**
Z	→	**C**

Мисол.

Матн сифатида KOMPUTER сўзини оладиган бўлсак, Цезар усули натижасида қуйидаги шифрланган ёзув ҳосил бўлади: NRPSBXHU.

Цезар усулининг камчилиги бу бир хил ҳарфларнинг ўзнавбатида, бир хил ҳарфларга алмашишидир.

Ҳозирги вақтда компьютер тармоқларида тижорат ахборотлари билан алмашишда учта асосий алгоритмлар, яъни DES, CLIPPER ва PGP алгоритмлари қўлланилмоқда. DES ва CLIPPER алгоритмлари интеграл схемаларда амалга оширилади. DES алгоритмининг криптомустаҳкамлигини қуйидаги мисол орқали хам баҳолаш мумкин: 10 млн. АҚШ доллари харажат қилинганда DES шифрлаш очиш учун 21 минут, 100 млн, АҚШ доллари харажат килинганда эса 2 минут сарфланади. CLIPPER тизими SKIPJACK шифрлаш алгоритмини ўз ичига олади ва бу алгоритм DES алгоритмидан 16 млн, марта кучлирокдир.

PGP алгоритми эса 1991 йилда Филипп Циммерман (АҚШ) томонидан ёзилган ва электрон почта орқали кузатиладиган хабарларни шифрлаш учун ишлатиладиган PGP дастурлар пакети ёрдамида амалга оширилади, FGP дастурий воситалари Internet тармоғида электрон почта орқали ахборот жўнатувчи фойдаланувчилар томонидан шифрлаш мақсадида кенг фойдаланилмоқда.

PGP (Pretty Good Privacy) криптография дастурининг алгоритми калитли, очиқ ва ёпиқ бўлади.

Очиқ калит қуйидагича кўринишни олиши мумкин:

EDF2lpI4------BEIN PGP PUBLIC KEY BLOCK----------
Version: 2.6.3i
mQCNAzF1IgwAAAEEAnOvroJEWEq6npCLZTqssS5EscVUPV
aRu4ePLiDjUz6U7aQr
Wk45dIxg0797PFNvPcMRzQZeTxY10ftlMHL/6ZF9wcx64jy
LH40tE2DOG9yqwKAn
yUDFpgRmoL3pbxXZx91O0uuzlkAz+xU6OwGx/EBKYOKPTTt
DzSL0AQxLTyGZAAUR
tClCb21gU3dbhNvbiA8cmpzdFuQHNIYXR0bGUtd2Vid29ya
3MuY29PokA1QMF
h53aEsqJyQEB6JcD/RPxg6gtfHFi0Qiaf5yaH0YGEVoxcd-
FyZXr/ITz

rgztNXRUi0qU2MDEmh2RoEcDsIfGVZHSRpkCg8iS+35&Az
9c2S+q5vQxOsZJz72B
LZUFJ72fbC3fZZD9X9lMsJH+xxX9cDx92xm1IgIMT25S0x
2o/uBAd33KpEI6g6xv
----END PGP PUBLIC KEY BLOCK----

Ушбу очиқ калит бевосита Web саҳифаларда ёки электрон почта орқали очиқчасига юборилиши мумкин.Очиқ калитдан фойдаланган жўнатилган шифрли ахборотни ахборот юборилган манзил эгасидан бошқа шахс ўқий олмайди. PGP орқали шифрланган ахборотларни очиш учун, суперкомпьютерлар ишлатилганда бир аср ҳам камлик қилиши мумкин.

Булардан ташқари, ахборотларни тасвирларда ва товушлар да яшириш дастурлари ҳам мавжуд. Масалан, S-toots дастури ахборотларни BMP, GIF, WAV кенгайтмали файлларда сақлаш учун қўлланилади.

Кундалик жараёнда фойдаланувчилар офис дастурлари ва архиваторларни қўллаб келишади. Архиваторлар, масалан PkZip дастурида маълумотларни пароль ёрдамида шифрлаш мумкин. Ушбу файлларни очганда иккита, яъни луғатли ва тўғридан-тўғри усулдан фойдаланишади. Луғатли усулда бевосита махсус файлдан сўзлар пароль ўрнига қўйиб текширилади, тўғридан-тўғри усулда эса бевосита белгилар комбинацияси тузилиб, пароль ўрнига қўйиб текишрилади.

Офис дастурлари (Word, Excel, Access) орқали ҳимоялаш умуман таклиф этилмайди. Бу борада мавжуд дастурлар Internet да тўсиқсиз тарқатилади.

Идентификациялаш ва аутентификациялаш усуллари

Компьютер тизимида рўйхатга олинган ҳар бир субъект (фойдаланувчи ёки фойдаланувчи номидан ҳаракатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боғлиқ.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект индентификатори деб юритилади. Агар фойдаланувчи тармоқда рўйхатга олинган индентификаторга эга бўлса у легал (қонуний), акс ҳолда легал бўлмаган (ноқонуний) фойдаланувчи ҳисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) бўйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган

функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) – маълум қилинган фойдаланувчи, жараён ёки қурилманинг ҳақиқий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки қурилма) ҳақиқатан айнан ўзи эканлигига ишонч хосил қилишига имкон беради. Аутентификация ўтқазишда текширувчи тараф текширилувчи тарафнинг хақиқий эканлигига ишонч ҳосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол қатнашади.Одатда фойдаланувчи тизимга ўз хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчи-ларнинг) ҳақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлиқ. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

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

Маъмурлаш (Accounting) – фойдаланувчининг тармоқдаги ҳаракатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини қайд этиш. Ушбу ҳисобот ахбороти хавфсизлик нуқтаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, тахлиллаш ва уларга мос реакция кўрсатиш учун жуда муҳимдир.

Аутентификация протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

- ўзаро аутентификациянинг мавжудлиги. Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёқлама аутентификациянинг зарурлигини акс эттиради;
- ҳисоблаш самарадорлиги. Протоколни бажаришда зарур бўлган амаллар сони;

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

- учинчи тарафнинг мавжудлиги. Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;

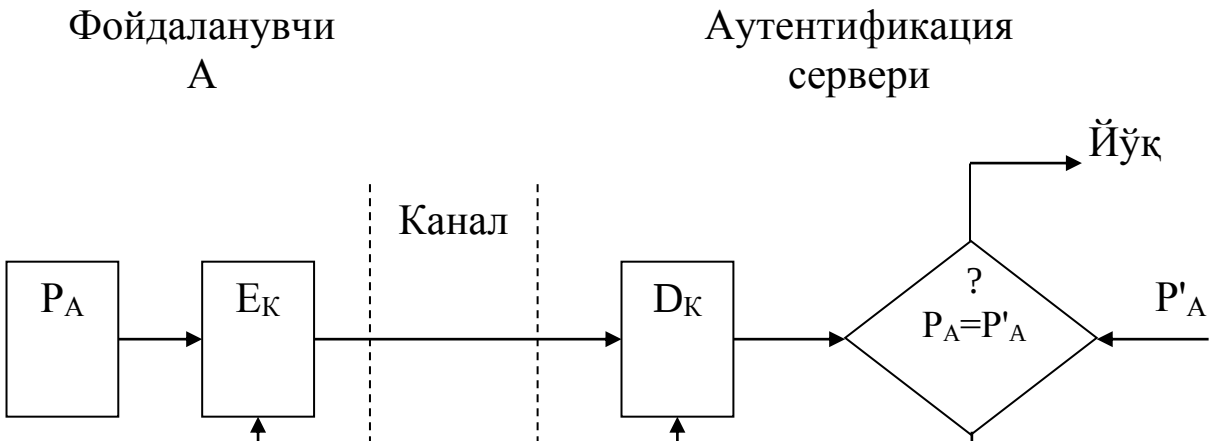
- хавфсизлик кафолати асоси. Мисол сифатида нуллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;

- сирни сақлаш. Жиддий калитли ахборотни сақлаш усули кўзда тутилади.

Пароллар асосида аутентификациялаш. Аутентификациянинг кенг тарқалган схемаларидан бири оддий аутентификациялаш бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган ҳуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган ҳолда оддий аутентификациялаш схемаси 11.1.–расмда келтирилган.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни ҳимоялаш учун уни ҳимояланмаган канал орқали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва расшифровка қилиш $D_к$ воситалари киритилган.



Бу воситалар бўлинувчи махфий калит К орқали бошқарилади.

Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат $P_A^{'}$ ни таққослашга асосланган. Агар P_Aва $P_A^{'}$ қийматлар мос келса, парол P_A ҳақиқий, фойдаланувчи А эса қонуний ҳисобланади.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.
3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология SecurityDynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, хусусан CiscoSystems компаниясининг серверларида амалга оширилган.

Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вақтнинг маълум оралиғидан сўнг генерациялаш алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- ҳар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг аппарат калитида сақланувчи ноёб 64-битли сондан иборат махфий калит;
- жорий вақт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация номери PINни киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат калити дисплейида аксланувчи тасодифий соннинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вақт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

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

Ушбу муаммони ҳал этишда SecurityDynamics компанияси қуйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аниқ ўлчанади. Четлашишнинг бу қиймати сервер алгоритми параметри сифатида ҳисобга олинади;
- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият туғилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боғлиқ. Аппарат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида ҳақиқий парол ҳисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи ҳисобланади.

Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант – «сўров-жавоб» схемаси бўйича аутентификациялаш. Фойдаланувчи тармоқдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва сервернинг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган кўринишда серверга

қайтарилади. Сервер ҳам ўз навбатида ўша DES алгоритми ва серверниг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброқ.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки набори бўлиб, ҳар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантига биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, ҳар бир жуфт фақат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг қуйидаги вариантлари мавжуд:

- ўзгартирилувчи бир мартали пароллар кетма-кетлиги. Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади;
- бир томонлама функцияга асосланган пароллар кетма-кетлиги. Ушбу усулнинг моҳиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машҳур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал ҳисобланади.

Кенг тарқалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internet да стандартлаштирилган S/Key (RFC1760) протоколидир. Ушбу протокол масофадаги фойдаланувчиларнинг ҳақиқийлигини текширишни талаб этувчи кўпгина тизимларда, хусусан, Cisco компаниясининг TACACS+тизимида амалга оширилган.

Компьютер вируслари ва улардан ҳимояланиш

Компьютер вируси нима?

Вируслардан ҳимояланиш ҳар бир компьютер фойдаланувчиси олдида турган асосий муаммолардан бири ҳисобланади. Компьютер вирусларидан келадиган зараралар миллиардлаб долларлар билан белгиланади.

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

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

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

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

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

- баъзи дастурлар ишлашдан тўхтайдилар ёки нотўғри ишлайди;
- экранга бегона хабар ёки белгилар чиқади;
- компьютернинг ишлаш тезлиги секинлашади;
- баъзи бир файллар бузилиб қолади ва ҳ.к.

Бу вақтга келиб, қоидага кўра, фойдаланувчи ишлаётган етарлича кўп (ёки хатто кўпчилик) дастурлар вируслар билан зарарланган, баъзи бир файл ёки дисклар эса ишдан чиққан ҳисобланади. Бундан ташқари, фойдаланувчи

компьютеридаги зарарланган дастурлар дискеталар ёрдамида ёки локал тармоқ бўйича фойдаланувчи ҳамкасблари ва ўртоқларининг компьютерига ўтиб кетган бўлиши мумкин .

Вирусларнинг баъзи бир кўринишлари ўзларини янада хавфлироқ кириб тушадилар. Улар бошланишда катта миқдордаги дастурларни ёки дискларни билдирмасдан зарарлантирадилар, кейин эса жиддий шикастланишларини келтириб чиқаради, масалан, компьютердаги бутун қаттиқ дискни форматлайди. Дастур – вирус сезиларсиз бўлиши учун у катта бўлмаслиги керак. Шунинг учун, қоидага кўра, вируслар етарлича юқори малакали дастурловчилар томонидан Ассемблер тилида ёзилади.

Компьютер вирусларини пайдо бўлиши ва тарқатилиши сабаблари, бир томондан, инсон шаҳсиятининг руҳиятида ва унинг ёмон хислатларида яширинади (ҳаваслар, қасос олишлар, тан олинмаган ижодкорларнинг мансабпарастлиги, ўз қобилиятларини конструктив қўллаш имконияти йўқлиги), иккинчи томондан эса, ҳимоя қилишнинг аппарат воситаларини ва шахсий компьютернинг операцион тизими томонидан қарши ҳаракатларнинг йўқлиги билан боғлиқдир.

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

Зарарланган диск бу юкланиш секторида дастур – вирус жойлашган дискдир.

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

Зарарланган дастур, бу унга тадбиқ қилинган дастур – вирусни ўз ичига олган дастурдир. Компьютер вируси билан зарарланишда ўз вақтида уни пайқаш жуда муҳимдир. Бунинг учун вирусларни пайдо бўлишининг асосий белгилари тўғрисида билимларга эга бўлиш керак. Уларга қуйидагилар тегишли бўлиши мумкин:

- олдин муваффақиятли ишлаган дастурларнинг ишлашини тўхтатиш ёки нотўғри ишлаши;
- компьютернинг секин ишлаши;
- операцион тизимни юклашни имкони йўқлиги;
- файл ва каталогларни йўқолиб қолиши ёки уларнинг мазмунини бузилиши;
- файлларни ўзгартирилганлик санаси ва вақтининг ўзгариши;
- дискда файллар сони бехосдан жуда ошиб кетиши;
- бўш тезкор хотира ўлчамининг жиддий камайиши;
- экранга кўзда тутилмаган хабарларни ёки тасвирларни чиқариш;
- кўзда тутилмаган товушли хабарларни бериш;
- компьютер ишлашда тез-тез бўладиган осилиб олишлар ва бузилишлар.

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

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

Таъкидлаш лозимки, дастур ва ҳужжатларнинг матнлари, маълумотлар базасининг ахборотли файллари, жадвалли процессор жадваллари ва бошқа шунга ўхшаш файллар вирус билан зарарланиши мумкин эмас, бу файлларни вируслар бузиши мумкин.

Вирус билан «зарарланиши» мумкин бўлган файлларнинг турлари қуйидагилардир:

1. Бажариладиган файллар, яъни .COM ва .EXE кенгайтмали

файллар ҳамда бошқа дастурлар бажарилганда юкланадиган оверлокли (такрорланадиган) файллардир. Зарарланган бажариладиган файллардаги вирус шу вирус жойлашган дастур ишга туширилганда ўзининг ишини бошлайди. Вирус билан зарарланишнинг энг хавфлиси DOS буйруқли процессорини COMMAND.COM дастурини зарарланишидир, чунки бу вирус DOSнинг исталган буйруғи бажарилганда ишлайди ва исталган бажариладиган дастур зарарланади (агар вирус уни зарарлантира олса).

Антивирус дастурлари

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

Детекторлар – вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича оператив хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлай олмаслиги детекторларнинг камчилиги ҳисобланади.

Фаглар – ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги ҳолатига қайтаради.

Вакциналар - юқоридагилардан фарқли бўлиб, у ҳимояланаётган дастурга ўрнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис, ушбу антивирус дастурлар кенг тарқалмаган.

Прививка - файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар прививка қилинган файлга ёпишмайди.

Фильтрлар – қўриқловчи дастурлар кўринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақида 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 ҳакида хабар беради.

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

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

Бу ҳаракатлар қуйидагича бўлиши мумкин :

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

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

Вирусларга қарши чора-тадбирлар

Компьютерни вируслар билан зарарланишидан ва ахборотларни ишончли сақлашини таъминлаш учун қуйидаги қоидаларга амал қилиш лозим:

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

Компьютер вирусларига қарши курашнинг қуйидаги турлари мавжуд:

- компьютер вируслари компьютерга кирганда файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компьютерга парол билан кириш, диск юритувчиларнинг ёпиқ туриши;
- дискларни ёзишдан ҳимоялаш;
- лицензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- киритилаётган дастурларни вирусларнинг мавжудлигига текшириш;
- антивирус дастурларидан кенг фойдаланиш;
- даврий равишда компьютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Вирусларни аниқлаш ва даволаш усуллари

Ҳозирги кунда компьютер вирусларига қарши курашга ихтисослашган компаниялар вужудга келган. Улар ҳар кун, ҳар соат мижозларнинг компьютеридаги мавжуд вирусларни топиб, уларни йўқ қиладиган антивирус дастурларини яратадилар. Ҳозирги кунда компьютер вирусларига қарши курашувчи антивирус дастурларидан энг асосийлари **KasperskyAnti-Virus (AVP) ScriptChecker, NortonAntivirus, DrWeb, Adinf, AVP**лар ҳисобланади. **KasperskyAnti-Virus**дастури бугунги кунда компьютер вирусларининг 100000 дан ортиқ турини аниқлайди ва даволайди.

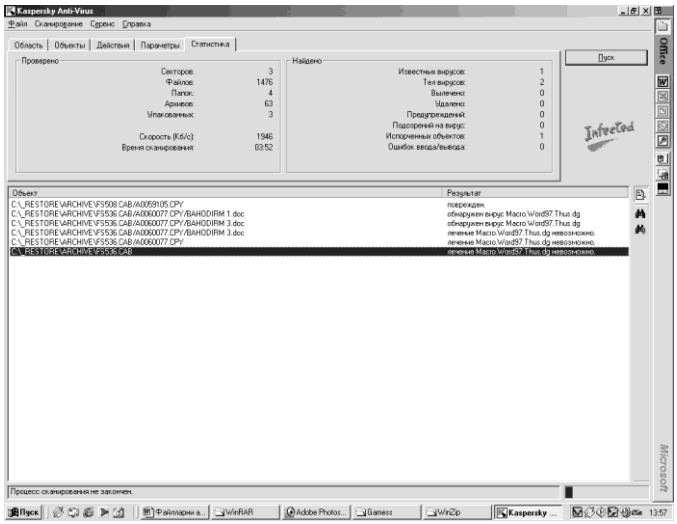
KasperskyAnti-Virus (AVP) ScriptCheckerдастурини ишга тушириш қуйидагича амалга оширилади:

ПУСК →Программы→KasperskyAnti-Virus→AVPСканер.

KasperskyAnti-Virus (AVP) дастурини ишга тушириш.

Дастур ишга тушгандан сўнг, экранда унинг ишчи ойнаси пайдо бўлади.

Агар диск хотирасида вирус мавжуд бўлса, у ҳолда зарарланган файллар рўйхати ишчи ойнада пайдо бўлади(3-расм). Ишчи ойнанинг **Объект** бўлимида зарарланган файллар номлари, **Результат** бўлимида эса вирус турлари кўрсатилади.



Компьютер вирусларидан ҳимоя қилиш усуллари

Компьютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

– вирусларнинг кириб келишини бартараф этиш;

– агар вирус барибир компьютерга кирган бўлса, вирус ҳужумини бартараф этиш;

– агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф этиш.

Ҳимоя қилишни амалга оширишнинг учта усули мавжуддир:

– ҳимоя қилишнинг дастурли усуллари;

– ҳимоя қилишнинг аппаратли усуллари;

– ҳимоя қилишнинг ташкилий усуллари.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: «касаликни даволагандан кўра унинг олдини олган яхшироқ». Афсуски, айнан у энг бузувчи оқибатларни келтириб чиқаради. Компьютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустаҳкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум, бу муҳим маълумотларни йўқотишни ягона бўлмаган ҳаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операцион тизимни ишдан чиқариш мумкин ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқатсиз қилиб қўйиш қобилиятига эгадирлар. Ўғирлаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда компьютерни йўқотиш эҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда «охиридан» бошлаш керак – исталган таъсирни, у вирус ҳужуми, хонада ўғирлик ёки қаттиқ дискни физик ишдан чиқиш

бўлишидан қатъий назар, бузувчи оқибатларини бартараф этишдан бошлаш керак.

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

Электрон рақамли имзо билан ишлаш ва унинг ахамияти

Ушбу амалий ишида қабул қилиб олинган маьлумотларнинг ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласини, яьни маьлумотлар аутентификацияси масаласининг моҳияти ҳақида маьлумотларга эга буламиз.Бу масала маълумотларни узатишда муҳим аҳамиятга эга саналади.Бу жараён ҳозирда **электрон рақамли имзо** деб аталади.

Ҳужжатлардаги қуйилган шахсий имзоларни соҳталаштириш нисбатан мураккаб булиб, шахсий имзоларнинг муаллифларини ҳозирги замонавий илғор криминалистика услубларидан фойдаланиш орқали аниқлаш мумкин. Аммо электрон рақамли имзо хусусиятлари бундан фарқли булиб, иккилик саноқ системаси хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ.

Шундан келиб чиқиб ҳозирда ЭРИ ни ахборот хавфсизлиги соҳасида қўллаш муҳим аҳамиятга эга саналади. Бунинг натижаси ўлароқ ҳозирда йетакчи давлатлар ўзининг шахсий ЭРИни яратдилар, шу жумладан Ўзбекистон ҳам ўзининг ЭРИси, УзДСт 1092:2005ни яратди.Бунда ассиметрик шифрлаш алгоритмидан фойдаланилган. Амалий иши икки қисмдан иборат бўлиб, биринчи қисмда элестрон рақамли имзо ҳақида маълумот, унинг ишлаш жараёни, унга фойдаланилган алгоритмлар таҳлили кўриб ўтилган. Иккинчи қисмда эса, ЭРИ дастурининг дастурий модулининг ишлаш жараёни кўрсатилган.

Электрон рақамли имзонинг ишлаш жараёни

Қабул қилиб олинган маьлумотларнинг ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласини, яьни маьлумотлар аутентификацияси масаласининг моҳияти ҳақида туҳталамиз.

Очиқ калитли криптографик тизимлар қанчалик қулай ва криптобардошли булмасин, аутентификация масаласининг тула йечилишига жавоб бера олмайди. Шунинг учун аутентификация услуби ва воситалари криптографик алгоритмлар билан биргаликда комплекс ҳолда қулланилиши талаб этилади.

Қуйида иккита (А) ва (Б) фойдаланувчиларнинг алоқа муносабатларида аутентификация тизими рақиб томоннинг уз мақсади ёлидаги қандай хатти-ҳаракатларидан ва криптотизим фойдаланувчиларининг фойдаланиш протоколини узаро бузилишлардан сақлаши кераклигини курсатувчи ҳолатлар куриб чиқилади.

Рад этиш (ренегацтво)- Фойдаланувчи (А) фойдаланувчи (Б) га ҳақиқатан ҳам маьлумот жунатган булиб, узатилган маьлумотни рад этиши мумкин.Бундай қоида бузилишининг (тартибсизликнинг) олдини олиш мақсдида электрон (рақамли) имзодан фойдаланилади.

Модификациялаш (узгартириш) -Фойдаланувчи (Б) қабул қилиб олинган маьлумотни узгартириб, шу узгартирилган маьлумотни фойдаланувчи (А) юборди, деб таькидлайди (даьво қилади).

Соҳталаштириш -Фойдаланувчи (Б)нинг узи маьлумот тайёрлаб, бу соҳта маьлумотни фойдаланувчи (А) юборди деб даьво қилади.

Фаол модификациялаш (узгартириш) - (А) ва (Б) фойдаланувчиларнинг узаро алоқа тармоғига учинчи бир (В) фойдаланувчи ноқонуний тарзда боғланиб, уларнинг узаро узатаётган маьлумотларини узгартирган ҳолда деярли узлуксиз узатиб туради.

Ниқоблаш (имитациялаш) - Учинчи фодаланувчи (V) фойдаланувчи (В)га фойдаланувчи (А) Номидан маьлумот жунатади.

Юқорида санаб утилган: модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш каби алоқа тизими қоидаларининг бузилишини

олдини олиш мақсадида рақамли сигнатурадан - рақамли имзо ва узатиладиган маьлумотнинг бирор қисмини тула уз ичига олувчи рақамли шифрматндан иборат булган маьлумотдан фойдаланилади.

Такрорлаш - Фойдаланувчи (В) фойдаланувчи (А) томонидан фойдаланувчи (Б)га жунатилган маьлумотни такроран (Б)га жунатади. Бундай ноқонуний хатти-ҳаракат алоқа усулидан банклар тармоқларида электирон ҳисоб-китоб тизимидан фойдаланишда ноқонунийлик билан узгалар пулларини талон-тарож қилишда фойдаланилади. Ана шундай ноқонуний усуллардан муҳофазаланиш учун қуйидаги чора - тадбирлари курилади.

- имитациялашга бардошлилик - имитабардошлилик;
- криптотизимга кираётган маьлумотларни муҳофаза мақсадларидан келиб чиқиб тартиблаш.
- Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таьминлайди, яьни: махфий калит фақат фойдаланувчи (А)нинг узигагина маьлум булса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маьлумотни фақат (А) томонидан жунатилганлигини рад этиб булмайди;
- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;
- алоқа тизимидан фойдаланувчиларнинг узаро боғлиқ ҳолда иш юритиши муносабатидаги куплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

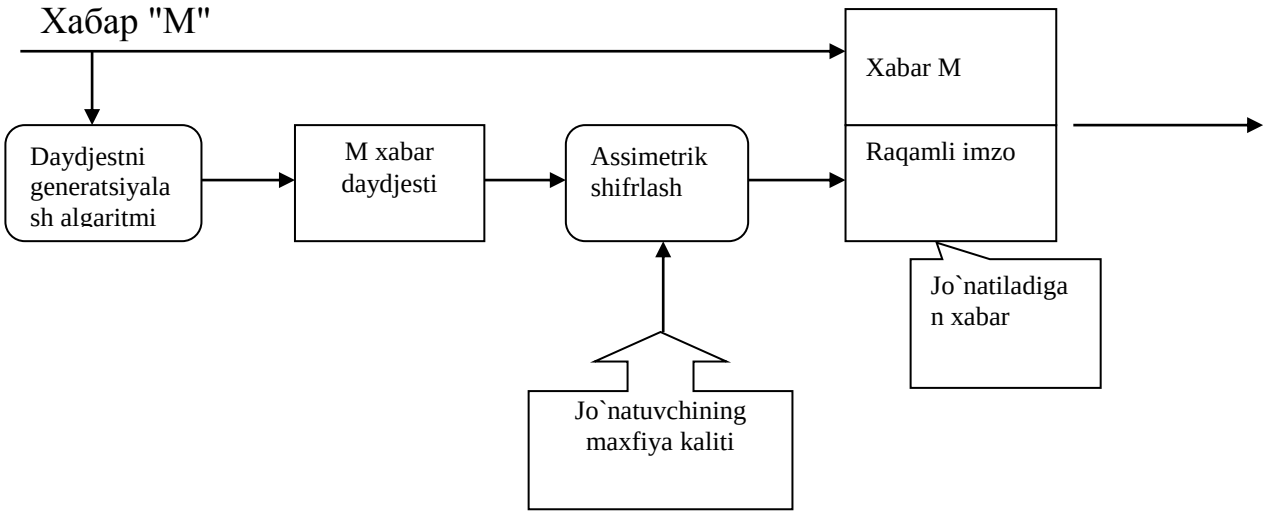
Куп ҳолларда узтилаётган маьлумотларни шифрлашга ҳожат булмай, уни электрон рақамли имзо билан тасдиқлаш керак булади. Бундай ҳолатларда очиқ матн жунатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жунатилади. Маьлумотни қабул

қилиб олган томон жунатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

Рақамли имзони шакллантириш муолажаси

Ушбу муолажани тайёрлаш босқичида хабар жунатувчи абонентА иккита калитни генерациялайди: маҳфий калитk_A. ва очиқ калит K_A. Очиқ калитK_A унинг жуфти булган махфий калити k_A ҳисоблаш орқали олинади.Очиқ калит K_A тармоқнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жунатувчиА аввало имзо чекилувчи матн M нинг хеш функсияси L(M) қийматини ҳисоблайди (1-расм). Хеш-функсия имзо чекилувчи дастлабки матн"М"ни дайджест "м"га зичлаштиришга хизмат қилади. Дайджест М-бутун матн"М" ни характерловчи битларнинг белгиланган катта булмаган сонидан иборат нисбатанқисқа сондир. Сунгра жунатувчиА узининг маҳфий калитикАбилан дайджест "м" ни шифрлайди. Натижада олинган сонлар жуфти берилган "М"матн учун рақамли имзоҳисобланади.Хабар "М" рақамли имзо билан биргаликда қабул қилувчининг адресига юборилади.



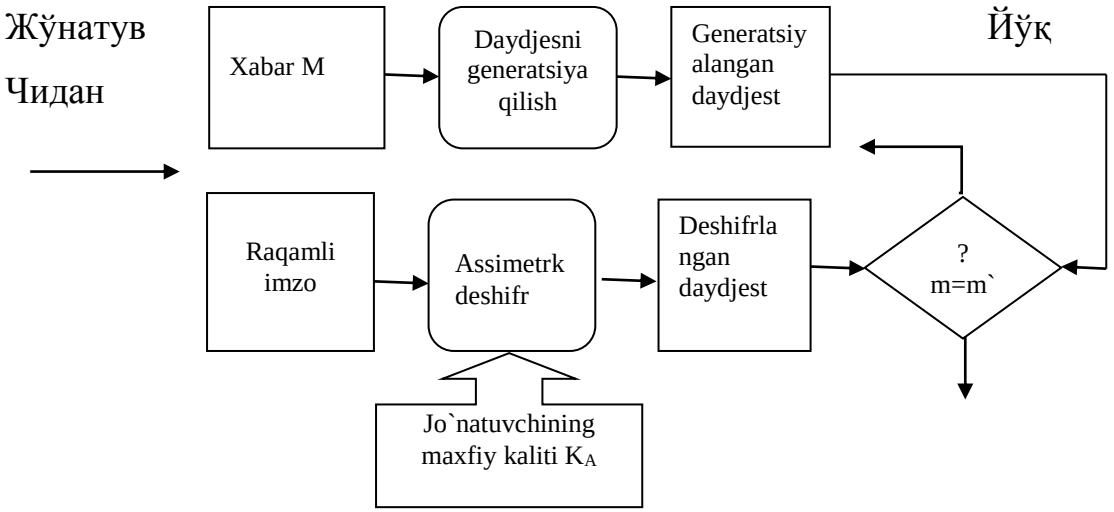
Электрон рақамли имзони шакллантириш схемаси

Рақамли имзони текшириш муолажаси

Тармоқ абонентлари олинган хабар "М"нинг рақамли имзосини ушбу хабарни жўнатувчининг очик калити КАёрдамида текширишлари мумкин .

Электрон рақамли имзони текширишда хабар"М" ни қабул қилувчи"Б" қабул қилинган дайджестни жўнатувчининг очиқ калити "КА" ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хеш функсия ҳ(М) ёрдамида қабул қилинган хабар "М" нинг дайджести М"м" ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест "м" ва "мь" мос келса рақамли имзо ҳақиқий ҳисобланади.Акс ҳолда имзо қалбакилаштирилган, ёки ахборот мазмуни ўзгартирилган бўлади.

Қабул қилинган хабар



Электрон рақамли имзони текшириш схемаси

Электрон рақамли имзо тизимининг принсипиал жиҳати фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги махфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир.

Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана;
- ушбу имзо калити таьсирининг тугаши муддати;

- ❖ файлга имзо чекувчи шахс хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);
- ❖ имзо чекувчининг индентификатори (очиқ калит номи);
- ❖ рақамли имзонинг ўзи.

ЭРИ ахборот коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани йечиш имконини беради:

- ❖ Электрон ҳужжат манбаининг ҳақиқийлигини аниқлаш;
- ❖ Электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;
- ❖ Электрон ҳужжатга рақамли имзо қўйган субьектни муаллифликдан бош тортмаслигини таьминлайди.

Интернет тармоғидан электрон хужжатлар алмашинуви асосида молиявий фаолият олиб боришда маьлумотлар алмашинувини ҳимоя қилиш ва электрон хужжатнинг юридик мақомини таьминлаш биринчи даражали аҳамият касб этади.

Электрон хужжатли маьлумот алмашинуви жараёнида ЭРИни қўллаш ҳар хил турдаги тўлов тизимлари (пластик карточкалар), банк тизимлари ва савдо соҳаларининг молиявий фаолиятини бошқаришда электрон хужжат алмашинуви тизимларининг ривожланиб бориши билан кенг тарқала бошлади.

Ҳозирда ЭРИ тизимини яратишнинг бир нечта йўналишлари мавжуд.Бу йўналишларни учта гуруҳга бўлиш мумкин:

1) очиқ калитли шифрлаш алгоритмларига асосланган;
2) симметрик шифрлаш алгоритмларига асосланган;
3) имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидир.

Амалда, учинчи турдаги имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидан кенг фойдаланилади.

Махсус ЭРИ алгоритмлари рақамли имзони ҳисоблаш ва имзони текшириш қисмларидан иборат. Рақамли имзони ҳисоблаш қисми имзо қўювчининг маҳфий калити ва имзоланиши керак бўлган ҳужжатнинг хеш қийматига боғлиқ бўлади.

НАЗОРАТ САВОЛЛАРИ

1.Криптография ҳақида асосий тушунчалар;
2.Ахборотларни криптографияли ҳимоялаш тамойиллари;
3.Симметрияли криптотизим асослари;
4.Ўринларни алмаштириш усуллари;
5.Идентификацияга таъриф;
6.Аутентификацияга таъриф;
7.Аутентификацияда паролнинг ўрни;
8.Паролдан фойдаланган ҳолда оддийаутентификациялаш.
9.Компьютер вируси нима?
10.Файл ва дискларда компьютер вируслари мавжудлигини текшириш.
11.Элементларни, узел(тугун) ва қурилмаларда компьютер вируслари мавжудлигини текшириш.
12.Вирусга қарши дастурлар билан танишиш.
13.Вирус нима ва унинг бажарадиган вазифаси?
14.Вируслар компьютерда қандай пайдо бўлади?
15.Вирусларнинг қандай турларини биласиз?
16.Компьютерда вируслар мавжудлиги қандай аниқланади?
17.Антивирус дастурларининг қандай турларини биласиз?
18.Компьютер вирусларидан ҳимояланишда эҳтиёткорлик чоралари нималардан иборат?
19.Электрон рақамли имзо хусусиятлари айтинг
20.Электрон рақамли имзонинг ишлаш жараёни.
21.Ноқонуний усуллардан муҳофазаланиш учун қандай чора - тадбирлари курилади?
22.ЭРИ тизимини яратишнинг қандай йўналишлари мавжуд?

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Антивирусные программы Москва 2000.
5. Н.Д. Угринович. Информатика и информатсионные технологии. М., Лаборатория базовўх знаний, 2002.
6. Интернет ресурслари.