ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА
ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

БУХОРО ОЗИҚ-ОВҚАТ ВА ЕНГИЛ САНОАТ
ТЕХНОЛОГИЯЛАРИ ИНСТИТУТИ

КАСБИЙ ТАЪЛИМ ФАКУЛЬТЕТИ
ИНФОРМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ

“ҲИМОЯГА РУХСАТ ЭТИЛДИ”
Факультет декани
_____Мусаев С.С.
“____”_____ 2009 йил

“Глобал компьютер тармоғида ахборотларни ҳимоялашнинг замонавий усуллари” мавзусидаги

БИТИРУВ МАЛАКАВИЙ ИШИ

ИЛМИЙ РАҲБАР: Т.ф.н. Юнусов Ғанишер Ғафирович
БАЖАРДИ: Турдиева Зебунисо Рахматовна

ТОШКЕНТ -2009

МУНДАРИЖА

IV Бўлим ТЕХНИКА ХАВФСИЗЛИГИ МУҲОФАЗАСИ

4.1. Компьютер хонасига қўйиладиган талаблар

4.2. Операторнинг ишчи жойини ташкил этиш

4.3. Иш жойининг ёритилганлиги

4.4. Стол ва стулларнинг жойлашувига бўлган талаблар

4.5. Монитордан инсоннинг кўзигача бўлган оптимал масофа

4.6. Компьютер билан ишлаганда чарчаш сабаблари

4.7. Электр токидан зарарланган инсонга биринчи ёрдам кўрсатиш

4.8. Ёнғин чиқиш сабаблари

ХУЛОСА

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

Ҳар ким бошқаларни сирини билишни ёқтиради,
лекин ўзининг сирини очилиб қолишидан қўрқади
Даниил Гранин

КИРИШ

Маълумотлар қадрини одамлар қадим замонларданоқ англаб етишган. Бекордан - бекорга хат ёзишиш дўст ва душманларнинг эътиборини ўзига жалб қилиб келмаган.

Ўша пайтлардан бошлаб ўта қизиқувчан кишилардан номаларни ҳимоя қилиш муаммоси пайдо бўлган. Қадимги кишилар бу муаммони ҳал қилишда турли хил усулларни қўллаб кўрганлар: улардан бири махфий ёзишув бўлиб, унда хат шундай ёзилганки бу сирдан воқиф одамдан ташқари ҳеч ким унинг маъносини тушунолмаган. Махфий ёзишув қадимги даврларда пайдо бўлгани тўғрисида турли далиллар мавжуд. Қадимги тарихий асрлар мобайнида ва яқин йилларгача махфий ёзишув санъати асосан жамиятнинг юқори табақаларидаа, ҳокимият деворларидан ташқарига чиқмай туриб элчи ва кузатувчиларга хат ёзиш учун ишлатилган. Атиги бир неча ўн йилликлар олдин ҳаммаси тубдан ўзгарди – маълумотлар мустақил молиявий (иқтисодий) қадрга эга бўлди ва оддий маҳсулот сингари кенг ёйила бошлади. Маълумотларни яратишади, сақлашади, кўчиришади, сотишади ва сотиб олишади, яъни ўғирлашади ва сохталаштиришади, демак уларни ҳимоялаш лозим.

Ҳозирги давр борган сари маълумотларга боғлиқ бўлиб бормоқда, қайси турдаги фаолият туридан қатъий назар унинг равнақ топиши рақобатчиларга нисбатан кўпроқ маълумотга эга бўлиш даражасига қараб қолди. Кўрсатилган таъсирнинг кучлироқ кўрингани сари маълумотлар оламида улардан нотўғри фойдаланишдан келадиган зарар даражаси кўпайиб бормоқда ва борган сари маълумотларни ҳимоя қилиш эҳтиёжи кучаймоқда.

Бир сўз билан айтганда, ахборотлар (маълумотлар) алмашинувининг қатъий эҳтиёжининг пайдо бўлгани маълумотларни ҳимоя қилиш воситалари саноатининг вужудга келишига олиб келди.

Замон тараққий этган сари жамиятда ахборотга бўлган талаб ва эҳтиёж ҳам ортиб бормоқда, айниқса, ахборот технологияларининг кун сайин ривожланиб бориши ахборотлар ҳажмининг ҳам ортиб боришига хизмат қилиб келмоқда. Бу каби ахборотлар ичида маълум маънода ҳимояни, махфийликни ва сир сақланишини талаб этадиганлари ҳам бўлади, негаки, бу тоифадаги маълумотларнинг ошкор бўлиши, ўғирланиши ёки йўқ қилиниши каби ҳолатлар ташкилот учун катта талофотларни, молиявий ёки моддий зарарларни олиб келиши мумкин. Бу каби ҳолатларни олдини олиш учун эса қандай соҳа бўлмасин албатта, ахборот хавфсизлигини, унинг ҳимояси ва муҳофазасини амалга ошириши лозим.

Ҳозирги фан-техника тараққиёти ривожланиб бораётган бир пайтда тармоқлараро ахборот алмашиниш ҳам ривожланиб бормоқда. Лекин тармоқлараро ахборот алмашишда ахборотнинг маълум қисмлари ва умуман ўзи ҳам йўқолиб қолиш ҳоллари мавжуд бўлиб унинг олдини олиш бир муаммо бўлиб қолмоқда. Шунинг учун республикамизда "Ахборот хавфсизлигини ҳуқуқий ва ташкилий жиҳатдан таъминлаш" чоралари ишлаб чиқилди.

"Халқаро ахборот алмашишда иштирок этиш тўғрисида" ги қонунга мувофиқ ахборот хавфсизлиги деганда жамиятда ахборот муҳитининг фуқаролар, ташкилотлар ва давлат манфаатларини шаклланиши ва ривожланиш ҳолати ҳимояланганлиги тушунилади.

Ахборот хавфсизлиги сиёсати компьютер тизимлари ва тармоқларини ҳимоя қилиш воситаларини чегаралайди ва турли вазиятларда тизимнинг ҳатти – ҳаракатини аниқлаган ҳолда ахборотни қайта ишлаш жараёнини барча йўналишларини қамраб олади. Ахборот хавфсизлиги сиёсати йўналишида 3 хил даража мавжуд бўлиб юқори даражали сиёсат йўналишида

ташкилотга тегишли қарорлар асосида "АХС" ётади. Бундай сиёсат умумий характерда ташкилот раҳбарияти томонидан ишлаб чиқилади.

Ташкилот томонидан белгиланган қарорларга мисол тарзида қуйидаги элементларни келтириш мумкин:

- қарорларни шаклантириш ёки ахборот хавфсизлигини таъминлашнинг дастурлар мажмуасини ишлаб чиқариш ва ушбу дастурларнинг бажарилишига жавобгар шахсни тайинлаш,
- ташкилотнинг ахборот хавфсизлиги соҳасидаги мақсадини шакллантириш ва ушбу мақсадга эришишда умумий йўналишларни тиклаш,
- қонун ва қоидага риоя қилиш базасини таъминлаш,
- ташкилот даражасида қараладиган хавфсизлик сиёсатини амалга ошириш бўйича маъмурий қарорларни шакллантириш.

Юқори даражали "Ахборот хавфсизлиги сиёсати" сифатида қуйидаги йўналишларга ажратиш мумкин.

- ҳимоялаш ашёларини бошқариш ва уларни фойдаланишда мувофиқлаштириш,
- критик муҳит тизимни ҳимоялаш учун махсус шахсни тайинлаш,
- хавфсизлик тартибини таъминлаш ва назорат этиш вазифасини бажарувчи ташкилотлар билан узвий алоқа қилиш.

Юқори даражали "АХС" ни ўз таъсир доирасини аниқлаб ахборот хавфсизлиги дастурларини ишлаб чиқариш бўйича мансабдаги жавобгар шахснинг бурчи ва вазифасини белгилаш ҳамда ҳаётга тадбиқ этиш заруриятини кўрсатиш керак. Ушбу сиёсат эса қонун ва унинг бажарилишида 3 та йўналиш бўйича иш юритади.

- ташкилотнинг мавжуд қонунларга риоя қилиши,
- Ахборот хавфсизлиги дастурини ишлаб чиқаришга маъсул шахс фаолиятини назоратга олиш,

- дастурни бажарувчи шахс маъсулиятини аниқлашни таъминлаш бунинг учун рағбатлантириш ва жазолаш тизимларидан фойдаланиш.

Ўрта даражали сиёсат сифатида турли ташкилотлар томонидан компьютер тизимлари ва тармоқларидан фойдаланиладиган ахборот хавфсизлигининг алоҳида йўналишларига тегишли бўлган масалаларига эътибор қаратилади. Ушбу сиёсатнинг йўналиши қуйидагилардир:

- илғор технология муносабатлари,
- интернет тармоғидан фойдаланиш ҳуқуқи,
- уй шароитида компьютердан фойдаланиш,
- расмий бўлмаган (лицензиясиз ва рухсатсиз) дастурий таъминотдан фойдаланиш кабилар киради.

Қуйи даражали сиёсат сифатида аниқ ахборот хизмати қаралади:

- мақсадли йўналиш,
- ахборот хизмати қоидаси йўналиши,
- ахборотларнинг бутунлигини таъминлаш.

Уларни сақлашда ахборот элементларининг алмаштирилиб қўйилишига йўл қўймаслик, рухсатга эга бўлмаган шахсларни фойдаланишини олдини олиш кабилар тушунилади.

Ахборотнинг бутунлигини бузилиши икки ҳолатда тасодифан ва қасддан амалга оширилиши мумкин.

Фойдаланувчилар томонидан тасодифан йўл қўйилган хатолар, техник носозликлар сабаб бўлиши мумкин.

Бузғунчилар томонидан ғаразли мақсадларни кўзлаб олиб борилган ҳаракатлар сабаб бўлади.

Ахборот бутунлиги бузилишининг сабабларидан қатъий назар бу кўзда тутилмаган ҳар қандай натижаларни келтириб чиқариши мумкин. Амалиёт шуни кўрсатадики ахборотларни киритиш, сақлаш, қайта ишлаш ҳамда

узатиш жараёнида ташқи таъсирлар билан учрашишимиз мумкин. Натижада ахборотларнинг сигнал шаклидаги жисмоний ўзгаришлари кузатилади.

Компьютер тармоқлари фаолиятига тасодифий таъсирлар сабаблари қуйидагилар:

- аппаратларнинг сифатсизлиги, эскириши натижасида бузилиши,
- ташқи муҳит таъсирида алоқа каналлари ва линияларида ахборотнинг ўзгариши,
- авария ҳолатлари,
- компьютер ишлаб чиқариш ва лойиҳалаштирилувчиларнинг схема ва систематехник хатолари,
- алгоритмик ва дастурий хатолар,
- фойдаланувчилар йўл қўядиган хатолар.

Шу ўринда айтиш жоизки ахборотларни қайта ишлаш тизими пайдо бўлиши билан ахборотларни ҳимоялаш муаммоси юзага келади. Бу тизимларда ишончли ҳимояни ташкил этиш катта моддий ва молиявий харажатларни, мураккаб тадқиқотларни талаб этади. Шунингдек ахборотларни қимматлигига қараб ҳимоя харажатлари оптимал мақсадга мувофиқ даражасини ишлаб чиқариш зарурияти туғилади. Юқори даражадаги ахборотларни хавфсизлигини таъминловчи харажатларни ҳисоблаш мумкин бўлган тажовузларни тўлиқ ўрганиш, ҳар бир тажовузнинг қилинадиган хавфсизлик даражаси микдорини билиш талаб этилади.

Шахсий компьтерлардан фойдаланишнинг дастлабки вақтларида кўпроқ бузғунчилар хавф солишган бўлса кейинги йилларда ахборотлар мустаҳкамлигига дастур воситалари, компьютер вируслари, интернет глобал тармоғи сабаб бўлмокда.

Ахборот хавфсизлиги амалиёти ахборотларда рухсатсиз фойдаланишнинг кўплаб усуллари мавжудлигини кўрсатади.

- рухсатсиз кириш,

- маълумотларни кўчириб олиш ва алмаштириш,
- алоқа каналларига боғланиш натижасида ёлғон хабарлар ва дастурлар тарқатиш,
- ахборот ташувчилардаги қолдиқ ахборотларни тиклаш ва кўриб олиш,
- электромагнит нурланиш ва тўлқинсимон характердаги сигналларни қабул қилиш,
- махсус "текин" дастурлар ва аппарат воситаларидан фойдаланиш.

Ахборот хавфсизлигини таъминлашда қуйидаги уч муаммонинг ечилиши назарда тутилади.

- Пинҳоналик ёки конфеденциаллик.
- Бутунлик ва қобиллик.

Кўплаб қўшимча хизматлар ва қўллаб – қувватлаш хизматлари мазкур асосий хавфсизлик тизимини тўлдиришга хизмат килади. WEB тугунининг тўла хавфсизлик йўналишларини қамраб олган бўлиши шарт. Бунда тегишли хавфсизлик воситалари ва механизмлари дастурий маҳсулотлар таркибига киритилган бўлиши лозим.

Аутентификациялашни ташкиллаштириш, қайта ишлатиладиган паролларга хос камчиликларни бартараф этишни ва шу мақсадда бир марта ишлатиладиган парол тизимидан тартиб идентификациялашни юқори технологик, биометрик тизимларигача қўллашни назарда тутади.

Идеал вариантда бу тизим ер юзининг ҳар қандай икки нуқтасидаги фойдалнувчи учун сертификатлар занжирини тузиб беради. Бу хат кимгадир махфий хатни имзолаш, ҳисоб бўйича пул ўтказиш ёки эълон, шартнома ўтказиш, бошқага эса ҳужжат манбаини имзоловчини текшириб бериш имкониятини беради.

Интернетга уланган тармоқлар бузғунчиларни тажовузи туфайли очиқ мулоқотга халақит берса ҳам уларни "Брандмауер" -тармоқлараро экран ўрнатиб олдилар. Бу ташкилотнинг энг асосий ҳимоя воситасидир. Тармоққа

кирувчи ва ундан чиқувчи трафикни назорат килади. У трафикнинг бирор турини тугиб қўйиши ёки текшириб туриши мумкин.

Тажовузкорлар кўпинча тармоққа унинг аҳамиятга молик жойларидан ўтувчи трафикни тиклаш орқали, уларнинг паролларини ажратиб олиш ёрдамида суқилиб киралилар. Шунингдек олисда машиналар билан боғланишлар парол воситасида ҳимояланганда шифрланиши шарт. Бу айниқса интернет каналлари орқали боғланишда амалга оширилганда ёки аҳамиятли сервер билан боғланганда зарурдир. Бунинг учун биз "Криптография" фанини чуқур ўрганишимиз лозим.

I-БЎЛИМ. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОҚЛАРИДА АХБОРОТ ХАВСИЗЛИГИНИ ТАЪМИНЛАШ

1.1. Ахборот хавфсизлигини таъминлашнинг меъёрий - ҳуқуқий асослари

Замон тараққий этган сари жамиятда ахборотга бўлган талаб ва эҳтиёж ҳам ортиб бормоқда, айниқса, ахборот технологияларининг кун сайин ривожланиб бориши ахборотлар ҳажмининг ҳам ортиб боришига хизмат қилиб келмоқда. Бу каби ахборотлар ичида маълум маънода ҳимояни, махфийликни ва сир сақланишини талаб этадиганлари ҳам бўлади, негаки, бу тоифадаги маълумотларнинг ошкор бўлиши, ўғирланиши ёки йўқ қилиниши каби ҳолатлар ташкилот учун катта талофотларни, молиявий ёки моддий зарарларни олиб келиши мумкин. Бу каби ҳолатларни олдини олиш учун эса қандай соҳа бўлмасин албатта, ахборот хавфсизлигини, унинг ҳимояси ва муҳофазасини амалга ошириши лозим.

Буни физик, дастурли - техник, меъёрий - ҳуқуқий услуб билан амалга ошириш мумкин. Ташкилот мисолида олсак, бутун бир тизимни таҳлил қилган ҳолда, биринчи навбатда ахборот муҳофазаси бўйича меъёрий - ҳуқуқий базани яратиб олиш муҳим аҳамиятга эга. Негаки, айнан, шу меъёрий - ҳуқуқий ҳужжатлар кейинги амалга ошириладиган (физик ҳимоя, дастурли - техник ҳимоя) ишлар учун ҳам режа, ҳам дастур, ҳам пойдевор бўлиб хизмат қилади. Шунинг учун, ташкилотларда замон талаблари асосида ахборот хавфсизлигини таъминлаш учун шу соҳа бўйича ишлаб чиқилиши ва қўлланиллиши тавсия этиладиган асосий меъёрий - ҳуқуқий ҳужжатлар рўйхати ва намуналарини қисқача келтириб ўтиш лозим. Ушбу тавсиялар хавфсизлик бўйича Халқаро ISO 17799 стандартига асосланган ҳолда тузилган. Бу хавфсизлик стандарти комплекс характерга эга бўлиб, аввало ташкилотларда ахборот хавфсизлигини таъминлашнинг меъёрий ҳуқуқий

пойдеворини яратиш дастури бўлиб, бу ўз навбатида ахборот тизимлари хавфсизлигини бошқариш вазифаларини енгиллаштиради.

"Ташкилотнинг хавфсизлик сиёсати" ҳужжати

Бу ҳужжат ташкилотда ахборот хавфсизлигининг мақсад ва принципларини аниқлаш учун мўлжалланган бўлиб, ўз навбатида ахборот хавфсизлиги объектлари рўйхати кўрсатиб ўтилади. Бундан ташқари, ташкилотда ахборот хавфсизлигини таъминлаш учун керакли бўлган ички ҳужжатлар рўйхати ҳам келтириб ўтилади.

Ҳужжат тури – Низом.

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ахборот тизимлари ёки воситалари таркиби ўзгарган ҳолда ёки бир йилда энг камида бир мартта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

Ташкилотда ахборот хавфсизлигининг ўрнини ҳамда унинг ташкил этувчиларини белгилаш. Ахборот хавфсизлиги тушунчасини белгилаш, ташкилотнинг ахборот хавфсизлиги объектларини санаб ўтиш. Хавфсизлик сиёсатининг, уни ташкил этишнинг, ҳамда ташкилот учун алоҳида аҳамиятга эга стандарт ва талабларга жавоб беришининг қисқача мазмуни кўрсатиб ўтилади:

• хавфсизлик сиёсатининг маҳаллий ва халқаро меъёрларга зид эмаслигини;

• хавфсизлик масалалари бўйича ходимларни ўқитиш ва малакасини ошириш бўйича талаблар;

• вирус ва бошқа зараркунанда дастурларни аниқлаш ва йўқотиш бўйича талаблар;

• ахборот хавфсизлигини ва ташкилот фаолиятини узлуксиз ишлашини таъминлаш бўйича талаблар;

• хавфсизлик сиёсатини бузганлик бўйича жавобгарлик;

• раҳбарларнинг лавозим мажбуриятномаларига қўшимчалар - ахборот хавфсизлигини таъминлаш бўйича жавобгарлик ҳамда юзага келган қоидабузарликни ўз вақтида маълум қилиш бўйича жавобгарлик;

• масъул шахслар томонидан ахборот хавфсизлиги бўйича жавобгарликнинг тақсимланиши.

Тизимни ва ундаги ўзгаришларни бошқариш

Ахборот хавфсизлиги сиёсати билан биргаликда ахборот хавфсизлигига алоқадор бошқа ҳужжатларнинг тўлиқ рўйхати. "Ахборот хавфсизлигини таъминлаш бўйича жавобгарликни тақсимлаш" ҳужжати. Ташкилотда ахборот хавфсизлиги ресурсларини ва бу ресурслардан фойдаланиш ваколатига эга шахсларни жавобгарлигини белгилаш учун мўлжалланган.

Ҳужжат тури - Фармойиш

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ахборот хавфсизлиги сиёсати, технологик қисмлар ҳамда ахборот ресурслари таркиби ўзгарган тақдирда қайта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

Ҳар бир тизимдаги ахборот хавфсизлигига даҳлдор ресурсларни белгилаш.

Ҳар бир ресурс (ёки жараён) учун тегишли жавобгар раҳбар ходимларни тайинлаш. Масъулиятни тақсимлаш ва белгилаш ҳужжатлаштирилиши лозим. Ҳар бир ресурс учун алоҳида фойдаланиш ваколатлари белгиланиши ва ҳужжатлаштирилиши лозим.

"Янги ахборот тизимини татбиқ этиш" ҳужжати

Ташкилотда янги ахборот тизимини татбиқ этиш жараёнларини белигилаб ўтиш учун мўлжалланган.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ташкилотда янги ахборот технологиялари татбиқ этилаётган тақдирда ҳамда ахборот хавфсизлиги сиёсати ўзгарган тақдирда қайта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

Ресурсларни бошқариш. Янги тизимнинг мавжуд фойдаланувчиларни бошқариш тизимига мослилигини таъминлаш. Татбиқ этилаётган барча компонентларни мавжуд тизим қисмлари билан мослилигини текшириш.

"Ресурсларни инвентаризатциялаш" ҳужжати

Инвентаризатциялашга мойил русурсларни тоифалашни аниқлаш учун мўлжалланган.

Ҳужжат тури - Йўриқнома.

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Инвентаризатция ўтказишдан олдин, бир йилда бир мартта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

Ахборот ресурслари. Маълумотлар ва файллар омбори, тизимга даҳлдор ҳужжатлар, фойдаланувчи ҳужжатлари, ўқув материаллари, фойдаланиш бўйича йўриқномалар, ташкилот фаолиятининг узлуксизлигини таъминловчи режалар, камчиликларни бартараф этиш бўйича тадбирлар, ахборот ва маълумотлар архиви.

Дастурли таъминотлар

Иловалар, операцион тизимлар ва системали дастурий таъминотлар, дастурлаш воситалари.

Физик ресурслар. Ҳисоблаш техникалари (процессор, мониторлар ва бошқалар), коммуникатция қурилмалари (модем, маршрутизаторлар, телефон

қурилмалари, факслар), магнит ташувчилар (винчестрлар, дискет, дисклар) ва бошқа техник қурилмалар.

Ҳисоблаш ва коммуникатция ва ёрдамчи хизматлар.

Иссиқлик тизими, ёритиш тизимлари ва ҳоказо. Ташкилотдаги барча йўриқномавий, меъёрий - ҳуқуқий ҳужжатларни инвентаризатциялаш.

"Ресурсларни таснифлаш" ҳужжати

Хавфсизлик нуқтаи назаридан ресурсларни таснифлаш учун мўлжалланган.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Бир йилда энг камида бир мартта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

Барча ресурслар муҳимлик даражаси билан таснифланиши лозим:

• кўпайтириш;

• сақлаш;

• почта, факс, электрон почта орқали узатиш, қабул қилиш;

• овозли узатиш, қабул қилиш, жумладан, мобил алоқа ва овозли почталар ҳам; йўқ қилиш.

"Ресурсларни тақсимлаш" ҳужжати

Мақсадли йўналтирилган ва фойдаланилишга мўлжалланган ресурсларни тақсимланишини белгилайди.

Ҳужжат тури - Фармойиш.

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ахборот тизимлари таркибида ўзгаришлар амалга оширилганда қайта кўриб чиқилиши ва янгиланиши мумкин.

Ҳужжат таркиби

Фойдаланиш мақсади бўйича ресурсларни тақсимлаш:

• тақсимлаш бўйича перспективани ишлаб чиқиш;

• тестдан ўтказиш (карантин);

• бевосита амалга ошириладиган бизнес операциялар (операцион муҳит);

• янги дастурий таъминотларни, воситаларни операцион тизимга татбиқ этиш қоидалари;

• ишлаб чиқиш, тизим утилиталари, таҳрирлагичлар кабилар белгилаб ўтилиши;

• ходимлар билан ишлашда ахборот хавфсизлиги.

"Ходимларни танлаш ва улар билан ишлашда ахборот хавфсизлиги" ҳужжати

Ташкилотда ходимларни танлашда ва улар билан ишлашда ахборот хавфсизлигини таъминлаш чора - тадбирларини аниқлаш учун мўлжалланган.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Заруриятдан келиб чиққан ҳолда, қайта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби

• Ходимни ишга қабул қилишда текшириш:

• Тавсифномаларни текшириш;

• Резюмедаги маълумотларни текшириш;

• Маълумоти ва илмий даражаларини текшириш;

• Шахсий маълумотларини текшириш;

Ташкилотдаги ахборот хавфсизлиги режимига риоя қилиниши ва амал қилинишига келишув.

Ходим билан меҳнат келишувининг шартлари

Лавозим мажбуриятларининг ёзма формулировкаси. Ахборот хавфсизлигини таъминлаш бўйича вазифаларни барча ходимларнинг лавозим

мажбуриятларига киритиш. Ташкилот ресурсларига (жумладан, ахборот ресурсларига) кириш ва фойдаланиш ваколатларининг ёзма формулировкаси. Махфийликни таъминлашга, сир сақлашга келишув. Махсус келишувлар (тизим маълумотларини, телефондаги сўзлашувларни, факслар мониторинги).

"Ахборот хавфсизлиги соҳасида қоидабузарликлар ҳамда турли носозликлар, хатоликлар содир бўлган тақдирда кўриладиган чоралар" ҳужжати

Ахборот хавфсизлиги соҳасида қоидабузарликлар содир бўлган тақдирда, ахборот тизимларида носозликлар, хатоликлар юзага келганда кўриладиган ва амалга ошириладиган чора - тадбирлар тартибини белгилайди.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Юзага келган қоидабузарлик, хатолик ва носозликлардан сўнг ҳамда заруриятдан келиб чиққан ҳолда, қайта кўриб чиқилиши ва янгиланиши мумкин.

Ҳужжат таркиби

Қоидабузарликлар бўйича ҳисоботлар. Хавфсизлик тизимидаги камчиликлар бўйича ҳисоботлар. Компютер тизимларида юзага келган носозликлар ва хатоликлар бўйича ҳисоботлар. Шу жумладан, ностандарт ва номаълум вазиятлар юзага келган ҳолда амалга оширилиши лозим бўлган чора - тадбирлар. Бундан ташқари, кўриладиган чоралар, жазолар (интизомий, маъмурий вазиятдан келиб чиққан ҳолда (ҳатто жиноий).

Ахборот хавфсизлиги соҳаси бўйича ходимлар малакасини доимий равишда ошириб бориш.

Физик хавфсизлик

"Мол - мулк, бойликлар ва қурилмалар хавфсизлиги" - ҳужжати

Ташкилотнинг мол - мулки, бойликлари ва қурилмаларининг даҳлсизлигига физик таҳдид солувчи омиллардан ҳимоялаш қоидаларини аниқлашдан иборат.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Заруриятдан келиб чиққан ҳолда қайта кўриб чиқилиши ва янгиланиши мумкин.

Ҳужжат таркиби

Мол - мулк, бойликлар ва қурилмаларнинг жойлашуви, улардан фойдаланиш ҳуқуқини белгиланган талаблар асосида чегаралаш. Муҳим аҳамият касб этадиган маълумотларни қайта ишловчи ва сақловчи қурилмаларнинг хавфсизлиги ва даҳлсизлигини таъминлаш. Ўз хизмат вазифасини ўтаб бўлган қурилма ва тизимларни хавфсиз йўқ қилиш чоралари. Махсус ҳимояни талаб этадиган обектларни ҳимоялаш чоралари.

Қуйидаги таҳдидлардан ҳимоялаш чораларини белгилаш:

• ўғирланиш;

• ноқонуний фойдаланиш, даҳл этилиши, кўпайтирилиши ва бошқалар;

• йўқ қилиниши;

• ёнғин;

• портлаш;

• вибрация;

• кимёвий моддалар;

• электромагнит ва акустик таъсирлар ва йўналтиришлар;

• турли табиий офатлар;

• қурилмалар олдида ноўрин ҳаракатлар қилиш (чекиш, овқатланиш, ичимликлар ичиш ва ҳоказо).

• қўшни объектларнинг таъсир этиши мумкин бўлган омиллар ва бошқа турдаги омиллар.

Мақсад - ташкилот мол - мулки, бойликлари, қимматликлари ва қурилмаларини турли таҳдидлардан ҳимоя қилиш, улардан нотўғри ва ноқонуний фойдаланилишидан ҳимоя қилиш, уларнинг етарли даражадаги даҳлсизлигини ва бутлигини таъминлаш, ташкилотга зарар келтирувчи омиллардан ҳимояланиш.

"Ишчи ўрин хавфсизлиги" ҳужжати

Ишчи ўриндан маълумотларнинг чиқиб кетишининг олдини олиш ва ходим учун ишчи ўрнини тўғри ташкил этишни белгилайди.

Ҳужжат тури - Йўриқнома.

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Заруриятдан келиб чиққан ҳолда, қайта кўриб чиқилиши ва янгиланиши мумкин.

Ҳужжат таркиби:

• Ҳужжатларни сақлаш.

• Турли воситалардаги маълумотларнинг тўғри сақланишини таъминлаш.

• Техника хавфсизлигини таъминлаш.

• Тегишли шарт - шароитлар.

• Кўпайтирувчи ва босмага чиқарувчи воситалардан фойдаланиш.

Процессларни ва коммуникацияларни бошқариш. Хизмат йўриқномалари ва мажбуриятлар.

"Ахборот хавфсизлиги бўйича лавозим мажбуриятномалар" ҳужжати.

Ахборот хавфсизлиги бўйича ходимларнинг лавозим мажбуриятларига киритиладиган ваколатлар, ҳуқуқлар ва мажбуриятларни белгилаш.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлим томонидан ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади.

Заруриятдан келиб чиққан ҳолда, қайта кўриб чиқилиши ва янгиланиши мумкин.

Ҳужжат таркиби

Лавозим мажбуриятларига киритилиши лозим бўлган омиллар:

• маълумотларни қайта ишлаш ва улардан фойдаланиш тартиби;

• бошқа тизимлар билан ўзаро муносабатлари;

• фойдаланиш чегараси ва ваколатлари;

• кўзда тутилмаган ҳолатларда кўриладиган чора - тадбирлар тартиби;

• ходимларнинг хизмати бўйича ўзаро муносабатлари;

• ахборотни қайта ишлашда ва конфиденциаллигини таъминлаш бўйича қўшимча ва махсус йўриқномалар.

"Зараркунанда дастурлардан ҳимояланиш (вируслар, троянлар, СПАМ)" ҳужжати.

Ахборот тизимларини заракунанда дастурлардан ҳимояланиш қоидалари ва усулларини аниқлаш учун мўлжалланган.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлими ҳамда ахбротлаштириш ва ахборот технологиялари билан шуғулланувчи бўлими билан биргаликда ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ахборот ресурслари таркиби ва иш фаолиятида ахборот тизимларида камчиликлар аниқланган тақдирда қайта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби.

Фақатгина лицензияга эга антивирус дастурларидан фойдаланишни таъкидлаш ва тасдиқланмаган дастурлардан фойдаланишни тақиқлаш.

Дастурий воситаларни олиш ва татбиқ этиш тартиби.

• қўлланиладиган антивирус дастури.

• дастурий воситаларнинг бутлиги.

• кирувчи чиқувчи маълумотларни антивирус дастури текширувидан ўтказиш.

• вирус атакаларидан сўнг тизимни қайта тиклаш қоидалари.

• барча ахборотларнинг мониторинги.

"Ички ресурсларни бошқариш. Маълумотларнинг заҳира нусхаси" ҳужжати

Ташкилотда ички ресурсларни бошқариш ва маълумотларнинг заҳира нусхаларини олиниши тартибини белгилайди.

Ҳужжат тури - Йўриқнома

Ташкилотнинг хавфсизлик масалалари билан шуғулланувчи бўлими ҳамда ахбротлаштириш ва ахборот технологиялари билан шуғулланувчи бўлими билан биргаликда ишлаб чиқилади. Ташкилот раҳбари томонидан тасдиқланади. Ахборот ресурслари таркиби ва иш фаолиятида ахборот тизимларида камчиликлар аниқланган тақдирда қайта кўриб чиқилади ва янгиланади.

Ҳужжат таркиби:

• ички ресурсларни бошқарилиши ва мониторинги.

• заҳира нусхаларнинг сақланиши.

• ахборот тизимлари ва сақловчи воситаларнинг ишончлилигини текшириш.

• тизимни қайта тиклаш тартиби.

• тизимни қайта тиклаш бўйича ходимлар тренинги ва бошқалар.

Булардан ташқари, ташкилотнинг веб - саҳифаси, локал ёки глобал тармоғи мавжуд бўлган тақдирда, веб - саҳифага маълумотларни киритиш тартибини, веб - саҳифага, локал - глобал тармоққа бўладиган турли ҳужумлардан ҳимояланиш ва тизимда тўлақонли ахборот хавфсизлигини таъминлаш бўйича йўриқнома, локал - глобал тармоққа кириш ва фойдаланиш учун рухсат бериш тартиби, локал ва глобал тармоқлар хавфсизлигини таъминлаш ҳамда унинг доимий мониторинги бўйича

йўриқнома каби меъёрий ҳужжатларнинг ишлаб чиқишлиши ҳам тавсия этилади. Яна шуни таъкидлаш керакки, ташкилотларда ахборот хавфсизлиги соҳаси бўйича ишлаб чиқилиши лозим бўлган ҳужжат намуналарининг асосийлари келтирилган бўлиб, фақатгина ушбу келтириб ўтган ҳужжатлар рўйхати билангина чегаралиниб қолинмаслигини таъкидлаб ўтмоқчимиз. Балки, ташкилотнинг ички хусусиятларидан келиб чиққан, унинг фаолият турига қараб ва бошқа омилларга асосланган ҳамда маҳаллий қонунчилик ва меъёрий ҳужжатларга асосланган ва зид келмаган ҳолда, бу каби ҳужжатлар тўлдирилиши, қўшимчалар қўшилиши, янги меъёрий ҳужжатлар билан бойитилиши мумкин.

Ўйлаймизки, бу нафақат ахборот хавфсизлиги бўйича раҳбар ва мутахассислар учун, балки ташкилот раҳбарлари учун ҳам ташкилот фаолиятини тўғри ташкил этиш ва ташкилотда етарли даражада ахборот хавфсизлигини таъминлашда озгина бўлсада ёрдам беради.

1.2. Миллий ахборот тизимининг муҳофазаси, таҳдиди ва унинг хавфсизлиги

Бу режада "Ўзинфоком" компьютер ва ахборот технологияларини ривожлантириш ҳамда жорий этиш маркази ҳузурида фаолият олиб бораётган Компьютер ҳодиса (таҳдид) ларига чора кўриш хизмати (UZ-CERT), унинг вазифалари, хизмат турлари ва янгиланган расмий сайти тўғрисида маълумотлар келтирилган.

Таркибий тузилиши. Ўзбекистон Республикасининг ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон тамойилларини ҳисобга олган ҳолда, миллий ахборот тизимини яратишга қаратилган. Таъкидлаш жоизки, миллий ахборот тизимига давлат органлари, шунингдек, юридик ҳамда жисмоний шахслар,

тармоқ ва ҳудудий ахборот тизимлари киради. Ахборот тизими эса ахборотни тўплаш, сақлаш, излаш, унга ишлов бериш ҳамда ундан фойдаланиш имконини берадиган, ташкилий жиҳатдан тартибга солинган жами ахборот ресурслари, ахборот технологиялари ва алоқа воситаларидир. Ахборот тизими таркибидаги электрон шаклдаги ахборот, маълумотлар банки, маълумотлар базаси ахборот ресурсларини ташкил этади.

Муҳофазага эҳтиёж. Бугунги кунда турли кўринишдаги (иқтисодий, ижтимоий, мудофаа, ахборот, экологик) хавфсизликка таҳдид бор экан муҳофазага ҳам эҳтиёж муқаррар. Зеро, Юртбошимиз: "Шуни эсда тутишимиз керакки, бутун тарих таҳдидлар ва уларни даф этишдан иборат", деб таъкидлагани бежиз эмас, албатта. Улуғ аллома Абу Наср Форобий ҳам бу борада: "Давлатни ақл - идрок билан бошқариш, халқ бошига тушган хавф - хатарни камайтириш ва бартараф этишдан иборатдир" - деб ёзганди. Шу маънода, ахборот, ахборот ресурслари, компьютер тармоқлари ва корпоратив тизимларга нисбатан хавфсизликка таҳдидларнинг олдини олиш масаласи - бугунги кунда янада долзарб ҳисобланади. Негаки, ҳар қандай корхона (ташкилот, муассаса, бирлашма, компания) нинг самарали фаолият кўрсатиши моддий, табиий, меҳнат, молиявий, энергетик ресурслар билан кафолатланмайди. Улардан қандай қилиб оқилона фойдаланиш учун соҳадаги технологиялар тўғрисида етарлича, ахборотга эга бўлиш ҳам талаб этилади. Зотан, ахборот қолган барча ресурслардан самарали фойдаланиш учун кенг имкониятлар яратиб берадиган ягона ресурс ҳисобланади. Шунинг учун ҳам нафақат хорижда, балки республикада ҳам ахборот ресурслари ва ахборот тизимларини муҳофаза қилишга жиддий эътибор қаратилмоқда.

Масаланинг долзарблиги. Тарихда энг "ҳалокатли" ўнта вирус келтирган зарар статистик маълумотларга кўра, қуйидагича баҳоланган:

(http://www.1on.ru/2006_07_19/desiat_samyh_razrushitelnyh_virusovв_%20v_istorii.html, 19 июля 2006):

• CIH (1998) - $20-80 млн., йўқотилган жуда катта ҳажмдаги маълумотларни ҳисобга олмаганда;

• Melissa (1999) - $300-600 млн.;

• ILOVEYOU (2000) - $10-15 млрд.;

• Code Red (2001) - $2,6 млрд.;

• SQL Slammer (2003) - вирус шанба куни тарқала бошлагани сабабли иш вақтини йўқотишдан кўрилган зарар унча катта бўлмаган, лекин у бутун дунёдаги ярим миллион серверни "шикастлаб" улгурган ва Жанубий Кореяни глобал тармоқдан 12 соат яккалаб қўйган;

• Blaster (2003) - $2-10 млрд.;

• Sobig.F (2003) - $5-10 млрд., 1 млн дан ортиқ компьютерга "касаллик юқтирган";

• Bagle (2004) - бир неча $10 млн., зарар тобора ортиб бормоқда;

• MyDoom (2004) - эпидемия энг кучайган даврда глобал тармоқда ўртача жавоб вақти 10 фоизга, сайтларнинг юкланиш тезлиги 50 фоизга пасайган;

• Sasser (2004) - бир неча $10 млн.

Ахборот хавфсизлиги ва қонунчилик. Ўзбекистон Республикасининг "Ахборотлаштириш тўғрисида" ги қонуни (11.12.2003 йил) 19-моддасида кўрсатилганидек, ахборот ресурслари ва ахборот тизимларини муҳофаза қилиш аввалambор, шахс, жамият ва давлатнинг ахборот хавфсизлигини таъминлаш мақсадида амалга оширилади. Мазкур қонуннинг 20-моддасида: "Ахборот ресурслари ва ахборот тизимлари, агар улар билан ғайриқонуний муносабатда бўлиш натижасида ахборот ресурсларининг ёки ахборот тизимларининг мулкдорларига, эгаларига ёҳуд бошқа юридик ҳамда жисмоний шахсларга зарар етказилиши мумкин бўлса, муҳофаза қилиниши керак. Давлат органлари, юридик ва жисмоний шахслар давлат сирлари ҳамда махфий сирлар тўғрисидаги ахборотни ўз ичига олган ахборот

ресурслари ва ахборот тизимларининг муҳофаза қилинишини таъминлаши шарт", деб алоҳида кўрсатилган.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг "Ахборотлаштириш соҳасида норматив ҳуқуқий базани такомиллаштириш тўғрисида" ги қарори (22.11.2005 йил) да тасдиқланган "Давлат ахборот ресурсларини шакллантириш тартиби тўғрисидаги Низом" нинг 1-иловасига мувофиқ Давлат органи ўзининг расмий сайтида жойлаштирилган ахборотларнинг йўқ қилиниши, тўсиб қўйилиши, бузиб талқин қилиниши, қалбакилаштирилиши ва сохталаштирилишининг ҳамда бошқа шакллардаги рухсатсиз аралашувларнинг олдини олиш бўйича тегишли муҳофаза чора - тадбирларини кўриши керак бўлади.

Бошқарув ва иқтисодиётнинг турли соҳа ва тармоқларида ахборот - коммуникация технологияларини қўллаш жараёнида ахборот хавфсизлигини таъминлаш тизимини такомиллаштириш ва фойдаланувчиларга компьютер таҳдидларини ўз вақтида аниқлаш, уларнинг олдини олиш ҳамда нейтраллаштиришда амалий ёрдам кўрсатиш мақсадида ЎзИнфоКом маркази ҳузурида Компьютер ҳодисаларига чора кўриш хизмати (UZ-CERT) ташкил этилган (CERT – Computer Emergency Response).

UZ-CERT: асосий вазифалар, режалар ва хизматлар

Ташкил этилиши. Ўзбекистон Республикаси Президентининг 2005 йил 5 сентабрдаги "Миллий ахборот - коммуникация тизимларида компьютер хавфсизлигини таъминлаш бўйича қўшимча чора - тадбирлар тўғрисида" ги қарорига биноан "Ўзинфоком" компьютер ва ахборот технологияларини ривожлантириш ҳамда жорий этиш маркази ҳузурида Компьютер ҳодиса (таҳдид) ларига чора кўриш хизмати (UZ-CERT) ташкил этилган. "Ўзинфоком" марказининг директори Джалолатдин Рахимовнинг таъкидлашича, бундай хизмат Марказий Осиё ҳудудида ягона ҳисобланади. Ахборот хавфсизлиги соҳасида таниқли эксперт Искандер Конеевнинг фикрича, фойдаланувчилар муаммо юзага келганда тегишли Хизматга (она

тилида) мурожаат этиш (айниқса, унчалик малакали бўлмаганлар учун) имкониятининг пайдо бўлиши, вазиятдан осон чиқишларида ниҳоятда фойдали бўлиши мумкин

(http://www.cert.uz/addons/news.php? type=1&id=28&num=1).

Таркибий тузилмаси. Хизмат таркибида компьютер ҳодисаларига тезкор чора кўриш гуруҳи, таҳлил ҳамда маслаҳат ва дастурий ёрдам кўрсатиш гуруҳи, мувофиқлаштириш ва ўзаро ҳамкорлик гуруҳи фаолият кўрсатмоқда.

Асосий вазифалари:

• компьютер ва ахборот технологияларидан фойдаланишда улар билан ғайриқонуний муносабатда бўлишга йўл қўймаслик масалалари бўйича операторлар ҳамда провайдерларнинг компьютер хавфсизлиги бўлинмалари ҳамда миллий ахборот тизимининг бошқа субъектлари саъй - ҳаракатларини мувофиқлаштириш;

• фойдаланувчилар, компьютер техникаси ва дастурий таъминот ишлаб чиқарувчилар томонидан компьютер тармоқлари хавфсизлигига бугунги кунда мавжуд таҳдидлар тўғрисидаги ахборотларни, шунингдек, муайян компьютер ҳодисалари ва компьютер тизимларини муҳофаза қилишда қўлланилаётган техник - дастурий воситаларнинг самарадорлигига оид материалларни йиғиш, уларни тегишли маълумотлар базасида жамлаш ва таҳлил қилиш;

• фойдаланувчиларга хатарларни баҳолашда консултатив хизмат ва техник ёрдам кўрсатиш, уларни рўй бериши мумкин бўлган хавф - хатарлардан ўз вақтида хабардор қилиш, компьютер хавфсизлигини таъминлаш борасидаги ҳуқуқий - норматив базани такомиллаштириш бўйича таклифлар бериш ва бошқалар.

Хизмат турлари:

• корпоратив тармоқ хавфсизлиги аудити;

• web - сайтларнинг технологик аудити;

• серверлар ахборот хавфсизлиги ҳолатининг таҳлили;

• корпоратив тармоққа техник ёрдамдан кейинги кўмаклашув ва мониторинг.

Корпоратив тармоқ хавфсизлиги аудити деганда, мустақил аудиторлик хизмати томонидан компания ахборот ресурсларининг хавфсизлигини ҳар томонлама таҳлил қилиш тушунилади. Бунда компания хавфсизлик тизимидаги заифликлар аниқланиб, тармоқнинг муҳофаза қилинганлик даражасини ошириш бўйича қатор чора - тадбирлар белгиланади. Маълум бўлишича, "бузиб очиш" ларнинг 80 фоизи компаниянинг ўзида, унинг ходимлари иштирокида содир этилар экан. Айнан, шу нарса мустақил аудиторлик хизмати таҳлили ўтказилиши кераклигини белгиловчи бош омиллардан биридир. Зотан, фақат моҳир ва юқори малакали мутахассисларгина хавфсизлик тизимининг барча заиф жиҳатларини аниқлаб, муҳофазанинг стратегияси, сиёсати ҳамда архитектурасини ишлаб чиқиш ҳамда жорий этишга қодир.

Компьютер тармоқларининг қай даражада муҳофаза қилинганлигини баҳолаш учун турли тестлар ўтказилади. Булар: сканерлаш, "енгил" ҳамда "оғир" тест ва бошқалардир. Рухсатсиз, хуфиёна кириб олишни аниқлаш тестларини ўтказиш ишончли муҳофаза тизимини яратиш борасидаги энг керакли дастлабки қадам дейиш мумкин. Кўрсатилган беминнат хизматлар учун Albatros, TPS, CronTelecom, Sarkor, UzNet, UzSciNet каби провайдерлардан миннатдорчилик изҳор этилган хатлар олинганини таъкидлаш ўринлидир.

Хизматнинг янгича расмий сайти. UZ-CERT хизматининг расмий сайти (http://www.cert.uz/) - 2005 йилнинг 1 декабрь куни илк бор компьютер технологиялари ва Интернет ишқибозлари эътиборига ҳавола этилган. 2006 йил 21 ноябр куни эса сайтнинг янгича варианти яратилгани тўғрисида (http://www.cert.uz/addonsc/news.%20php?type=1&id=180&num=1) хабар тарқатилди. Бу сайтнинг аввалгисидан фарқли жиҳатлари қуйидагилар:

янгича, мукаммаллаштирилган дизайн; тамомила янги тарзда фаолият кўрсатувчи муҳофаза тизими; мутлақо янги функциялар; қулай ва ихчам навигациядан иборат. Сайтдаги "UZ-CERT янгиликлари" ("Новости UZ-CERT") ва "Ахборот хавфсизлиги янгиликлари" ("Новости ИБ") деб номланган саҳифалардаги янгиликлар кўпчиликнинг эътиборини тортиши табиий. Эълон қилинган янгиликлар турли мавзуларда бўлиб, биринчи бўлимда (2006.12.01 ҳолати бўйича) олтита, иккинчисида эса 150 га яқин (жами 8 та саҳифадан иборат) дир.

Сайтга киритилган янги функциялар қаторида Хизмат янгиликларига обуна бўлиш; RSS лента (қисқа янгиликлар: RDF Site Summary; RDF - Resource Definition Framework); форум; фойдаланувчилар билан боғланиш; компьютер инсидентларига доир статистика каби бўлимлар борлигини таъкидлаш жоиз. Сайтдаги кундалик янгиликлар обуначиларга ўз вақтида етказилиб берилади. Янгиликлар лентаси ҳар куни, узлуксиз янгиланиб борилади. Ҳозирги кунда қизиқувчилар учун форум айни авжида. Мутахассислар доимо мунозарага шай. Фойдаланувчилар билан тўғридан-тўғри алоқа ("горячая линия") реал вақт режимида амалга оширилади. Шунингдек, саҳифаларда ҳисобот даври мобайнида кузатилган компьютер нохуш ҳодисалари тўғрисидаги статистик маълумотлар мунтазам ёритиб борилади. Улар билан танишиш жаҳон ўргимчак тўрида учрайдиган таҳдидларга ҳар бир фойдаланувчи қанчалик ҳушёр туриши зарурлигини англатади.

Сайтнинг "Ахборот хавфсизлигига доир мақолалар" ("Стати по информационной безопасности") номли бўлимида ахборот тизимлари хавфсизлигига оид ўнта мақола (улардан тўрттаси Хизмат ходимлари томонидан тайёрланган), спам (аноним оммавиий сўралмаган тарқатма) ларга оид учта, вирусларга тегишли учта мақола (биттасининг муаллифи UZ-CERT) ўрин олган. Сайтнинг қанчалар жозибадор эканлиги мазкур ресурс

тўғрисидаги тўлиқ статистик маълумотларда янада яққол кўринади (http://www.uz/rus/toprating/cmd/stat/id/369).

Энг хавфли инсидентлар: тармоқнинг асосий тугунлари ва йирик сервер ресурсларига уларнинг фаолиятини издан чиқариш, бузиб кириш ёки тизимий маълумотларни сифатсизлантиришга қаратилган хавф - хатарлар; тармоқ бошқарувидаги устуворликларни қўлга киритишга йўналтирилган турли таҳдидлар; миллий ахборот ресурслари ва айрим хостларга DoS (Denial of Service) ва DDoS (Distributed Denial of Service) таҳдидлари; атайин (ғаразли мақсадларда) компьютер вируслари тарқатиш; ахборот тармоқлари хавфсизлик тизимини бузиб кириш, шу жумладан, зарарли дастурларни хуфиёна "жорий этиш" йўли балан;

• миллий ахборот тармоқлари ва хостларини сканерлаш;

• парол ва бошқа аутентификация маълумотларини танлаш ҳамда қўлга киритиш;

• ахборот ресурсларидан ноқонуний фойдаланиш. UZ-CERT хизмати томонидан турли компьютер инсидентларининг олдини олиш бўйича тегишли тавсияномалар ишлаб чиқилган.

Вируслар фаоллиги шарҳи. "Касперский лабораторияси" нинг статистик маълумотлари турли вирусларнинг 2006 йил октабрь ойидаги фаоллиги билан таништиради. Унда биринчи йигирматаликдан ўрин эгаллаган вируслар номма - ном қайд этилган. "Октабрь якунлари" га кўра:

• йигирматаликда Warezov.dn, Warezov,ev, Warezov.do, Warezov.eu, Warezov.gen, Warezov.dh, Warezov.dc каби янги 7 та зарарли дастур пайдо бўлган;

• NetSky.b, Mytob.c, Bankfraud.od, Scano.aq каби дастурларнинг кўрсаткичи анчагина пасайган:

• Scano.gen ўз мавқеини ўзгартирмаган;

• NetSky.q, Bagle.gen, Bagle.mail, Mydoom.l, Mydoom.m, Scano.e, NetSky.aa, Bagle.dx сингари дастурлар яна йигирматаликдан ўрин эгаллаган.

Сўровнома. Компьютерлаштириш ва ахборот - коммуникация технологияларини ривожлантириш бўйича Мувофиқлаштирувчи кенгаш қарори (2006 йил 27 март) ва Ахборот тизимлари ва телекоммуникация масалалари бўйича ахборот - таҳлилий департамент қарори (2006 йил 1 август) нинг ижросини таъминлаш мақсадида UZ-CERT хизмати томонидан "Давлат органлари корпоратив тармоқларида ахборот хавфсизлигининг таъминланганлик ҳолатини ўрганиш бўйича сўровнома" ишлаб чиқилган. Сўровномага доир маълумотлар сайт саҳифаларида батафсил ёритилган.

(http://www.cert.uz/addons/news.%20php?type=1&id=118&num=1).

Статистика. UZ-CERT хизмати томонидан глобал тармоқнинг миллий сегментидаги айрим сайтларнинг ахборот хавфсизлиги борасидаги ҳолати ўрганилган ва натижалар таҳлил қилинган. Сайтларнинг талабларга мувофиқлик ҳолатини баҳолашнинг ягона рейтинг тизимида шартли тўрт гуруҳ ҳисобга олинган: 80-100% - аъло; 60-79,9% - яхши; 40-59,9% - ёмон; 0-39,9% - ниҳоятда ёмон. Барча сайтлардаги ахборот хавфсизлиги меъёрларига амал қилиш даражасини ўрганишнинг қиёсий таҳлили натижаларига кўра, ундаги бўшлиқлар салмоғи 48% атрофида эканлиги маълум бўлган. Сайтларнинг ахборот хавфсизлиги борасидаги умумий вазият тўғрисидаги якуний хулосаларда меъёрий талабларга тўлиқ (30,8%), қисман (38,5 %) мувофиқлик ва умуман, мувофиқлик (30,8%) улуший кўрсаткичлари ўз ифодасини топган.

Хавф - хатарнинг олдини олиш. Бугунги кунда UZ-CERT хизмати ходимлари томонидан олиб борилаётган изланишлар компьютер ҳодисалари бўйича маълумот берувчи автоматлаштирилган тизим яратиш ва уни имкон қадар тезроқ ишга туширишга қаратилган. Мутахассисларнинг фикрича, мазкур тизим ахборот хавфсизлиги борасидаги барча заифликлар ва рухсатсиз кириш усулларини жамлаш ҳамда таснифлаш, мавжуд таҳдидларнинг олдини олиш бўйича тавсияномалар бериш, шунингдек, рўй

берган нохуш ҳодиса (инсидент, таҳдид) лар статистикаси асосида айрим башоратлар ишлаб чиқиш учун кенг имкониятлар яратади.

Таъкидлаш жоизки, UZ-CERT хизмати республикада ахборот хавфсизлиги аудити ва мониторинги бўйича фаолият юритувчи ягона хизмат ҳисобланса ҳам, у назорат қилувчи ташкилот мақомига эга эмас. Шундай бўлсада, мутахассислар томонидан турли компанияларда ўтказилган кузатув натижалари асосида ишлаб чиқилган хулоса, тавсия ва таклифлар беқиёс аҳамиятга молик. Негаки, ахборот ресурслари ёки ахборот тизимлари муҳофазасини ташкил этишда уларнинг мулкдорлари ва эгалари амалга ошириши зарур бўлган энг муҳим чора - тадбирлар мажмуаси сифатида жуда ҳам фойдали бўлиши мумкин.

Алишер Навоий сўзлари билан айтганда: "Хотир-и жамъ истасанг аввал хавотир дафъин эт, Кимда хавотир бўлмаса осуда хотир бўлғуси" дир.

1.3. Ахборотлар хавфсизлигини таъминлашда қўйиладиган талаблар

1. Тармоқлараро ахборот хавфсизлигини таъминлаш мақсадида Республикамизда ахборот хавфсизлигини ҳуқуқий ва ташкилий жиҳатдан таъминлаш бўйича қатор қарорлар ишлаб чиқилди. Жумладан:

1.1. ахборот хавфсизлигини таъминлашнинг дастурлар мажмуасини ишлаб чиқариш;

1.2. ахборот хавфсизлигини таъминлаш бўйича қабул қилинган қонун ва қоидага риоя қилиш ва ижросини таъминлаш мутахассисларнинг асосий вазифаларига айланган.

2. Ахборотларни ҳимоя қилишда қўлланиладиган услублар:

2.1. Сонлар назариясининг алгоритмлари;

2.2. Ахборотни бузиш учун ҳаракат қилинаётган турли ҳужумларга бардош бера оладиган, махфийлик даражаси юкори бўлган криптосистемаларни яратиш;

2.3. Ахборотларни ҳимоялашда қўлланиладиган криптоалгоритмларнинг математик структурасини ривожлантириш программистлар учун янги илмий йўналишларни белгилаб олиш имкони яратилади.

II- БЎЛИМ. ИНТЕРНЕТ ТАРМОҒИДА ИНФОРМАЦИОН ХАВФСИЗЛИК

2.1. Интернет тармоғи тушунчаси ва ундаги информацион хавфсизлик

Интернет – бу бутун жаҳон компьютер тармоқлари мажмуидир.

Интернет – **Interconnected Computer Networks** сўзларидан олинган бўлиб ягона стандарт асосида фаолият кўрсатувчи жаҳон глобал компьютер тармоғидир. Унинг маъноси: “Тармоқлараро” деган маънони англатади. У маҳаллий (локал) компьютер тармоқларини бирлаштирувчи информацион тизим бўлиб, унинг алоҳида ахборот майдонига эга бўлган виртуал тўпламдан ташкил топади. Интернет, унга уланган тармоққа кирувчи барча компьютернинг ўзаро маълумотлар алмашиш имконини яратиб беради. Ўзининг компьютери орқали интернетнинг ҳар бир мижози шаҳар ёки мамлакатга ахборот узатиши мумкин.

Интернет XX асрнинг буюк кашфиётларидан бири бўлиб, ушбу кашфиёт туфайли бутун жаҳон бўйлаб ёйилиб кетган 100 миллионлаб компьютерларнинг ягона информацион муҳитга бирлаштириш имкониятини берди. Интернет биринчи навбатда тармоқ мижозларига ўзаро маълумотлар алмашиш, виртуал мулоқот қилиш имкониятини яратиб берувчи ягона “Информацион магистрал” вазифасини ўтайди. Иккинчидан эса унда мавжуд бўлган маълумотлар базаси мажмуаси дунё билимлар ахборотининг омборини ташкил этади. Интернет бугунги кунда дунё бозорини ўрганиш, маркетинг ишларини ташкил этишдаги замонавий бизнеснинг энг муҳим воситаларидан биридир.

Юқорида таъкидлаб ўтганимиздек, интернет тармоқлараро информациялар алмашувини таъминловчи магистралдир. Унинг ёрдамида дунё билимлар манбаига кириш, қисқа вақт ичида кўплаб маълумотларни

йиғиш, ишлаб чиқаришни ва унинг техник воситаларини масофадан туриб бошқариш мумкин. Шу билан бир қаторда интернетнинг ушбу имкониятларидан фойдаланиб тармоқдаги бегона компьютерларни бошқариш, уларнинг маълумотлар базасига кириш, нусха кўчириш, ғаразли мақсадда турли хил вируслар тарқатиш каби ноқонуний ишларни амалга ошириш мумкин. Интернетда мавжуд бўлган ушбу хавф, яъни информацион хавфсизлик муаммолари бевосита тармоқнинг хусусиятларидан келиб чиқади. Тармоқ хизматини эса ўзаро келишилган қоида ("протокол") асосида ишловчи жуфтлик "сервер" ва "мижоз" программа таъминоти бажаради. Ушбу протоколлар миқёсида ҳам "сервер", ҳам "мижоз" программалари рухсат этилган операцияларни бажариш воситаларига эга. Масалан, HTTP протоколидаги форматлаш командалари, Web саҳифаларда жойлаштирилган товуш, видеоанимациялар ва ҳар хил актив объектлар кўринишидаги микропрограммалар. Худди шундай рухсат этилган операциялар, актив объектлардан фойдаланиб интернетда баъзи бир ноқонуний ҳаракатларни амалга ошириш, тармоқдаги компьютерларга ва маълумотлар базасига кириш, ҳамда уларга таҳдид солиш мумкин бўлади.

Бу хавф ва таҳдид қуйидагилар иборат:

1. Тармоқдаги компьютерларга рухсатсиз кириш ва уни масофадан туриб бошқариш, уларга сизнинг манфаатингизга зид бўлган программаларни жойлаштириш мумкин.

2. Web саҳифаларда жойлаштирилган "актив объект" лар агрессив программа кодлари бўлиб, сиз учун хавфли "вирус" ёки жосус программа вазифасини ўташи мумкин.

3. Интернетда узатилаётган маълумотлар йўл – йўлакай алоқа каналлари ёки тармоқ тугунларида тутиб олиниши, улардан нусха кўчирилиши, алмаштирилиши мумкин.

4. Давлат муассаси, корхона (фирма) фаолияти, молиявий аҳволи ва унинг ходимлари ҳақидаги маълумотларни разведка қилиши, ўғирлаши ва шу орқали сизнинг шахсий ҳаётингизга, корхона ривожига таҳдид солиши мумкин.

5. Интернетда эълон қилинаётган ҳар қандай маълумот ҳам жамият учун фойдали бўлмаслиги мумкин. Яъни, интернет орқали бизнинг маънавиятимизга, маданиятимизга ва эътиқодимизга зид бўлган информацияларни кириб келиш эҳтимоли ҳам мавжуд.

2.2. Интернет тармоғида хавфсизликнинг олдини олиш чора-тадбирлари

Интернет фойдаланувчиси, ушбу хавфларни олдини олиш учун қуйидаги техник ечим ва ташкилий ишларни амалга ошириши зарур:

1. Шахсий компьютерга ва маҳаллий компьютер тармоғига, ҳамда унда мавжуд бўлган информацион ресурсларга ташқаридан интернет орқали киришни чекловчи ва ушбу жараённи назорат қилиш имконини берувчи техник ва программавий усуллардан фойдаланиш;
2. Тармоқдаги информацион мулоқот иштирокчилари ва улар узатаётган маълумотларни асл нусхасига мослигини текшириш;
3. Маълумотларни узатиш ва қабул қилишда криптография усулларидан фойдаланиш;
4. Вирусларга қарши назоратчи ва даволовчи программалардан фойдаланиш;
5. Шахсий компьютер ва маҳаллий компьютер тармоғига бегона шахсларни қўймаслик ва уларда мавжуд бўлган маълумотлардан нусха олиш имкониятларини чекловчи ташкилий ишларни амалга ошириш.

Бундан ташқари информацион хавфсизликни таъминлаш борасида интернет фойдаланувчилари орасида ўрнатилмаган тартиб қоидалар мавжуд. Улардан баъзи бирларини келтирамиз:

- Ҳеч қачон ҳеч кимга интернетдаги ўз номингиз ва паролингизни айтманг;
- Ҳеч қачон ҳеч кимга ўзингиз ва оила аъзоларингиз ҳақидаги шахсий, ҳамда ишхонангизга оид маълумотларни (исми шарифингиз, уй адресингиз, банкдаги ҳисоб рақамингиз, иш жойингиз ва унинг ходимлари ҳақидаги маълумотларни ва ҳ.о) интернет орқали юборманг;
- Электрон адресингиздан (ЕтаП) мақсадли фойдаланинг, интернет орқали программалар алмашманг;
- Интернетда тарқатилаётган дуч келган программалардан фойдаланманг. Программаларни фақат ишончли, эгаси маълум бўлган серверлардан кўчиринг.
- Электрон почта орқали юборилган "актив обоект"лар ва программаларни ишлатманг, **.exe** қўшимчали ўз – ўзидан очилувчи Сизга номаълум архив ҳолидаги материалларни очманг;
- Электрон почта хизматидан фойдаланаётганингизда маълумотларни шифрлаш зарур, яъни криптография усулларидан албатта фойдаланинг;
- Эгаси сиз учун номаълум бўлган хатларни очманг;
- Эгаси маълум бўлган ва унинг сифатига кафолат бурувчи антивирус программаларидан фойдаланинг ва уларни мунтазам янгилаб боринг;
- Интернетда мавжуд бўлган информацион ресурслар ва программалардан уларнинг авторлари рухсатисиз фойдаланманг;
- Тармоқдаги бегона компьютер ва серверларнинг IP адресларини аниқлаш ва шу орқали рухсат этилмаган серверлар ва

информацион ресурларга кириш, нусха кўчириш, вируслар тарқатиш каби ноқонуний программалаштириш ишлари билан шуғулланманг, бу жиноятдир.

2.3. Интернет тармоғида ахборотларни ҳимоя қилишнинг стандартлари ва усуллари

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

Аслида эса бундай эмас. Ўтмишда Интернетдаги ахборот хусусий **VAN** ёки корпаратив тармоқларга нисбатан камроқ ҳимоя қилинган бўлса ҳам, хозирги вақтда Интернетда трафикни ҳимоя қилиш механизмларини тадбиқ қилиш учун кўп хатти-ҳаракатлар қилинмокда.

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

Кўриб чиқилаётган стандартларни улар нимани ҳимоя қилинаётганлигига: уланишларними ёки иловаларними - қараб мос равишда таснифлаш мумкин. **SSL** ва **S/WAN** каби стандартлар Интернетда коммуникацияларни ҳимоя қилиш учун мўлжалланган, шунга қарамай **SSL**

асосан **Web-**иловалар билан ишлатилади. Бошқа томондан **S/HTTP** ва **S/MIME** махфийликни ва аутентификацияни таъминлашга йўналтирилгандир (**S/HTTP-Web-**иловалар учун, **S/MIME** эса - электрон почта учун). **SET** фақат электрон тижоратнинг транзакциясини ҳимоя қилишни таъминлайди. **S/HTTP** ва **SSL Web-** иловаларни ҳимоя қилиш учун.

Интернет учун маълумотларни ҳимоя қилишнинг баъзи бир стандартлари

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

Web-иловалар иккита баённомалар: **Secure HTTP** ва **Secure Sockets Layer** билан ҳимоя қилингандир, улар серверлар ва браузерлар учун аутентификацияни, ҳамда Web-сервер ва браузер ўртасидаги уланишлар учун

маълумотларни махфийлигини ва бутунлигини таъминлайди. Биринчи навбатда гиперматнни узатиш баённомасини (HTTP) қўллаб-қувватлаш учун мўлжалланган **S/HTTP** ҳужжатларни муаллифлаштиришни ва ҳимоя қилишни таъминлайди.

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

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

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

Интернетда электрон почтани ҳимоя қилиш учун кўплаб турли хил баённомалар мавжуддир, лекин улардан фақат битта ёки иккитаси етарлича кенг ишлатилади.

PEM (Privaci Enhanced Mail) - бу очиқ ёки симметрик калитларни ишлатиб электрон почтани ҳимоя қилиш учун Интернетнинг стандартидир. У камроқ қўлла-нилади, чунки у MIME қўллаб-қувватлайдиган электрон жўнатмаларнинг янги шаклини қайта ишлаш учун мўлжалланмаган ва, бундан ташқари, калитларни бериш учун сертификатланган марказларнинг қатъий иерархиясини талаб этади.

S/MIME - бу янги стандартдир. У патентланган ва лицензияланган RSA Data Security Inc. компанияларнинг кўплаб криптографик алгоритмларни ишга туширади. **S/MIME** рақамли сертификатларни

ишлатади, ва натижада, аутентификацияни таъминлашда сертификацияланган марказга (корпоратив ёки глобал) асосланади.

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

2.4. Маълумотларни узатиш тармоқларида ахборот хавфсизлигини таъминлаш масаласи

Ҳозирги кунда ахборот тизимида долзарб масалалардан бири маълумотларни узатиш тармоғи (МУТ) да хавфсизликни таъминлаш масаласидир. Чунки МУТ нинг ривожланиши, кенгайиши унинг хавфсизлигини таъминлашга қийинчилик туғдирмоқда.

МУТ га таҳдид турли хил йўллар билан уюштирилиши мумкин ва натижада қуйидаги кўринишдаги қоидабузарликлар келиб чиқиши мумкин:

- дастурий қисмига янги қўшимча функция қўшиш билан, яъни вирус ва бошқа дастурий таъминотлар;
- ахборот тизимида маълумотлардан рухсатсиз, эркин фойдаланиш;
- бошқа бир фойдаланувчи номидан иш юритиш, яъни унинг ҳуқуқларидан фойдаланиш;

- қайта узатгич сифатида иккита ўзаро фойдаланувчининг алоқа линиясига боғланиш;
- қачон, ким қандай маълумотни қайси тармоқ ресурсидан олишини ўрганиш;
- нотўғри ахборот киритиш;
- нотўғри ахборот киритиш йўли билан баённомани бузиш.

Юқорида келтирилган ҳодисаларнинг олдини олиш учун МУТ да хавфни таҳлил қилиш жуда муҳим хусусиятга эга. МУТ да ахборот хавфини таҳлил қилишдан мақсад тармоқлардаги ва унинг ресурсларидаги хавф тавсифини аниқлашдан иборат.

Хавфни таҳлил этиш усули

МУТ да хавфни таҳлил қилиш усули бошқа ахборот тизимларидан деярли, фарқ қилмайди. Ажралиб турадиган қисми шундаки, МУТ даги бошланғич омилларни, шунингдек, ишчан қисмининг муҳимлигини, таҳдиднинг қоидабузарлигига боғлиқлигини ва тизимнинг заиф жойларини аниқланишидадир.

МУТ да хавфни таҳлил этиш жараёни қуйидаги босқичлардан иборат:

- ҳимоя ўлчови (чегараси) ва объектни тасвирлаш;
- ресурсларни идентификатциялаш (айнанлаш) ва унинг сонли кўрсаткичини таҳлил қилиш;
- ахборот хавфсизлигини бузишга олиб келувчи таҳдидни таҳлил этиш;
- заифлигини таҳлил этиш;
- ахборот хавфсизлигини таъминлашдаги мавжуд ва гумон воситаларни таҳлил этиш;
- хавфни таҳлил этиш.

Ахборот хавфсизлигини таҳлил этиш - бу - МУТ даги ахборот хавфсизлигининг тизим тавсифномаларини ўрганиш жараёни бўлиб, у номувофиқ воқеалар рўй берган тақдирда кутилаётган зарарни аниқлаш мақсадида эҳтимоллик ҳисоблашлар ёрдамида ўтказилади.

Хавф таҳлилининг вазифаси тизим у ёки бу хавфнинг номувофиқлик даражасини аниқлашдан иборатдир.

МУТ даги хавфни таҳлил этишни олиб боришда қуйидаги ҳолатларга эътибор бериш керак:

- мавжуд хавф ва унинг даражасига;
- мумкин бўлган хавф даражасига;
- МУТ даги заиф жойларга;
- хавфни мумкин бўлган йўқолиш даражасига;

Ҳар бир бўлимлар учун махсус текширув олиб бориш талаб этилади.

Хавфни таҳлил этиш ўз ичига ахборот идентификатсияси ресурсини, қийматини аниқлаш ва таҳдид натижасида ахборот хавфсизлигининг зарарини аниқлашдан иборатдир. Хавфни таҳлил этишнинг турли хил: асосий ва тўлиқ қарашлари мавжуд. Булардан фойдаланиш талабга қараб танланади. Масалан, корхонанинг ахборот хавфсизилиги даражасига, таҳдиднинг тавсифига ва унга қарши чоранинг самарадорлигига боғлиқдир.

Асосий вариант - бу кам меҳнат талаблиги билан ажралиб туради. Асосий вариант корхона ахборот ресурслари ҳамда ресурс қиймати катта бўлмаганда ишлатилади. Шунинг учун, асосий вариантда таҳдидни таҳлил қилишда оддийроқ усул ишлатилади. Унинг камчилиги шундаки, у таҳдид хавфсизлигини эҳтимоллигини баҳоламайди.

Бу усул фақат, агар корхонанинг ҳимоя ресурси катта бўлмаганда қўллаш мақсадга мувофиқдир, акс ҳолда, бу усул хавфсизликни таъминлашга етарли бўлмайди. Бундай ҳолларда тўлиқ вариант қўлланилади. Тўлиқ хавф таҳлилини ўтказишда қуйидагиларни аниқлаш зарурдир:

- таҳдиднинг эҳтимоллигини баҳолаш;
- ресурсларнинг қийматини аниқлаш;
- ресурсларнинг заифлигини аниқлаш;
- хавфни баҳолаш.

Хавф эҳтимоллигини баҳолаш жараёни, бу - тармоқ ресурсларини ва уларнинг инфраструктурасининг ахборотларини биргаликда боғланишдаги қиймати ҳамда заифлик томонлари ҳимоя тармоғи тизимида ахборот хавфининг сонли ўлчовини ташқи янги технологиялар ёки янги лойиҳалар билан боғлиқ равишда аниқланишидир. Тўлиқ хавфни таҳлил этишдан мақсад хавф тавсифини ва унинг ресурсларини аниқлашдир, яъни МУТ ахборот хавфсизлигини таъминлашнинг зарурий воситасини танлашдан

иборат. МУТ хавфсизликни таъминлаш қуйидаги хавф эҳтимолликларни баҳолашни талаб этади:

- ресурсларни идентификатциялашни ва унинг сонли кўрсаткичларини баҳолаш;
- таҳдидни баҳолаш;
- заифликни баҳолаш;
- мавжуд ва таҳмин қилинаётган ахборот таъминлашдаги воситани баҳолаш;
- хавф эҳтимоллигини баҳолаш.

Маълумотларни узатиш тармоқлари (МУТ) да вужудга келадиган хавфни олдини олишга қаратилган бир қанча дастурий воситалар ишлаб чиқилган, шуларнинг баъзи бирлари билан III бобда танишиб чиқамиз.

III- БЎЛИМ. АХБОРОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ДАСТУРИЙ ВОСИТАЛАРИ

3.1. Маълумотларни узатиш тармоқларида хавфни бартараф этишга мўлжалланган дастурий воситалар

Маълумотларни узатиш тармоқлари (МУТ) да вужудга келиши мумкин бўлган хавфни таҳлил этиш етарлича қийин бўлгани, катта меҳнат талаб қилганлиги учун хавфни таҳлил этишнинг дастурий воситалари ишлаб чиқилган.

Ҳозирги кунда сотувда бир қанча хавфни таҳлил қилиш учун мўлжалланган дастурий воситалар мавжуддир. Ҳозирда кенг қўлланилаётган дастурий воситалардан Кондор + (ёки Кондор 2006) ва Гриф 2006 ни кўриб чиқамиз. Бунда Кондор ахборот хавсизлиги сиёсатини текширишга ва таҳлил этишга мўлжалланган, Гриф эса ахборот хавфини бошқариш ва таҳлил қилишга мўлжалланган. Бу дастурий воситалар алоҳида вазифаларни бажарсада, улар алоҳида маҳсулотлар эмас. Бу икки дастурий воситалардан фойдаланиш учун биринчи навбатда Россияданинг Digital Security компанияси маҳсулоти ҳисобланган Digital Security Office 2006 ни компьютерга ўрнатиш керак бўлади.

Хавфни бошқаришнинг Кондор+ тизими Россиядаги Digital Security компанияси мутахассисларга (АТ - бошқарувчилари, хавфсизлик зобитларига) корхона ахборот хавфсизлиги сиёсатини текширишга мўлжалланган ISO 17799 стандартига асосан Кондор+ дастурий маҳсулотини яратди.

Кондор+ асосий таҳлил учун кўпроқ мўлжалланган бўлиб, икки юздан ортиқ саволларга ISO 17799 стандартига асосан мутахассислар тўлиқ

маълумот оладилар. Ҳисоботда барча хавфсизлик сиёсатидаги стандартлар кўрсатилади.

Бу тизимдан фойдаланувчи ҳисоботни диаграмма кўринишида олиш мумкин, яъни бу тизим хавфни эҳтимоллигини сифат усули билан аниқлайди, яъни юқори, ўртача, паст даражалар билан.

Гриф - дастурий воситаси Россиянинг Digital Security компанияси томонидан яратилган бўлиб, у ресурсларни ҳимоя хавфини таҳлил этишга мўлжалланган қулай ва кучли дастурий воситадир.

Ахборот хавфсизлигида тўлиқ ахборот хавфини таҳлил этишда Гриф дастурий воситаси қўлланилади. Гриф ёрдамида мустақил тарзда АТ бошқарувчиси ва тизим маъмури, компаниянинг ахборот хавфсизлигида масъул шахс оддий ва осон йўл билан хавфни эҳтимоллигини баҳолаш имкониятига эга бўлади.

Гриф хавфни таҳлил этиш усули беш босқичдан иборат:

- Биринчи босқичда корхонанинг тўлиқ ахборот ресурслари аниқланади.
- Иккинчи босқичда ахборот тизими учун қимматли бўлган ҳамма кўринишдаги ахборотлар киритилади. Киргизилган гуруҳнинг қимматли ахбороти фойдаланувчи томонидан олдин кўрсатилган жойга жойлаштирилиши керак. (Сервер, ишчи станциялар ва ҳоказо) ҳар бир гуруҳнинг қимматли ахборотининг зарари кўрсатилади.
- Учинчи босқичда барча кўринишдаги фойдаланувчи гуруҳлар аниқланади, кейин бу гуруҳлар қайси ахборот ресурсидан фойдаланиши аниқланади. Охирида қимматли ахборотдан иборат ресурсдан фойдаланувчиларни кўриниши (маҳаллий ва ёки масофавий) ва ҳуқуқлари (ўқиш, ёзиш, ўчириш) аниқланади;

- Тўртинчи босқичда ҳимоя воситасини аниқлаш учун сўров ўтказилади. Шунингдек, ҳимоя воситасини таъминлашга кетадиган сарф ҳам тизимга киритилади;
- Тугалланувчи босқичда хавфсизлик сиёсати саволлари рўйхатига жавоб бериш зарурдир, амалга оширилаётган тизим, тизимнинг ҳимоя даражасини баҳолашга ва хавф эҳтимоллигини баҳолашга имконият туғдиради.
- Бу босқич мавжуд хавф тизимини ишончли баҳолаш учун зарурдир.
- Гриф дастурий комплексининг ҳисобот тизими 3 қисмдан ташкил топган: биринчи "ресурсларнинг ахборот хавфи", иккинчи "хавф ва зарарнинг ўзаро боғлиқлиги", учинчи "ахборот тизимидаги мавжуд хавф тўғрисида" умумий хулоса.

Хулоса қилиб айтганда, бу соҳада ижод қилган бир қатор олимлар қарашлари ҳамда юқоридаги фикрларнинг таҳлили шуни кўрсатадики, МУТ да ахборот хавфсизлигини таъминлашда аниқ таҳлил ва баҳолашнинг усул-воситаларидан фойдаланиш зарурдир.

3.2. PGP (Pretty Good Privacy) криптографик дастури

PGP – бу тўлиқ конфиденциал (сирли) лик асосида электрон кўринишда фойдаланувчиларга маълумотлар билан алмашиш имконини берадиган юқори даражадаги қулайликка эга криптографик (шифрли) дастурдир.

Бу дастурнинг асосий устунлиги шундаки, шифрланган хабарлар билан алмашинишда фойдаланувчилар бир – бирига калитларни узатишлари шарт эмас. Бу дастур ишлашнинг янги принципи асосида қурилган бўлиб, унда фойдаланувчилар бир – бирларига интернет орқали бемалол конфиденциал хабарлар билан алмаша оладилар ва бунда уларда бирон учинчи шахснинг

уларнинг хабарларига рухсатсиз кириши мумкинлиги тўғрисида хавотирланиш пайдо бўлмайди ҳам, чунки бу дастур очиқ калитлар алмашинувига ёки жамоавий криптография асосида қурилган.

PGP да бир – бирига боғлиқ иккита калит принципи ишлатилади: очиқ ва ёпиқ калитлар. Ёпиқ калит фақат сизга киришга рухсат бўлади, очиқ калитни эса ўз танишларингизга тарқатишингиз мумкин.

Бу дастурнинг ажойиб устунлиги устунлиги шундаки, шунингдек: у бепул, яъни, унга ҳеч қанақа сарф – харажат қилиб ўтирмайсиз, ихтиёрий фойдаланувчи ярим соат давомида интернет орқали бу дастурни ўз компьютерига юклаб олса бўлади. PGP хабарни шундай шифрлайдики, уни қабул қилиб олувчидан ташқари ҳеч ким шифрлай олмайди. PGP дастурининг яратувчиси Филипп Циммерман очиқ – ойдин бу дастур кодини эълон қилди ва бу кодни бир неча марта юқори савияли крипто – аналитиклар текшириб кўришганда бу дастурдан бирорталари камчилик топишолмади.

Филипп Циммерман дастур яратилиши сабабини қуйидагича тушунтиради: “Одамларга сирлилик зарур. PGP шундай информацион асрда ўз хабари сирлилиги тўғрисида хавотир оладиган одамлар томонидан алангаланаётган оловдек тарқалмоқда.Ҳозирги кунда инсон ҳуқуқларини ҳимоя қилувчи ташкилотлар PGP ни ўз одамларини чет юртларда ҳимоя қилиш учун ишлатадилар. Шунингдек, Amnesty International ташкилоти ҳам бу дастурдан фойдаланади”.

Интернет фойдаланувчилари бу дастурдан фойдаланишнинг сабаби худди одамлар ихтиёрий одам ўқий оладиган откриткаларда эмас, балки конвертларда хат жўнатишлари сабабидек. Гап шундаки, ҳозирда мавжуд бўлган формат кўринишидаги электрон хабарлар интернет провайдер серверига доступи бўлган ихтиёрий одам томонидан ўқилиб, архив қилиб

олиниб қўйилиши мумкин. Ҳозирги кунда махсус хизмат намоёндалари телефон тармоғида гаплашишдан кўра кўпчилик шахсларнинг электрон манзилига уланиш ҳам арзон, ҳам осондир. Умуман ҳеч бир иш қилиниши шарт эмас. Ҳаммасини компьютер бажаради. Махсус хизмат агенти ёки бошқа бир киши компьютерга ўтириб хатларни кўриб чиқиш қолади холос. Илмий – техник ривожланиш бундай одамларни ишини ривожлантирди, зероки, худди шу ривожланиш интернет тармоғидан фойдаланувчилар, учинчи шахс аралашувидан, ҳаттоки бир неча миллион доллар турадиган компьютер шифрлай олмайдиган сирларни имконини яратиб берди.

PGP қандай ишлайди

Фойдаланувчи PGP ёрдамида хабарларни шифрлайди, шифрлашни ишончлилигини оширишда модем орқали хабарни жўнатиш вақтини қисқартириш мақсадида биринчи бўлиб дастур матнини қисқартиради. Криптоанализнинг асосий усуллари (шифрланган хабарларни очиш) калитни топишга ёрдам берадиган матнли файлларга хос “расмлар” тадқиқотига асосланган қисиш бу “расмлар”ни ликвидирлайди, шундай қилиб, шифрланган хабарнинг ишончлилигини оширади. Кейинчалик PGP клавиатура тугмаларини тасодифий ишлатиш ва сичқончани тасодифий ҳаракатига асосланган сонлардан иборат сессион калитни тўғрилайди.

Хабар шифрланган заҳоти шифрланган матн билан биргаликда қабул қилувчи жўнатадиган калит қабул қилинган жамоат калити ёрдамида сессион калит шифрланади.

Калит орқали шифрни очиш тескари изчиллик билан бўлади. Қабул қилувчи хабари PGP дастури шифрланган матн шифрини кейинчалик очиш учун қабул қилувчининг вақтинчалик ёпиқ сессион калитини ишлатади.

Калитлар

Калит – бу матнни шифрлашда криптографик алгоритм ишлатиладиган рақамдир. Қоидага кўра, калитлар жуда катта рақамлардир. Унинг ўлчови битда ҳисобланади, 1024 бит ўлчовли калитлар жуда катта ҳисобланади. Оммавий криптографияда калит қанчалик катта бўлса, хабарни очиб кириш ҳам шунчалик қийин бўлади. Очиқ ва ёпиқ калитлар бир – бири билан боғланган бўлсада очиқ калитни сонига қараб ёпиқ калитни топиш жуда мушкул, зеро катта қудратли компьютерларда бу иш анча осон кечади. Шунинг учун мос ўлчовли калит танлаш жуда муҳимдир: етарли даражада каттаси хафвсизликни, кичкинаси эса ишлаш режимининг тезлигини таъминлайди. Бундан ташқари, матнни ўқишга қизиқадиган шахснинг қанчалик шифрни очишга қизиқишини, қанча вақт лозимлигини ва унинг қўлида қандай ресурслар борлигини ҳисобга олиш лозим. Қанчалик калит катта бўлса, у шунчалик узоқ вақт давомида ишончли бўлади. Шунинг учун ҳам шифрланган хабарингиз узоқ вақт сақланишини истасангиз, у учун каттароқ калитдан фойдаланиш лозим. Калит компьютернинг қаттиқ дискида шифрланган ҳолатда 2 хил файл кўринишида сақланади: бири очиш учун, иккинчиси эса ёпиш учун. Бу файллар “узуклар” (key rings) деб аталади. PGP дастури билан ишлаш давомида, қоидага биноан сиз танишларингизнинг очиқ калитларини очиқ узукларга киритасиз. Сизнинг ёпиқ калитингиз ёпиқ узукингизда сақланади. Ёпиқ калитни ёқотсангиз ёпиқ узукда сақланаётган калитлар билан хабарларни расшифровка қилолмайсиз.

Рақамли имзо

Қабул қилинган хатнинг бус – бутунлиги ва унинг ким томонидан жўнатилганлигини кўриш имконини берадиган яна бир бу дастурнинг устунлиги бу рақамли имзодан фойдаланиш имкониятидир. Рақамли имзо қўл имзоси бажарадиган вазифани бажаради. Лекин қўл имзосини сохталаштириш осон, рақамли имзони эса сохталаштириб бўлмайди.

ХЭШ – функция

Яна бир устунлиги PGP дастурида хэш – функцияни ишлатишдир, хабарни бирор – бир ўзгартириш, ҳаттоки 1 бит чиқмайдиган ўзгартириш киритилганда ҳам хэш – функция натижаси ўзгармайди. Матн билан бирга жўнатиладиган “имзо” ёпиқ калит ва хэш – функция ёрдамида яратилади. Хабар қабул қилишда қабул қилувчи PGP дан фойдаланиб имзони текширади ва хабарнинг бошланғич ҳолатини тиклайди. Хэш – функциянинг ишончли формуласини ишлатишда ундан мзони олиб бошқа бир ҳужжатга қўйиб бўлмайди, ёки хабарга ўзгартириш киритиб бўлмайди. Имзоланган ҳужжатни бирор – бир ўзгартириш имзони текширганда дарров намоён бўлади.

Парол ибора

Кўпчилик одамлар учинчи шахсдан ҳимоялайдиган компьютерларнинг парол тизимидан хабардордир. Парол ибора – назарий жиҳатдан парол сўздан анча ишончлироқ бўлган бир нечта сўзларнинг мужассамлашувидир. Бир нечта парол сўзлардан иборат парол ибора “луғат ҳужуми” деб аталадиган луғатга уланган дастури ёрдамида сизнинг паролингизни топишга ҳаракат қиладиган ҳужумчилар ҳужуми олдида улкан қалъадир(ишончлидир). Энг ишончли пароллар бу пунктуацион белгилар, сонлар ва катта – кичик ҳарфлардан иборат сўзлардан тузилган узун парол иборалардир.

Парол ибора учинчи шахс топа олмайдиган ва кейинчалик эсдан чиқариб қўйилмайдиган бўлиши керак. Парол иборангизни унутсангиз, ҳеч қачон шифрланган хабарни қайта тиклай олмайсиз. Сизнинг очиқ калитингиз парол иборасисиз ҳеч нарса ва сиз бу ҳолатда ҳеч нарса қила олмайсиз.

PGP дастурини ишлатишда асосий одимлар

1. Дастурни компьютерингизга ўрнатинг.

2. Очиқ ва ёпиқ калит яратинг. PGP дастурини ишлатишдан олдин иккита калитлар жуфтини яратиш лозим, яъни, фақат сизга киришга рухсат берадиган ёпиқ калит ва танишларингизга бериладиган очиқ калит.

3. Очиқ калитингизни танишларингиз очиқ калитлари билан алмаштиринг. Сизнинг очиқ калитингиз атиги кичкина файл, шининг учун уни серверга жойлаштириш ёки, почта хабарини бириктириш, файлларни кўчириш ёки хабарни киритиш мумкин.

4. Очиқ калитнинг тўғрилигиги ишонч ҳосил қилиш. Танишларингизнинг очиқ калитларини олган заҳотиёқ уларни очиқ калитлар узугига киритишингиз мумкин. Кейинчалик сиз албатта ҳақиқатдан ҳам танишларингиз очиқ калитлари эканлигига ишонч ҳосил қилишингиз лозим, яъни, улар билан боғланиб, телефонда очиқ калитлар беришини айтиш ва ўзингиз ҳам калитингизни унга айтишингиз орқали. Ҳақиқатдан ҳам калит уникилигига ишонч ҳосил қилган заҳотингиз уни ёзиб қўйиб, бу очиқ калитни тасдиқлашингиз мумкин.

5. Шифрлаш ва рақамли имзо орқали корреспонденцияларга гувоҳлик бериш, жуфт калитлар киритилиши ва очиқ калитлар алмашинувидан ўз рақамли имзоингиз билан тасдиқлашингиз мумкин. Агар электрон почта PGP дастурини қўлласа, сиз ўз хабарингизни худди шу дастурда бўла туриб шифрлашингиз ва шифрни очишингиз мумкин. Агар электрон почтангиз PGP ни қўлламаса, унда сиз бошқа усулда хабарингизни шифрлашингиз мумкин (алмашув буфери ёки бутун файлни ишлатиш). Жўнатувчининг асллилигини текшириш ва келган хабарни дешифровкалашингиз

6. Сизга биров шифрланган хабар жўнатганда, уни дешифровкалашингиз, жўнатувчи шахсини аслилигини текширишингиз ва хабарнинг бутунлилигини кўришингиз мумкин. Агар электрон почтангиз PGP дастурини қўлламаса, уни алмаштириш буфери билан текшириб кўришингиз мумкин.

7. Файлларни йўқотиш. Бирор – бир файлни тўлиқ йўқ қилмоқчи бўлсангиз, wipe командасидан фойдаланишингиз мумкин. Шунда файлларни қайта тиклаб бўлмайди.

PGP дастурининг ўрнатилиши

Қуйида дастурни ўрнатилишида чиқадиган хабарлар ва буйруқлар берилган, уларни ўрнатишда албатта бажариш лозим:

PGP Installation program

Next ни босинг

Software License agreement

Yes ни босинг

User information

Name_____

Company _____

Исмингиз ва компания номини киритиб, Next ни босинг

Setup: choose installation directory

Next ни босинг

Select components:

Бу ерда ўрнатиш компонентларини танлаш лозим

* Program files

Eudora Plugin

* Microsoft Exchange/Outlook plugin

* Microsoft Outlook Express plugin

* User's manual Adobe

* PGP disk for Windows

Ўрнатиши лозим бўлган компонентларни ажратинг. Eudora электрон почта дастуридан фойдалансангиз, уни ажратиш шартмас. Агар интернетда ишлаш учун Microsoft Exchange/Outlook дан фойдалансангиз, уни танланг. Windows-98 да қурилган электрон дастур Microsoft Outlook ҳам худди шундай.

Next ни босинг

Check setup information

Next ни босинг

Қаттиқ дискка дастурлаш файлларини кўчириш бошланади.

Компьютер перезагрузкасидан сўнг автоматик равишда калитлар яратиш операциясини бошлаш учун "Yes I want to run PGP keys" тугмасини босинг.

Finish ни босинг

Windows ни перезагрузка қилиш учун Restart Windows ни босинг. O'K ни босинг

Компьютер перезагрузка қилгандан кейин дастур ўрнатилиши тугатилади. Энди компьютерга иккита калитни ўрнатиш лозим:

public key – очиқ калит; private key – ёпиқ калит.

Калитлар генерацияси

Пережагрузкадан сўнг экраннинг пастки ўнг томон бурчагида PGP нинг белгиси – омбор қулфи рамзи пайдо бўлади.

Сичқонча билан уни босиб, очилган менюдан Launch PGP keys буйруғини танланг. Keys менюсига кириб, NEW KEY буйруғини бажаринг. Next ни босиб, исмингиз ва электрон почта манзилингизни киритинг. Next ни босиб, 2048 калити ўлчовини танланг ва яна next ни босиб key pair never expires иборасини ажратинг ва next ни босинг.

Икки марта махфий паролни киритиб next ни босинг.

Дастур калит жуфтини яратишга киришади. Агар дастурга маълумотлар етишмаса бир неча марта тугмаларни босишни ва сичқончани қимирлатишни сўрайди. Буларни албатта бажариш керак.

Кейин дастур калитлар яратилишини тугаллаганини хабар беради. Кейин next ни босинг. Яна бир марта next ни босинг. Кейин done ни босиш лозим. Ва калитлар жуфтлигини яратиш тугатилади ва дастурдан фойдаланса бўлади.

Дастур ўрнатилгандан кейин танишлар билан очиқ калитларни алмашиш лозим. Бунинг учун LAUNCH PGP KEYS буйруғини бажариб, ўз калитингизни ойнадан танлаб, сичқончанинг ўнг тугмасини босиб, EXPORT буйруғини танлаш лозим.

Ойна пайдо бўлади, унда <ваше имя.asc> номли файл сақланган йўлни кўрсатиш мумкин. Бу файлни ўз танишингизга унинг очиқ калити эвазига жўнатиш лозим. Танишингиз очиқ калитни олган заҳоти, уни сичқончани икки марта босиш орқали ишлатиш лозим, уни ойнада танлаб, IMPORT

буйруғини бажариш лозим. Энди бир – бирингизга хабар олувчи очиқ калитлари билан шифрланган хабарлар билан алмашишингиз мумкин.

Шифрланган хабарни қандай жўнатиш мумкин

Компьютерингизга танишингиз очиқ калитини ўрнатганингиздан сўнг хабарни қуйидагича жўнатишингиз мумкин: Outlook Express почта дастурида хабар тузамиз. Хабар жўнатилишига тайёр бўлгандан сўнг ёки бир марта панелни ўнг томондан 3-белгиси Outlook Express қулф ва сариқ конверт белгисини босамиз, ёки менюнинг tools ва encrypt using PGP га босиш керак ва менюнинг send later номли файлини босамиз. Шунда PGP нинг Recipient selection номли ойнаси пайдо бўлади, унда танишнинг оммавий калитини танлаб, O'K ни босиш лозим. Дастур автоматик равишда хабарни шифрлайди ва уни outbox га жойлаштиради. Энди, интернетга кириб жўнатишга тайёр бўлган хабарни жўнатиш мумкин.

Хабарларни шифрини очиш

Олинган шифрланган хабарни очамиз ва ойнанинг ўнг томонинг 2-белгиси Outlook Express ни ёки менюнинг PGP decrypt message буйруғини босамиз. Бир неча секундда хабар шифри очилиб ойнада пайдо бўлади.

Outlook Express шифрланишидан озгина қийинроқ бўлган PGP нинг яна бир усули мавжуд. PGP ни Outlook Express билан ўрнатиб бўлмаганда бу усулни ишлатиш мумкин.

Outlook Express да хабар яратамиз ва уни edit - select all буйруғи билан ажратиб, copy орқали Windows буферига кўчирамиз. Кейин сичқончани PGP белгисига қўйиб сичқончани босиб encrypt clipboard буйруғини бажарамиз. PGP нинг key selection dialog номли диалог ойнаси пайдо бўлади. Очиқ калитни танлаб пастда ойнада бўлиши учун сичқончани икки марта босиб, O'K ни босиш лозим ва дастур clipboard да сақланганларни шифрлайди.

Кейин олдиндан ажратиб қўйилган матнли хабарни киритиб, хабар майдонига сичқончани қўямиз, ўнг томонини босиб paste бўйруғини бажарамиз. Натижада clipboard да шифрланганлар олдинги хабар билан алмашади ва шифрлаш тугайди. Энди оддий усулда хабар жўнатиш мумкин. Олинган хабарни шифрини очиш ҳам худди шу усулда бажарилади: шифрланган олинган матнни ажратамиз, буфер Windows clipboard ни кўчириб, Windows нинг PGP менюсини киритамиз ва decrypt and verify clipboard буйруғини танлаймиз. Парол киритиш лозим бўлган PGP ойнаси пайдо бўлади, паролни киритиб, OK ни босамиз ва шифри очилган хабар пайдо бўлади. Табиийки, бундан олдинроқ айтилганидек калитлар жуфтлигини яратиш лозим.

IV-БЎЛИМ. ТЕХНИКА ХАВФСИЗЛИГИ МУҲОФАЗАСИ

4.1. Компьютер хонасига қўйиладиган талаблар

Хонани шифти оқ кўк фон билан оқланиши ва деворлари эса яшил рангга оқланиши керак. Бу ранглар офтоб нурланишини бизга ранг иқлимини яратиб беради. Хоналарга қўйилган талаблар ишчи муҳит ишчининг (оператор) иш жойи ташқи муҳит факторлари йиғиндиси бўлиб улар қуйидаги ишлардан иборат: физик, химик, биологик, ахборот, социал – психологик ва эстетик факторлар ташқи муҳит хоссалари бўлиб операторга таъсир этади. Ишчи муҳит турлича бўлиши мумкин: иш жойида ҳаёт фаолиятини таъминловчи воситалар операторнинг талаб этилган меҳнат қобилияти шароитини ҳосил қилади ва уни нохуш факторлар таъсиридан ҳимоя қилади.

Ходимлар самарали фаолият кўрсатиш учун шароит яратиш ва техник воситаларни ишлаш учун хоналар ёруғ, тоза, товуш ва тебранишдан изоляцияланган ҳолатда лойиҳаланади. Шкаф ва деворлар товуш ютувчи плиткалар билан қопланиши мақсадга мувофиқдир.

Хона ҳарорати оптимал ҳароратда 21-23°С да оптимал намлик 40-60 %, чанг концентрацияси 0,2 Мг/м3 дан ва чанг максимал заррача ўлчаш 3 Мк дан ошмаслиги лозим. Хоналарда бундай шароитни ушлаб туриш мақсадида, хоналарни ҳаво алмаштириб туриш кўзда тутилади.

4.2. Операторнинг ишчи жойини ташкил этиш

Операторнинг камфорт ишлашига операторнинг иш жойини ташкил этилганлиги, ахборотнинг кўрсатиш манбаи ва машинанинг бошқариш органлари таъсир кўрсатади. Улар шовқин чиқармаслиги ва иш жараёнида дискомфорт ҳисини уйғотмаслиги, инсон учун максимал қулай бўлиши

керак. ЭҲМ оператори комфорт шароит билан таъминлашнинг асосий йўли уни ишчи жойини ташкилаш киради. Бунда ҳар нарсага эътибор бериши керак кўзга кўринмаган кичкина нарса ҳам узоқ вақт давомидаги жараёндан кейин дискомфорт келтириб чиқариши мумкин ва касаликларга олиб келиши мумкин . Операторнинг узоқ вақт давомида монитор ортида ўтириши натижасида кўриш апаратининг зўриқиши, ишдан қониқмаслик, бош оғриғи, бузилиши чарчоқ ва кўз, бўйин, бел, қўларда оғриклар сезила бошланади.

ЭҲМ операторининг иш жойи дейилганда техник манбалар ва ёрдамчи қурилмалар билан жиҳозланган конкрет ишлаб чиқариш масаларни ечишга мўлжаланган “оператор – одам” иш фаолияти билан шуғуланадиган ҳудуд тушинилади.

Иш жойни меҳнат хавфсизлиги қоидалари ва стандартлар талабларига мос равишда жиҳозлаш керак.

Иш жойи элеменларини жойлаштиришда қуйдагиларга эътибор бериш керак:

- оператор одамнинг ишчи позаси;
- операторга керакли ҳаракатларни амалга оширувчи жой;
- ператор ва ускунани боғловчи жисмоний, кўриш ва эшитиш алоқаси;
- ишчи жойидан ташқарини кўриш имконияти;
- ёзиш ҳамда оператор томонидан ишлатиладиган ҳужжатларни сақлаш имконияти.

Ускунанинг ташқи ва конструктив кўринишини жиҳозлаш минимал чарчаш учун шароит яратади. Иш мебелининг конструкцияси ГОСТ 12.2.032-78(9), ГОСТ 2226976(10) талабларига мос тушувчи ишчининг бўйига қараб созланадиган ва қулай озода турадиган бўлиши керак. Операторнинг иш жойини тўғри ташкил этилганида унинг меҳнат унумдорлиги 8-20% ошади .

Комьютер ўрнатиладиган хонага комьютер сонига қараб туриб қуйидаги талаблар қўйилади: ахборотлаштириш, бу тингловчиларни ёки

ишловчиларнинг компьютерда назарий ва амалий машғулотлар ўтказиш билан бажарилади. Шунинг учун компьютер хонасида 2 тадан 5 тагача компьютер ўрнатилиши мумкин ва шу билан бирга компьютер хонасини ўлчамлари қуйидагича бўлиши керак (3х6х2,8 м).

4.3. Иш жойининг ёритилганлиги

Иш жойини лойиҳалаш вақтида суъний ва табиий ёритиш масаласи ҳал қилиниши керак. Ёритиш нафақат ишлаб чиқариш масаларини ҳал қилиш балки у ишлаётган одамнинг психологик ҳамда физик ҳолатига таьсир кўрсатади. Ишлаб чиқариш жойларидаги рационал ёритганликка қўйилган талаблар:

- ёруғлик манбаи ва ёритиш тизимини тўғри танлаш;
- ишлаб чиқариш тепаликларини керакли даражадаги ёруғлик даражаси билан таъминлаш;
- кўзни оладиган ёруғликни чеклаш;
- ўликларни йўқотиш, текис ёруғликни ташкилаш;
- ёруғлик оқимининг вақтга нисбатан тебранишини йўқотиш ёки чеклаш.

Керакли даражадаги ёритилмаганлик оқибатида ва кўриш ҳолатининг зўриқишида бажарилётган иш давомида кўзнинг чарчаши кучаяди, умумий ишлаши ва ишлаб чиқариш унумдорлиги тушиб кетади ва хатолар сони кўпаяди.

Иш жойидаги ёритганлик гигиеник талабларга биниоан меҳнатнинг кўриш шароитларига тўғри келиши керак. ГОСТ 12.01.006-84 (11) га биноан дисплей билан ишлаш вақтида ёритилганлик 200лк ҳужжатлар билан ишлаш пайтида 400лк бўлиши керак.

Тарқатилган ёритишдан, шифтларнинг, деворларнинг, ускуналарнинг оч рангларга бўяш қўланилади.

Операторнинг кўриш майдонида ёруғлик майдони бўлса тўғри ялтираш, кўриш майдони ичида қайтарадиган ёруғлик текисликлари мавжуд бўлса қайтарувчи ялтираш дейилади.

Тўғри ялтирашни кўриш майдонидан ярқилаган ёруғликни 60 см камайтириш йўли билан камайтириш мумкин. қайтарувчи ялтирашдан эса ёруғликни тарқатувчи манбалар ҳамда полировка қилинган текисликлар ўрнига матовий ишлатиш йўли билан камайтириш мумкин. Экран мониторидаги бликларни камайтириш учун тасвирни конрастлигини кучайтирувчи ва бликларни камайтиртирувчи экран филтрларидан фойдаланиш керак ёки антиблик қопламаси мавжуд мониторлардан фойдаланиш зарур .

Ёруғликни турини танлаш муҳим масала ҳисобланади (табиий ёки суъний). Табиий ёруғликдан фойдаланиш кўп камчиликларга эга:

- ёруғлик тушиши фақат бир томондан;
- ёруғликни вақтда ва ҳажмда бир хил бўлмаганлиги;
- равшан қуёш нурларининг кўзни олиши ва бошқалар.

Суъний ёруғликдан фойдаланиш юқоридаги камчиликларни бартараф этади ва оптимал ёруғлик режимини яратишга ёрдам беради. лекин ойналарсиз иншотлардан фойдаланиш инсонларда ўзига ишончсизлик ва уялувчанликни келтириб чиқаради. Тўғри ёруғлик узатишни ташкил этиш учун қуёш нурларига яқин суъний ёруғликни танлаш керак.

4.4. Стол ва стулларнинг жойлашувига бўлган талаблар

Компьютер хонасида стол ва стулларга талаблар мавжуд бўлиб, стол баландлиги ердан 68-77 см, стуллар эса айланувчан бўлиши керак ва орқасида суянчиғи бўлиши керак. Чунки стол стуллар ўз габарити билан тўғри келмаса фойдаланувчи тезда чарчаб қолади. Стол ва стуллар шундай жойлаштирилиши керакки, улар инсонларга туриб юришга халақит

бермаслиги керак. Бундан ташқари, операторлар бемалол ҳар бир операторлар олдига бориб бирга ишлай олиши керак.

Иш жойининг конструктивиги ва элеменларининг жойлашинуви (ўтирғичлар, ахборотнинг кўрсатиш, бошқариш органлари) антропометрик, физиологик ва психологик талабларга ҳамда ишнинг характерига тўғри келиши керак.

Шундай конструкцияланган иш жойи монитор майдонидан ташқаридаги бажарилиши қийин бўлган операцияларни бажариш имконини беради. Ахборотнинг кўрсатиш манбалари бу ҳолда ЭҲМ нинг дисплейи СНиП 2.01.02-85 (5) га тўғри келади.

Кўзга тушаётган нагрузкани камайтириш учун дисплей эргономика нуқтаи назаридан оптимал ўрнатилиши керак, дисплейнинг тепа бурчаги кўз билан бир текисликда бўлиши керак, экрангача масофа 28-60 см бўлиши керак. Экранинг милтилаши мил>70 Гц бўлиши керак.

Антропометрик мос тушиши операторнинг иш бораётган вақтда фазода, кенгликда тананинг жойланиши имконияти ва турли позани эгаллаши назарда тутилади. Бу масалани ҳал қилиш учун биринчи навбатда бошқариш пульти асбобларидан операторнинг оёғи бориб етадиган зона аниқланади. Бу мос келишини таъминлаш қийинчилик билан эришилади, чунки ҳар бир кишининг антропометрик кўрсаткичлари турлича. Ўрта бўйли кишини қониқтирган ўриндиқ, баланд ёки паст бўйли бўлган кишига ноқулай бўлиши мумкин.

Хавфсиз фаолият кўрсатиш мақсадида инсон танаси ўлчамлари қуйидаги ҳолатларда ҳисобга олинади:

- полдан ёки иш майдонидан, машиналар ишлашини назорат қилиш, тўғрилаш зонаси, сигнализация ва назорат асбобларига бўлган сатҳни оптимал баландлигини ўлчашда;
- баландликда қўлда бошқариладиган машиналар фронтини жойлаштиришда, айниқса авария органларининг пухта жойлаштиришда;

- бошқариш органларини шакли ва ўлчамларини танлашда.

Машиналарни лойиҳалашда инсон антропометрик кўрсатгичларни тўғри танлаш учун ўзини топография қилиш усули ёки моделлаш усули қўлланилади. Ўзини топография қилишда инсон ишчи танасини турли ҳолатларини схематик Конструкциялаш ва ишчи бажарадиган ишлар ва операциялар билан боғлаш киради. Моделлаш усулига инсон фигурасини ҳажмий ва текисликда моделлаш киради. Инсоннинг антрапометрик қуйидагича: ўртача баландлиги 1 метр 72 см, елка кенглиги 39 см, қўллар ёйилмаси 160 см агар бу антропометрик ўлчовлар ҳисобга олинмаса операторлар иш пайтида бир – бирига халақит бериши мумкин. Шунинг учун антропометрик ўлчовларни ҳисобга олиш катта аҳамиятга эга.

4.5. Монитордан инсоннинг кўзигача бўлган оптимал масофа

Монитор кўздан озгина пастроқда ва 50 см дан кам бўлмаган масофада жойлашиши керак. Монитор ва кўз орасидаги масофа 80 см гача бўлиши тавсия қилинади, бу масофа кичик бўлса инсоннинг кўзи тез чарчайди. Мониторни дизайни ва рангги ўзига эътиборни жалб қилмаслиги керак. Шунинг учун мониторнинг сирт томонида ҳар хил реклама ёпиштиргичлар бўлмаслиги керак. Мониторнинг экрани зангори ва кўк рангларга бўялиши мақсадга мувофиқ ҳисобланади. Чунки бу ранглар инсон кўзига энг яхши ранглардан ҳисобланади.

Қисман монитор олдидаги ўтиришда хавфсизликни ва камфорт иш жойини рационал ташкил этиш лозим. Фойдаланувчи усул асосий хавфсизлик видиоманитор экран дисплейдан чиқади деб бўлмайди. Энг кучли нурланиш одатда маниторни ён ва орқа томонидан ҳам тарқалади. Шунинг учун фойдаланучи жойини бир неча компьютер қарама – қарши турган жойда ундан ҳам ёмони орқама – кетин жойлаштиришдир. Видеомонитор хиллари орасидаги тавсия этиладиган орадаги масофа 2 м дан

кам бўлмаслиги ва ён томондаги масофа 1,2 м дан кам бўлмаслиги лозим. Компьютерлар жойлашган хона етарли даражада кенг ва доимий равишда ҳавоси алмашиб туриши керак. Битта дисплей учун минимал стандарт норма 6м ни, минимал ҳажм эса 20 м ташкил этиши керак.

Дисплей олдида ишлаганда хонани ёритилиши яхши бўлиши ва имкони борича табиий кундузги ёритилишга яқин бўлиши керак. Ёритиш учун дисплейга яқин жойлашган люминицент лампочкалардан фойдаланиб бўлмайди. Бу стробактик эффект деб айтилади, дисплей экранда маълумотни бузилишига олиб келади.

Ёритишни энг мақбул усули галтен нурланишли манбадир. Америкалик олимларнинг ҳам фойдаланувчиларга тавсияси диққатга лойиқдир:

- Дисплей экранига яхши ҳимоя фильтри ўрнатиш, тўрли фильтрлардан фойдаланманг;
- Экран ўз сатҳидан 20 см пастда ва кўздан 65 см масофада бўлиши керак(агар шу яқиндан ёки кўрсангиз ҳам дисплей билан бурнингизни унинг яқинига олиб бориб ишламанг, ҳатто бурун ҳам зарар кўриши мумкин);
- Экранни ойнага нисбатан тўғри бурчак ҳолида ўрнатинг;
- Экраннинг ёритиш хонасининг ёритишига тенг бўлиши керак (тахминан 500-700 лк) ёрқин люменсент нурдан сақланиш;
- Ёрқин фонда қора ҳарфлар осон ўқилади;
- Ҳар 10 минутда нигоҳни экрандан бошқа томонга олинг;
- Черновикдан маълумотни ШКга киритишда уни экран яқинроқ жойга қўйинг;
- Кўзга дисплей ёнида ишлаганда алоҳида кўзойнак лозимлигини кўз доктори билан гаплашиб кўринг. (масалан перфорировамний ойнак)

Барча нурлантиришларни яхши ютувчи айрим ўсимликлар бор. Улар кўпгина нурланишларда улар жуда зўр ривожланади. Шунинг учун кўпгина офисларда хонани безаш учун эмас, балки нураланиш камайтириш учун

хона ўсимликлардан фойдаланишади. Шунинг учун ушбу тавсия компьютердан фойдаланувчилар учун бериш мумкин. Умуман хулоса шуки:

- Экранни липпиллаши ва ярқираши, яқинда ёмон кўриш, асаб стресслари ва асабийликка олиб келади.
- Паст частотали майдон нур касалликлари, стресслар, ҳомиладорларни бузилишлар билан ўтишга, репродуков функционал бузилишга ва ёмон шароитли ишлар пайдо бўлишига олиб келади.
- Электрон майдон ҳужжатларини ўзгартириш ва ривожланишни тўхтатишга олиб келади. Бу кўзнинг хуристалини хиралашиш – катаракта келтириб чиқариш мумкин.

4.6. Компьютер билан ишлаганда чарчаш сабаблари

Компютер билан ишлаш вақтида инсон қуйидаги факторлардан чарчайди:

- экранинг меъёридан ортиқ ёруғлиги;
- контраст ва фон ўртасидаги аниқлиги;
- компьютерда ишлаш пайтидаги иссиқликдан нурланиши;
- компьютерда нурланишнинг инсонга таъсири;
- компьютер бузуқлиги.

Компьютердан нурланишнинг олдини олиши учун ҳимоя фильтрларидан фойдаланилади.

Шундай қилиб, монитор бутунлай халқаро стандарт MPR-2 (LOW radiation дисплейлари) талабларини қониқтирганда ҳам, уни нурланишда қўшимча ҳимоя керак бўлади. Бу тўғрисида таклифлар жуда кўпдир. Америкалик мутахасислар, масалан, экранда қўл чўзилгандагина бўлган масофада жойлашишни маслаҳат берилади, қўшни мониторлар 222,8 масофада жойлашиши лозим. Энг эффектли (фойдали) восита ривожланган

дунёда тан олинган экран қисми фильтрларидир. Мониторлар учун ҳимоя фильтрлари қуйидаги турларда бўлади.

1. Турли фильтрлар – амалда электромагнит нурлардан ва статик электрдан ҳимоя қилмайди, бундан ташқари суръатнинг контрастлигини камайтиради. Лекин улар ташқи ёрқинликда ва экранни бикирлашидан ҳимоя қилади, бу кўз учун катта аҳамиятга эгадир.

2. Плёнкали фильтрлар статик электрни тўсмайди паст частотали электромагнит майдонидан деярли ҳимоя қилмайди, лекин суръатни талбанинг конрастлигини ортиради, ультрафиолет нурланишларни бутунлай ютади ва ренген нурларини камйтиради. Яшиндан фақат полеризация плёнкали фильтрлар ҳимоя қилади. Энг таниқлилиси Polorid фирмасининг плёнкали фильтрлардир (CP 50): уларни кўплари суръатни контрастлиги ва аниқлийлигини оширади. Лекин ҳақиқатдан шуни таъкидлаш керакки, полеризация фильтрлари полеэфир симолалари остида тайёрланади. Бу материал юқори даражада мустаҳкам эмас ва узоққа чидамайди ва тез физик қоришиш ва тузилишига олиб келади.(Плёнка Polorid CP 50 фильтрларни универсал ишлашини полеризация фильтрлари билан чалкаштириб бўлмайди. Кейинги фильтрлар ҳам статик ва электромагнит майдонлардан ёмон ҳимоя қилмайди).

3. Шиша фильтрлар энг кенг тарқалгандир. Уларнинг бир неча модификацияси мавжуддир.

а) Оддий шиша фильтрлар, одатда осиёда ишлаб чиқилган (Defender GL14B, Optical Class) ўзини эффективлиги билан тахминланган турли филътрларга тенгдир. Уларни кўплари сифат сертификати ва бошқа ҳужжатлар билан таъминланмайди.

б) Ерга улаган шиша филътрлар сезиларли даражада эффективдир: улар қисман статик зарядни камайтиради, электромагнит майдон, ультрабинафша нурлари кучини камайтиради, суръат контраситлигини оширади. Бу фильтрлар жуда автоматлашгандир.

в) Тўлиқ ҳимояли шишали фильтрлар (Ergoster Xenium Vnus) - одатда, юқори сифатли маҳсулотдир, оптик ойна асосида кўп қатламли махсус ўқламалар билан тайёрланган, ўзида полиризация филътрни ҳам мужассам этган. Бу филътрлар ультрафиолет нурларини, статик майдонларни бартараф этади кўп даражада электромагнит майдон ва рентген нурланишларини камайтиради. Суратда сакрашлар бўлмайди, суратни контрастлилиги ошади, лекин бу фильтрлар жуда қимматдир.

г) Россия федерациясида ишлаб чиқилган фильтрлар шишали фильтрлар (Global Shield ва Defended Argon фильтрлари) улар ҳам тўла ҳимоя синфига мансуб. Ўзини характеристикаси билан хорижий фильтр намуналардан қолишмайди, 2-3 маротаба арзон, нисбатан янги фильтрлар уларни сифати кўпгина техник хулосалар ва сертификатлар билан тасдиқланган, улар меҳнат принципи паст ИТИ тестдан ўтказилган, швецил нурланишдан ҳимоя ва кўрсаткич воситалари эргономикаси ИТУ дан ҳам синовда ўтказилган режим Давлат Стандарти сертификати ва гигиена сертификатига эга.

Компьютер хонасида ҳамма жиҳозлар электр токида ишлайди. Шунинг учун электрдан шикастланишига учраш мумкин. Бунинг олдини олиш учун компьютерларни ерга улаш талабларига амал қилиш шарт. Ҳамма компьютерларда электр тармоғига улаш учун махсус система ишлатилади ва унда "0" улаш ҳимояси қўлланилган. "0" га улаш ҳимояси бу "0" симини корпусларга боғлаш ва ҳар хил иссиқликда ишлайдиган автоматларни ишга туширувчи системадир. Ҳимояловчи ерга улаш қурилмалари 2 хил:

1. Контурли ерга улаш;
2. Ташқарига чиқарилган ерга улаш – бу усул кўпинча уловчи асбоб – ускуналар турган жойдан ташқарига чиқариб маълум бир майдончага тўпланиб ўрнатилади. Ерга улашнинг бу тури асосан кучланиши 1000 В гача бўлган қурилмаларда ишлатилади. Бунинг афзаллиги шундаки, электрод

вазифасини бажарувчи қозиқларни ерга қоқиш учун қаршилиги кам бўлган ерларни танлаш имкони бор.

4.7. Электр токидан зарарланган инсонга биринчи ёрдам кўрсатиш

- Шикастланган одамни электр токи таъсиридан бир неча усуллар билан халос қилиш мумкин.
- Агар ток урган киши ҳушидан кетган бўлса, унга медицина ёрдамини кўрсатиш керак бўлади.

4.8. Ёнғин чиқиш сабаблари

Электр токларини қисқа туташуви натижасида кучланиш ортиб қизиш юзага келади. Натижада ёнғин чиқиш хавфи туғилади. Бу ёнғин чиқиш сабабларидан бири ҳисобланади. Хоналарнинг ёнғинга қарши тоифасига қараб бўлинади. Ёнғин чиққан пайтда оператор дарҳол ёнғинни сабабини билиши ва уни бартараф этиш усулларини кўриши лозим. Бунинг учун электр токидан ёнғин чиққан бўлса линияни электр токидан узиб, сўнг ўчиришга киришиш керак. Шу билан биргаликда ўт ўчирувчи гуруҳларга хабар қилиши лозим. Ёнғин кучайган ҳолатда эвакуация йўллари орқали (қўшимча чиқиш эшиклари) ишчиларни эвакуация қилиш керак. Эвакуация йўлларининг ёритилиши камида 5 лк бўлиши, йўлакларининг эни эса ишчилар сонига нисбатан кенг бўлиши керак. Ҳар бир ташкилотда ёнғин учун сув таъминоти бўлиши керак.

ХУЛОСА

Интернетга уланган тармоқлар бузғунчиларни тажовузи туфайли очиқ мулоқотга халақит берса ҳам уларни "Брандмауер" -тармоқлараро экран ўрнатиб олдилар. Бу ташкилотнинг энг асосий ҳимоя воситасидир. Тармоққа кирувчи ва ундан чиқувчи трафикни назорат килади. У трафикнинг бирор турини тугиб қўйиши ёки текшириб туриши мумкин.

Тажовузкорлар кўпинча тармоққа унинг аҳамиятга молик жойларидан ўтувчи трафикни тиклаш орқали, уларнинг паролларини ажратиб олиш ёрдамида суқилиб киралилар. Шунингдек олисда машиналар билан боғланишлар парол воситасида ҳимояланганда шифрланиши шарт. Бу айниқса интернет каналлари орқали боғланишда амалга оширилганда ёки аҳамиятли сервер билан боғланганда зарурдир. Бунинг учун биз "Криптография" фанини чуқур ўрганишимиз лозим.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Каримов И.А. “Ўзбекистон буюк келажак сари” Тошкент – “Ўзбекистон”, 1998 й.
2. Каримов И.А. “Озод ва обод Ватан, эркин ва фаравон ҳаёт-пировард мақсадимиз” 8-жилд, Т,: “Ўзбекистон”, 2000 й.
3. Ўзбекистон Республикаси Вазирлар Маҳкамасининг «2001-2005 йилларда компьютер ва ахборот технологияларини ривожлантириш, Интернетнинг халқаро ахборот тизимларига кенг кириб боришини таъминлаш дастурини ишлаб чиқишни ташкил этиш чора тадбирлари тўғрисида» ги Қарори. 2001 йил 23 май.
4. С. С. Ғуломов ва бошқ. «Ахборот тизимлари ва технологиялари». Тошкент, «Ўзбекистон», 2000 й.
5. А.Р. Марахимов, С.И. Рахмонқулова. «Интернет ва ундан фойдаланиш». Тошкент, 2001 й.
6. «Ваш ключ к Интернету» Руководство пользователя Гласнета. 3е издание август 1997 г.
7. В.Г. Олифер, Н.А. Олифер. «Компьютерные сети». С.-Петербург. 2001.
8. А.Д. Хомоненко. «Основы современных компьютерных технологий». С. – Петербург. 1998 г.
9. Е. Нечаева. «Персональный компьютер, Internet и Электронная почта» Москва «Майор» 2001 г.
10. А.И. Тихонов. «Публикация данных в Internet» Учебное пособие. Москва Издательство МЭИ» 2000 г.
11. Электронный журнал «Protoplex» № 1- 10 2001 HTTP: Protoplex.COM
12. ХоффманД.Д. Современные методы защиты информации.- М.: Бином 1980 г.
13. Федеральный закон Российской Федерации. «Об информации, информатизации и защите информации» 20 февраля 1995 г.

14. Савельев А. Я. Основы информатики: Учебник для вузов. – М.: Оникс 2001 г.

15. Баричев С. Введение в криптографию. Электронный сборник.- М.: Вече1998 г.

16. Ведеев Д. Защита данных в компьютерных сетях. Открытые системы.- М.: Дрофа 1995 г.

17. Энциклопедия компьютерных вирусов Евгения Касперского – электронная версия от 16.10.1999.

18. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование.- СПБ.: Питер 1994 г.

19. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ.- М.: Айрис 1982 г.

20. Правовая информатика и управление в сфере предпринимательства. Учебное пособие. – М.: Юристъ 1998 г.

21. Леонтьев В.П. ПК: универсальный справочник пользователя.- М: Айрис 2000 г.

22. Зегжда П. Теория и практика. Обеспечение информационной безопасности. – М: Альфа 1996 г.