ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ИЧКИ ИШЛАР ВАЗИРЛИГИ

А К А Д Е М И Я

И. М. КАРИМОВ, Н. А. ТУРГУНОВ

АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ

Дарслик

Тошкент–2016

Ўзбекистон Республикаси ИИВ Академиясининг
Таҳририят-ноширлик ҳайъатида маъқулланган

Тақризчилар:

Тошкент Ахборот технологиялари университетининг ахборот хавфсизлиги кафедраси доценти, техника фанлари номзоди **А.А. Ганиев;**

Тошкент шаҳар ИИББ Ахборот маркази бошлиғи, техника фанлари номзоди **М. Ражабов**

Каримов И. М.

К-23 **Ахборот хавфсизлиги асослари:** Дарслик / И. М. Каримов, Н. А. Тургунов. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2016. – 98 б.

Дарсликда ахборот хавфсизлиги ва ташкил этувчилари, ахборотни муҳофаза қилиш, ҳимояланган ахборотга таҳдидлар, ахборотларни муҳофаза қилишга комплекс ёндашув ва уни амалга ошириш чора-тадбирлари; ахборотни муҳофаза қилишнинг асосий объектлари, Ўзбекистон Республикасида ахборот хавфсизлиги ва маълумотларни муҳофаза қилишга оид норматив-ҳуқуқий ҳужжатлар, ахборот ҳимояси соҳасида халқаро стандартлар, маълумотларни рухсатсиз олишнинг объектлари, усуллари ва воситалари, ҳимоянинг техник воситалари, маълумотлар чиқиб кетиш техник каналлари таснифи, маълумотларни тутиб олиш, криптография ва криптотаҳлил, шифрлар ва уларнинг хоссалари, шифрловчи дастурлар, электрон рақамли имзо, маълумотларни ҳимоялашнинг аппарат-дастурий воситалари, ахборотни муҳофаза қилишнинг давлат тизими, уни амалга оширувчи қонун, норматив ҳужжатлар, етакчи чет эл мамлакатларида ахборот хавфсизлигини таъминлаш тизимларига оид маълумотлар келтирилган. Ушбу маълумотлар билан танишиш орқали китобхонлар ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича ўз назарий билимларини шакллантириб, унинг ташкил этувчилари имкониятлари ҳақида батафсил тушунчаларга эга бўладилар.

ИИВ Академияси тингловчилари, курсантлари, ҳуқуқни муҳофаза қилиш идоралари ходимлари ва бошқа турдош соҳаларда фаолият юритаётган мутахассисларга мўлжалланган.

ББК 73я73

КИРИШ

Ахборот-коммуникация технологиялари шиддат билан ривожланиб бораётган ҳозирги даврда ҳар қандай давлатнинг ахборот ресурслари унинг иқтисодий ва ҳарбий салоҳиятини белгиловчи муҳим омиллардан бири ҳисобланади. Мазкур ресурслардан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантирилишини таъминлайди. Бундай жамиятда ахборот алмашинув тезлиги юксалиб, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот-коммуникациялар технологияларини қўллаш кенг кўламда амалга оширилади.

Бугунги кунда ахборотлашган жамият жадал суратлар билан шаклланиб, ахборотлар дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Глобал компьютер тармоғи жаҳон давлатларининг ижтимоий-иқтисодий, сиёсий, маънавий ва маданий ҳаётида алоҳида аҳамият касб этмоқда. Шунинг учун ахборотни муҳофаза қилиш ҳар қандай мамлакатда муҳим давлат вазифаси бўлиб ҳисобланади. Ўзбекистонда ахборотни муҳофаза қилишнинг зарурияти ахборотни муҳофаза қилишнинг давлат тизимини яратилишида ва ахборот хавфсизлигининг ҳуқуқий базасини ривожлантиришда ўз ифодасини топди. Бу борада Ўзбекистон Республикасининг «Давлат сирларини сақлаш тўғрисида»ги, «Ахборотлаштириш тўғрисида»ги ва бошқа қонунлар қабул қилинди ҳамда амалда татбиқ этиб келинмоқда.

Мамлакатимизда 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[1].

Ўзбекистон Республикасининг Биринчи Президенти Ислом Каримов бугунги кунда жамият тараққиётида ахборот технологияларининг аҳамиятига тўхталиб, қуйидагиларни таъкидлаган:

[1] Ўзбекистон Республикасининг «Ахборотлаштириш тўғрисида»ги қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2004. – №1-2. – 10-м.

«Бугунги шароитда, Интернет ва электроника даврида иқтисодиёт тармоқларида замонавий ахборот-коммуникация технологияларини кенг жорий этиш, «Электрон ҳукумат» тизими фаолиятини янада ривожлантириш устувор аҳамиятга эгадир.

Жаҳон тажрибаси шундан далолат беради, айни пайтда глобал иқтисодиётда компьютер ва телекоммуникация технологиялари, дастурий таъминот маҳсулотларини ишлаб чиқариш ва улар асосида кенг турдаги интерфаол хизматлар кўрсатишни ўз ичига олган ахборот-коммуникация технологиялари соҳасининг роли ва аҳамияти тобора ортиб бормоқда.

Ахборот-коммуникация технологияларининг ривожланиши мамлакатнинг рақобатдошлик даражасига таъсир кўрсатиши, катта ҳажмда ахборот тўплаш ва уни умумлаштириш имконини бериши, бошқаришни стратегик даражада ташкил этиш учун кенг имкониятлар очиб беришини унутмаслигимиз зарур».[1]

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонунида[2] ахборот хавфсизлигини таъминлаш соҳасидаги давлат сиёсати ахборот соҳасидаги ижтимоий муносабатларни тартибга солишга қаратилган ҳамда шахс, жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлашдан иборат деб белгиланган. ««Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги Қонуннинг қабул қилиниши ҳар кимнинг ахборотни эркин ва монеликсиз олиш ҳамда фойдаланиш ҳуқуқларини амалга оширишда, шунингдек, ахборотнинг муҳофаза қилиниши, шахс, жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлашда муҳим аҳамият касб этди»[3].

---

[1] Ўзбекистон Республикасининг Биринчи Президенти Ислом Каримовнинг мамлакатимизни 2015 йилда ижтимоий-иқтисодий ривожлантириш якунлари ва 2016 йилга мўлжалланган иқтисодий дастурнинг энг муҳим устувор йўналишларига бағишланган Вазирлар Маҳкамаси мажлисида сўзлаган маърузасидан.

[2] Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2003. – № 1. – 2-м.

[3] *Каримов И.А.* Мамлакатимизда демократик ислоҳотларни янада чуқурлаштириш ва фуқаролик жамиятини ривожлантириш концепцияси. – Т., 2010.

I. АХБОРОТ ХАВФСИЗЛИГИ ВА АХБОРОТНИ МУҲОФАЗА ҚИЛИШ

1.1. Ахборот хавфсизлиги ва ахборотни муҳофаза қилиш тушунчалари

Ахборот хавфсизлиги – кўп қиррали фаолият соҳаси бўлиб, унга фақат тизимли, комплекс ёндашув муваффақият келтириши мумкин. Ушбу муаммони ҳал этиш учун ҳуқуқий, маъмурий, процедурали ва дастурий-техник чоралар қўлланилади.

Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборотни муҳофаза қилиш эса давлатнинг бирламчи масалаларига, давлат сиёсати даражасига айланмоқда.

Ахборот хавфсизлигининг миллий хавфсизлик тизимидаги ўрни. XXI асрда шахс, жамият ва давлат тараққиётида ахборот ресурслари ва технологияларининг ролини ортиши натижасида Ўзбекистон Республикасида фуқаролик жамиятини ахборотлаштирилган жамият сифатида қуриш масаласини ҳал этиш билан бирга қуйидаги омиллар миллий хавфсизликни таъминлаш тизимида ахборот хавфсизлигининг етакчи ўрин эгаллашини белгилайди:

– миллий манфаатлар, уларга тажовуз ва уларни бу тажовузлардан ҳимоялаш ахборот ва ахборот соҳаси орқали ифодаланади, амалга оширилади;

– инсон ва унинг ҳуқуқлари, ахборот ва ахборот тизимлари ҳамда уларга эгалик қилиш – бу нафақат ахборот хавфсизлигининг асосий объектлари, шу билан бирга жами хавфсизлик соҳаларидаги хавфсизлик объектларининг асосий элементларидир;

– ахборот ёндашувидан асосий илмий-амалий усул сифатида фойдаланиш орқали миллий хавфсизлик масалаларини ҳал этиш мумкин;

– миллий хавфсизлик муаммоси яққол ажралиб турувчи ахборот тавсифига эга.

Ахборот хавфсизлиги тизими давлатнинг ахборот соҳасидаги сиёсатини мамлакатда миллий хавфсизликни таъминлаш давлат сиёсати билан чамбарчас боғлайди. Бунда ахборот хавфсизлиги тизими давлат сиёсатининг асосий ташкил этувчиларини яхлит бир бутун-

ликка бириктиради. Бу эса ахборот хавфсизлигининг роли ва унинг мамлакат миллий хавфсизлиги тизимидаги мавқеини белгилайди. Ахборот соҳасидаги Ўзбекистоннинг миллий манфаатларини, уларга эришишининг стратегик йўналишларини ва уларни амалга ошириш тизимларини ўзида акс эттирувчи мақсадлар яхлитлиги давлат ахборот сиёсатини англатади. Шу билан бирга давлат ахборот сиёсати мамлакатнинг ташқи ва ички сиёсатининг асосий ташкил этувчиси ҳисобланади ва жамиятнинг барча жабҳаларини қамраб олади.

Ахборот хавфсизлигининг замонавий концепцияси ахборот хавфсизлигини таъминловчи мақсадлар, вазифалар, тамойиллар ва асосий йўналишлар бўйича расмий нуқтаи назарлар мажмуини билдиради.

Қуйида ахборот хавфсизлигининг асосий ташкил этувчилари ва жиҳатлари келтирилган:

– ахборотни муҳофаза қилиш (шахсий маълумотларни, давлат ва хизмат сирларини ва бошқа турдаги тарқатилиши чегараланган маълумотларни қўриқлаш маъносида);

– компьютер хавфсизлиги ёки маълумотлар хавфсизлиги – компьютер тармоқларида маълумотларнинг сақланишини, фойдаланишга рухсат этилганлигини ва конфеденциаллигини таъминловчи аппарат ва дастурий воситалар тўплами, ахборотдан муаллифлаштирилмаган фойдаланишдан ҳимоя қилиш чоралари;

– ахборот эгаларига ёки ахборотдан фойдаланувчиларга ҳамда уни қўллаб қувватловчи инфратузилмага зарар етказиши мумкин бўлган табиий ёки сунъий характердаги тасодифий ёки қасддан таъсир этишлардан ахборот ва уни қўллаб қувватловчи инфратузилманинг ҳимояланганли;

– фуқаролар, алоҳида гуруҳлар ва ижтимоий қатламлар, умуман олганда аҳолининг яшаш фаолияти, таълим олиш ва ривожланишлари учун зарур бўлган сифатли ахборотга бўлган талабларининг ҳимояланганлиги.

Хавфсизлик сиёсати – хавфсизлик объектлари ва субъектларининг берилган кўплигининг хавфсизлигини таъминлаш процедуралари ва механизмларини белгиловчи қоидалар тўплами[1]. Тизим хавфсизлигини таъминлашнинг аниқ механизмларини танлаш қабул қилинган хавфсизлик сиёсатига мувофиқ амалга оширилади.

[1] «Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги: Атамалар ва таърифлар». Тармоқ стандарти: TSt 45-010:2010.

Ўзбекистон Республикаси Президентининг 2015 йилнинг 4 февраль куни эълон қилинган «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигини ташкил этиш тўғрисида»ги Фармонига1 кўра «Ахборот хавфсизлигини таъминлаш ва коммуникация тармоқлари, дастурий маҳсулотлар, ахборот тизимлари ва ресурсларини ҳимоя қилишнинг замонавий технологияларини татбиқ этиш чора-тадбирларини амалга ошириш, ахборот ресурсларини ҳимоя қилиш бўйича техник инфратузилмани янада ривожлантириш» устувор вазифалардан бири сифатида қайд этилган.

Ахборот хавфсизлиги деганда табиий ёки сунъий характердаги тасодифий ёки қасддан қилинган таъсирлардан ахборот ва уни қўллаб-қувватлаб турувчи инфратузилманинг ҳимояланганлиги тушунилади. Бундай таъсирлар ахборот муносабатларига, жумладан, ахборот эгаларига, ахборотдан фойдаланувчиларга ва ахборотни муҳофаза қилишни таъминловчи инфратузилмага жиддий зарар етказиши мумкин.

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонунида[2] ахборот хавфсизлиги *ахборот борасидаги хавфсизлик* деб белгиланган ва у ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлик ҳолатини англатади.

Конфиденциаллик, бутунлик ва рухсат этилганлик ахборот хавфсизлигини таъминлаш борасида учта муҳим хусусият ҳисобланади.

– **ахборотнинг конфиденциаллиги** – ахборотнинг ҳолати бўлиб, бунда ахборотга рухсат, фақат тегишли ҳуқуққа эга бўлган субъектларгагина берилади.

– **ахборотнинг бутунлиги** – ахборотда ҳеч қандай ўзгартиришлар бўлмаган ёки ўзгартиришлар фақат алоҳида ҳуқуққа эга бўлган субъектлар томонидан амалга ошириладиган ахборотнинг ҳолати.

– **ахборотнинг рухсат этилганлиги** – ахборотга рухсат этилган субъектларнинг, уни амалга оширишга тўсиқлар мавжуд бўлмаган ҳолати.

Рухсат этилганлик ҳуқуқига ахборотни ёки унинг ресурсларини ўқиш учун, ўзгартириш, нусха олиш, ахборотни йўқ қилиш ҳуқуқлари киради.

---

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2015. – №5. – 52-м.

[2] Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2003. – № 1. – 2-м.

Ахборотни муҳофаза қилиш – бу ахборот ҳимоя тизимини яратиш билан боғлиқ жараён. Ахборот ҳимоя тизими ҳеч қачон юз фоизлик ҳимояни таъминлай олмаслигини англаш муҳимдир. Бу эса ахборотни мумкин бўлган даражадаги ўзгартириш, ўғирлаш ёки йўқ қилиш таваккалчилигига асосланган ахборот хавфсизлиги ҳақида фикр юритишни тақозо этади.

Амалга оширилиш усулларига кўра барча ахборот ҳимояси чораларини қуйидаги турларга ажратиш мумкин:

– ҳуқуқий;

– маънавий-этик;

– технологик;

– ташкилий;

– физик;

– техник (қурилмавий ва дастурий).

Юқорида қайд этилганлар ҳимоя турлари орасида асосийлари ҳуқуқий, ташкилий ва техник ҳимоя ҳисобланади.

Ҳуқуқий ҳимоя – ахборотни ҳимоялаш бўйича субъектларнинг муносабатларини тартибга солувчи, амалда жорий этувчи ҳамда уларнинг бажарилишини назорат қилувчи қонунчилик ва норматив-ҳуқуқий ҳужжатлар асосида ахборотни ҳуқуқий усуллар билан ҳимоялашдир. Ахборотни ҳуқуқий ҳимоялаш чораларига Ўзбекистон Республикасининг мазкур соҳадаги қонунлари, Президент фармонлари ва қарорлари, Вазирлар Маҳкамасининг қарор ва фармойишлари ва бошқа норматив-ҳуқуқий ҳужжатлар киради. Ахборотга мурожаат қилиш қоидалари, ахборот муносабати қатнашчилари, уларнинг ҳуқуқлари ва мажбуриятлари, шунингдек, қонунчилик талаблари бузилган ҳолларда жавобгарлик қонунчилик даражасида кўриб чиқилади ва тартибга солинади.

Ҳимоянинг ташкилий чоралари – ташкилий характерга эга бўлган, ахборот тизими фаолиятини, ходимлар ишини, фойдаланувчиларнинг тизим билан ўзаро алоқаларини ташкиллаштиришга мўлжалланган чоралардир. Ушбу чоралар ичидан қуйидаги асосийларини кўрсатиш мумкин:

– хавфсизлик сиёсатини шакллантириш;

– бинога киришни тартиблаш;

– ходимларнинг ахборот тизимидан фойдаланиш учун рухсат этишни тартиблаш;

– ахборот хавфсизлиги талабларига риоя этмаган ҳолларда жавобгарликни аниқлаш ва таъминлаш.

Ташкилий чоралар ўз ҳолича ахборот хавфсизлиги вазифаларини ҳал эта олмайди. Улар ҳимоянинг физик ва техник чоралари билан биргаликда ишлаши зарур.

Физик ҳимоя назорат қилинувчи ҳудудга ғаразгўй кимсаларнинг жисмоний киришига қаршилик қилувчи воситалар тўпламини англатади. Улар турли кўринишдаги механик, электр ёки электро-механик қурилмалар бўлиши мумкин. Корхона ёки ташкилотнинг ахборот хавфсизлигини таъминлаш одатда, айнан физик ҳимояни ташкил этишдан бошланади.

Ахборот ҳимояси чоралари орасида **техник ҳимоя** муҳим аҳамиятга эга. У ахборот тизимларида маълумотларни техник, дастурий ва дастурий-техник воситалар ёрдамида ҳимоя қилишни назарда тутади.

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонунида[1] ахборотни муҳофаза қилиш бўйича қуйидаги таъриф келтирилган:

Ахборотни муҳофаза этиш - ахборот борасидаги хавфсизликка таҳдидларнинг олдини олиш ва уларнинг оқибатларини бартараф этиш чора-тадбирлари.

Сақлаш, ўзгартириш, узатиш ва маълум мақсадлар учун фойдаланиш объекти бўлган теварак олам ҳақидаги маълумотларни, кенг маънода ахборот деб тушуниш мумкин. Бу тушунчага кўра инсон, унинг ҳаёт тарзига ва ҳаракатларига таъсир этувчи доимий ўзгарувчи ахборот майдони таъсирида бўлади. Ахборот ўз тавсифига кўра сиёсий, ҳарбий, иқтисодий, илмий-техник, ишлаб чиқаришга ёки тижоратга оид ҳамда махфий, конфиденциал ёки махфий бўлмаган бўлиши мумкин.

Махфий ахборот – фойдаланилиши қонун ҳужжатларига мувофиқ чеклаб қўйиладиган ҳужжатлаштирилган ахборот[2].

Ҳужжатлаштирилган ахборот эса идентификация қилиш имконини берувчи реквизитлари қўйилган ҳолда моддий жисмда қайд этилган ахборотдир.

---

[1] Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2003. – № 1. – 2-м.

[2] Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги 2002 йил 12 декабрь қонуни // Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2003. – № 1.

Конфиденциал ахборот деганда мамлакат қонунчилиги билан фойдаланиш чекланадиган ҳужжатлардаги ахборот тушунилиб, унга хизмат, касбий, тижорат ва бошқа турдаги ахборотлар киради[1].

Ўзбекистон Республикасининг 1993 йил 7 майдаги 848-XII – сонли «Давлат сирларини сақлаш тўғрисида»ги қонуннинг[2] 1-моддасида давлат сирлари тушунчаси берилган:

«Давлат томонидан қўриқланадиган ва махсус рўйхатлар билан чегаралаб қўйиладиган алоҳида аҳамиятли, мутлақо махфий ва махфий ҳарбий, сиёсий, иқтисодий, илмий-техникавий ва ўзга хил маълумотлар Ўзбекистон Республикасининг давлат сирлари ҳисобланади».

Мазкур қонуннинг 3-моддасида давлат сирларининг категориялари келтирилган:

«Ўзбекистон Республикасининг давлат сирлари – давлат, ҳарбий ва хизмат сирларини қамраб олади.

Ошкор этилиши республика ҳарбий-иқтисодий имкониятларининг сифат ҳолатига салбий таъсир этиши ёки Ўзбекистон Республикасининг мудофаа қобилияти, давлат хавфсизлиги, иқтисодий ва сиёсий манфаатлари учун бошқа оғир оқибатлар келтириб чиқариши мумкин бўлган маълумотлар давлат сирини ташкил этади.

Ошкор этилиши Ўзбекистон Республикасининг мудофаа қобилияти, давлат хавфсизлиги ва Қуролли Кучлари учун оғир оқибатлар келтириб чиқариши мумкин бўлган ҳарбий хусусиятга эга маълумотлар ҳарбий сирни ташкил этади.

Ошкор этилиши Ўзбекистон Республикаси манфаатларига зарар етказиши мумкин бўлган фан, техника, ишлаб чиқариш ва бошқарув соҳасига доир маълумотлар хизмат сирини ташкил этади».

Ахборотлаштириш жараёнининг жадаллашуви муносабати билан жамиятнинг барча соҳаларида ахборот муҳофаза қилиш муаммоси тобора долзарб бўлиб бормоқда. Конфиденциал ахборотлар ва давлат сирларига тааллуқли бўлган махфий ахборотлар муҳофазага муҳтождир.

Умуман олганда *ахборот муҳофаза қилиш* ёки *ахборот ҳимояси* ахборот хавфсизлиги соҳаси мутахассислари ва ғаразгўй кимсалар орасидаги қарама-қаршиликни ифодалайди. *Ғаразгўй кимса* – ноқону-

---

[1] «Ахборот-коммуникация технологиялари изоҳли луғати (иккинчи нашри) – www/undp.uz, www.ictp.uz.

[2] Ўзбекистон Республикаси Олий Кенгашининг ахборотномаси. – 1993. – № 5 – 232-м.

ний йўллар билан ахборотнинг қонуний фойдаланувчиларидан ахборотни олувчи, ўзгартирувчи ёки йўқ қилувчи субъектдир.

Ахборот ҳимояси заиф тузилмали вазифа бўлиб, уни қуйидагича тавсифлаш мумкин:

– самарали ҳимояни тузишга таъсир кўрсатувчи омилларнинг кўплиги;

– аниқ дастлабки кириш маълумотларининг йўқлиги;

– дастлабки маълумотлар тўплами бўйича аниқ оптимал натижаларни олиш имконини берадиган математик усулларнинг йўқлиги.

Заиф тузилмали вазифаларни ечишда тизимли ёндашув асос бўлиб хизмат қилади. Шу сабабли ахборот ҳимояси масаласини ҳал этишда хизмат вазифаси ахборот хавфсизлигини таъминлашга қаратилган элементлар тўпламидан иборат бўлган ахборот ҳимоя тизимини ҳосил қилиш лозим бўлади. Ҳар қандай тизимга кириш – бу тизим ҳолатини ўзгартирувчи таъсирлардир. Ахборот ҳимоя тизими учун кириш ҳам ички, ҳам ташқи таҳдидлар ҳисобланади.

1.2. Ҳимояланган ахборотга таҳдидлар ва ҳимоя объектларини тоифалаш

Ахборот хавфсизлигига таҳдид – ахборот хавфсизлиги бузилишига олиб келиши мумкин бўлган реал ёки потенциал хатарларни ифодаловчи шароит ёки омиллар йиғиндисидир. Ана шундай хатарларни амалга ошириш – ҳужум дейилиб, ушбу вазифани бажарувчи – ғаразгўй кимса деб аталади.

Ахборот хавфсизлигига таҳдид манбаи – бу ахборот хавфсизлигига бевосита таҳдидни юзага келтиришга сабаб бўлувчи субъект (жисмоний шахс, моддий объект ёки физик ҳодиса). Ташкилот ичидаги техник воситалар, ташкилот ходимлари, ғаразгўй кимсалар, ахборот тизимидаги ёндош физик ҳодисалар *таҳдид манбаи* бўлиши мумкин. Ахборот ҳимоя тизимининг катталикларига қуйидагиларни киритиш мумкин:

– мақсад ва вазифалар;

– тизимнинг кириш ва чиқишлари;

– тизимнинг кириш ва чиқишини ўзгартирувчи, тизимдаги ички жараёнлар.

Мақсад – бу тизим ҳимоясини ҳосил қилишда кутилган натижа, вазифа эса – ана шу мақсадга эришиш учун қилиниши керак бўлган ишлар. Ахборот ҳимоясининг мақсади ахборот хавфсизлигини таъминлаш ҳисобланади. Ахборот хавфсизлиги деганда нафақат ахборотнинг, балки уни қўлловчи инфратузилманинг хавфсизлигини ҳам тушуниш лозим. Агар ахборотнинг ўзини алоҳида олиб қаралса, у ҳолда ахборот хавфсизлиги тушунчаси – ахборотнинг ҳимояланганлик ҳолатини билдириб, бунда унинг конфиденциаллиги, бутунлиги ва рухсат этилганлиги таъминланади.

Таҳдидлар ва ҳимоя объектларини тоифалаш. Ахборот айрим символлар (белгилар) тўплами сифатида ҳар хил турдаги ахборот ташувчиларда турли шаклларда мавжуд бўлиши мумкин. Ахборотлаштириш жараёнларининг жадал суратлар билан ривожланиши натижасида замонавий ҳисоблаш воситалари асосидаги автоматлаштирилган тизимларда тўпланувчи, сақланувчи ва қайта ишланувчи ахборот ҳажми тобора ортиб бормоқда.

Автоматлаштирилган тизим – ходимлардан ва қўйилган вазифани бажаришда ахборот технологиясини қўлловчи автоматлаштириш воситалари мажмуасидан иборат бўлган тизимдир. Демак, автоматлаштирилган тизим қуйидаги қисмлар тўпламидан иборат:

– маълумотларни қайта ишлаш ва узатиш техник воситалари;

– дастурий таъминот;

– турли ахборот ташувчилардаги маълумотлар;

– хизмат кўрсатувчи ходимлар ва тизим фойдаланувчилари.

Автоматлаштирилган тизимда ахборот хавфсизлигини таъминлаш муаммосининг асосий йўналишларидан бири – бу ахборот тизимига мумкин бўлган таҳдидларни аниқлаш, таҳлил қилиш ва тоифалашдан иборат. Аҳамияти катта бўлган таҳдидлар рўйхатини тузиш, уларнинг эҳтимоллигини баҳолаш ва ғараз ниятли кимсалар томонидан содир этилиш моделини яратиш ҳимоянинг оптимал тизимини ҳосил қилишда асосий ахборот ҳисобланади.

Ахборот хавфсизлигига таҳдид – ахборот хавфсизлигининг бузилишига имкон берувчи ёки реал хатарларни вужудга келтирувчи шароит ва омиллар тўпламидир.

Автоматлаштирилган тизимнинг ахборот хавфсизлигига таҳдид – бу автоматлаштирилган тизимда қайта ишланувчи ахборотга, унинг конфиденциаллиги, бутунлиги ва рухсат этилганлигини бузиш-

га олиб келувчи таъсирни амалга ошириш имконияти. Шунингдек, автоматлаштирилган тизимни заифлаштириш, йўқ қилиш ёки издан чиқаришга олиб келувчи, унинг таркибий қисмларига таъсир этиш имконидир.

Ахборот хавфсизлигига таҳдид манбаи – ахборот хавфсизлигига таҳдидни юзага келишига бевосита сабаб бўлувчи субъектдир.

Автоматлаштирилган тизимларда хавфсизликни бузишнинг асосий манбалари қуйидагилар ҳисобланади:

– авария ёки табиий офатлар (ёнғин, ер силкиниши, сув тошқини ва бошқалар);

– техник воситаларнинг инкор этиши ва бузилиши;

– автоматлаштирилган тизим қисмларини лойиҳалаш ва ишлаб чиқишдаги хатолар (дастурий воситалар, маълумотларни қайта ишлаш технологиялари, қурилма воситалари ва бошқалар);

– фойдаланишдаги хатолар;

– тартиббузарларнинг мақсадли ҳаракатлари.

Таҳдидларни тоифалашнинг кўплаб мезонлари мавжуд. Улардан кенг тарқалганлари қуйидагилар:

1. **пайдо бўлиш табиатига кўра:** табиий ва сунъий.

Табиий таҳдидлар – бу инсонларга боғлиқ бўлмаган ҳолда объектив физик жараёнлар ёки табиий офатларнинг автоматлаштирилган тизимлар ва уларнинг қисмларига таъсири туфайли юзага келувчи таҳдидлар. Ўз навбатида сунъий таҳдидлар – инсон фаолияти билан боғлиқ ҳолда келиб чиқувчи автоматлаштирилган тизимларга таҳдидлардир.

2. **мотивация даражасига кўра:** олдиндан бирор мақсадни кўзламаган ҳолда (тасодифий) ва олдиндан мақсадли (қасддан).

Тасодифий таҳдидлар турли хатолар билан боғлиқ бўлиб, булар автоматлаштирилган тизим қисмларини лойиҳалашдаги, дастурий таъминотдаги, хизмат кўрсатувчи ходимларнинг автоматлаштирилган тизим билан ишлашдаги ва шу каби хатоликлар бўлиши мумкин. Олдиндан мақсадли таҳдидлар ғараз ниятли шахсларнинг ғаразли, ғояли ва бошқа мақсадлари билан боғлиқ ҳолда юзага келади. Бунга сабаб моддий фойда кўриш, қасос, маънавий эътиқод ёки бошқалар бўлиши мумкин.

Асосий **тасодифий таҳдидлар**га қуйидагиларни киритиш мумкин:

– тизимнинг меъёрда фаолият кўрсатишини бузилишига ёки тўлиқ тўхтаб қолишига олиб келувчи атайлаб қилинмаган ҳаракатлар.

Бу тоифага шунингдек, тизимнинг қурилмалари, дастурлари ҳамда ресурслари бузилиши ҳам киради;

– қурилмани тасодифан ўчириб қўйиш;

– ахборот ташувчиларни тасодифан бузиб қўйиш;

– нотўғри ишлатилганда тизимнинг иш фаолиятини издан чиқаришга қодир бўлган (тизимнинг осилиб қолиши) ёки тизимни қайтариб бўлмас ўзгаришларга (файлларни ўчириб ташлаш, форматлаш ва шу кабилар) олиб келувчи дастурий таъминотдан фойдаланиш;

– мансаб вазифаларини бажариш учун керак бўлмаган дастурлардан фойдаланиш. Буларга ўйин, таълимий ва бошқа дастурларни киритиш мумкин. Уларни ишлатиш тизим ресурсларининг, хусусан, процессор ва тезкор хотиранинг мақсадсиз сарфланишига олиб келади.

– компьютернинг вируслар билан тасодифий зарарланиши;

– эҳтиётсиз ҳаракатлар туфайли конфиденциал маълумотларнинг ошкор бўлиши;

– хато маълумотларни киритиш;

– пароль, шифрлаш калити, рухсатнома, идентификацияловчи карточка каби идентификаторларни йўқотиш, бошқаларга бериш ёки ошкор қилиш;

– заиф жойларга эга бўлган тизим яратиш, маълумотларни қайта ишлаш технологиясидан фойдаланиш, дастурларни тузиш;

– хавфсизлик сиёсатига ёки тизим билан ишлашга ўрнатилган қоидаларга риоя қилмаслик;

– хизмат кўрсатувчи ходимлар томонидан ҳимоя воситаларини ўчириб қўйиш ёки улардан нотўғри фойдаланиш;

– абонентлар билан хато электрон манзиллар орқали алоқа ўрнатиш.

Асосий **қасддан таҳдидлар**га қуйидагиларни киритиш мумкин:

– тизим ёки унинг алоҳида ташкил этувчилари (қурилмалар, ахборот ташувчилар, хизмат кўрсатувчи ходимлар)нинг меъёрдаги фаолияти бузилишига, ишдан чиқишига, хато ишлашига олиб келувчи физик таъсир кўрсатиш;

– ҳисоблаш тизимининг фаолиятини таъминловчи тизимостиларни ўчириб қўйиш ёки ишдан чиқариш (электр манба, совутгич ва вентилация, алоқа канали ва бошқ.)

– тизимнинг меъёрий ишлашини бузишга қаратилган ҳаракатлар (қурилма ёки дастурларнинг иш режимини ўзгартириш, тизим қурил-

малари ишловчи частоталарда фаол радиошовқинлар ҳосил қилиш ва бошқ.)

– хизмат кўрсатувчи ходимларни ёки алоҳида ваколатга эга бўлган фойдаланувчиларни шантаж қилиш, сотиб олиш ёки бошқа таъсир йўлларини қўллаш;

– масофавий фото-, видео-тасвирга олиш, эшитувчи қурилмаларни қўллаш ва шу кабилар;

– алоқа каналлари орқали узатилувчи маълумотларни тутиб олиш ва уларни тизимга кириш қоидаларини, фойдаланувчиларни муаллифлаштириш ва уларни имитация қилиш орқали тизимга кириш йўлларини аниқлаш мақсадида таҳлил қилиш;

– ахборот ташувчилар (магнит дисклар, тасмалар, хотира микросхемалари, сақловчи қурилмалар ва бутун компьютерлар)ни ўғрилаш;

– ахборот ташувчилардан ноқонуний нусха кўчириш;

– ишлаб чиқариш чиқиндилари (чоп этилган қоғозлар, ёзувлар, рўйхатдан чиқарилган ахборот ташувчилар ва бошқ.)ни ўғирлаш;

– ташқи хотира қурилмалари ёрдамида тезкор хотирадаги қолдиқ ахборотларни ўқиш;

– рухсатни чегараловчи паролларни ва бошқа реквизитларни ноқонуний (айғоқчи орқали, фойдаланувчиларнинг эътиборсизлиги туфайли, танлаш орқали ва бошқалар) қўлга киритиш ва уларни кейинчалик рўйхатдан ўтган фойдаланувчи сифатида қўллаш;

– фойдаланувчиларнинг ўзига хос физик тавсифга эга бўлган терминаллари (масалан, тармоқдаги ишчи станция рақами, физик манзил, алоқа тизимидаги манзил ва бошқалар)дан ноқонуний фойдаланиш;

– ахборотнинг криптоҳимояси шифрини очиш;

– тизимга ноқонуний ва яширин кириш имконини яратувчи «махсус иловалар», «ўрнашмалар», «вируслар»ни киритиш ва тизимда рўйхатдан ўтиб, ундаги маълумотларни узатиш ёки ишдан чиқариш мақсадида тизим ресурсларига ноқонуний рухсатни амалга ошириш;

– алоқа каналларига ноқонуний уланиб олиш ва қонуний фойдаланувчи ишидаги тўхташ (пауза)лар вақтида унинг номидан ёлғон хабарлар киритиш узатилаётган маълумотларни модификация қилиш;

– алоқа каналларига, қонуний фойдаланувчини тизимга кириб олганидан сўнг уни алмаштириш ҳисобига ноқонуний уланиб олиш ва кейинчалик нотўғри маълумотларни киритиш ҳамда ёлғон хабарлар бериш.

Таъкидлаш жоизки, мақсадга эришиш учун ғараз ниятли кимсалар юқорида келтирилган усулларнинг биридан эмас, балки уларнинг бир нечтасидан биргаликда фойдаланадилар.

Таҳдидларни тоифалашнинг бошқа мезонлари:

3. **Нисбатан назорат қилинувчи соҳа ҳолатига кўра**: ташқи ва ички таҳдидлар. Ташқи таҳдидларга мисол сифатида тизимда узатилувчи ёки ёндош электромагнит нурланишлар ва наводкалар орқали маълумотларни тутиб олишни келтириш мумкин. Ички таҳдидларга конфиденциал ахборотга эга бўлган ахборот ташувчини, қурилма қисмини ўғрилаш кабилар киради.

4. **Автоматлаштирилган тизимга таъсир кўрсатиш даражасига кўра**: пассив ва фаол таҳдидлар. Пассив таҳдидлар – автоматлаштирилган тизим таркиби ва фаолиятини бузмайдиган таҳдидлардир. Уларга мисол сифатида конфиденциал ахборотдан нусха кўчириш, ахборотни чиқиб кетиш техник канали орқали чиқариб юбориш, эшитиш ва шу кабиларни келтириш мумкин. Фаол таҳдид эса мос равишда автоматлаштирилган тизим фаолиятини, унинг тузилиши ва таркибини бузилишига олиб келади.

5. **Ахборотнинг бузилувчи хусусияти турига кўра**: конфиденциалликка, рухсат этилганликка ва бутунликка таҳдидлар. Рухсат этилганликка таҳдидларга мисол тариқасида сунъий таҳдидлар билан бир қаторда табиий таҳдидлар, яъни чақмоқ ёки қисқа туташув оқибатида қурилмаларнинг бузилишини келтириш мумкин. Ҳозирги вақтда ахборотнинг рухсат этилганлигига таҳдид сифатида тармоқ ҳужумлари – DDoS (Distributed Denial of Service – хизмат кўрсатишда тақсимланган рад этиш) – ҳужумлар кенг қўлланилмоқда.

Шунингдек, таъкидлаш жоизки бутунликнинг бузилишига нафақат маълумотлар, балки дастурлар муҳити ҳам тааллуқлидир. Тизимнинг вирус билан зарарланиши бутунликка таҳдиднинг амалга оширилишига мисол бўла олади.

Конфиденциалликка таҳдидларга ахборотга ноқонуний рухсат билан боғлиқ бўлган ихтиёрий таҳдидни киритиш мумкин. Масалан, махсус дастур ёрдамида тармоқ орқали узатилаётган ахборотни тутиб олиш ёки танланган паролдан фойдаланиб, ноқонуний рухсатга эга бўлиш.

6. **Таҳдид йўналтирилган тизимнинг турига кўра**: автоном иш жойи асосидаги тизимлар ва умумий фойдаланиш тармоғига уланган тизимлар.

7. **Амалга ошириш усулига кўра**: ҳимояланувчи ахборотга ноқонуний рухсат (шу жумладан тасодифий), ахборотга мақсадли таъсир кўрсатиш, ахборотни чиқиб кетиш техник каналлари орқали чиқариб юбориш.

Энг кенг тарқалган ва оммалашган ахборотга таҳдид тоифаларига: *амалга ошириш усулига кўра* ҳамда *ахборотнинг бузилувчи хусусияти турига кўра*лар киради.

1.3. Ахборот хавфсизлиги бўйича норматив ҳуқуқий ҳужжатлар

Маълумки, ҳуқуқ – бу ҳукумат томонидан турмушнинг маълум бир соҳаларига, давлат органлари, ташкилотлари ёки аҳолига нисбатан ўрнатилган ёки санкцияланган умуммажбурий қоидалар ва меъёрлар тўпламидир.

Ўзбекистон Республикасининг 2012 йил 24 декабрдаги «*Норматив-ҳуқуқий ҳужжатлар тўғрисида (янги таҳрирда)*»ги қонунининг[1] 3-моддасига асосан «Норматив ҳуқуқий ҳужжат ушбу қонунга мувофиқ қабул қилинган, умуммажбурий давлат кўрсатмалари сифатида ҳуқуқий нормаларни белгилашга, ўзгартиришга ёки бекор қилишга қаратилган расмий ҳужжатдир».

Норматив ҳуқуқий ҳужжат – бу ҳуқуқ ижодкорлиги ҳужжати бўлиб, маълум бир тартибда, қатъий белгиланган субъектлар томонидан қабул қилинади ва ҳуқуқ меъёрига эга бўлади.

Норматив ҳуқуқий ҳужжат ҳуқуқнинг асосий манбаи ҳисобланади. Норматив ҳуқуқий ҳужжат (бошқа ҳуқуқ манбаларига нисбатан) кафолат доирасида фақат масъул давлат органлари томонидан қабул қилинади ҳамда маълум бир кўринишга, ҳужжат шаклига эга бўлади. Норматив ҳуқуқий ҳужжатлар мамлакат бўйича амал қилади ва ягона тизимни ҳосил қилади.

Норматив ҳуқуқий ҳужжатлар белгилари:

– меъёрий характер;

– ҳуқуқий акт;

– ҳуқуқ ижодкорлиги натижаси ҳисобланади;

– умуммажбурийлик;

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2012. – №52. – 583-м.

– расмий ҳужжат кўринишида тузилади;

– ҳуқуқ меъёрларини гуруҳлашда маълум бир тартибга риоя қилинади.

«*Норматив-ҳуқуқий ҳужжатлар тўғрисида*»ги қонуннинг 5-моддаси норматив ҳуқуқий ҳужжатларнинг турларини аниқлайди. Қуйидагилар норматив ҳуқуқий ҳужжат ҳисобланади:

- Ўзбекистон Республикаси Конституцияси;
- Ўзбекистон Республикаси қонунлари;
- Ўзбекистон Республикаси Олий Мажлиси палаталари қарорлари;
- Ўзбекистон Республикаси Президенти фармонлари, қарорлари ва фармойишлари;
- Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари;
- вазирликлар, давлат қўмиталари ва идораларнинг буйруқлари ҳамда қарорлари;
- маҳаллий давлат ҳокимияти органларининг қарорлари.

Норматив-ҳуқуқий ҳужжатлар қонун ҳужжатлари ҳисобланади ва Ўзбекистон Республикаси қонун ҳужжатлари мажмуини ташкил этади.

Ўзбекистон Республикасининг Конституцияси ва қонунлари, Ўзбекистон Республикаси Олий Мажлиси палаталарининг қарорлари қонунлардир.

Ўзбекистон Республикаси Президенти фармонлари, қарорлари ва фармойишлари, Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари, вазирликлар, давлат қўмиталари ва идораларнинг буйруқлари ҳамда қарорлари, маҳаллий давлат ҳокимияти органларининг қарорлари қонун ости ҳужжатлари ҳисобланади (ушбу қонуннинг 6-моддаси).

Ахборот хавфсизлигини таъминлашда норматив ҳуқуқий бошқарувнинг зарурлиги. Ҳуқуқий база ахборотга эгалик ҳуқуқига ва уни муҳофаза қилишга оид вазифаларни ечиш имконини бериши зарур. Ҳимояланаётган ахборотга таҳдидни аниқлаши ва уни ҳимоялаш тартибини белгилаши керак. Ҳуқуқий давлатда барча ташкилот ва муассасалар, раҳбар шахслар ва фуқаролар фаолияти амалдаги қонунлар доирасида ташкил этилиши лозим.

Ахборотни муҳофаза қилиш соҳасига оид норматив ҳуқуқий ҳужжатларда:

– ахборотни муҳофаза қилиш, унинг махфийлиги ва ҳимоя учун ўрнатилган қоидалар соҳасида турли субъектларнинг ҳуқуқлари ифодаланиши;

– ҳимояланаётган ахборотга ноқонуний таҳдид қилиш ёки унинг эгасига зарар етказувчи оқибатларни келтириб чиқариши мумкин бўлган ҳаракатлар учун жиноий, маъмурий, моддий ва маънавий жавобгарлик белгиланиши керак.

Ахборотни ҳуқуқий ҳимоялаш захира сифатида давлат ва халқаро миқёсда тан олинган ҳамда халқаро шартнома, конвенция ва декларацияларда аниқланади. Давлат миқёсида ахборотни ҳуқуқий ҳимоялаш давлат ва ташкилот ҳужжатлари орқали назорат қилинади.

Ахборот хавфсизлигини таъминлаш муаммоси комплекс характерга эга. Уни ҳал қилиш учун ҳуқуқий ҳамда ташкилий чоралар ва дастурий-техник таъминотни (идентификация ва аутентификация; рухсатни бошқариш; протоколлаштириш ва аудит; криптография) биргаликда кўриш талаб этилади (мисол учун, корхона бошқаруви миқёсида унинг компьютер ахборот тармоғида ахборот хавфсизлигини таъминлаш учун хавфсизлик сиёсатини ишлаб чиқиш ҳамда керакли ресурслар талаб этилади).

Ўзбекистон Республикасининг 2015 йил 9 декабрда эълон қилинган «Электрон ҳукумат тўғрисида»ги қонунининг[1] 12-моддаси «Ахборот хавфсизлигини таъминлаш принципи» деб номланади. Ушбу моддага биноан электрон давлат хизматлари кўрсатувчи давлат органлари электрон давлат хизматлари кўрсатишда фойдаланиладиган ахборот тизимлари ва ахборот ресурсларининг ахборот хавфсизлигини таъминлаши шарт.

Электрон давлат хизматлари кўрсатувчи давлат органлари шахсга доир маълумотлар, шунингдек давлат сирларини ёки қонун билан қўриқланадиган бошқа сирни ташкил этувчи маълумотлар муҳофаза қилинишини ва улардан рухсатсиз фойдаланишнинг олди олинишини таъминлаш юзасидан зарур ташкилий-техник чоралар кўради.

Электрон давлат хизматлари кўрсатувчи давлат органларининг ахборот тизимларида ва ахборот ресурсларида сақланадиган шахсга доир маълумотлардан улар қайси ариза берувчига тааллуқли бўлса, ўша ариза берувчининг розилиги билан уларга ишлов бериш, уларни узатиш ва олиш учун фойдаланилади, бундан қонун ҳужжатларида белгиланган ҳоллар мустасно.

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2015. – № 49. – 611-м.

Ахборотни муҳофаза қилиш соҳасида халқаро стандартлар. 1983 йил АҚШ Мудофаа Вазирлиги (МВ) компьютер хавфсизлиги Агентлиги **TSEC** (Ишончли Тизимларнинг Ҳимояланганлигини Баҳолаш Критерийлари) номли ҳисоботини чоп этди. У бошқача айтганда ***Тўқ сариқ рангли китоб*** (китоб рангига кўра) деб номланди. Унда кўп фойдаланувчили компьютер тизимларида махфий маълумотларни ҳимоялаш учун хавфсизликнинг 7 та даражаси ажратилган. Булар: Al – кафолатли ҳимоя; Bl, B2, B3 – рухсатни тўлиқ бошқариш; Cl, C2 – рухсатни танлаш орқали бошқариш; D – минимал хавфсизлик.

АҚШ Мудофаа Вазирлиги компьютер тизимларини баҳолаш мақсадида АҚШ МВ қошидаги компьютер хавфсизлиги Миллий Маркази **NCSC-TG-005** ва **NCSC-TG-011** номли ***Қизил китоб*** (китоб рангига кўра) деб номланган қўлланмасини чиқарди.

Бунга жавоб тариқасида Германия ахборот хавфсизлиги Агентлиги **Green Book** (***Яшил китоб***) ни тайёрлади. Унда хусусий ҳамда давлат миқёсида ахборот хавфсизлигини таъминлашда вужудга келувчи талаблар комплекс тарзда ўз аксини топган.

1990 йилда *Яшил китоб* Германия, Буюк Британия, Франция ва Голландия давлатлари томонидан маъқулланди ва Европа Иттифоқига юборилди. Унинг асосида Европа стандартини ифодаловчи **ITSEC** (Ахборот Технологияларининг Ҳимояланганлигини Баҳолаш Критериялари) ёки ***Оқ китоб*** тайёрланди. Бу китобда хавфсиз ахборот тизимларини ташкил этиш критериялари келтирилган.

Оқ китобда хавфсизлик критерияларининг қуйидаги асосий қисмлари берилган:

1. Ахборот хавфсизлиги.
2. Тизим хавфсизлиги.
3. Маҳсулот хавфсизлиги.
4. Хавфсизликка таҳдид.
5. Хавфсизлик функцияси тўплами.
6. Хавфсизликнинг кафолатланганлиги.
7. Хавфсизликнинг умумий баҳоси.
8. Хавфсизлик синфлари.

Европа критерияларига кўра **ITSEC** ахборот хавфсизлигининг олти асосий элементи ва унинг қисмларини ўз ичига олади:

1. Ахборот конфиденциаллиги (ахборотни ноқонуний олишдан ҳимоялаш).

2. Ахборот бутунлиги (ахборотни ноқонуний ўзгартиришдан ҳимоялаш).

3. Ахборотдан фойдалана олишлик (ахборот ва тизим ресурсларини ноқонуний ёки тасодифий тутиб олишлардан ҳимоялаш).

4. Хавфсизлик мақсадлари (ахборот хавфсизлиги функциялари нима учун керак?).

5. Ахборот хавфсизлиги вазифаларининг таснифи:

– идентификация ва аутентификация (фойдаланувчининг ҳақиқийлигини анъанавий текширишгина эмас, янги фойдаланувчиларни рўйхатга олиш, эскиларини ўчириш, шунингдек аутентификация, ахборотларини ўзгартириш ва текшириш учун функциялар, шу жумладан бутунликни назорат қилувчи воситалар ҳам тушунилади);

– фойдаланиш ҳуқуқини бошқариш (шу жумладан, умумфойдаланилувчи объектларнинг бутунлигини таъминлаш мақсадида уларга рухсатни вақтинча чегараловчи хавфсизлик функциялари, рухсат бериш ҳуқуқини тарқатишни бошқариш кабилар);

– ҳисобот беришлилик (протоколлаштириш);

– аудит (мустақил назорат);

– объектлардан қайта фойдаланиш;

– ахборотнинг аниқлиги (маълумот турли қисмларининг ўзаро мослигини таъминлаш (алоқа аниқлиги) ҳамда ахборотни узатишда уни ўзгармаслигини таъминлаш (коммуникация аниқлиги));

– хизмат кўрсатишнинг ишончлилиги (қисқа вақт ичида вақт бўйича критик ҳаракатлар бажарилишини таъминловчи функциялар; критик бўлмаган, яъни керакли вақтда маълумотни олиш имконини бериш; хатоларни топиш ва уларни бартараф этиш функциялари; коммуникация хавфсизлигини таъминловчи режаловчи функциялар);

– маълумот алмашиш.

6. Хавфсизлик механизмларини ифодалаш.

Европа критерияларида хавфсизликнинг 10 та синфи ўрнатилган (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-D1, F-DC, F-DX). Уларнинг дастлабки бештаси Американинг TCSEC критериясидаги Cl, C2, Bl, B2, B3 даражаларга мос келади. F-IN синфи ахборот бутунлигига бўлган юқори талабга асосланган бўлиб, МББТ (маълумотлар базасини бошқариш тизими)га мос келади ҳамда рухсатнинг қуйидаги турлари фарқланади: ўқиш, ёзиш, қўшиш, ўчириш, ҳосил қилиш, қайта номлаш ва объектларни белгилаш. F-AV синфи ахборот тизимлари

иш қобилиятини таъминлаш учун юқори талабга мўлжалланган. F-D1 синфи ахборот каналлари орқали узатилувчи маълумотларнинг бутунлигига бўлган юқори талабга мўлжалланган. F-DC синфи ахборот конфеденциаллигига бўлган юқори талабга мослашган. F-DX синфи эса бир вақтда F-D1 ва F-DC синфлари талабларига нисбатан кучайтирилган талабга асосланган.

Ахборот ҳимоясининг комплекс ташкил этилишига криптографик ҳимоя воситаларидан фойдаланиш алгоритмини давлат стандартларига мос равишда таъминлаш ҳисобига эришилади.

Назорат учун саволлар

- Ахборот хавфсизлиги тушунчаси нимани англатади?
- Ахборот хавфсизлигининг қандай ташкил этувчилари мавжуд?
- Ахборот хавфсизлигини таъминлашнинг учта муҳим хусусияти нималардан иборат?
- Ахборотни муҳофаза қилиш деганда нима тушунилади?
- Ахборотни муҳофаза қилишнинг қандай усуллари ва турлари мавжуд?
- Ахборотни муҳофаза қилиш воситаларига нималар киради?
- Ахборотни муҳофаза қилиш тизимлари қандай вазифани бажаради?
- Ахборот хавфсизлигига таҳдид деганда нима тушунилади?
- Ахборот хавфсизлиги бўйича норматив-ҳуқуқий ҳужжатлар нимани ифодалайди?
- Ахборотни муҳофаза қилиш соҳасида қандай халқаро стандартлар мавжуд?

II. АХБОРОТЛАРНИ ТЕХНИК ҲИМОЯЛАШ

2.1. Техник ҳимоя объектлари ва ҳимоя воситалари

Ахборот тизимларида маълумотларни техник ҳимоялаш масаласи бугунги кунда долзарб вазифалардан бири ҳисобланади.

Замонавий ахборот тизимларида сақланувчи, қайта ишланувчи ва узатилувчи ахборотларни ҳамда объектларни ҳимоялаш учун мураккаб ва такомиллашган усулларидан фойдаланилади. Таҳдидлар спектри кенглигини инобатга олиб, ахборот ҳимояси масаласига комплекс ёндашиш талаб этилади.

Ахборот ҳимояси тизимининг жуда кенг кўламга эга бўлган чораси – бу техник ҳимоя бўлиб, у муҳим аҳамиятга эга.

Ахборотнинг техник ҳимояси – амалдаги қонунчиликка мос равишда техник, дастурий ва дастурий-техник воситалар ёрдамида ахборот хавфсизлигининг нокриптографик усуллари билан таъминлашни инобатга олувчи ахборот ҳимоясидир. Шунга алоҳида эътибор қаратиш муҳим-ки, техник ҳимоя деганда нафақат техник каналлар орқали маълумотнинг чиқиб кетишини олдини олиш, балки ахборотни ноқонуний рухсатлардан, математик таъсирлардан, зарарлантирувчи дастурлардан ва бошқалардан ҳимоя қилиш ҳам тушунилади. Ахборотни техник ҳимоялаш объектларига қуйидагиларни киритиш мумкин:

– ахборотлаштириш объекти;

– ахборот тизими;

– ахборот тизими ресурслари;

– ахборот технологиялари;

– дастурий воситалар;

– алоқа тармоқлари.

Назорат ҳудуди – бу қўриқланувчи (ҳудуд, бино, офис ва бошқ.) соҳа бўлиб, унинг ичида коммуникация қурилмалари ҳамда ахборот тармоғининг локал таркибий қурилмаларини бирлаштирувчи барча нуқталар жойлашади.

Ахборот тизимларида таъсир этилиши мумкин бўлган **объектлар**га қуйидагиларни киритиш мумкин:

– аппарат таъминоти;

– дастурий таъминот;

– коммуникациялар (алоқа каналлари ёки коммуникация қурилмалари орқали маълумотларни узатиш ва қайта ишлаш);

– хизмат кўрсатувчи ходимлар.

Ахборотнинг конфиденциаллиги, бутунлиги ва рухсат этилганлигини бузиш мақсадида таъсир кўрсатиш объектларига нафақат ахборот тизими элементлари, балки уни қўллаб турувчи инфратузилма (электр, иссиқлик таъминоти, совитиш тизимлари) ҳам киради. Бундан ташқари техник воситаларнинг жойлашиш ҳудудига ҳам эътибор қаратиш лозим, яъни уларни қўриқланувчи ҳудудга жойлаштириш зарур. Симсиз алоқа воситаларини ўрнатишда, уларнинг амал қилиш масофаси (ҳаракат зонаси) назорат қилинувчи ҳудуддан чиқиб кетмаслиги тавсия этилади.

Техник ҳимоя воситалари – бу техник қурилмалар, комплекслар ёки тизимлар ёрдамида объектни ҳимоялашдир. Техник воситаларнинг афзаллиги кенг кўламдаги масалаларни ҳал этилишда, юқори ишончлиликда, комплекс ривожланган ҳимоя тизимини яратиш имкониятида, рухсатсиз фойдаланишга уринишларга мос муносабат билдиришда ва ҳимоялаш амалларини бажариш усулларидан фойдаланишнинг анъанавийлигида намоён бўлади.

Маскировкаловчи (ниқобловчи) белгиларнинг очилиши (демаскировка белгилари) деганда объектнинг бошқа объектлардан бирон-бир тавсифи билан фарқ қиладиган хусусияти тушунилади. Фарқловчи тавсифлар сон ёки сифатда баҳоланиши мумкин. *Объектнинг демаскировка белгилари* – бу ҳимоя объектига хос хусусият бўлиб, ундан техник разведка объектни топиши ёки аниқлаши ҳамда объект ҳақида керакли маълумотларни олиш учун фойдаланилиши мумкин. Ахборотга эгалик демаскировка белгиларини таҳлил этиш орқали амалга оширилади. Демак, бу белгилар ахборотни ўзига хос чиқиб кетиш канали ҳисобланади. Демаскировка белгиларни тарқатувчилар бўлиб тўғридан-тўғри бу белгилар билан боғлиқ бўлган физик майдонлар ҳисобланади.

Ахборот тизимида техник характердаги тадбирлар. Ахборот хавфсизлиги тизимининг инженер-техник элементи техник разведка воситаларига ҳамда уларнинг комплекси асосида назорат соҳасини ҳосил қилишга қарши фаол ва пассив қаршилик кўрсатиш учун мўлжалланган. Ахборотни ҳимоя қилишда ушбу элемент муҳим аҳамиятга эга бўлиб, унинг таркибига қуйидагилар киради:

– бино, иншоат, алоқа линиялари жойлашган ҳудудга бегона шахсларнинг киришига қарши физик ҳимояни ташкиллаштириш;

– компьютер қурилмалари, алоқа воситалари, модемлар, факслар ва алоқа канали орқали маълумот узатишда иштирок этувчи бошқа қурилмалар билан ишлаш жараёнида вужудга келувчи ахборотнинг чиқиб кетиш техник каналларига қарши техник воситалар;

– бинони визуал усуллар билан техник разведка қилишдан ҳимояловчи воситалар;

– кузатиш воситалари, хабар бериш, сигнализация, ахборот бериш, техник воситаларнинг иш фаолияти бузилганда ёки тармоқ алоқаси катталиклари ўзгартирилганда уларни идентификация қилиш;

– техник разведка асбоблари ва қурилмалари (эшитиш, кузатиш, узатиш ва бошқ.)ни аниқловчи воситалар;

– хизмат кўрсатувчи ходимлар томонидан иш жойидан махсус ниқобланган (маскировка) буюмларни, ахборот ташувчилар, ташқи хотиралар ва шу кабиларни олиб чиқиб кетишни олдини олувчи назорат техник воситалари;

– техник воситаларнинг захирасини яратиш, ахборот ташувчиларнинг нусхасини ҳосил қилиш.

Ахборот ҳимоя тизимининг асосий элементларидан бири – бу тизимдаги барча электрон қурилмаларни узлуксиз ишлаши учун уларни электр манбаи билан таъминлаш. Кўпчилик ахборот ташувчиларга электр энергияси узатишнинг тўлиқ узилиши компьютер ёки бошқа электрон қурилмаларнинг иш ҳолатига салбий таъсир кўрсатади деган нотўғри фикрга эга. Аксинча, электр тармоғидаги оддий кўз билан илғаб бўлмайдиган кучланиш ўзгаришлари ёки халақит беришлар тизимдаги қурилмаларга энг катта зарар келтириши мумкин. Юқори сезгирли электрон қурилмалар, шу жумладан компьютер, коммутатор ва маршрутизаторлар электр тармоғидаги кучланиш ўзгаришини дарҳол сезади ва муносабат билдиради.

Бундан ташқари, шунга эътибор бериш керакки, ғаразгўй кимсалар объект (корхона, ташкилот)даги ахборот муҳитида қайта ишланаётган маълумотларни 127/220/380 В кучланишли электр тармоғи воситасида ечиб олишлари мумкин. Ёндош электромагнит нурланишлар даражасини камайтириш учун махсус ахборот ҳимоя воситалари қўлланилади. Булар:

– бинони экранлаш;

– ҳимоя объектлари кучланишини қўшимча равишда ечиш (ерга уланиш);

– тармоқ шовқин-пасайтиргич фильтрлар ёрдамида электр манбаи занжирларини ажратиш;

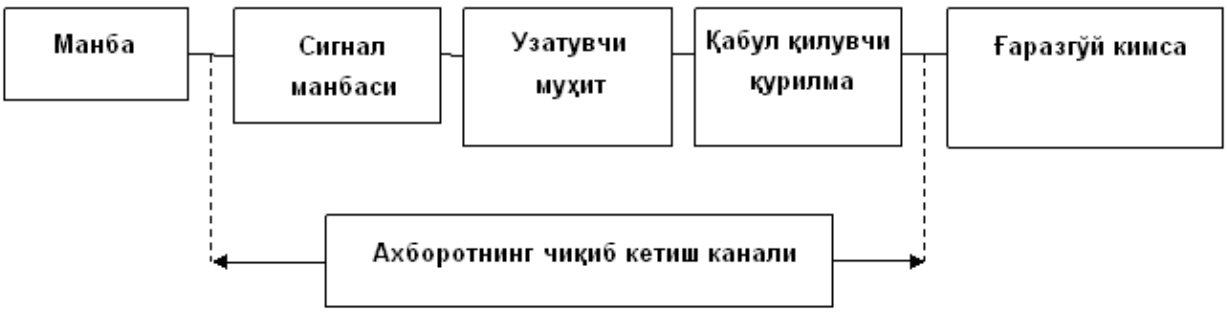
– назорат қилинувчи соҳадаги ахборот занжирлари ва ташқи алоқа линиялари орасида электромагнит майдонини ажратиш.

2.2. Ахборотнинг чиқиб кетиш техник каналлари таснифи

Маълумки, ахборот майдон ёки моддий буюм орқали узатилади. Бу акустик тўлқин ёки электромагнит нурланиш ёки матн жойлашган қоғоз варағи бўлиши мумкин. Бошқача айтганда у ёки бу физик майдонлардан фойдаланган ҳолда инсон ахборот узатиш тизимини ёки алоқа тизимини яратади. Алоқа тизими, умуман олганда узаткич, ахборот узатиш канали, қабул қилгич ва ахборотни қабул килувчидан ташкил топади. Легитим алоқа тизимлари ахборотни қонуний равишда алмашиш учун ҳосил қилинади ва қўлланилади. Бироқ ахборот узатишнинг физик табиатини инобатга олганда, маълум бир шартларни бажаришда алоқа тизимида ахборотни жўнатувчи ва қабул қилувчига боғлиқ бўлмаган ҳолда ахборотни узатувчи алоқа канали – *ахборотнинг чиқиб кетиш техник канали* вужудга келиши мумкин.

Чиқиб кетиш – конфеденциал маълумотнинг ташкилот ёки маълум бир шахслар доирасидан назоратсиз чиқиб кетишидир.

Техник канал орқали маълумотларнинг чиқиб кетиши – физик муҳит орқали ҳимояланган ахборот ташувчидан ахборотни тутиб олувчи техник воситага ахборотнинг назоратсиз чиқиб кетиши. Ахборотнинг чиқиб кетиш техник канали (АЧКТК) худди ахборотни узатиш канали каби сигнал манбаи, уни тарқатувчи физик муҳит ва ғаразгўй кимсанинг қабул қилгич қурилмасидан ташкил топади. Ахборотнинг чиқиб кетиш техник канали тузилиши 1-расмда келтирилган.



1-расм. *Ахборотнинг чиқиб кетиш техник канали тузилиши*

Ахборотнинг чиқиб кетиш техник каналларини тоифалашнинг асосий белгиси сифатида ахборот ташувчининг физик табиати олинади. Ушбу белгига кўра АЧКТК қуйидагиларга бўлинади:

– оптик;

– радиоэлектрон;

– акустик;

– моддий-буюмли.

Электромагнит майдон (фотонлар) оптик каналда ахборот ташувчи ҳисобланади. Оптик тўлқинлар диапазони қуйидагиларга бўлинади:

– олис инфрақизил диапазон 100-10 мкм (3-30 ТГц);

– ўрта ва яқин инфрақизил диапазон 10-0,76 мкм (30-400 ТГц);

– кўринувчи диапазон (кўк-яшил-қизил) 0,76-0,4 мкм (400-750 ТГц).

Ахборотни чиқиб кетиш радиоэлектрон каналида ахборот ташувчи сифатида радиодиапазондаги электр, магнит ва электромагнит майдонлар, шунингдек, металл ўтказгичларда тарқалувчи электр токи (электронлар оқими) фойдаланилади. Радиоэлектрон каналда частота диапазони бир неча ўн ГГц дан товуш частотасигача бўлган соҳани эгаллайди. Ушбу диапазон қуйидагиларга бўлинади:

– паст частотали 10-1 км (30-300 кГц);

– ўрта частотали 1 км – 100 м (300 кГц – 3 МГц);

– юқори частотали 100-10 м (3-30 МГц);

– ультраюқори частотали 10-1 м (30-300 МГц);

– шу тартибда ўта юқори частоталигача 10-1 см (3-30 ГГц);

Муҳитда тарқалувчи эластик акустик тўлқинлар акустик каналда ахборот ташувчи ҳисобланади. Унда қуйидаги диапазонлар ажратилади:

– инфратовушли диапазон 1500-75 м (1-20 Гц);

– қуйи товушли диапазон 150-5 м (1-300 Гц);

– товушли диапазон 5-0,2 м (300-16000 Гц);

– ультратовушли диапазон 16000 Гц дан 4 МГц гача.

Моддий-буюмли каналда ахборотнинг чиқиб кетиши назорат қилинувчи соҳада ҳимояланган ахборотга эга моддий ташувчиларнинг ноқонуний тарқалиши оқибатида юзага келади. Аксарият ҳолларда бундай моддий ташувчилар – ҳужжатларнинг қораланма варианти ёки нусха кўчиришда фойдаланилган қоғоз бўлиши мумкин.

Ахборотнинг чиқиб кетиш каналларини яна ахборотлаштирилганлигига кўра тоифалаш мумкин, яъни ахборотлаштирилган, кам ахборотлаштирилган ва ахборотлаштирилмаган. Каналнинг ахборот-

лаштирилганлиги ундаги узатилаётган ахборотларнинг қимматлилигига кўра баҳоланади.

Пайдо бўлиш вақтига кўра каналлар: доимий, даврий ва эпизодик (ҳар замонда) турларига бўлинади. Доимий каналда ахборотнинг чиқиб кетиши деярли доимий характерга эга бўлади. Эпизодик каналларда бу ҳолат тасодифий бир марталик характерга эга бўлади.

Ахборотнинг чиқиб кетиш техник каналлари қуйидаги таҳдидларни юзага келтириши мумкин:

– акустик ахборотнинг чиқиб кетиш таҳдиди;

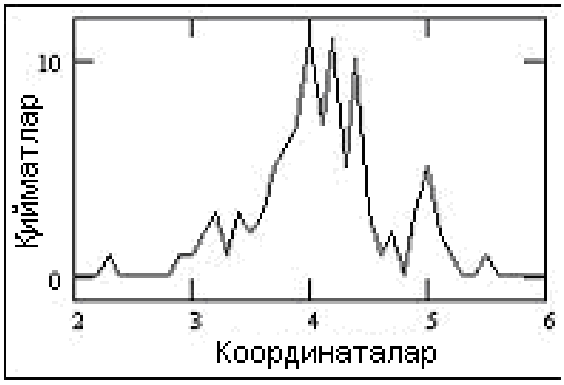
– кўринувчи ахборотнинг чиқиб кетиш таҳдиди;

– каналларга ёндош бўлган электромагнит нурланиш орқали чиқиб кетиш таҳдиди.

Узатиш қурилмаси, тарқалиш муҳити ва қабул қилиш қурилмасидан иборат бўлган ахборотнинг чиқиб кетиш канали бир каналли ҳисобланади. Бироқ, айрим ҳолларда ахборотнинг чиқиб кетиши мураккаброқ йўл билан – бир нечта кетма-кет ёки параллел каналлар орқали амалга оширилади. Бунда ахборотнинг бир ташувчидан бошқасига ёзиб олиш усулидан фойдаланилади. Масалан, бирор хонада махфий суҳбат олиб борилаётганда, ахборотнинг чиқиб кетиши фақатгина ойна, девор, эшик орқали акустик канал воситасида эмас, балки лазер нури орқали ойна воситасида маълумотни олиш – оптик канал орқали ёки хонага радиоўрнашма қўйиш билан радиотўлқинларни тутиб олиб, сўнгра узатиш воситасида – радиоэлектрон канал орқали амалга оширилиши мумкин. Кейинги икки ҳолатда акустик ва оптик ёки акустик ва радиоэлектрон каналлардан иборат бўлган таркибий канал ҳосил бўлади.

Ахборот сигнали тушунчаси. Турли физик табиатга эга бўлган сигналлар моддий ахборот ташувчилари бўлиши мумкин. Тор маънода сигнал деганда электр токи, кучланишининг тебранишлари – электромагнит тўлқинлар, механик тебранишлар тушунилади. Ахборот сигналлари маълум бир қонуниятлар асосида ахборот ташувчининг у ёки бу катталикларини ўзгариши орқали ҳосил бўлади. Демак, катталиклари узатилувчи ахборотга боғлиқ равишда ўзгарувчи ихтиёрий физик жараён – ахборот сигнали бўлиши мумкин.

Сигналнинг физик муҳит орқали ўтишида унга турли мувозанатдан чиқарувчи омиллар (факторлар) таъсир кўрсатади. Бунинг оқибатида турли табиатга эга бўлган шовқинлар ва халақит беришлар юзага келади (2-расм).



Сигнал *Сигнал ҳалақит беришлар билан*

2-расм.

Тузилишига кўра сигналлар **аналогли** ва **рақамли** турларга бўлинади. Аналогли сигнал узлуксиз аргументнинг узлуксиз функцияси сифатида ифодаланади. Бундай сигналлар вақт давомида узлуксиз бўлиб, уларнинг манбаи сифатида ихтиёрий физик жараёнлар ёки ҳодисаларни олиш мумкин. Рақамли сигналлар 0 ёки 1 кўринишидаги сигналлар бўлиб, улар вақт давомида сигналнинг бор ёки йўқлигини англатади.

Хавфли сигналлар ва уларнинг манбалари. Ғаразгўй кимсалар томонидан тутиб олиниб, кейинчалик уларни очиш мумкин бўлган ҳимояланган маълумотларни узатувчи сигналлар хавфли сигналлар деб аталади. Бундай сигналлар икки кўринишга бўлинади: ***функционал*** ва ***тасодифий***. Функционал сигналлар маълумотларни қайта ишловчи техник воситалар томонидан уларга қўйилган вазифаларни бажариш учун ҳосил қилинади. Бундай сигналларнинг асосий манбаларига қуйидагилар киради:

– алоқа тизими манбалари;

– радиотехник тизимлар узаткичлари;

– ўзидан акустик сигнал чиқарувчилар;

– инсонлар.

Функционал сигналларнинг тасодифий сигналлардан фарқли жиҳати шундаки, ахборот эгаси уларнинг хавфсизлиги бузилишига таҳдидлар мавжудлигини олдиндан билади ва уларни олдини олиш ёки камайтириш чораларини кўриши мумкин.

Бироқ замонавий ахборотни қайта ишлаш, сақлаш ва узатиш воситалари ўзларининг иш жараёнида ёндош радио- ёки электр сигналларини ҳосил қилиши мумкин. Бундай сигналлар тасодифий

хавфли сигналлар деб номланади. Ушбу сигналлар ахборот эгасининг хоҳишига боғлиқ бўлмаган ҳолда ҳосил бўлади ва уларни махсус тадқиқотлар ўтказмай туриб аниқлаб бўлмайди.

Тасодифий хавфли сигналлар манбаи бўлиши мумкин бўлган техник воситаларга қуйидагилар киради:

– ўтказгичли телефон алоқаси воситалари;

– мобиль алоқа ва радиоалоқа воситалари;

– электрон почта воситалари;

– ҳисоблаш техникаси воситалари;

– аудиоқурилмалар ва товуш кучайтиргич воситалари;

– радио қабул қилувчи қурилмалар;

– видеоқурилмалар;

– телевизион воситалар;

– чизиқли радиоэфир воситалари.

Тасодифий хавфли сигналлар қуйидаги электр жиҳозлари томонидан пайдо бўлиши мумкин:

– тизимда вақтни электрон тақсимлаш воситалари;

– қўриқлаш сигнализацияси воситалари;

– ёнғин хавфсизлиги сигнализацияси воситалари;

– оргтехника (шу жумладан принтерлар);

– совитиш ва вентиляция тизими воситалари;

– таркибида акустик ахборотларни электромагнит сигналларга айлантириб берувчи элементларга эга бўлган маиший ва бошқа техникалар;

– назорат қилинувчи ҳудуддан ўтувчи электр ўтказувчи алоқа иншоотлари.

Техник воситалар асосий техник воситалар ва тизимлар (АТВТ) ҳамда ёрдамчи техник воситалар ва тизимлар (ЁТВТ)га бўлинади. Бунда эътиборли жиҳати шундаки, ЁТВТ ҳимояланган ахборотни қайта ишламайди. Аммо улар АТВТ билан биргаликда назорат зонасида жойлашган бўлиши мумкин. Маълум бир шароитларда ЁТВТ тасодифий хавфли сигналлар манбаи бўлиб қолиши мумкин. Шунинг учун улар ҳам ҳимояга муҳтож ҳисобланади.

Акустик ахборотларни чиқиб кетиш техник каналлари.

Товуш – бу эшитиш органи орқали қабул қилинувчи, эластик муҳит зарраларининг механик тебраниши. Товуш аслида тўлқин бўлганлиги учун уни характерловчи катталиклар амплитуда ва частота

спектри ҳисобланади. Инсон 16-20000 Гц частота диапазонидаги товушларни эшитади. Ундан паст частотали диапазондаги товушлар инфратовуш деб номланади. 20000 Гц дан 1 ГГц гача частота оралиғидаги товушлар – ультратовушлар, 1 ГГц дан юқорилари эса – гипертовушлар деб аталади.

Ташувчиси акустик сигналлар бўлган ахборотлар акустик ахборотлар дейилади. Акустик тебранишларнинг бирламчи манбаи - механик тизимлар, масалан, инсоннинг нутқ органлари, иккиламчи манбалари эса турли ўзгартиргичлар, жумладан электроакустик қурилмалар ҳисобланади.

Товуш босими – бу муҳитда товуш тўлқинлари тарқалиши билан боғлиқ бўлган ўзгарувчи босим. Товуш босими катталиги товуш тўлқинининг юза бирлигига таъсир кўрсатиш кучи билан баҳоланади ва барларда ($Н/м^2$) ўлчанади.

Товуш босими ўзгарувчан бўлишига сабаб, у бир заррачадан бошқасига узатилади ва бу ҳолат эластик муҳитда заррачанинг кескин силжиши билан амалга ошади, натижада ана шу жойда босим ортиши содир бўлади. Бу жараён кейинги қўшни заррачаларга узатилади ва шу тартибда давом этади. Бу жараённи эластик муҳитда босим ортиши кўчиб юриши билан ифодалаш мумкин. Бунда муҳитда тўлқин кўринишида тарқалувчи босим ортган ва камайган соҳалар кетма-кетлиги кузатилади. Муҳитдаги ҳар бир зарра тебранувчи ҳаракатни содир этади.

Суюқ ва газсимон муҳитларда акустик тебранишлар бўйлама характерга эга бўлиб, унда заррачалар тебраниши тўлқин тарқалиши йўналишига мос тушади. Қаттиқ жисмларда бўйлама деформациядан ташқари силжиш эластик деформацияси ҳам пайдо бўлиб, унинг таъсирида кўндаланг тўлқинлар ҳам ҳосил бўлади. Бу ҳолда заррачалар тўлқин тарқалиш йўналишига перпендикуляр йўналувчи тебранишларни содир этади. Бўйлама тўлқинларнинг тарқалиш тезлиги силжиш тўлқинлариникига нисбатан анча юқори бўлади.

Товуш кучи – бу бирлик вақт ичида бирлик юзадан ўтувчи товуш энергияси миқдори бўлиб, у квадрат метрдаги ваттларда ўлчанади ($Вт/м^2$). Таъкидлаш керакки, товуш босими ва товуш кучи ўзаро квадрат кўринишда боғлиқ, яъни товуш босими 4 баробар оширилса, товуш кучи 16 баробар ортади.

Товуш баландлиги – товушни сезиш интенсивлиги бўлиб, у товуш кучи ва частотасига боғлиқ. У товуш кучининг логарифмига пропорционал бўлиб, децибелларда ифодаланади. Товуш баландлигининг ўлчов бирлиги – фон ҳисобланади.

Динамик диапазон – товуш баландлиги диапазони ёки децибелларда ифодаланувчи товуш босимининг энг юкори ва энг қуйи товушлари фарқи.

Ахборотларни чиқиб кетиш акустик канали ҳосил бўлишининг манбаи – булар инсоннинг товуш бўғини каби тебранувчи жисм ва механизмлар, машиналарнинг ҳаракатланувчи элементлари, телефон аппаратлари, товуш кучайтиргич қурилмалар ва бошқалар бўлиши мумкин.

Ахборот сигналининг пайдо бўлиш физик табиатига, шунингдек акустик тебранишларнинг тарқалиш муҳити ва уларни тутиб олиш усулига кўра акустик ахборотларнинг чиқиб кетиш каналларини қуйидаги турларга ажратиш мумкин: ҳаво, тебранувчи, электроакустик, оптик-электрон ва параметрли.

Ахборотларни ҳаво акустик чиқиб кетиш каналида акустик сигналларни тарқалиш муҳити сифатида ҳаво қаралади, асосий тутиб олиш қурилмаси сифатида эса микрофондан фойдаланилади. Микрофон акустик сигнални электр сигналга айлантириб беради ва ёзиб олиш қурилмасига ёки бирор бир узатувчи қурилмага уланган бўлади. Олинган сигналларни ғаразгўй кимсага узатишни эса турли каналлар: радиоканал, оптик канал, электр тармоғи ва бошқалар орқали амалга ошириш мумкин.

Ахборотларни чиқиб кетиш оптик каналлари. Оптик каналлар демаскировка белгиларига кўра энг кучсиз ҳисобланади, яъни махсус техник воситалар, масалан, махсус фототасвир ёрдамида масофадан туриб ахборотни тутиб олиш мумкин.

Кўриниш тирқиши кичик бўлган, мураккаб тузилишга эга ва яхши ёритилмаган соҳаларни визуал кузатиш учун оптик-толали қурилмалар – **эндоскоплар** ишлаб чиқилган. Бундай қурилма кучли ёруғлик манбаи, ёритиш световоди, тасвир световоди, ёруғлик равшанлигини бошқарувчи окуляр, световоднинг ишчи қисми эгилувчан соҳасининг манипуляторидан ташкил топади. Ёруғлик манбаи сифатида интерференцион қопламали акслантирувчи билан жиҳозланган галоген лампадан фойдаланилади. Ёритиш световоди орқали ёруғлик кузатилиши қийин бўлган яхши ёритилмаган соҳага юборилади. Объектив билан

катталаштирилган тасвир световод орқали операторга узатилади. Тасвир сифати равшанликни бошқарувчи ёрдамида ўзгартирилади. 3-расмда ЭТГ сериясидаги эндоскоп тасвири келтирилган.

3-расм. *ЭТГ сериясидаги эндоскоп.*

Оптик канал орқали ахборотни тутиб олишда, мисол учун бинонинг юқори қаватларида жойлашган хоналардаги тасвирларни тўғридан-тўғри кўриш ёки кузатиш мумкин эмас. Бунинг учун албатта ушбу хонага қарама-қарши бинодан туриб, махсус оптик қурилма ёрдамидан фойдаланиш зарур бўлади. Бироқ, агар хона ойналари ахборот билан ишлаш жараёнида тўлиқ ёпилса, яъни махсус пардалар билан беркитилса, у ҳолда ахборот чиқиб кетиши учун визуал оптик каналнинг ўзи мавжуд бўлмайди. Бошқача айтганда, бундай хонада ахборотни оптик тутиб олиш канали ҳосил бўлмайди. Бунга қўшимча равишда хоналар ойнасини тонировка қилиш ёки уларга сиртига махсус ишлов берилган ойналар ўрнатиш ҳам мумкин.

Ахборотни чиқиб кетиш радиоэлектрон каналлари. Радиоэлектрон каналлар демаскировка белгиларига кўра ахборотни тутиб олишнинг асосий канали ҳисобланади.

Радиоэлектрон воситалар ва электр қурилмалари фаолият кўрсатиш жараёнида улар атрофида ёндош электромагнит майдон нурланиши юзага келиб, улар ҳимояланган ахборотни ўзида сақлаши мумкин. Аксарият ҳолларда статик ва динамик зарядларга эга бўлган электр токи занжирлари ана шундай нурланиш манбалари бўлади. Электр занжирида ахборотни бевосита қайта ишлаш жараёнида ахборотни ўзида акс эттирувчи ёндош нурланишлар вужудга келади.

Электромагнит майдоннинг нурланиш тури ва унинг тарқалиш хусусияти майдоннинг тебраниш частотаси ва нурлантиргич турига боғлиқ. Бунга асосланган ҳолда паст частотали ва юқори частотали хавфли нурланишлар фарқланади.

Товуш кучайтирувчи қурилмалар (микрофон, аудиомагнитофон, телефон аппарати, уларни боғловчи кабеллар ва шу кабилар)дан тарқалувчи товуш диапазонидаги нурланишлар паст частотали ҳисобланади.

Радиоэлектрон воситалар занжиридан нурланувчи, юқори частотали сигналлар тарқатувчи электромагнит майдонлар юқори частотали хавфли нурланишларга тааллуқли бўлиб, улар ўзида ҳимояланган ахборотни мужассамлайди. Аудио- ва видеомагнтофонларнинг ўчириш ва магнитлаш генераторлари, монитор ва телевизорларнинг электрон-нур трубкалари, компьютернинг юқори частотали сигналлар билан ишловчи элементлари кабилар бундай нурланишларни тарқатувчи қурилмаларга мисол бўлиши мумкин.

Реал ҳаётда электромагнит тўлқинларнинг тарқалишига тўсиқларнинг кўплиги сабабли уларнинг тарқалиш хусусияти жуда ҳам мураккаб ҳисобланиб, уларни аниқ бир математик ифодалашнинг имкони йўқ.

Радиосигналларни тутиб олиш воситалари. Электромагнит, электр, магнит майдонларни ҳамда ахборотга эга бўлган электр сигналларини тутиб олиш радио- ёки радиотехник разведка деб аталади. Унинг асосий босқичларига қуйидагиларни киритиш мумкин:

– муҳитда тарқалувчи сигналларни топиш;

– сигналларни кучайтириш;

– қабул қилинаётган сигналларни таҳлил қилиш ва улардан ахборотни ечиб олиш;

– сигнал манбаи жойлашган манзилни аниқлаш.

Радиосигналларни тутиб олишнинг намунавий комплексига қуйидагиларни киритиш мумкин:

– қабул қилувчи антенна;

– радиоприемник;

– сигналнинг техник хусусиятини таҳлил қилувчи қурилма – анализатор;

– радиопеленгатор;

– рўйхатга олувчи қурилма.

Радио- ёки радиотехник разведка воситаларига қуйидагилар киради:

– портатив сканерловчи приёмниклар (қабул қилувчи қурилмалар), спектрнинг рақамли анализаторлари, радиотестерлар ва бошқ.;

– радиотелефонлар ва уяли алоқа воситаларини назорат қилувчи махсус воситалар;

– сканерловчи приёмниклар асосида қурилган дастурий-аппарат комплекслар;

– портатив радиопеленгаторлар ва бошқалар.

Сканерловчи приёмниклар радиоразведкаларни ўтказишда кенг қўлланилиб, улар ўлчами ва вазнига кўра портатив (қўлда олиб юрувчи) ва ташиб юрилувчи турларига бўлинади. Портатив сканерловчи приёмникларнинг вазни 150-350 граммни ташкил этиб, улар автоном ток манбаига эга бўлади. Ўзининг ихчамлиги ва енгиллигига қарамай бундай приёмниклар 100-500 кГц дан 1300 МГц гача, айримлар ҳатто 2060 МГц («HSC-050») бўлган частота диапазонидаги разведкани олиб бориш имконини беради. Портатив сканерловчи приёмниклар 100 дан 1000 тагача хотира каналларига эга бўлиб, бир сонияда созлашнинг 50-500 Гц дан 50-1000 кГц гача частота қадамида 20 дан 30 тагача каналларни сканерлаш тезлигини таъминлайди. Бундай приёмникларнинг айримларини, масалан AR-2700, AR-8000, IC-R20, IC-R10 русумлиларини компьютер ёрдамида бошқариш мумкин. AR-8000 ва IC-R20 русумидаги портатив сканерловчи приёмникларнинг умумий кўринишлари 4-расмда келтирилган.

Icom фирмаси томонидан ишлаб чиқилган IC-R20 русумидаги портатив сканерловчи приёмниги ўзининг мукаммаллиги билан ажралиб туради. Ушбу приёмник сигналларни қабул қилишда юқори сифатни кафолатлаш билан бирга бир вақтнинг ўзида икки хил частотада кузатиш олиб бориш имконини беради. Унинг оғирлиги 320 граммни ташкил этади.

AR-8000 русумидаги портатив сканерловчи приёмник.

IC-R20 русумидаги портатив сканерловчи приёмник.

4-расм. *Портатив сканерловчи приёмниклар.*

Ташиб юрилувчи сканерловчи приёмниклар портатив сканерловчи приёмниклардан ўзларининг катта ҳажми ва оғирлиги билан фарқланади. Уларнинг оғирлиги 1,2 кг дан 6,8 кг гача бўлиши мумкин. Ҳажм ва массанинг ортиши билан приёмникларнинг функционал имкониятлари ҳам ортиб боради. Ташиб юрилувчи сканерловчи приёмникларнинг деярли барчаси компьютер ёрдамида бошқарилиши мумкин. AR-3000A русумли ташиб юрилувчи сканерловчи приёмникнинг умумий кўриниши 5-расмда келтирилган.

5-расм. *AR-3000A русумли ташиб юрилувчи сканерловчи приёмник.*

Ҳар икки турдаги сканерловчи приёмниклар қуйидаги режимлардан бирида ишлаши мумкин:

– берилган частота диапазонида автоматик сканерлаш режими;

– фиксирланган частота бўйича автоматик сканерлаш режими;

– қўлда бошқариш режими.

Радиотехник разведкаларда сканерловчи приёмниклар билан бир қаторда спектр анализаторларидан ҳам фойдаланиш мумкин.

Спектр анализаторлари жуда кенг частота диапазонидаги сигналларни қабул қилиш ва уларнинг тузилишини таҳлил қилиш имконини яратади. Портатив анализаторлар ўртача 9,5 дан 20 кг гача оғирликка эга бўлиши мумкин. Бундай қурилмаларнинг сигнал катталикларини ўлчаш аниқлиги жуда ҳам юқори бўлиб, сезгирлиги 125-145 Дб ни ташкил этади. Шу сабабли ҳам улар қимматбаҳо ҳисобланади. Tektronix фирмаси томонидан ишлаб чиқарилган RSA5103A русумли анализаторнинг умумий кўриниши 6-расмда келтирилган.

6-расм. *RSA5103A русумли спектр анализатори.*

2.3. Маълумотларни тутиб олиш воситалари

Акустик тебранишларнинг тебранувчи каналларда тарқалиш муҳити сифатида бинолар, деворлар, шифтлар, металл трубали конструкциялар ва бошқа қаттиқ буюмлар бўлиши мумкин. Бундай ахборотни тутиб олиш қурилмаси **стетоскоп**лар бўлиб, уларда узатувчи қурилма сифатида контактли микрофонлардан фойдаланилади. Электрон стетоскоплар ёрдамида ахборотни тутиб олиш учун ҳимояланган бинога рухсат керак эмас. Портатив стетоскопнинг кўриниши 7-расмда келтирилган.

7-расм. *Кичик ўлчамли контакт микрофонига эга бўлган PKI 2850 маркали электрон стетоскоп.*

PKI 2850 маркали стетоскоп портатив электрон стетоскопларнинг вакили ҳисобланади. Унинг кучайтиргич блоки ўлчамлари - 95x60x25 мм, микрофони – 50x35x15 мм ни ташкил этади. Бундай кичик ўлчамга эга бўлишига қарамай ушбу стетоскопнинг кучайтириш коэффициенти 80 дБ дан кам эмас. Ишлаш давомийлиги тўлиқ зараядланган аккумулятор билан 800 соатни ташкил этади.

Замонавий электрон стетоскоплар 80-100 дБ тартибидаги кучайтириш коэффициентига эга бўлиб, ҳатто шивирлаш ёки соат секундомерининг товуши каби кучсиз товуш тебранишларини ҳам тутиб олиш имкониятига эга. Бундай электрон стетоскопларни деворларга, эшик четидаги қобиқларга, хона шифтига, иситиш тизими ёки сув трубаларига, ҳаво совутгичлари қопламалари ичига жойлаштирилиши ва кучайтириш блоки билан махсус уланган кабель орқали уланади.

Ахборотларни электроакустик чиқиб кетиш каналлари электроакустик айлантиришлар, яъни акустик сигналларни электр сигналларига айлантириш жараёнида ҳосил бўлади. Бундай жараённи амалга оширувчи қурилмалар орасида бизга яхши танишлари булар - телефонлар, микрофонлар ва товушли алоқа тизимларидир.

Оптик-электрон каналда ахборотни тутиб олиш лазер орқали амалга оширилади ва шу сабабдан баъзида уни лазерли канал деб ҳам аталади. Товуш тўлқинлари таъсирида ойна ёки тошойна каби қайтарувчи сиртлар тебрана бошлайдилар. Агар уларга лазер нурини йўналтирилса, улар ойна сиртида модуляцияланади ва сиртдан қайтган нурлар оптик нурланишли қабул қилувчи қурилмага киради. Қабул қилувчи қурилмада ушбу сигнал демодуляцияланади ва кучайтирилади ҳамда ундан дастлабки акустик сигнални олиш мумкин бўлади.

Акустик разведка воситалари. Умумий ҳолда акустик разведка объектнинг ишлаб чиқариш шовқинларини ёки нутқли ахборотларни тутиб олиш билан амалга оширилади.

Фойдаланиш усулига кўра акустик ахборотларни тутиб олиш воситаларини икки тоифага бўлиш мумкин:

1. Ҳимояланган объектга физик жиҳатдан киритилиши талаб этилувчи воситалар:

– радиоўрнашмалар;

– ИҚ-диапазондаги акустик ахборотларни узатувчи ўрнашмалар;

– 220 вольтли тармоқ орқали узатувчи ўрнашмалар;

– телефон тармоқлари орқали ахборот узатувчи ўрнашмалар;

– диктофонлар;

– ўтказгичли микрофонлар;

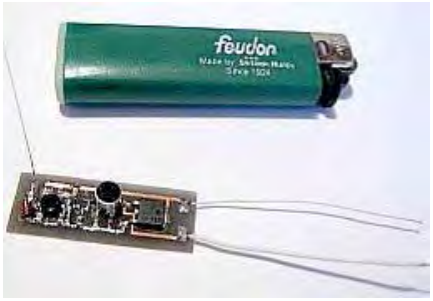
– «телефон қулоқ»лари.

2. Ҳимояланган объектга физик жиҳатдан киритилиши талаб этилмайдиган воситалар:

– «микрофон эффекти»дан фойдаланувчи қурилмалар;

– стетоскоплар;
– лазерли микрофонлар;
– йўналтирилган микрофонлар.

Радиоўрнашмалар. Бундай қурилмаларнинг вазифаси ҳимояланган объектдан акустик ахборотларни радиоканаллар орқали узатиб беришдир. Ўрнашмалар алоҳида модул сифатида турли кундалик маиший буюмлар (масалан зажигалка, калькулятор, авторучка ва бошқ.) кўринишида тайёрланиши мумкин. Радиоўрнашмаларнинг ташқи кўринишлари 8, 9, 10-расмларда келтирилган.



8-расм. *Зажигалка кўринишидаги радиоўрнашма.*

9-расм. *Танга кўринишидаги радиоўрнашма.*

10-расм. *Оддий кўринишдаги радиоўрнашма.*

Радиоўрнашмалар радиодиапазондаги электромагнит тўлқинлар ёрдамида ахборотларни узатади. Мазкур усулдан фойдаланишда албатта қабул қилувчи қурилма керак бўлади. Бундай қабул қилувчи қурилма сифатида оддий маиший буюмлар (плеер, мусиқа маркази, магнитофон кабилар)дан фойдаланиш мумкин. Фақатгина бу ерда радиоўрнашманинг қайси частотада ишлаётганини ҳисобга олиш

керак бўлади. Бу эса ғаразгўй кимсага қўл келиб, уни махсус қабул қилиш қурилмасини сотиб олишга мажбур қилмайди. Шунингдек, бу ҳолда ушбу сигнални бошқа кимсалар ҳам тутиб олиш эҳтимолини вужудга келтиради.

Акустик ахборотларни тутиб олиш техник воситаларига диктофонлар ҳам киради. Диктофон – товушли ахборотни тасмага, ички хотира микросхемасига қайд қилувчи қурилма. Турли диктофонларнинг ёзиб олиш вақти турлича бўлиб, у 15 минутдан 8 соатгача бўлиши мумкин.

Замонавий рақамли диктофонлар ахборотни ички хотирага бир неча соат мобайнида ёзиб олиш имкониятини беради. Бу диктофонлар деярли шовқинсиз бўлиб, ўз хотирасидаги маълумотларни компьютер хотирасига ўтказиш ва кейинчалик уни қайта ишлашга шароит яратади.

11-расм. *Edic-Mini Tiny B21 русумли мини-диктофон.*

Кўпчилик диктофонларнинг электр манбаси батарейкалар бўлиб, уларнинг оғирлиги ўнлаб ёки юзлаб граммларни ташкил этади. Шунинг учун замонавий диктофонлар жуда ҳам кичик ўлчамларга (11-расм) эга бўлиб, уларни ҳимояланган объектнинг ихтиёрий жойига ўрнатиш мумкин.

Бино ёки иншоатларни қуриш ёки таъмирлаш жараёнида уларга яширин равишда кичик ўлчамли микрофонларни ўрнатиб қўйиш мумкин. Микрофонлар симлар орқали сигнални қабул қилувчи қурилмага уланади ва улар манбадан 7-10 метр узоқликдаги нутқларнинг ўртача товушларини қайд қила олади. Бунда частота диапазони 20 – 100 Гц дан 6 – 20 кГц гачани ташкил этади. Бундай микрофонлар электр манбаининг доимий кучланиши 9-15 вольтга тенг. Одатда микрофон кучайтиргич билан таъминланади. Ахборотни узатиш ва

кучайтиргични электр манбаи билан таъминлаш учун 2 ёки 3 талик симлардан фойдаланилади.

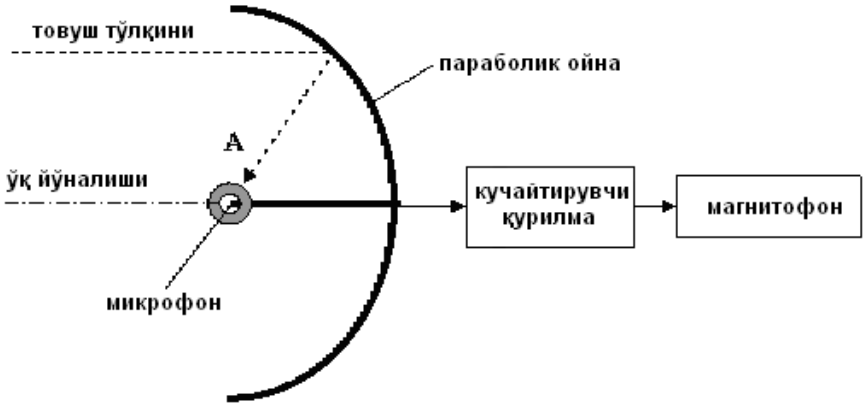
12-расм. *3 та симли Шорох-8 микрофони.*

Акустик ахборотларни телефон тармоғи орқали узатиш учун «телефон қулоқ» туридаги ўрнашмалардан фойдаланилади. Ушбу қурилма телефон корпусига ёки телефон розеткасига яширин равишда ўрнатилади (13-расм). У кучайтирувчи қурилма ва телефон линиясига уланиш имконини берувчи махсус қурилмага эга бўлган электрет (қутбланган диэлектрик) туридаги микрофондан иборат.

13-расм. *ТУ-2 русумли «Телефон қулоқ».*

Ҳимояланган объектга физик жиҳатдан киритилиши талаб этилмайдиган воситалар. Агар ҳимояланган бинода дераза ёки форточка очиқ бўлса, у ҳолда ундан акустик ахборотларни тутиб олишда йўналтирилган микрофонлардан фойдаланиш мумкин. Йўналтирилган микрофонлар қуйидаги турларга ажратилади: параболик, трубкали, ясси ва градиентли. Улар орасидан дастлабки учтаси кўпроқ қўлланилади.

Параболик микрофон марказида оддий микрофон жойлашган, парабола шаклидаги оптик жиҳатдан ялтироқ ёки ялтироқ бўлмаган материалдан иборат 20-30 см диаметрга эга бўлган товушни қайтарувчи мосламадан иборат (14-расм).



14-расм. *Параболик микрофон схемаси.*

Ўқ йўналишидаги товуш тўлқинлари параболик ойнадан қайтиб, А фокус нуқтасида фаза бўйича жамланади. Бу ерда товуш майдонининг кучайиши содир бўлади. Парабола ойнасининг диаметри қанча катта бўлса, қурилма товушни шунча катта кучайтириш имконини беради. Агар келаётган товуш тўлқинининг йўналиши ўқ йўналишига мос келмаса, у ҳолда А нуқтага йиғилаётган сигналлар йиғиндиси бир фазага жамланмайди ва оқибатда кучайтириш кам натижа беради. Келаётган товуш сигнали ва ўқ йўналиши орасидаги бурчак ортиб боргани сари кучайтириш тобора камайиб боради. Шундай қилиб қурилманинг бурчакли танлаш вазияти юзага келади. Параболик микрофонларнинг ташқи кўриниши 15-расмда келтирилган.

15-расм. *«Супер Ухо – 100» русумли параболик микрофон.*

Ясси микрофон тузилиши фазаланган акустик панжара шаклида бўлиб, унинг тугунларида микрофонлар жойлаштирилади. Улардан келаётган сигналлар жамланиб, кучайтирувчи қурилманинг киришига узатилади. Бундай қурилма келаётган товуш йўналишига перпенди-

куляр жойлаштирилган бирор текисликнинг аниқ бир нуқталарида товуш тўлқинини қабул қилиш ғоясига асосланган. Агар товуш тўлқини ўқ йўналишига мос равишда келса, яъни панжара сирти текислиги товуш йўналишига перпендикуляр жойлашса, қабул қилинаётган сигналларнинг фазалари мос келади ва товуш максимал даражада бўлади. Аксинча, панжара сирти текислиги товуш йўналишига перпендикуляр жойлашмаса, бунда турли микрофонларда қабул қилинаётган сигналлар фазаси орасида фарқ юзага келади. Шу сабабли, товуш йўналиши ва панжара сирти текислиги орасидаги бурчак қанчалик ортиб борса, сигналнинг кучайтирилиши шунчалик камайиб боради.

16-расм. *G.R.A.S. фирмасининг ясси микрофони.*

Акустик разведкалар учун мўлжалланган юқоридаги каби қурилмалардан фойдаланишда ғаразгўй кимсалардан алоҳида билим даражаси талаб этилади. Мини-диктофон ёки микрофонни ўрнатиб, ундан ёпиқ бино ичида фойдаланиш учун аввало, қурилмалар ишлашининг физик моҳиятини яхши билиш зарур. Акустик разведка учун у ёки бу воситани танлаш биринчи галда эгалланмоқчи бўлган ахборотнинг қийматига боғлиқ. Ҳар қандай ҳолатда ҳам ахборот хавфсизлиги бўйича мутахассис ахборот ҳимоя объектларини жойлашиши ва фаолиятини самарали ташкил этиши учун ахборотни ноқонуний эгаллаб олишнинг қандай таҳдидлари мавжудлигини билиши лозим.

Назорат учун саволлар

– Ахборотларни муҳофаза қилишнинг техник воситалари тушунчаси нимани англатади?

– Маскировкаловчи белгиларнинг очилиши тушунчасини нимани билдиради?

– Демаскировка белгилари нималар билан фарқ қилади?

– Техник воситалар билан ҳимояланадиган маълумотларнинг манбалари ва ташувчилари нималардан иборат?

– Нималар маълумот ташувчи воситалар ҳисобланади?

– Маълумотлар чиқиш канали деб нимага айтилади?

– Маълумотлар чиқиб кетиш каналининг пайдо бўлиш сабаблари ва шароитлари нималардан иборат?

– Техник канал бўйича маълумотлар чиқиб кетишидан ҳимоялашда қандай амаллар бажарилиши талаб этилади?

– Тутиб олишдан ҳимоялашнинг қандай усуллар мавжуд?

– Акустик разведкалар учун қандай қурилмалар мавжуд?

III. АХБОРОТЛАРНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

3.1. Криптография ва унинг асосий тушунчалари

Инсоният тараққиётида ёзув пайдо бўлган даврдан бошлаб ахборотни ҳимоя қилиш муаммоси ҳам юзага кела бошлади. Бу муаммо ҳарбий ва дипломатик маълумотларни яширинча узатиш заруратидан келиб чиққан. Масалан, антик спарталиклар ҳарбий ҳаракатлар вақтида маълумотларни шифрлаш усулларидан фойдаланганлар. Хитойликлар томонидан эса оддий ёзувни иерогрифлар кўринишида тасвирлаш усули қўлланилиб, бу уларга маълумотларни рақиблардан яшириш имконини берган.

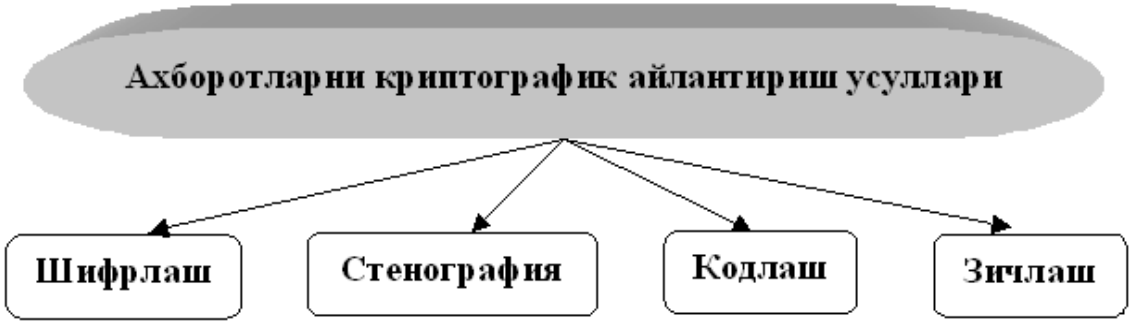
Криптография қадимий юнон тилида «яширин ёзаман» деган маънони англатиб, ахборотнинг конфиденциаллигини ва аутентлигини таъминлаш усуллари ҳақидаги фандир. Криптография маълумотни, ғаразгўй кимсалар томонидан эгалланган тақдирда, бефойда кўринишга айлантириб берувчи усуллар тўпламини ташкил этади. Бундай усуллар ахборот хавфсизлигига тааллуқли иккита асосий масалани ечишга имкон беради. Булар:

– конфиденциаллик ҳимояси;

– бутунлик ҳимояси.

Ахборотнинг конфиденциаллиги ва бутунлиги ҳимояси муаммолари бир-бири билан узвий боғлиқ бўлиб, уларнинг бирини ечими иккинчиси билан боғлиқ бўлади.

Ахборотларни криптографик айлантириш усулларини тоифалашга турлича ёндашишлар мавжуд. Дастлабки маълумотларга таъсир этиш кўринишига кўра криптографик айлантириш усулларини 4 та гуруҳга бўлиш мумкин.



Шифрлаш жараёни дастлабки ахборотни қайта тиклаш имкони билан математик, мантиқий, комбинацион ва бошқача айлантиришларни амалга оширишни ўз ичига олади. Бунинг натижасида шифрланган ахборот ҳарфлар, рақамлар, бошқа символлар ва иккилик кодларининг хаотик тўпламидан иборат бўлади.

Ахборотни шифрлаш учун айлантириш алгоритми ва калитдан фойдаланилади. Одатда бирор шифрлаш усули учун алгоритм ўзгармас бўлади. Шифрлаш алгоритми учун дастлабки маълумотлар – бу шифрланувчи ахборот ва шифрлаш калити ҳисобланади. Калит бошқарувчи ахборотни ўзида сақлайди. Бундай ахборот алгоритмнинг муайян қадамларида қандай айлантириш танлашнишини ва шифрлашда ишлатиладиган операндлар катталикларини аниқлайди. Операнд – бу устида амал бажарилаётган дастурлаш тилининг константаси, ўзгарувчиси, функцияси, ифодаси ва бошқа объектидир.

Ахборотни криптографик айлантиришнинг бошқача усулларидан фарқли равишда **стенография** усуллари сақланувчи ёки узатилувчи ахборотнинг нафақат маъносини, балки ёпиқ ахборотнинг сақланиши ва узатилишини ҳам яшириш имконини беради. Стенография усуллари асосида ёпиқ ахборотни очиқ файллар орасида ниқоблаш (маскировкалаш) ётади.

График ва товушли ахборотлар рақамли кўринишда ифодаланади. График объектларнинг энг кичик тасвир элементи бир байт билан кодланиши мумкин. Тасвирнинг кичик разрядли аниқ байтларига криптографик айлантириш алгоритмига мос равишда яшириш файлнинг битлари жойлаштирилади. Агар айлантириш алгоритми ва тасвир тўғри танланса, дастлабки тасвир ҳамда фонида яширинган файл жойлашган, ҳосил қилинган тасвир орасидаги фарқни инсон кўзи билан ажратиб бўлмайди. Стенография воситалари ёрдамида матнларни, тасвирларни, рақамли имзоларни, шифрланган хабар-ларни ниқоблаш мумкин.

Яширинган файл ҳам шифрланиши мумкин. Агар бегона шахс яширин файлни тасодифан топиб олса, у ҳолда шифрланган ахборот тизим фаолиятидаги хатолик сифатида қабул қилинади. Стенография ва шифрлашдан умумий ҳолда фойдаланиш, конфиденциал ахборотни топиш ва уни очиш вазифаси мураккаблигини кўп карра ошириб юборади.

Ахборотларни **кодлаш** жараёни маълумот (сўз, гап)нинг дастлабки маъносини кодлар билан алмаштиришдан иборат. Бунда кодлар

сифатида ҳарфлар, рақамлар, белгилар мослигидан фойдаланиш мумкин. Маълумотларни кодлаш ва уларни қайта тиклашда махсус жадваллар ёки луғатлардан фойдаланилади. Ахборот тармоқларида маълумотни (ёки сигнални) дастурий-аппарат воситалар ёрдамида кодлаш узатилаётган ахборотнинг ишончлилигини ошириш учун қўлланилади.

Аксарият ҳолларда кодлаш ва шифрлашни бир-бири билан алмаштириб юборишади. Кодланган ахборотни қайта тиклаш учун алмаштириш қоидасини билиш етарли. Бироқ шифрланган ахборотни ширфдан очиш учун эса шифрлаш қоидасидан ташқари шифрлаш калитини ҳам билиш талаб этилади.

Ахборотни **зичлаш** усулини криптографик айлантириш усулларига маълум бир четланишлар билан киритиш мумкин. Чунки, ахборотни зичлашдан мақсад маълумотнинг ҳажмини қисқартиришдир. Зичлаш воситаларига эгалик қилиш имконияти кенглиги ва уларни қайта тиклаш осонлигини инобатга олган ҳолда, бу усулга ахборотни ишончли криптографик айлантириш воситаси сифатида қараб бўлмайди. Ҳатто зичлаш алгоритми махфий сақланган ҳолда ҳам уларни статистик усуллар билан нисбатан енгил очиш мумкин. Шунинг учун конфиденциал ахборотларнинг зичланган файллари кейинчалик шифрланиши лозим. Маълумотларни узатиш вақтини камайтириш учун зичлаш ва шифрлаш жараёнларини бирлаштириш мақсадга мувофиқ.

Криптотаҳлил – бу калитни билмай туриб, шунингдек, шифрлаш алгоритми ҳақида маълумотлар йўқ бўлган ҳолда ёпиқ ахборотни шифрдан очиш жараёнидир.

Шифрнинг криптомустаҳкамлиги – самарадорликнинг асосий кўрсаткичи бўлиб, у вақт билан ёки криптотаҳлилчининг калит маълум бўлмаган ҳолда шифрматндан дастлабки маълумотни чиқариб олиши учун керак бўладиган воситалар нархи билан ўлчанади.

Кенг қўлланилувчи шифрлаш алгоритмларини махфий сақлаш мумкин эмас. Шунинг учун шифрлаш алгоритмини яшириш зарурати йўқ. У ҳолда шифрлашнинг криптомустаҳкамлиги калит узунлиги билан белгиланади. Чунки, ёпиқ ахборотни шифрдан очиш учун йўл фақатгина калитни тўғри танлашдир. Демак, криптотаҳлилга кетадиган харажат, яъни вақт ва маблағ калитнинг узунлиги ва шифрлаш алгоритми мураккаблигига боғлиқ бўлади.

3.2. Ахборотларни криптографик ҳимоялаш усуллари

Ахборотларни криптографик ҳимоялаш усуллари ахборот хавфсизлиги учун курашда самарали восита бўлиб, бугунги кунда улар ахборот тизимларида кенг қўлланилмоқда.

Криптография усуллари – ахборотнинг конфиденциаллиги ва бутунлигини таъминлашнинг кучли қуролларидан бири ҳисобланади. Криптографиянинг асосий элементи – бу шифрлашдир. Таъкидлаш жоизки, шифрлаш усулининг вужудга келиши жуда ҳам қадимий тарихга эга.

Қадимий юнон саркардаси Ю. Цезарь галлар билан уруш вақтида (эрамизнинг 56 йили) шифрлаш усулларидан бири бўлган алмаштириш шифрини қўллаган. Очиқ матн алифбоси остига маълум бир цикл бўйича (Цезарда учта тартибга) силжитиш орқали янги алифбо ёзилган. Шифрлашда очиқ матндаги алифболар, яъни юқори қисмда жойлашган ҳарфлар қуйи қисмдаги мос ҳарфлар билан алмаштирилган. Бу турдаги шифрлаш Ю.Цезаргача маълум бўлган бўлса-да, лекин бундай шифрлаш усули унинг номи билан юритилади.

Мураккаб алмаштиришлар шифри сифатида юнонлар шифри – «Полибий квадрати» саналади. Алифбо квадрат жадвал кўринишида тасвирланади. Шифрлашда очиқ матн ҳарфи жадвалдаги иккита сонга алмаштирилган, яъни жадвал бўйича керакли ҳарфнинг жойлашган устун ва қатор рақамларига. Алифбони жадвалда ихтиёрий тарзда жойлаштириш ва у орқали қисқа хабарни шифрлаш замонавий қарашлар нуқтаи назари бўйича ҳам мустаҳкам шифрлаш ҳисобланади. Бу ғоя биринчи жаҳон урушида махфий маълумотларни шифрлашда амалда қўлланилган.

Германиялик Иоганн Тритемий (1462–1516 йй) криптография бўйича биринчи дарсликлардан бирини ёзган. «Ave Maria» деб номланган кўп қийматли алмаштиришли оригинал шифрлашни таклиф этган. Очиқ матннинг ҳар бир ҳарфи шифрловчининг танлови бўйича бир эмас, балки бир нечта ҳарфларга алмаштирилиши мумкин бўлган. Бунда ҳарфлар ҳарф ёки сўзлар билан шундай алмаштирилганки, натижада псевдоматн ҳосил бўлган. Кўп қийматли алмаштириш усулидан ҳозирги кунда ҳам фойдаланилади (масалан, ARJ архиваторида).

XVI асрга келиб алмаштириш шифрлари математик Джованни Батиста Порт ва дипломат Блеза де Вижинер ишларида ўз ривожини

топди. Вижинер тизими у ёки бу кўринишда ҳозирги пайтда ҳам қўлланилмоқда.

Лорд Френсис Бэкон (1562-1626 й) биринчи бўлиб ҳарфларни 5 қийматли иккилик код билан белгилаган: A= 00001, B =00010,... ва ҳоказо. Бэкон бу кодларга қайта ишлов бермаган, шунинг учун бундай яшириш усули мустаҳкам бўлмаган. Уч асрдан сўнг, бу кодлаш тамойили электр ва электрон алоқада асос қилиб олинди. Бунда Морзе ва Бодо кодларини, 2-сонли халқаро телеграф кодини, ASCII кодини, эслаш ҳам ўринли, чунки улар ҳам оддий алмаштириш асосида яратилган.

Бугунги кунда ахборот тизимларида хавфсизликни таъминлаш борасида юқори криптомустаҳкамликка эга бўлган криптотизимлар қўлланилмоқда. Маълумотларни криптографик ўзгартиришнинг янги усуллари интенсив равишда такомиллашиб бормоқда ва уларнинг қўлланиш доираси тобора кенгаймоқда.

Замонавий шифрлаш усуллари қуйидаги талабларга жавоб бериши лозим:

– шифрнинг мустаҳкамлиги криптотаҳлилга шундай қарши тура олиши керакки, бунда шифрдан очиш фақатгина калитларни тўлиқ топиш орқали амалга оширилиши мумкин бўлсин;

– криптомустаҳкамлик шифрлаш алгоритмининг махфийлиги билан эмас, балки, калитнинг махфийлиги билан таъминланиши лозим.

– шифрматн ҳажм жиҳатидан дастлабки ахборотдан сезиларли даражада юқори бўлиб кетмаслиги керак;

– шифрлаш жараёнида юзага келадиган хатолар ахборот бузилиши ва йўқотилишига олиб келмаслиги керак;

– шифрлаш вақти катта бўлмаслиги керак;

– шифрлаш нархи шифрланаётган ахборот қиймати билан мос келиши керак.

Очиқ ва ёпиқ калитлар билан шифрлаш тизими.

Калитдан фойдаланиб шифрлаш алгоритмининг икки хил кўриниши мавжуд: *симметрик* ва *асимметрик (очиқ калитли)*.

Маълумотларни шифрлаш учун фойдаланилган калит шифрни очиш калитидан олинган ёки аксинча бўлса, бундай криптографик алгоритмлар симметрик деб номланади. Кўпгина симметрик алгоритмларда ягона калитдан фойдаланилади. Бундай алгоритмлар *бир калитли* ёки махфий калитли алгоритмлар деб аталади ҳамда хабарни

юборувчи ва уни қабул қилувчи қандай калитдан фойдаланишни келишиб олишларини талаб этади. Бир калитли алгоритмларнинг ишончлилиги калитни танлаш билан аниқланади. Агар ғаразгўй кимсага калит маълум бўлса, у ҳеч қандай қийинчиликларсиз барча тутиб олинган маълумотларни шифрдан очиш имконияти эга бўлади. Демак, бундай шифрлаш усулида танланган калитни бегоналардан сир сақлаш муҳим аҳамиятга эга.

Шифрлашнинг симметрик алгоритмлари икки турда бўлади. Улардан бири очиқ матнга битлар бўйича ишлов беради. Улар *потокли алгоритмлар* ёки *потокли шифрлар* деб номланади. Иккинчисида эса, очиқ матн бир неча битдан иборат бўлган блокларга бўлинади. Бундай алгоритмлар *блокли алгоритмлар* ёки *блокли шифрлар* деб номланади. Блокли шифрлашнинг замонавий алгоритмларида, одатда, блок узунлиги 64 битни ташкил этади.

Симметрияли тизимларда куйидаги иккита муаммо мавжуд:

1) Ахборот алмашишда иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари;

2) Жўнатилган хабарнинг ҳақиқийлигини аниқлаш.

Электрон рақамли имзо ва очиқ калитлар структураси. Электрон рақамли имзони қўллашдан мақсад, аввало, электрон ҳужжатдаги ахборот асл нусха эканлигини тасдиқлаш, шунингдек учинчи тарафга (арбитрга, судга ва бошқаларга) ҳужжатнинг муаллифи ушбу шахс эканлигини исботлаш. Ушбу мақсадга эришиш учун муаллиф ўзининг махфий индивидуал рақами (индивидуал калит, пароль) билан ҳужжатга ўрнатилган тартибда «электрон имзо қўйиш» жараёнини бажариши лозим. Бундай имзо қўйишда, ҳар гал индивидуал калит электрон ҳужжатдаги маълумотлар билан маълум қоидага мувофиқ аралашиб кетади. Бундай бириктирилиш натижасида ҳосил бўлган рақам (маълум разряд узунлигидаги рақамлар кетма-кетлиги) ушбу ҳужжатга муаллиф томонидан қўйилган электрон рақамли имзо ҳисобланади. Шундай қилиб, электрон рақамли имзо қўйиш ва уни текшириш процедурасининг ҳар бирида ишлатиладиган иккита калитдан биттаси фойдаланилади. Лекин бунда имзо қўйиш калитини текшириш калити ёрдамида аниқлаш имконияти умуман мумкин эмаслиги кафолатланган бўлиши керак. Ҳозирда таклиф этилган усулларда, амалда имзо қўйиш калитини (ёпиқ калит), текширув калити ёрдамида (очиқ калит) қайта тиклаш учун узоқ давом этадиган мураккаб ҳисоблаш ишларини бажариш лозимлиги назарда тутилади.

Электрон имзо ғояси биринчи марта Диффи ва Хеллман асарида ҳужжатнинг асл нусха эканлигини ва муаллиф томонидан имзолан-ганлигини аниқлаш учун таклиф этилган.

Ҳозирги вақтда ахборот тизимларида электрон рақамли имзо кенг қўлланилмоқда (узатиладиган ёки сақланадиган шифрланган матнга бириктирилган рақам, ушбу ахборотнинг бутунлигини ва муаллифнинг ҳақиқийлигини текшириш имкониятини кафолатлайди).

3.3. Шифрловчи дастурлар ва уларнинг имкониятлари

Бугунги кунда маълумотларни шифрловчи кўплаб дастурлар ишлаб чиқилган. Улар орасида **TrueCrypt** дастури ўз афзалликлари ва юқори имконияти туфайли кенг оммалашган.

Мазкур дастурнинг ўзига хос жиҳати мавжуд бўлиб, унинг воси-тасида компьютернинг доимий хотирасида маълум бир соҳа ажратиб олинади ва шифрланган маълумотлар ана шу соҳада сақланади. Ушбу соҳани ҳосил қилиш жараёни бир неча босқичлардан иборат бўлади.

Шифрловчи дастурларнинг яна бир вакили **AxCrypt** дастури фойдаланиш учун қулай бўлиб, унда ортиқча созлаш ишларини амалга ошириш талаб этилмайди. Дастур компьютерга ўрнатилганда, у *Проводник*нинг контекстли менюсига, яъни сичқончанинг ўнг тугмаси босилганда ҳосил бўлувчи менюга жойлашади. Ушбу дастур ёрдамида шифрланаётган ёки шифрдан чиқарилаётган файл ёки папка белгиланади ва контекстли менюдаги **AxCrypt** дастурида керакли амал танланади.

AxCrypt дастури қуйидаги имкониятларга эга:

– **AES-128** ва **SHA-1** шифрлаш алгоритмидан фойдаланиб, маъ-лумотнинг асл нусхаси ўрнига ёки алоҳида янги шифрланган файлни ҳосил қилиш;

– дастур орқали ҳосил қилинган калитли файл ёрдамида ҳимоя қилиш;

_ ўзи очилувчи (**.exe** кенгайтмали) шифрланган файлни яратиш. Бундай ҳолатда шифрланган маълумотни очиш учун **AxCrypt** дасту-ри зарур бўлмайди. Фойдаланувчи паролни билиши, агар зарурият бўлса, калитли файлга эга бўлиши керак;

– шифрланган файлни шифрдан чиқармасдан, пароль (калитли файл) орқали ишга тушириш. Бу ҳолда файлнинг асл нусхаси ахборот ташувчида ҳосил бўлмайди;

– папкалар ичидагиларни пакетли шифрлаш;

– ўчирилган маълумотларни тиклашдан ҳимоялаш. Ўчирилган файллар эгаллаган жойга тасодифий сонлар ёзилади.

Маълумки, ҳар қандай ёзма ҳужжатни тайёрлашда муаллиф унинг ҳақиқатан ҳам асл нусха эканлигини исботловчи шахсий имзосини қўяди. Бу ҳолат бугунги кунда электрон ҳужжатларни тайёрлаш ва уларни алмашишда ҳам ўз аксини топмоқда. Электрон ҳужжат билан иш юритишда маълумотни қабул қилувчи ўзига аввал берилган имзони олинган маълумотдаги имзога солиштириб, унинг ҳақиқийлигини текшириб олиши мумкин. Шунингдек, имзо маълумот ҳужжатига юридик жиҳатдан муаллифликни кафолатлайди. Бундай кафолат эса барча соҳаларда, жумладан, банк ва савдода алоҳида аҳамиятга эга.

Электрон ҳужжат. Электрон ҳужжатга Ўзбекистон Республикасининг «Электрон ҳужжат айланиши тўғрисида» 2004 йил 29 апрелдаги 611-II-сон қонунида[1] қуйидагича таъриф берилган: «Электрон шаклда қайд этилган, электрон рақамли имзо билан тасдиқланган ва электрон ҳужжатнинг уни идентификация қилиш имкониятини берадиган бошқа реквизитларига эга бўлган ахборот электрон ҳужжатдир».

Электрон ҳужжат техника воситаларидан ва ахборот тизимлари хизматларидан ҳамда ахборот технологияларидан фойдаланилган ҳолда яратилади, ишлов берилади ва сақланади.

Электрон ҳужжатнинг мажбурий реквизитлари қуйидагилардан иборат:

– электрон рақамли имзо;

– электрон ҳужжатни жўнатувчи юридик шахснинг номи ёки электрон ҳужжатни жўнатувчи жисмоний шахснинг фамилияси, исми, отасининг исми;

– электрон ҳужжатни жўнатувчининг почта ва электрон манзили;

– ҳужжат яратилган сана.

Қонун ҳужжатларида ёки электрон ҳужжат айланиши иштирокчиларининг келишуви билан электрон ҳужжатнинг бошқа реквизитлари ҳам белгиланиши мумкин.

Электрон ҳужжат қоғоз ҳужжатга тенглаштирилади ва у билан тенг юридик кучга эга бўлади.

---

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2004. – № 20. – 230-м.

Электрон ҳужжат алмашиш. Бунда ҳужжат электрон кўринишда компьютер, телекоммуникация ва Интернет тармоғи орқали узатилади. Электрон ҳужжатларни алмашиш жараёнида махсус ихтисослаштирилган тизимлардан (масалан, E-hujjat) ёки электрон почта хизматидан фойдаланилади.

Электрон ҳужжат алмашиш тизимлари – электрон ҳужжатларни ахборот тизимлари орқали жўнатиш ва қабул қилиш жараёнлари йиғиндисидир. Электрон ҳужжат айланишидан битимлар (шу жумладан, шартномалар) тузиш, ҳисоб-китобларни, расмий ва норасмий ёзишмаларни амалга ошириш ҳамда бошқа ахборотларни алмашишда фойдаланиш мумкин.

Электрон рақамли имзо. Электрон рақамли имзо (ЭРИ) Ўзбекистон Республикасининг «Электрон рақамли имзо тўғрисида» 2003 йил 11 декабрдаги 562-II-сон қонунига[1] биноан қуйидагича таърифланади: «Электрон рақамли имзо — электрон ҳужжатдаги мазкур электрон ҳужжат ахборотини электрон рақамли имзонинг ёпиқ калитидан фойдаланган ҳолда махсус ўзгартириш натижасида ҳосил қилинган ҳамда электрон рақамли имзонинг очиқ калити ёрдамида электрон ҳужжатдаги ахборотда хатолик йўқлигини аниқлаш ва электрон рақамли имзо ёпиқ калитининг эгасини идентификация қилиш имкониятини берадиган имзо».

Қонунда талаб этилган шартларга риоя этилган тақдирда, электрон рақамли имзо қоғоз ҳужжатга шахсан қўйилган имзо билан бир хил аҳамият, кучга эгадир. ЭРИ манба ва маълумотлар бутлигини текшириш ҳамда сохталаштиришдан муҳофазалаш имконини беради. ЭРИ калитлари сертификатлари рўйхатга олиш марказлари томонидан берилади.

Электрон калитлар ва сертификатлар. Ўзбекистон Республикасининг «Электрон рақамли имзо тўғрисида»ги қонунида қуйидаги асосий тушунчаларнинг таърифлари келтирилган:

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

[1] Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2004. – № 1–2. – 12-м.

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

электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш — электрон рақамли имзонинг электрон рақамли имзо ёпиқ калитининг эгасига тегишлилиги ва электрон ҳужжатдаги ахборотда хатолик йўқлиги текширилгандаги ижобий натижа».

ЭРИ калитининг сертификати ЭРИнинг очиқ калити унинг ёпиқ калитига мослигини тасдиқлайдиган ва ёпиқ калитнинг эгасига рўйхатга олиш маркази томонидан берилган ҳужжатдан иборат бўлади. Бу сертификат электрон ҳужжат ва қоғоз ҳужжат шаклларида тайёрланиши мумкин.

ЭРИ калитлари сертификати, унинг очиқ ва ёпиқ калитлари билан ишлаш, файл ва папкаларга ЭРИ қўйиш ёки уларни шифрлаш, ЭРИни текшириш, шифрланган маълумотларни очиш каби амалларни бажаришда кўпгина махсус дастурлар, жумладан, «**КриптоАРМ**» ва «**PGP**» дастурларидан фойдаланиш мумкин.

КриптоАРМ дастури ихтиёрий кўринишдаги электрон ҳужжат айланишида ахборотни ҳимоя қилиш вазифаларини ҳал этиш учун мўлжалланган. Ушбу дастур фойдаланувчи учун қулай график интерфейсга эга бўлиб, криптографик амалларни бажариш, маълумотларни шифрлаш ва шифрдан очиш, маълумотларни имзолаш ва ЭРИнинг тўғрилигини текшириш имконини беради. Дастур ёрдамида оддий сертификатлар билан ишлашга оид масалаларни ҳам бажариш мумкин.

PGP (Pretty Good Privacy) дастури Ф. Циммерман томонидан яратилган бўлиб, у маълумотларни шифрлаш ва уларга ЭРИ қўйишга мўлжалланган. Ушбу дастур ёрдамида электрон ҳужжатларни ишончли ҳимоя қилиш мумкин. Дастур очиқ калит орқали шифрлашни амалга оширади. Ҳар бир фойдаланувчининг иккита: очиқ ва ёпиқ калитлари бўлади. Очиқ калит барчага эълон қилинади. Ёпиқ калит эса фақат сертификат эгасида бўлиб, уни махфий сақлаш керак.

Мисол учун, **X** фойдаланувчи **Y** фойдаланувчига хабарни шифрлаб юбормоқчи бўлса, у **Y** фойдаланувчининг очиқ калитидан фойдаланиб, хабарни шифрлайди. **Y** фойдаланувчи эса, ўзининг ёпиқ калити билан хабарни шифрдан чиқаради.

Назорат учун саволлар

- Криптография нима?
- Криптография ривожланишининг қандай босқичлари мавжуд?
- Замонавий криптография қанақа муаммоларни ҳал этувчи билим соҳаси ҳисобланади?
- Ахборотларни содда шифрлашни қандай усуллари бор?
- Цезарнинг шифрлаш усули қандай амалга оширилади?
- Калит деганда нима тушунилади?
- Симметрик шифрлаш қандай амалга оширилади?
- Симметрик ва асимметрик калит ёрдамида шифрлаш қандай амалга оширилади?
- Рақамли сертификатлар нима?
- Шифрлашга қанақа талаблар қўйилади?
- Қайси шифрлаш алгоритмлари кенг тарқалган?
- Электрон рақамли имзо нима мақсадда ишлатилади?

IV. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АППАРАТ-ДАСТУРИЙ ВОСИТАЛАРИ

4.1. Ахборотни муҳофаза қилишнинг асосий ва ёрдамчи аппарат-дастурий воситалари

Ахборотни муҳофаза қилишнинг аппарат-дастурий воситалари – бу ахборотни муҳофаза қилиш функциялари (фойдаланувчиларни идентификация ва аутентификация қилиш, ресурслардан фойдаланишни чеклаш, воқеаларни қайд қилиш, ахборотни криптографик беркитиш ва бошқалар)ни мустақил ёки бошқа воситалар билан биргаликда бажарадиган турли электрон қурилмалар ва махсус дастурлардир.

Ахборотни муҳофаза қилишнинг *аппарат воситаси* – бу махсус ҳимоя қурилмаси ёки ахборотни қайта ишлаш техник воситасининг таркибига кирувчи мослама.

Ахборотларни муҳофаза қилишнинг асосий аппарат воситаларига қуйидагиларни киритиш мумкин:

– фойдаланувчини идентификацияловчи маълумотларни киритиш қурилмалари (магнит ва пластик карталар, бармоқ излари ва бошқалар);

– маълумотларни шифрловчи қурилмалар;

– иш станциялари ва серверларга ноқонуний уланиб олишга ҳалақит берувчи қурилмалар (электрон қулфлар ва блокираторлар).

Маълумотларни муҳофаза қилишнинг ёрдамчи аппарат воситаларига қуйидагилар мисол бўла олади:

– магнитли ташувчилардаги маълумотларни йўқ қилувчи қурилмалар;

– компьютер воситаларидан фойдаланувчиларининг ноқонуний ҳаракатлари бўйича хабардор қилувчи (сигнализация берувчи) қурилмалар ва бошқалар.

Ахборотларни муҳофаза қилишнинг *дастурий воситалари* – бу ахборот хавфсизлигини таъминлашга мўлжалланган ва компьютер воситаларининг дастурий таъминоти таркибига киритилган махсус дастурлардир.

Ахборотларни муҳофаза қилишнинг дастурий воситалари ахборотлар хавфсизлигини таъминлашга мўлжалланган ва компьютер воситаларининг дастурий таъминоти таркибига киритилган махсус дастурлардан иборат.

Ахборотларни муҳофаза қилишнинг асосий дастурий воситаларига қуйидагиларни киритиш мумкин:

– компьютер тизимларида фойдаланувчиларни идентификацияловчи ва аутентификацияловчи дастурлар;

– компьютер тизимлари ресурсларидан фойдаланувчиларнинг ҳуқуқларини чекловчи дастурлар;

– ахборотларни шифрловчи дастурлар;

– ахборот ресурсларини (тизимли ва амалий дастурий таъминотни, маълумотлар базаларини, таълимнинг компьютер тизимларини ва ҳ.к.) ноқонуний ўзгартиришлардан, фойдаланишлардан ва кўпайтиришлардан ҳимояловчи дастурлар.

Компьютер вирусларидан ва бошқа зарарловчи дастурлар таъсиридан ҳимояланиш компьютер тизимларида ахборотларни қайта ишлаш жараёнини ҳимоялашнинг мустақил йўналишларидан бири ҳисобланади. Ушбу хавфга етарлича баҳо бермаслик ахборот тизимларида фойдаланувчиларнинг ахборотлари учун жиддий салбий оқибатларни келтириб чиқариши мумкин.

Юқорида таъкидланганидек, ахборот ҳимоя тизими – бу чора-тадбирлар комплекси бўлиб, улар мос равишда воситалар ва усуллар мажмуини ташкил этади. Ахборот хавфсизлиги тизимининг аппарат - дастурий ташкил этувчиси (компонети) турли ахборот тизимларининг компьютер ва локал тармоқ серверларида сақланувчи ва қайта ишланувчи маълумотларни ҳимоя қилиш учун мўлжалланган. Одатда у қуйидаги жараёнлар билан узвий боғлиқликда амалга оширилади:

– рухсат этишни ҳамда рухсат этиш сиёсатини бошқариш;

– фойдаланувчиларни идентификация ва аутентификация қилиш;

– ҳодисаларни рўйхатга олиши ва аудит қилиш;

– криптографик ҳимоя;

– тармоқ ҳимояси;

– вирусга қарши ҳимоя;

– дастурий воситалар орқали ҳужумларни аниқлаш.

Рухсат этишни бошқариш воситалари фойдаланувчилар томонидан ахборот устида амалга ошириладиган ҳаракатларни чегаралаш ва

назорат қилиш имконини беради. Буларга тизимга кириш учун рухсатни чегаралаш, муаллифланган фойдаланувчи рухсатини чегаралаш кабиларни киритиш мумкин. Ушбу жараёнда рухсат этишни бошқариш дастурий воситалар орқали амалга оширилади. Рухсат этиш ҳуқуқларини назорат қилиш дастур муҳитининг турли ташкил этувчилари – тармоқ операцион тизимининг ядроси, маълумотлар базасини бошқариш тизими, қўшимча дастурий таъминот ва бошқалар томонидан амалга оширилади.

Идентификация фойдаланувчининг ўз номини хабар юбориш орқали ўзини идентификация қилишига имкон яратиш учун мўлжалланган. Аутентификация ёрдамида эса иккинчи томон тизимга киришга ҳаракат қилаётган фойдаланувчининг ҳақиқатан ҳам ўзи эканлигига ишонч ҳосил қилади.

Ҳодисаларни рўйхатга олиш (протоколлаштириш, журналлаштириш) – бу тизимда рўй бераётган ҳодисалар ҳақида ахборотларни йиғиш ва жамлаш жараёнидир. Ҳодисаларни икки гуруҳга бўлиш мумкин:

1. Ташқи ҳодисалар: муаллифланган ва муаллифланмаган фойдаланувчилар ҳаракатлари орқали юзага келувчи;

2. Ички ҳодисалар: фойдаланувчилар ва администраторлар ҳаракатлари орқали юзага келувчи.

Аудит – бу ҳодисаларни журналлаштириш натижасида жамланган ахборотларни таҳлил қилиш жараёнидир. Бундай таҳлил реал вақтда ёки даврий тарзда тезкор амалга оширилиши мумкин.

Тармоқ ҳимояси одатда, тармоқ чегараларига экран деб номланувчи қурилмаларни ўрнатиш орқали амалга оширилади. Экран бир тармоқдаги фойдаланувчиларга бошқа тармоққа тегишли ресурслардан фойдаланиш учун рухсатни чегаралаш воситаси ҳисобланади. Икки тизим орасидаги барча ахборот оқимини назорат қилиш экраннинг вазифасига киради. Бунга мисол тариқасида тармоқ экранини келтириш мумкин. У бирор ташкилотга тегишли, интернетга чиқиш имконига эга бўлган локал тармоқни ҳимоя қилиш учун ўрнатилади.

Бугунги кунда ахборот хавфсизлигини таъминловчи аппарат-дастурий воситаларни ишлаб чиқарувчиларнинг деярли барчаси вирусга қарши ҳимояни ҳамда зарарлантирувчи дастурий воситалар ҳужумини аниқловчи ва улардан ҳимояловчи тизимларни инобатга олади. Бунга мисол тариқасида D-Link тармоқлараро экран қурилмасини келтириш мумкин (17-расм). У зарарловчи дастурларни ва трафикни текшириш имконини беради.

17-расм. *SOH тармоқлари учун DFL-260E – тармоқлараро экрани.*

Умуман олганда ахборот хавфсизлиги тизимининг аппарат-дастурий воситалари ҳақида фикр юритганда, локал тармоқдаги объектларни очиқ тармоқлар (интернет) таъсиридан юқори самарали ҳимоя қилиш усули – бу улар орасида оқиб юрувчи тармоқ пакетларини назорат қилувчи ва фильтрловчи қурилмани белгиланган қоидаларга мос равишда ўрнатишга алоҳида эътибор берилади. Бундай қурилма – **тармоқлараро экран** деб номланиб, у яна **файрволл** (инглизча firewall) ёки **брандмауэр** (немис тилида brandmauer) деб ҳам аталади.

Экран ёки **тармоқлараро экран** – аппарат ва дастурий воситалар мажмуи бўлиб, ўзидан ўтказувчи тармоқ пакетларини белгиланган қоидалар асосида турли протоколлар бўйича назорат қилади ва фильтрлайди.

Тармоқлараро экраннинг асосий вазифаси компьютер тармоқларини ноқонуний рухсат этишлардан ҳимоя қилишдир. Баъзида уларни **фильтр**лар деб ҳам аташади. Чунки улар белгиланган тузилишга (конфигурацияга) ва мезонларга мос келмайдиган пакетларни ўтказмаслик (фильтрлаш) вазифасини бажаради.

Яқин вақтларга қадар кўплаб компьютер фойдаланувчилари Интернетда ишлаганда ёки бошқа тармоқлардан фойдаланганда ўз компьютерлари вируслар билан «касалланиши» мумкинлиги ҳақида тушунчаларга эга бўлмаганлар. Бугунги кунда эса деярли барча интернетдан фойдаланувчилар ўз компьютерларига таъсир этиши мумкин бўлган хавфларни биладилар ҳамда ҳар қандай вирус ва ҳужумлардан ҳимояланиш зарурлигини тушунадилар.

Замонавий IT-бозори хавфсизликни таъминловчи қурилмаларнинг турли вариантларини таклиф қилмоқда. Умуман олганда, алоҳида ҳолда компьютерлар антивирус дастурлари ва тармоқлараро экранлар (брандмауэрлар, файрволлар) ёрдамида муваффақиятли ҳимоя қилинади. Компьютер тармоқларини ҳимоя қилиш эса мураккаброқ

бўлиб, бунда алоҳида дастур таъминоти билан ҳимояни таъминлаб бўлмайди. Компьютер тармоқларида ахборот хавфсизлигини таъминлаш учун тармоқ чегараларига тармоқлараро экранларни ўрнатиш талаб этилади.

Тармоқлараро экранларнинг асосий вазифасига ташқи тармоқлар орқали ғаразгўй кимсаларнинг ахборотни ўзгартириш, тарқатиш ёки ўчириш мақсадида компьтерга ҳужум қилишидан ҳимоя қилиш киради. Керакли конфигурацияга эга бўлган тармоқлараро экранни ташқи тармоқ чегарасига ўрнатиш орқали ўз компьютерингиз ташқаридан «кўринмас» ҳолга ўтишига ишонч ҳосил қилиш мумкин. Замонавий тармоқлараро экранлар «рухсат этилмаган барча амаллар тақиқланади» тамойили асосида ишлайди, яъни фойдаланувчи қайси протоколларга ёки дастурларга ички тармоққа рухсат беришни ўзи ҳал қилади. Тармоқлараро экранлар ҳимоя вазифасидан ташқари тармоқ иловаларининг меъёрда ишлашини ҳам таъминлайди.

Албатта, тармоқлараро экран компьютер оламида барча офатлардан сақлашни кафолатлай олмайди. Бунда шунингдек, ҳар доим «инсон мезони»ни эътиборга олиш лозим. Чунки айнан у билмаган ҳолда (баъзан эса мақсадли равишда) хавфсизлик сиёсатини бузувчи ҳаракатларни қилиш орқали ахборот тизимига зарар келтириши мумкин. Бундай ҳаракатларга ташқи ахборот ташувчиларни улаш орқали ахборотни чиқиб кетиши, ҳимояланмаган қўшимча интернет-уланишларни ўрнатиш, қонуний фойдаланувчи томонидан ахборотни мақсадли равишда ўзгартириш кабиларни киритиш мумкин.

4.2. Компьютер тизимларидан фойдаланиш ҳуқуқини чеклаш

Ахборот хавфсизлигини таъминлашнинг асосий тамойилларини ахборот тизимларидаги турли алоқа ва хавфсизликни таъминловчи нимтизимлар, умумий техник воситалар, алоқа каналлари, дастурий таъминот ва маълумотлар базаларига эга ягона тизим интеграциясига асосланган комплекс ёндашув ташкил этади.

Ахборот тизими кенг маънода олиб қаралганда, тизимдан фойдаланувчиларни керакли ахборот билан таъминлаш учун зарур бўлган техник, дастурий ва ташкилий таъминот ҳамда хизмат кўрсатиш ходимларининг йиғиндиси ҳисобланади.

Ахборот хавфсизлиги – сақланувчи ахборотнинг салбий таъсирлардан ҳимояланганлик ҳолатидир.

Тармоқ хавфсизлиги – ташкилот ёки корхонанинг компьютер тармоғи инфратузилмасига ҳамда ундан фойдаланишда тармоқ ресурсларини рухсатсиз фойдаланишдан ҳимоялаш бўйича қўйилувчи талаблар мажмуидир.

Тармоқ хавфсизлиги деганда объектнинг ахборот инфраструктурасини (аутентификациялаш, муаллифлаш, тармоқлараро экран, рухсатсиз киришга ҳаракатларни аниқлаш тизимлари IDS/IPS (Intrusion Detection/Prevention System – ёриб киришларнинг аниқлаш/олдини олиш тизимлари) ва бошқа усуллар ёрдамида), ташқаридан ғаразгўй кимсаларнинг киришидан ҳамда тасодифий хатолардан (DLP технологияси воситасида), шунингдек рухсатга эга бўлган хизмат кўрсатувчи ходимларнинг мақсадли ҳаракатларидан ҳимоя қилиш тушунилади. DLP (Data Leak Prevention) технологияси – бу ахборот тизимидаги конфеденциал ахборотларни рухсатсиз чиқиб кетишидан дастурий ёки дастурий-қурилмавий воситаларни қўллаш орқали ҳимоя қилишнинг замонавий технологиясидир. Бунда чиқиб кетиш каналлари тармоқли (масалан, электрон почта) ёки локал (ташқи ахборот йиғувчилардан фойдаланиб) бўлиши мумкин.

Аутентификация – фойдаланувчининг ахборот тизимига кириши учун рухсат берилишида, унинг идентификация маълумотларини текшириш жараёни.

Муаллифлаш (Авторизация) – бирор фойдаланувчига маълум бир ҳаракатларни бажариш учун ҳуқуқ бериш. Муаллифлаш аутентификациядан кейин амалга оширилади ва фойдаланувчининг қайси ресурсларга рухсати борлигини аниқлашда идентификатордан фойдаланилади. Ахборот технологияларида муаллифлаш ёрдамида ахборот ресурслари ва қайта ишлаш тизимларидан фойдаланишга рухсат ҳуқуқи аниқланади ва амалга оширилади.

Ахборотни узатиш ва қайта ишлашда **аутентлик** – бу ахборотнинг бутунлиги бўлиб, у маълумотлар ҳақиқатан ҳам қонуний фойдаланувчилар томонидан ҳосил қилинганлигини ҳамда муаллифликдан бош тортиш имконияти йўқлигини тасдиқлайди.

Ахборотни ҳимоя қилиш – бу ҳимояланган ахборотни чиқиб кетиши, унга ноқонуний ва тасодифий таъсир кўрсатишнинг олдини олишга йўналтирилган фаолиятдир.

Комплекс хавфсизлик – вужудга келиши мумкин бўлган барча турдаги таҳдидлар (ноқонуний фойдаланиш, маълумотларни тутиб олиш, терроризм, ёнғин, табиий офатлар ва ҳ.к.)ни мажбурий ҳисобга олиб, замон ва макон (фаолиятнинг барча технологик цикллари) бўйича хавфсизликни таъминлашнинг мажбурий бўлган узлуксиз жараёнини назарда тутади.

Комплекс ёндашув қандай шаклда қўлланилишидан қатъий назар, у мураккаб ва турли йўналишдаги хусусий масалаларни, уларнинг ўзаро чамбарчас боғлиқликдаги ечими билан ҳал этилади. Бундай масалаларнинг энг долзарблари бўлиб, ахборотлардан фойдаланишни чеклаш, ахборотларни техник ва криптографик ҳимоялаш, техник воситаларнинг ёндош нурланишлари даражасини камайтириш, объектларнинг техник мустаҳкамланганлиги, уларнинг қўриқлаш ва таҳликадан хабардор қилиш (сигнализация) қурилмалари билан жиҳозланганлиги ҳисобланади.

Фойдаланувчилар, операторлар, администраторларга қурилмадан фойдаланишга рухсат беришни ташкил этишда қуйидаги ҳаракатлар амалга оширилади:

- рухсат олаётган субъектни идентификациялаш ва аутентификациялаш;
- қурилмани блокировкадан чиқариш;
- рухсат берилган субъектнинг ҳаракатларини ҳисобга олиш журналини юритиш.

Рухсат этилган субъектни идентификациялаш учун компьютер тизимларида кўп ҳолларда атрибутивли идентификаторлардан фойдаланилади. Биометрик идентификациялашнинг осон йўли – клавиатурада ишлаш ритми орқали аниқлашдир. Атрибутивли индентификаторлар ичидан, одатда, қуйидагиларидан фойдаланилади:

- пароллар;
- ечиб олинадиган ахборот ташувчилар;
- электрон жетонлар;
- пластик карточкалар;
- механик калитлар.

Конфиденциал маълумотлар билан ишлайдиган деярли барча компьютерларда фойдаланувчиларни аутентификациялаш пароллар ёрдамида амалга оширилади.

Пароль – бу символлар (ҳарфлар, рақамлар, махсус белгилар) комбинацияси бўлиб, уни фақат пароль эгаси билиши керак. Айрим ҳолларда хавфсизлик тизими маъмурига ҳам маълум бўлади.

Компьютернинг замонавий операцион тизимларида паролдан фойдаланиш ўрнатилган. Пароль автоном ток манбаига эга бўлган махсус хотирада сақланади. Паролларни таққослаш операцион тизим (ОТ) юклангунга қадар амалга оширилади. Агар бузғунчи пароль сақланаётган хотиранинг автоном ток манбаини ўчириб қўя олмаганида, ушбу турдаги ҳимоя жуда самарали ҳисобланар эди. Лекин, компьютернинг ОТ юкланишини амалга ошириш учун киритиладиган фойдаланувчи паролидан ташқари, Интернетда рўйхати келтирилган айрим «технологик» пароллардан ҳам фойдаланиш мумкин.

Кўпгина компьютер тизимларида идентификатор сифатида, фойдаланишга рухсат этилган субъектни идентификацияловчи код ёзилган *ечиб олинувчи ахборот ташувчилар*дан фойдаланилади.

Фойдаланувчиларни идентификациялашда, тасодифий идентификациялаш кодларини ҳосил қилувчи – электрон жетонлардан кенг фойдаланилади. Жетон – бу, ҳарфлар ва рақамларнинг тасодифий кетма-кетлигини (сўзни) яратувчи қурилма. Бу сўз компьютер тизимидаги худди шундай сўз билан тахминан минутига бир марта синхрон тарзда ўзгартириб турилади. Натижада, фақатгина маълум вақт оралиғида ва тизимга фақатгина бир марта кириш учун фойдаланишга ярайдиган, бир марталик пароль ишлаб чиқарилади. Бошқа бир турдаги жетон ташқи кўринишига кўра калькуляторга ўхшаб кетади. Аутентификациялаш жараёнида компьютер тизими фойдаланувчи мониторига рақамли кетма-кетликдан иборат сўров чиқаради, фойдаланувчи ушбу сўровни жетон тугмалари орқали киритади. Бунда жетон ўз индикаторида аксланадиган жавоб кетма-кетлигини ишлаб чиқади ва фойдаланувчи ушбу кетма-кетликни компьютер тизимига киритади. Натижада, яна бир бор бир марталик қайтарилмайдиган пароль олинади. Жетонсиз тизимга киришнинг имкони бўлмайди. Жетондан фойланишдан аввал унга фойдаланувчи ўзининг шахсий паролини киритиши лозим.

Аутентификациялаш жараёни компьютер тизимлари билан рухсат этилган субъект орасида амалга ошириладиган мулоқотни ҳам ўз ичига олиши мумкин. Рухсат этилган субъектга бир қатор саволлар берилади, олинган жавоблар таҳлил қилинади ва рухсат этилган субъектнинг асллиги бўйича якуний хулоса қилинади.

Компьютер тизимлари қурилмаларидан фойдаланишга рухсатни масофадан туриб бошқариш мумкин. Масалан, локал тармоқларда

ишчи станциянинг тармоққа уланишини администратор иш жойидан туриб блокировка қилиши мумкин. Қурилмалардан фойдаланишга рухсат этишни ток манбаини узиб қўйиш орқали ҳам самарали бошқариш мумкин. Бунда ишдан бошқа вақтларда, ток манбаи қўриқлаш хизмати томонидан назорат қилинадиган коммутацияли қурилмалар ёрдамида узиб қўйилади.

Хизмат кўрсатувчи ходимнинг қурилмадан фойдаланишига рухсат этишни ташкил этиш фойдаланувчига берилган рухсатдан фарқланади. Энг аввало, қурилма конфиденциал маълумотлардан тозаланади ҳамда ахборот алмашиниш имконини берувчи алоқалар узилади. Қурилмага техник хизмат кўрсатиш ва унинг иш қобилиятини тиклаш мансабдор шахс назорати остида амалга оширилади. Бунда ички монтаж ва блокларни алмаштиришга боғлиқ ишларни амалга оширилишига жиддий эътибор берилади.

4.3. Зарарлантирувчи дастурий таъминот

Зарарлантирувчи дастурий таъминот, аввало компьютер вируслари ахборот тизимига жиддий хавфни юзага келтиради. Бу хавфни менсимаслик фойдаланувчи ахбороти учун жиддий оқибатларни келтириб чиқариши мумкин. Ўз вақтида компьютер вируслари таҳдидларига ўта юқори эътибор қаратиш ҳам ахборот тармоғининг имкониятларидан тўлиқ фойдаланишга салбий таъсир кўрсатади. Зарарлантирувчи дастурий таъминот таъсири механизмлари ҳамда уларга қарши курашиш усул ва воситаларини билиш, уларнинг компьютер ва ахборотларга зарар етказишига қарши курашни самарали ташкил этишга имкон яратади.

Ахборот тизимида зарарлантирувчи дастур таъминоти мавжудлигини фойдаланувчи қуйидаги белгилар орқали билиб олиши мумкин:

– экранда зарарланганлик ёки зарарланиш эҳтимоли мавжудлиги ҳақида антивирус воситаларининг хабарлари пайдо бўлиши, антивирус воситаларининг ўз-ўзидан ишламай қолиши;

– монитор ёки принтерга узатилувчи хабарлар, товуш эффектлари, дастурларнинг тасодифан ишга тушиб кетиши, файлларнинг ўчириб юборилиши каби тизимда вирус мавжудлигини билдирувчи белгилар;

– компьютер тизимининг қурилма ва дастурий таъминотидаги ишдан чиқишлар, у ёки бу маълумотни қайта ишлаш вақтининг чўзилиб кетиши, дисклардаги бўш жойларнинг асоссиз камайиб кетиши, сканер-дастурлар томонидан вирусни сканер қилишни рад этилиши, тизимнинг «осилиб қолиш»и ва бошқалар;

– фойдаланувчи томонидан электрон почта орқали юборилмаган хабарларнинг тарқатилиши.

Зарарлантирувчи дастур (Malware, malicious software – ғаразмақсадли дастурий таъминот) – бу ахборот тизими ресурсларига, мавжуд қоидаларни четлаб ўтиш орқали, рухсатсиз киришни амалга ошириш ёки таъсир кўрсатиш учун мўлжалланган ҳар қандай дастурий таъминотдир.

Дастурий таъминотнинг зарарлилиги ёки фойдалилигини кўп жиҳатдан фойдаланувчи томонидан ёки уни қўллаш усули билан белгиланади. Зарарлантирувчи дастурларнинг умумэътироф этилган классификацияси (тоифаланиши) ҳозиргача мавжуд эмас. Бу борада биринчи уринишлар ўтган асрнинг 90-йилларида CARO (Computer AntiVirus Researcher's Organization) антивирус мутахассислари альянси томонидан амалга оширилган.

Бироқ, вақт ўтиши билан зарарлантирувчи дастурларнинг шиддат билан ривожланиб кетиши, янги платформаларнинг яратилиши ҳамда антивирус компаниялари сонининг ортиб бориши натижасида CARO тизими ишламай қўйди. Унинг ишламай қолишига янада кўпроқ таъсир қилган сабаб, бу турли антивирус компанияларининг детекторлаш тизими технологиялари турлича бўлиб, бунинг натижасида турли антивирус дастурларининг текшириш натижаларини яқ-қол таққослашнинг имкони бўлмай қолди. Шундай бўлса-да, баъзан антивирус дастурлари томонидан детекторланувчи объектларни янги умумий классификациясини ишлаб чиқишга ҳаракатлар қилинмоқда. Бу борада сўнгги эътиборли лойиҳа CME (Common Malware Enumeration) стандартининг тузилиши бўлиб, унинг моҳияти бир хил тоифадаги детекторланувчи объектларга ягона идентификатор беришдан иборат.

«Касперский лабораторияси» компанияси томонидан таклиф этилган классификацияга кўра, ундаги мутахассислар зарарлантирувчи дастурий таъминотни зарарлантирувчи дастурлар (Malware) ва энг кераксиз дастурларга (PUPs, Potentially Unwanted Programs) ажра-

тишни таклиф этадилар. Ўз навбатида зарарлантирувчи дастурларга қуйидагилар киради: компьютер вируси ва қуртлар, троян дастурлари, шубҳали таҳловчилар (упаковкаловчилар) ва зарарлантирувчи утилитлар.

Компьютер вируслари ва қуртлар. «Компьютер вируси» деган ибора бугунги кунда ҳеч кимни ажаблантирмайди. Бу тушунча ўтган асрнинг 80-йилларида пайдо бўлиб, зарарлантирувчи дастурлар биологик вирусларга хос бўлган белгиларга эга бўлганлиги сабабли шундай номланган. Улар компьютер тизимига тезкор ва сездирмай кириб бориб, тез тарқалиш, кўпайиш, зарарлаш ҳамда тизим фаолиятига салбий таъсир кўрсатиш хусусиятига эга. Ахборот тизимлари билан ишлашда «вирус» атамаси билан бирга «зарарланиш», «тарқалиш муҳити», «профилактика» каби тушунчалардан ҳам фойдаланилади.

Компьютер вируси – бу компьютер ёки компьютер тизимида фойдаланувчига бўйсунмаган ҳолда тарқалиш ва ўз-ўзидан кўпайиш хусусиятига эга бўлган кичик ўлчамли бажарилувчи ёки интерпретацияланувчи дастурлардир. Улардан олинган нусхалар ҳам шундай хусусиятларга эга бўлади. Вируслар ахборот сақланувчи объектда ёки компьютер тармоғи қурилмаларида сақланувчи маълумотларни ўзгартириш ёки йўқ қилиб юборишга мўлжалланиши мумкин. Вируслар тарқалиш жараёнида ўзини модификация қилиши мумкин.

Қуртлар вирусларга хос хусусиятларга эга бўлиб, улар бошқа файлларга зарар етказмаган ҳолда ўз-ўзидан кўпайиши мумкин. У бир компьютерга кириб олгач, бошқа компьютерларга тарқалиш йўлларини қидиради. Қурт – бу алоҳида файл, вирус эса мавжуд файлларга киритилувчи код.

Компьютер вируси ва қуртлар тоифасига қуйидагилар киради:

Virus (вирус) – компьютернинг локал ресурслари бўйича фойдаланувчи ихтиёридан ташқари ноқонуний равишда ўз-ўзидан кўпайиш хусусиятига эга бўлган зарарлантирувчи дастур. Қуртлардан фарқли равишда вируслар бошқа компьютерларга тарқалиш ва кириши учун тармоқ сервисларидан фойдаланмайдилар. Вирус нусхаси бошқа компьютерга фақатгина зарарланган объектнинг ўша компьютерда фаоллаштирилиши туфайли ўтиши мумкин. Масалан:

- вирус тармоқ ресурсида жойлашган файлга кириб олганда;
- вирус ахборот ташувчига ўз нусхасини кўчириб, ундаги файлларни зарарлаганда;

- фойдаланувчи вирус билан зарарланган иловани электрон почта орқали юборганда.

Worm (қурт) – компьютер тармоқларида, унинг ресурслари орқали фойдаланувчи ихтиёридан ташқари ноқонуний равишда ўз-ўзидан кўпайиш хусусиятига эга бўлган зарарловчи дастур. Куртни фаоллаштириш учун фойдаланувчи уни ишга тушириши керак. Бундай тоифадаги қуртлар тармоқда ўқиш ва ёзиш учун рухсати бўлган тармоқ каталогига эга компьютерларни қидириб, уларга ўзининг нусхасини кўчиради.

Net-Worm (тармоқ қурти) – компьютер тармоқларида фойдаланувчи ихтиёридан ташқари ноқонуний равишда ўз-ўзидан кўпайиш хусусиятига эга бўлган зарарловчи дастур.

Троян дастурлари. Бундай зарарловчи дастурлар ташқаридан қараганда қонуний дастурий маҳсулот кўринишида бўлиб, ишга туширилганда маълумотларни йўқ қилишга, блокировка қилишга, модификация ёки ахборотдан нусха олишга, компьютер ёки компьютер тармоғи фаолиятини ишдан чиқаришга йўналтирилган ноқонуний ҳаракатларни амалга оширади. Вирус ва қуртлардан фарқли равишда, бундай тоифадаги зарарловчи дастурлар ўзларининг нусхасини яратиш имконига эга эмас.

Backdoor (бэкдор) – зарарланган компьютерни ғаразгўй кимса томонидан яширин тарзда бошқариш учун мўлжалланган зарарловчи дастур. Бундай зарарловчи дастурлар компьютерда муаллиф томонидан қўйилган барча вазифаларни: файлларни қабул қилиш ва юбориш, уларни ишга тушириш ва йўқ қилиш, хабарларни чиқариш, маълумотларни ўчириш, компьютерни қайта ишга тушириш кабиларни бажариш имконини беради.

Exploit (эксплойт) – олдиндан ғаразли мақсадни кўзловчи, локал ёки тармоққа уланган компьютердаги дастурий таъминотнинг заиф жойларидан фойдаланиш имконини берувчи, маълумотлар ёки бажарилувчи кодларга эга бўлган дастурлар. Одатда, эксплойтлар ғаразгўй кимсалар томонидан компьютерга кириш ва кейинчалик унга зарарловчи кодларни юбориш мақсадида фойдаланилади (масалан, синдирилган Web-сайтга кирувчи барча фойдаланувчиларни зарарлаш).

Rootkit – тизимдаги алоҳида объектларни очиш ёки фаоллаштириш учун мўлжалланган дастур. Одатда, улар ёрдамида реестр калитлари, файллар ёки зарарланган компьютер хотирасидаги жараёнлар

очилиши мумкин. Rootkit ўз-ўзидан ҳеч қачон зарар келтирмайди, бироқ бу турдаги дастурлар аксарият ҳолларда зарарлантирувчи дастурлар томонидан ўзининг хусусий яшаш вақтини узайтириш учун фойдаланилади.

Trojan – ноқонуний ҳаракатларни амалга ошириш орқали маълумотларни йўқ қилишга, блокировка қилишга, модификация ёки ахборотдан нусха олишга, шунингдек, компьютер ёки компьютер тармоғи фаолиятини ишдан чиқаришга мўлжалланган зарарловчи дастур. У ўз тоифасидаги бошқа дастурларнинг бирортасига ўхшамайди.

Троянларга шунингдек, «кўпмақсадли» троян дастурлари ҳам киради. Улар бир вақтнинг ўзида бир нечта рухсат этилмаган ноқонуний ҳаракатларни содир этишга қодир бўлиб, уларнинг бирортасига алоҳида ёндашиб бўлмайди. Бир биридан фарқ қилувчи ҳаракатларни амалга оширадиган ҳамда «жабрланувчи»га ҳар хил таъсир кўрсатувчи троян дастурларнинг кўплаб турлари мавжуд. Уларга қуйидагиларни киритиш мумкин:

Trojan-Banker – фойдаланувчининг банк тизимларига, электрон маблағларга ва пластик карталарига тааллуқли ахборотларни ўғрилашга мўлжалланган.

Trojan-Dropper – фойдаланувчининг компьютерига ноқонуний тарзда зарарловчи дастурларни яширин равишда инсталляция қилишга мўлжалланган.

Trojan-Proxy – ноқонуний тарзда фойдаланувчининг компьютери орқали аноним равишда турли интернет ресурсларига рухсат беришни амалга ошириш учун мўлжалланган.

Trojan-Clicker – ноқонуний фойдаланувчи томонидан Интернет-ресурсларига мурожаатни амалга ошириш учун мўлжалланган (одатда Web-саҳифаларга).

Trojan-PSW (Password-Stealing-Ware) – зарарланган компьютердан фойдаланувчининг аккаунтлари (логин ва пароль)ни ўғрилаш учун мўлжалланган.

Trojan-DDoS – ноқонуний фойдаланувчи томонидан зарарланган компьютер орқали олдиндан аниқланган манзилга DoS-ҳужум уюштириш учун мўлжалланган.

Trojan-Downloader – ноқонуний фойдаланувчи томонидан зарарланган компьютерга зарарловчи дастурларнинг янги версияларини ўрнатиш ва ишга тушириш учун мўлжалланган. Интернетдан юкла-

ган дастурлар ёки ишга туширилади ёки операцион тизим имкониятларига мос равишда автомат тарзда юклаш учун троян дастури томонидан рўйхатга олинади.

Trojan-Spy – фойдаланувчи ортидан электрон айғоқчилик қилиш учун мўлжалланган. Олинган маълумотлар (клавиатура орқали киритилувчи маълумотлар, экрандаги тасвирлар, фаол иловалар рўйхати ва бошқ.). ғаразгўй кимсага узатиб турилади.

Шубхали таҳловчилар. Бундай турдаги зарарловчи дастурлар махсус усул билан тахлашни амалга ошириб, шифрланган файлларни кейинчалик қайта тиклашда эвристик усуллардан фойдаланишни мураккаблаштиради.

Зарарловчи утилитлар – бошқа турдаги вирусларни, троян ёки қуртларни яратишни автоматлаштириш, серверга DoS-ҳужумларни уюштириш, компьютерни ишдан чиқариш кабиларни амалга ошириш учун ишлаб чиқилган зарарловчи дастурлардир. Вирус, троян ёки қуртлардан фарқли равишда бундай тоифадаги дастурлар ўзлари иш юритувчи компьютерларга тўғридан-тўғри хавф туғдирмайди. Уларни ажратиб турувчи асосий жиҳати – бу улар томонидан амалга ошириладиган ҳаракатлардир.

Бундай тоифадаги дастурларга қуйидагиларни мисол келтириш мумкин:

Constructor – янги компьютер вируслари, қуртлари ва троян дастурларини тайёрлаш учун мўлжалланган дастурлар.

HackTool – ноқонуний фойдаланувчи томонидан локал компьютер ёки тармоқдаги компьютерга ҳужумлар уюштириш учун фойдаланиладиган дастурлар.

Spoofer– жўнатувчининг қалбаки манзили орқали хабарлар ва тармоқ сўровларини юбориш имконини берувчи дастурлар.

DoS – компьютерларга DoS-ҳужумларни уюштириш учун мўлжалланган дастурлар.

Назорат учун саволлар

- Ахборотларни муҳофаза қилишнинг асосий ва ёрдамчи аппарат воситаларига нималар киради?
- Ахборотларни муҳофаза қилишнинг дастурий воситалари қандай дастурлардан иборат?

- Ахборотларни муҳофаза қилишнинг дастурий воситаларининг афзалликлари ва камчиликлари нималардан иборат?
- Компьютер тизимларидан фойдаланиш ҳуқуқини чеклашнинг қандай усул ва воситалари мавжуд?
- Комплекс хавфсизлик нималардан иборат?
- Қандай атрибутивли индентификаторларни биласиз ва улар қандай тартибда ишлайди?
- Аутентификациялаш қандай амалга оширилади?
- Зарарлантирувчи дастур деб нимага айтилади?
- Ахборот тизимида зарарлантирувчи дастур мавжудлиги қандай аниқланади?
- Компьютер вируслари нима?
- Компьютер қуртлари нима?
- Троян дастурлари қандай вазифаларни бажаради?
- Троян дастурларнинг қандай турларини биласиз?
- Зарарловчи утилитлардан нима мақсадда фойдаланилади?

V. ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА АХБОРОТНИ МУҲОФАЗА ҚИЛИШНИНГ ДАВЛАТ ТИЗИМИ

5.1. Ахборотни муҳофаза қилишнинг давлат тизими

Маълумки, юртимизда ахборот хавфсизлиги соҳасидаги муносабатларни тартибга солиш борасида 1992 йил 8 декабрда қабул қилинган Ўзбекистон Республикаси Конституцияси асосий қонун ҳисоб-ланади. Конституциямизнинг 29-моддасига биноан: «Ҳар ким фикрлаш, сўз ва эътиқод эркинлиги ҳуқуқига эга. Ҳар ким ўзи истаган ахборотни излаш, олиш ва уни тарқатиш ҳуқуқига эга, амалдаги конституциявий тузумга қарши қаратилган ахборот ва қонун билан белгиланган бошқа чеклашлар бундан мустаснодир.»

Ахборот хавфсизлиги тизими ҳар қандай давлатнинг ахборот соҳасидаги сиёсатини миллий хавфсизликни таъминлаш борасидаги давлат сиёсати билан чамбарчас боғлайди. Бунда ахборот хавфсизлиги тизими давлат сиёсатининг асосий ташкил этувчиларини яхлит бир бутунликка бирлаштиради. Бу эса ахборот хавфсизлигининг роли ва унинг мамлакат миллий хавфсизлиги тизимидаги мавқеини белгилайди. Ахборот соҳасидаги Ўзбекистоннинг миллий манфаатларини, уларга эришишининг стратегик йўналишларини ва уларни амалга ошириш тизимларини ўзида акс эттирувчи мақсадлар яхлитлиги давлат ахборот сиёсатини англатади.

Ахборот хавфсизлиги соҳасида давлат сиёсатини амалга оширишга имкон берувчи шароитларни яратиш, мамлакатни иқтисодий ва илмий-техник тараққиётига кўмаклашиш, ахборотни муҳофаза қилишнинг усул ва воситаларини яратиш бугунги куннинг долзарб масалаларидан биридир.

Ахборотни муҳофаза қилишнинг давлат тизими ахборотни ҳимояловчи техникани қўллайдиган идоралар ва ижро этувчилар ҳамда ҳимоя объектлари мажмуини ифодалайди. Бу тизим ахборотни муҳофаза қилиш соҳасидаги ҳуқуқий, ташкилий-бошқарув ва норматив ҳужжатларга мувофиқ ташкил этилади ва фаолият юритади. Шу билан бирга мамлакат миллий хавфсизлигини таъминлаш тизимининг таркибий қисми ҳисобланади ва давлат хавфсизлигини ахборот соҳасидаги ички ва ташқи таҳдидлардан ҳимоялашга йўналтирилган.

Ахборотни муҳофаза қилишнинг давлат тизими ахборотни муҳофаза қилиш соҳасида ташкилотлар фаолиятини лицензиялаш нимтизимини, ахборотни муҳофаза қилиш воситаларини сертификациясини ва ахборот хавфсизлиги талаблари бўйича ахборотлаштириш объектларини аттестациясини ўз ичига олувчи мураккаб тизимдир.

Ахборотни муҳофаза қилишнинг давлат тизими фаолияти қуйидаги қонунлар ва норматив-ҳуқуқий ҳужжатлар асосида амалга оширилади:

– Ўзбекистон Республикасининг Конституцияси;

– «Давлат сирларини сақлаш тўғрисида»ги қонун;

– «Ахборотлаштириш тўғрисида»ги қонун;

– «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги қонун;

– «Фаолиятнинг айрим турларини лицензиялаш тўғрисида»ги қонун;

– «Стандартлаштириш тўғрисида»ги қонун;

– «Алоқа тўғрисида»ги қонун;

– «Телекоммуникациялар тўғрисида»ги қонун;

– «Ахборот олиш кафолатлари ва эркинлиги тўғрисида»ги қонун;

– «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонун;

– «Электрон ҳужжат айланиши тўғрисида»ги қонун;

– «Электрон рақамли имзо тўғрисида»ги қонун;

– «Электрон тижорат тўғрисида»ги қонун;

– «Электрон ҳукумат тўғрисида»ги қонун;

– Ўзбекистон Республикаси Президентининг фармонлари ва қарорлари;

– Ўзбекистон Республикаси Вазирлар маҳкамасининг қарорлари;

– Ахборотни муҳофаза қилиш соҳасидаги вазирлик, муассаса, агентлик ва хўжаликларнинг бошқа ҳуқуқий актлари.

Давлат хавфсизлиги соҳасида давлат сиёсатини амалга оширишга имкон берувчи шароитларни яратиш, мамлакатни иқтисодий ва илмий-техник тараққиётига кўмаклашиш, ахборотни муҳофаза қилиш усул ва воситаларини қўллаб, Ўзбекистон миллий хавфсизлигига бўлган зиённи жиддий камайтириш – буларнинг барчаси ахборотни муҳофаза қилишнинг давлат тизимида кўзланган мақсад бўлиб, уларни амалга ошириш учун қуйидаги вазифаларни бажариш керак:

– ягона техник сиёсатни ўтказиш, ҳарбий, иқтисодий, илмий-техник ва бошқа соҳалар фаолиятларида ахборотни муҳофаза қилиш бўйича ишларни мувофиқлаш ва ташкил этиш;

– разведканинг техник воситалар ёрдамида ахборотни қўлга киритишни жиддий қийинлаштириш ёки йўл қўймаслик;

– ахборотни муҳофаза қилиш соҳасида муносабатларни тартибга солувчи ҳуқуқий ҳужжатларни қабул қилиш;

– ахборотни муҳофаза қилиш воситаларини яратиш ва уларнинг самарадорлигини назорат қилиш кучларини ташкил этиш;

– давлат органлари ва ташкилотларида ахборотни муҳофаза қилиш ҳолатини назорат қилиш;

– ахборотни муҳофаза қилиш соҳасидаги давлат тизими ҳолатини таҳлил қилиш, асосий муаммоларни аниқлаш;

– ахборотни муҳофаза қилишни давлат тизимининг муҳим йўналишларини аниқлаш;

– ахборотни муҳофаза қилиш бўйича ишларни норматив-методик ва ахборий таъминлаш.

Ўзбекистон Республикасининг Фуқаролик кодексида банк, тижорат ва суғурта сирлари тушунчалари ҳамда уларни ҳимоя қилишнинг зарурий чоралари белгилаб қўйилган.

Ахборот хавфсизлиги борасида Ўзбекистон Республикасининг Жиноят кодекси муҳим ўрин эгаллайди. Ушбу кодекснинг «Ахборот технологиялари соҳасидаги жиноятлар» деб номланувчи XX[1] бобида ахборот технологиялари соҳасида содир этилувчи жиноятларга жазо белгилаб қўйилган.

Ахборотларни криптографик ҳимоялаш борасидаги масалаларни тартибга солиш 2007 йил 3 апрелдаги Ўзбекистон Республикаси Президентининг «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги ПҚ-614 сонли қарорида[1] ўз аксини топганган бўлиб, унга кўра ушбу соҳада Ўзбекистон Республикасининг Миллий хавфсизлик хизмати масъул орган ҳисобланади. Шунингдек, мазкур қарор билан Ўзбекистон Республикасида ахборотни криптографик ҳимоялаш бўйича Низом ҳамда Ўзбекистон Республикасида ахборотни криптографик ҳимоялаш воситаларини сертификациялаш Низомлари тасдиқланган.

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – № 14. – 140-м.

Ўзбекистон Республикаси Президентининг 2013 йил 27 июндаги «Ўзбекистон Республикаси Миллий ахборот-коммуникация тизимини янада такомиллаштириш чора-тадбирлари тўғрисида»ги қарорининг қабул қилиниши мамлакатимизда ахборот хавфсизлиги масалаларини ечиш борасида муҳим ташкилий қадам бўлди.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2013 йил 16 сентябрдаги 250-сонли қарори[1] билан, Ўзбекистонда электрон ҳукумат тизимини янада ривожлантириш мақсадида, махсус марказлар – «Электрон ҳукумат тизимини ривожлантириш маркази» ҳамда «Ахборот хавфсизлигини таъминлаш маркази»ни ташкил этиш белгиланган. Ушбу қарор билан, «Электрон ҳукумат тизимини ривожлантириш» ҳамда «Ахборот хавфсизлигини таъминлаш маркази»нинг тузилмаси ва фаолияти тартибини белгиловчи Низом қабул қилинган. «Ахборот хавфсизлигини таъминлаш маркази»нинг асосий вазифалари бири этиб қонун бузувчиларни таҳлил қилиш, идентификациялашда, ахборотлар маконидаги рухсатсиз ёхуд бузувчи ҳаракатларни амалга оширишда фойдаланиладиган методлар ва воситаларни таҳлил қилишда ҳуқуқни муҳофаза қилиш органлари билан ҳамкорлик қилиш белгиланган.

Ўзбекистон Республикаси Президентининг 2015 йил 4 февралдаги фармонига асосан «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги» ташкил этилди. Мазкур фармон билан юртимизда ахборот хавфсизлигини таъминлаш ва коммуникация тармоқлари, дастурий маҳсулотлар, ахборот тизимлари ва ресурсларини ҳимоя қилишнинг замонавий технологияларини татбиқ этиш чора-тадбирларини амалга ошириш, ахборот ресурсларини ҳимоя қилиш бўйича техник инфратузилмани янада ривожлантириш каби масалалар ушбу вазирликнинг асосий вазифалари ҳамда фаолият йўналишлари сифатида белгилаб қўйилди.

Бугунги кунда мамлакатимизда ахборот хавфсизлиги соҳасида ягона концептуал ҳужжатни яратиш замон талабидир. Бундай ҳужжат ахборот хавфсизлиги соҳасида норматив-ҳуқуқий базани такомил-

[1] «Ўзбекистон Республикасининг Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ҳузуридаги «Электрон ҳукумат» тизимини ривожлантириш маркази ҳамда Ахборот хавфсизлигини таъминлаш маркази фаолиятини ташкил этиш чора-тадбирлари тўғрисида»ги Қарор // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2013. – №38 – 492-м.; 2015. – №26. – 338-м.

лаштириш бўйича ишларни, ушбу соҳада ягона стандартни ишлаб чиқиш ва жорий этиш фаолиятини йўналтиришга, шунингдек, мазкур соҳада кадрлар сиёсатини ривожлантиришнинг зарурий чораларини аниқлашга имкон яратади.

5.2. Ахборот муҳофаза қилиш соҳасида лицензиялаш ва сертификациялаш

Ўзбекистон Республикасининг 2000 йил 25 майдаги «Фаолиятнинг айрим турларини лицензиялаш тўғрисида»ги 71-II-сонли қонуни[1] турли фаолият соҳасида лицензиялашни амалга ошириш бўйича асосий ҳужжат ҳисобланади.

Ушбу қонуннинг 3-моддасида қуйидаги асосий тушунчалар келтирилган:

лицензия – лицензияловчи орган томонидан юридик ёки жисмоний шахсга берилган, лицензия талаблари ва шартларига сўзсиз риоя этилгани ҳолда фаолиятнинг лицензияланаётган турини амалга ошириш учун рухсатнома (ҳуқуқ);

фаолиятнинг лицензияланаётган тури – Ўзбекистон Республикаси ҳудудида амалга оширилиши учун лицензия олиш талаб қилинадиган фаолият тури;

лицензиялаш – лицензия бериш тўғрисидаги аризани топшириш ва кўриб чиқиш, лицензиянинг амал қилишини тўхтатиб туриш ёки тугатиш, шунингдек уни бекор қилиш ва қайта расмийлаштириш жараёни билан боғлиқ тадбирлар комплекси;

лицензия талаблари ва шартлари – фаолиятнинг лицензияланаётган турини амалга ошираётганда лицензиат томонидан бажарилиши мажбурий бўлган, қонун ҳужжатларида белгиланган талаблар ва шартларнинг мажмуи;

лицензияловчи органлар – қонун ҳужжатларига мувофиқ лицензиялашни амалга оширувчи махсус ваколатли органлар;

лицензиат – фаолиятнинг лицензияланадиган турини амалга ошириш лицензияси бўлган юридик ёки жисмоний шахс;

---

[1] Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2000. №5-6. – 142-м.; 2003. – №1. 8-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – №14. – 110-м.; 2006. – 41. – 405-м.; – 2011. – №36. – 363-м.; – 2013. – №18. – 233-м.; – 2014. –№50. – 588-м.; – 2015. – №33. – 439-м. – №52., – 645-м.

лицензиялар реестри – берилган, тўхтатиб турилган, қайта тикланган, қайта расмийлаштирилган, бекор қилинган лицензиялар, шунингдек амал қилиши тугатилган лицензиялар тўғрисидаги маълумотларни ўз ичига олган лицензияловчи органларнинг маълумотлар базалари мажмуи.

Лицензиялаш соҳасини давлат томонидан тартибга солишни ушбу қонуннинг 4-моддасига кўра Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳамда лицензияловчи органлар амалга оширади.

Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилиш (АКМҚ) соҳасида фаолиятни лицензиялаш тизими.

Лицензиялаш талаблари ва шартлари Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги 242-сонли қарори[1] билан тасдиқланган «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги Низом»нинг II бўлимида келтирилган.

Ахборотни муҳофаза қилиш соҳасида фаолиятнинг лицензияланаётган турларига ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва қўллаш киради.

Ахборотни муҳофаза қилиши соҳасидаги фаолиятни лицензиялаш тизимининг норматив-ҳуқуқий базасини қуйидагилар ташкил қилади:

- Ўзбекистон Республикасининг 2007 йил 17 июлдаги 102-сонли қонуни[2] «Ўзбекистон Республикаси Олий Мажлисининг 2001 йил 12 майда қабул қилинган «Амалга оширилиши учун лицензиялар талаб қилинадиган фаолият турларининг рўйхати тўғрисида»ги 222-II-сонли қарорининг 1-иловасига ўзгартиш ва қўшимчалар киритиш ҳақида»;

- Ўзбекистон Республикаси Президентининг 2007 йил 3 апрелдаги «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги 614-сонли қарори[3] билан тасдиқланган Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилиш тўғрисидаги Низом;

---

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №46-47. – 471-м.

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №29-30. – 295-м.

[3] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №14. – 140-м.

- Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2007 йил 21 ноябрдаги 242-сонли қарори[1] билан тасдиқланган «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги Низом».

- Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 25 ноябрь кунидаги «Ахборотлаштириш соҳасида норматив-ҳуқуқий базани такомиллаштириш тўғрисида»ги 256-сонли қарори[2] билан тасдиқланган «Давлат органларининг ахборот тизимини яратиш тартиби тўғрисидаги Низом»нинг IV бўлими «Давлат органлари ахборот тизимларининг ахборот хавфсизлигини таъминлаш» деб номланиб, унинг 24-бандига мувофиқ давлат идораларининг ахборот тизимида қўлланиладиган ахборотни ҳимоялаш дастурий-техник воситалари лицензияланган ва сертификатлаштирилган бўлиши керак. Мазкур бўлимнинг 28[1]-бандида давлат органларининг давлат сирларига ёки махфий ахборотларга мансуб ахборот билан ишлаш учун мўлжалланган ахборот тизимлари қонун ҳужжатларида белгиланган тартибда ахборот хавфсизлиги талабларига мувофиқ мажбурий аттестациядан ўтказилиши кераклиги белгиланган.

Махсулотни сертификатлаштириш Ўзбекистон Республикасининг маҳсулотни (хизматларни) сертификациялашнинг Миллий тизими (СМТ) асосида амалга оширилади.

СМТ фаолиятини регламентация қилувчи асосий норматив-хуқуқий акт бўлиб Ўзбекистон Республикасининг 1993 йил 28 декабрь кунидаги «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги 1006-XII-сонли қонуни[3] ҳисобланади.

Ушбу қонуннинг 1-моддасида қуйидаги асосий тушунчалар келтирилган:

сертификатлаштириш миллий тизими — давлат миқёсида амал қиладиган, сертификатлаштириш ўтказишда ўз тартиб ва бошқарув қоидаларига эга бўлган тизим;

---

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №46-47. – 471-м.

[2] Ўзбекистон Республикасининг қонун ҳужжатлари тўплами. – 2005. – №47-48. – 355-м.; 2011. –№ 45-46. – 472-м.

[3] Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – 1994. – №2. – 50-м.; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2000. – №7-8. – 217-м.; 2003. – №5. – 67-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – №14. – 113-м.; 2006. – №41. – 405-м.; 2013. – №41. – 543-м.; 2014. – №50. – 588-м.; 2016. – №3(I). – 32-м.

маҳсулотларни сертификатлаштириш (матнда бундан кейин *сертификатлаштириш* деб юритилади) — маҳсулотларнинг белгиланган талабларга мувофиқлигини тасдиқлашга оид фаолият;

мувофиқлик сертификати — сертификатланган маҳсулотнинг белгиланган талабларга мувофиқлигини тасдиқлаш учун сертификатлаштириш тизими қоидаларига биноан берилган ҳужжат;

мувофиқлик белгиси — муайян маҳсулот ёхуд хизмат аниқ стандартга ёки бошқа норматив ҳужжатга мос эканлигини кўрсатиш учун маҳсулотга ёхуд кўрсатилган хизматга доир ҳужжатга қўйиладиган, белгиланган тартибда рўйхатга олинган белги.

Сертификатлаштириш (2-модда):

– одамларнинг ҳаёти, соғлиғи, юридик ва жисмоний шахсларнинг мол-мулки ҳамда атроф-муҳит учун хавфли бўлган маҳсулотлар реализация қилинишини назорат этиб бориш;

– маҳсулотларнинг жаҳон бозорида рақобат қила олишини таъминлаш;

– мамлакат корхоналари, қўшма корхоналар ва тадбиркорлар халқаро миқёсдаги иқтисодий, илмий-техникавий ҳамкорликда ва халқаро савдо-сотиқда иштирок этишлари учун шароит яратиш;

– истеъмолчини тайёрловчининг (сотувчининг, ижрочининг) виждонсизлигидан ҳимоя қилиш;

– маҳсулот тайёрловчиси (сотувчиси, ижрочиси) таъкидлаган сифат кўрсаткичларини тасдиқлаш мақсадларида амалга оширилади.

Сертификатлаштириш мажбурий ва ихтиёрий тусда бўлади.

Ўзбекистон Республикасининг сертификатлаштириш органлари (5-модда):

– Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлиги;

– Бир турдаги маҳсулотларни сертификатлаштиришга аккредитация қилинган органлар;

– Синов лабораториялари (марказлари).

Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлиги («Ўзстандарт») Ўзбекистон Республикасининг миллий сертификатлаштириш органидир.

Маҳсулотлар (шу жумладан дастурий ва бошқа илмий-техникавий маҳсулотлар), хизматлар, шунингдек сифат тизимлари сертификатлаштириш объектлари ҳисобланади (6-модда).

Сертификатлаштириш субъектлари — юридик шахслар СМТ доирасида сертификатлаштириш тизимлари тузишлари мумкин. Юридик шахсларнинг сертификатлаштириш тизимлари «Ўзстандарт» агентлиги белгилаган тартибда давлат рўйхатидан ўтказилиши шарт.

Ўзбекистон Республикаси ҳудудида мажбурий сертификатлаштирилиши лозим бўлган маҳсулотлар номлари (жумладан, ахборотни муҳофаза қилишнинг техник ва криптографик воситалари) «Мажбурий сертификатлаштирилиши лозим бўлган маҳсулот турлари рўйхати»да (Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2008 йил 7 май 90-сонли[1] ва 2011 йил 28 апрель 122-сонли[2] қарорлари) келтирилган.

Ахборот хавфсизлиги соҳасида мутахассисларни тайёрлаш, малакасини ошириш ва қайта тайёрлаш тизими.

Ҳозирги куннинг асосий масалаларидан бири бўлиб компьютер жиноятчилиги ва кибертеррорчиликка қарши кураш ҳисобланади. Ахборот технологиялари соҳасидаги жиноятчилик спектри ниҳоятда кенг, у интернет-фирибгарликдан тортиб то болалар порнографияси ва электрон-жосуслик (айғоқчилик) ҳамда террорлик актларга тайёргарлик каби потенциал хавфли ҳаракатларни ўз ичига олади. Тўғри танланган миллий кадрларни тайёрлаш сиёсати орқали ахборот технологиялари соҳасидаги жиноятларнинг ўсишига жиддий тўсқинлик яратиш мумкин.

Мутахассисларни тайёрлаш масаласи, айниқса жуда долзарб ҳисобланади. Чунки ҳозирги кунда компьютер тармоқларини бузишни ва бошқа кибержиноятларни амалга оширишни ўрганиш бўйича ахборотга эга бўлиш жуда осон. Компьютер жиноятчилигини содир этиш технологияси келтирилган босма ва электрон нашрлар эркин тарқатилади (мисол сифатида «Хакер» ва «Спецхакер» журналларини келтириш мумкин). Ҳозирги кунда ихтиёрий ўспирин ахборот тизимларига ҳужум қилишнинг элементар усулларини ўргатувчи китобни сотиб олиши ёки бирор сайтдан кўчириб олиши мумкин. Китобда баён этилган усулларни ўзлаштирган бундай ўспирин компьютер тизим-

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2008. – №19. – 161-м.

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2011. – №18. – 178-м.; 2012. – №38. 436-м.; 2013. – №2. – 24-м.; 2014. – №45. – 548-м.; 2015. – №42. – 534-м.

лари хавфсизлигига таҳдид солувчига айланиши мумкин. Интернетда компьютер бузғунчилигини ўргатувчи кўплаб сайтлар мавжуд. Интернет тармоғида компьютер жиноятчилигини содир этиш бўйича малака алмашишга имкон берувчи форумлар, виртуал конференциялар ўтказилади. Шундай қилиб, компьютер жиноятчилари ўз малакасини ошириш устида фаол иш олиб боришади, ўз қаторига ўсаётган авлодларни жалб қилиб, уларни ўқитишади. Буларнинг барчаси деярли легал равишда амалга оширилмоқда. Бу ҳолатлар долзарб ва муҳим бўлган яна бир масалани ечишни – жиноят оламига ёшларнинг киришига қарши курашиш ва ёшлар орасида тарбиявий ишларни олиб боришнинг самарали усулларини яратиш зарурлигини яна бир бор тасдиқлайди.

Компьютер жиноятчилигини содир этишга қарши иммунитетни ҳосил қилувчи юқори одоб-ахлоқни шакллантириш билан уйғунлашган замонавий ахборот технологияларини ўргатувчи таълим-тарбиянинг усулларини яратиш таълимнинг энг муҳим масалаларидан бири ҳисобланади.

Ҳозирги замон талабларини инобатга олган ҳолда ахборот хавфсизлиги соҳасида кадрлар тайёрлашнинг асосий принципларини қуйидагича ифодалаш мумкин: назарий билимлар даражаси халқаро даражага яқинлашиши керак; маҳаллий шароитларда иш юритишнинг амалий кўникмаларини олишга йўналтириш керак; асосий эътибор хавфсизликни таъминлаш масалаларига қаратилиши керак.

Ахборот хавфсизлиги соҳасида кадрларни тайёрлаш тизимини ривожлантириш энг долзарб муаммолардан бири бўлиб қолмоқда. Бунда кадрлар тайёрлашнинг барча сатҳларини қамраб олиш («вертикаль» бўйича) ҳамда гуманитар соҳада ва табиий–илмий, техник ва гуманитар йўналишлар туташган жойларда ахборот хавфсизлиги муаммоси ҳал этиш («горизонталь» бўйича) зарур. Биринчи навбатда ҳуқуқни муҳофаза қилувчи органларда ва судларда компьютер соҳасидаги жиноятчиликка қарши курашиш бўйича мутахассисларни тайёрлаш лозим.

Ўзбекистон Республикаси Вазирлар Махкамасининг 2002 йил 7 ноябрдаги «Тошкент ахборот технологиялари университети фаолиятини ташкил этиш тўғрисида»ги 385–сонли қарорига[1] мувофиқ бу

[1] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2002. – №21. – 169-м.; 2003. – №4. – 42-м.

университет республиканинг алоқа ва ахборот технологиялари соҳасида кадрлар тайёрлаш, қайта тайёрлаш ва мутахассислар малакасини ошириш бўйича базавий олий таълим муассасаси ҳисобланади.

Ўзбекистон Республикаси Президентининг 2014 йил 24 мартдаги «Тошкент шаҳрида Инха университетини ташкил этиш тўғрисида»ги ПҚ-2155-сонли қарорига[1] асосан халқаро стандартлар даражасидаги ахборот-коммуникация технологиялари соҳасида юқори малакали мутахассисларни тайёрлашни янада такомиллаштириш, шунингдек илғор хорижий олий таълим муассасалари билан ҳамкорликни кенгайтириш мақсадида Тошкент шаҳрида Инха Университети ташкил этилди. Мазкур университетининг асосий фаолият йўналиши этиб:

– ахборот-коммуникация технологиялари соҳасида халқаро стандартларга мос юқори малакали мутахассисларни, биринчи навбатда дастурий таъминотни ишлаб чиқиш, ахборот тизими ва компьютер тармоқларини бошқариш бўйича мутахассисларни тайёрлашни таъминлаш;

– республиканинг олий таълим тизимига ўқув жараёнини замонавий таълим технологиялари асосида ташкил этиш бўйича илғор хорижий тажрибани жорий этиш, очиқ ахборот-таълим муҳитининг ривожланишига кўмаклашиш;

– республикада ахборот-коммуникация технологиялари соҳасида узлуксиз таълим ва малака ошириш тизимини шакллантиришга кўмаклашиш, илмий тадқиқот ва таълим муассасалари, дастурий маҳсулот ишлаб чиқувчилар, ишлаб чиқариш корхоналари, саноат ва инфратузилма тармоқлари ҳамда бошқа замонавий ахборот-коммуникация технологиялари истеъмолчилари ўртасида ўзаро мустаҳкам ҳамкорликни ўрнатиш;

– иқтисодиёт реал сектори тармоқларининг аниқ эҳтиёжларини ҳисобга олган ҳолда ахборот-коммуникация технологиялари соҳасида юқори малакали кадрлар тайёрлашни назарда тутувчи халқаро стандартларга мос мақсадли таълим дастурларини ташкил этиш учун шароит яратиш белгиланган.

Қарорда Тошкент шаҳридаги Инха Университетида мутахассисларини ўқитиш ва тайёрлашнинг асосий йўналишлари этиб компью-

[1] Ўзбекистон Республикаси қонун ҳужжатлари маълумотлари миллий базаси. – www.lex.uz.

тер инжиниринги, дастурий инжиниринг ва компьютер тармоқлари инжиниринги белгиланган.

5.3. Хорижий мамлакатларда ахборотни муҳофаза қилиш тизими

Мамлакатнинг таҳдидларга мос акс таъсир кўрсатиш лаёқатига эга бўлган ахборот хавфсизлик тизимини яратиш учун, ривожланган чет эл мамлакатларида ахборот урушининг замонавий концепциялари, ўзига хос хусусиятлари, ахборот қуролининг турлари ва қўллаш самарадорлиги, шунингдек, чет эл мамлакатларида ахборот хавфсизлигини таъминлаш масалалари қай тарзда ечилиши ҳақида аниқ бир тасаввурга эга бўлиш керак.

Ахборот қуроли деб номланувчи воситалар:

- ахборот массивларини йўқ қилиш, бузиш ёки ўғирлаш;
- ҳимоя тизимларини енгиш;
- қонуний фойдаланувчилар ҳуқуқларини чеклаш;
- компьютер тизимларини, техник воситаларни ишини издан чиқариш;
- шулар каби бошқа амалларни бажаради.

Ҳозирда ҳужумкор ахборот қуролига қуйидагиларни келтириш мумкин:

- кўпайиш, дастурларга кириш, алоқа линиялари, маълумот узатиш тармоғи орқали узатиш, бошқарув тизимини ишдан чиқариш ва шу каби бошқа қобилиятларга эга бўлган компьютер вируслари;
- мантиқий бомба – дастурий ўрнатма қурилмалари, сигнал бўйича ёки аниқ вақтда ҳаракатга келтириш учун ҳарбий ёки фуқаролик инфратузилма ахборот-бошқарув марказларига олдиндан киргизилади;
- телекоммуникация тармоқларида ахборот алмашишини сусайтирувчи, давлат ёки ҳарбий бошқариш каналларида ахборотни сохталаштирувчи воситалар;
- текширувчи дастурларни нейтраллаш воситалари;
- объектнинг дастурий таъминотига рақиб томонидан онгли равишда турли хатоликларни киритиш.

Ахборот қуролини қўллаш оқибатини камайтириш ёки олдини олиш учун қуйидаги чора - тадбирларни кўриш керак:

- ахборот ресурсларини физик асосини ташкил этувчи материал-техник объектларни ҳимоялаш;

- маълумотлар базаси ва банкини нормал ва узлуксиз ишлашини таъминлаш;

- рухсат этилмаган киришлардан, бузиш ёки йўқ қилишдан ахборотларни ҳимоялаш;

- ахборот сифатини (вақтидалигини, аниқлигини, тўлалигини ва фойдалана олишликни) сақлаб қолиш.

Ахборот қуролидан ҳимояловчи дастурий таснифдаги амалий тадбирларга қуйидагилар киради:

1. Халқаро тармоқ орқали турли хил ахборот алмашинувида иқтисодий ва бошқа тузилмаларнинг эхтиёжини башоратлаш ва мониторингини ташкил қилиш. Бунинг учун трансчегара, шу қаторда Интернет орқали ҳам, алмашинувни назорат қилиш учун махсус тузилмаларни яратиш; очиқ тармоқларда ахборот хавфсизлиги таҳдидларини бартараф этиш бўйича давлат ва нодавлат идораларнинг чора-тадбирларини координация қилиш; халқаро ҳамкорликни ташкил этиш мумкин.

2. Ахборот ресурсларининг хавфсизлиги талабларига риоя қилган холда миллий ва корпоратив тармоқларни жаҳон очиқ тармоқларига уланишини таъминловчи ахборот технологияларни такомиллаштириш.

3. Жаҳон ахборот тармоқларида ишлаш учун оммавий фойдаланувчиларни ва ахборот хавфсизлиги бўйича мутахассисларни тайёрлаш ва малакасини ошириш комплекс тизимининг фаолиятини такомиллаштириш.

4. Интернет фойдаланувчиларининг масъулиятлари ва мажбуриятлари, регламент ҳуқуқи ва ахборот ресурслари билан фойдаланиш қоидаларининг миллий қонунчилик қисмини такомиллаштиришни давом эттириш. Жаҳон очиқ тармоқлари ишлашининг норматив-ҳуқуқий таъминотини ва халқаро қонунчилигини ишлаб чиқишда фаол иштирок этиш.

АҚШнинг миллий хавфсизлигини таъминлаш тизими. Миллий хавфсизлик агентлиги (МХА-НБА) – радиоэлектрон тутиб қолиш соҳасида жаҳонда пешқадам хисобланади. Агентликнинг мақсади – техник воситалар ёрдамида АҚШнинг миллий хавфсизлигини таъминлаш.

АҚШнинг ташқи хавфсизлигини таъминлашда Марказий разведка бошқармаси (МРБ-ЦРУ)га асосий ўринлардан бири ажратилган. У ерда бошқа давлатлар томонидан миллий ахборот инфратузилмага

қилинадиган таҳдидлар ҳақидаги ахборотларни қидириш ва қайта ишлаш бўйича разведканинг имкониятларини кенгайтиришга йўналтирилган режа ишлаб чиқилган ва татбиқ қилинган. Агентура ишига оид анъанавий усуллардан ташқари, МРБ техник йўл орқали ёпиқ маълумотлар базасига киришни ва очиқ манбаларнинг таҳлилига катта эътибор қаратади. Кейинги вақтларда МРБ ахборот ва компьютер технологиялари бўйича мутахассисларни, жумладан хакерлар орасидан танлашни амалга оширмоқда.

Федерал текширишлар бюроси (ФТБ-ФБР) ҳам, энг аввало АҚШ инфратузилмасини ҳимоялаш нуқтаи назаридан ахборот уруши доктринасини татбиқ қилишда иштирок этади. АҚШда компьютер жиноятчилигига қарши курашиш мақсадида 1996 йили «Компьютерларни қўллаш орқали фирибгарлик ва суиистеъмол қилишлар тўғрисида»ги федерал қонун қабул қилинган ва ушбу турдаги жиноятчилик билан курашиш бўйича ФТБ таркибида бўлинма ташкил этиш кўзда тутилган. ФТБ телекоммуникация тармоғи орқали амалга ошириладиган айғоқчилик, махфий маълумотларни ошкор қилиш, давлат инстанцияларни алдаш, терроризм, хийла ишлатиш ва фирибгарлик каби нохуш ҳолатларни текшириш билан шуғулланади. Унинг таркибига компьютер жиноятчилиги билан шуғулланувчи еттита бўлинма киради, уларнинг штати 300 кишини ташкил қилади.

АҚШнинг Мудофаа вазирлиги (МВ) халқаро Интернет тармоғининг аждоди ҳисобланиб, биринчи бўлиб мамлакатнинг хавфсизлигига янги таҳдиднинг ва ахборот қуролининг кучини англаб етди ва ҳозирги вақтда ҳарбий соҳада ахборот уруши доктринасини татбиқ қилишда етакчи ўринни эгаллайди. МВ илмий кенгашининг эксперт-лар комиссияси ахборот уруши ҳодисасига қарши ҳарбий телекоммуникация ва компьютер тармоқлари хавфсизлигини таъминловчи шошилинч чораларни қабул қилиш лозимлиги ҳақида доклад тайёрлади. Пентагон ҳарбий автоматлаштирилган ахборот тизимларини «қизил буйруқлар» деб аталувчи заифликка текшириш учун ҳарбий компьютер тармоқларини ҳимоясини таъминлаш билан шуғулланиш мақсадида хакерларни ишга қабул қилади.

Ҳозирги кунда АҚШ идоралари фаолиятидаги умумий тенденция ахборот уруши олиб боришнинг асосий ташкилий ва концептуал принципларини ишлаб чиқиш, ахборот технологияларни қўллаб янги иш усулларини қидириш ҳисобланади.

Буюк Британиядаги ахборотни ҳимоялаш тизими. Буюк Британияда ахборот хавфсизлигини таъминлаш давлат тизимини яратишда ахборот уруши душманнинг ахборот тизимига таъсир этувчи ва бир вақтда мамлакатнинг шахсий тизимларини ҳимояловчи ҳаракатлар деб қаралади.

Буюк Британиянинг Разведка ва хавфсизлик бўйича парлемент комитети Британия махсус хизматлари устидан назорат органи сифатида 1994 йилда ташкил этилган. Бу комитет «Разведка хизматлари тўғрисида»ги қонунга мувофиқ учта махсус хизмат: SIS (Secret Intelligence Service) разведкаси, Махфий хизмат (MI5 - Military Intelligence-5) ва Ҳукумат алоқа маркази томонидан бюджет маблағларининг сарфланишини, бу хизматларнинг бошқарилишини ва уларнинг олиб бораётган сиёсатини назорат қилиш учун тузилган.

SIS/MI6 - Буюк Британиянинг асосий разведка хизмати. SIS Ташқи ишлар вазирлиги (ТИВ) тизимига киритилган бўлиб хорижда 87 та қароргоҳга ва Лондонда штаб-квартирага эга. SISни Бош директор бошқаради ва у бир вақтнинг ўзида Ташқи ишлар вазирининг ўринбосари ҳам ҳисобланади. Шундай қилиб, формал равишда SIS Буюк Британиянинг ТИВ назорати остида ҳисобланади, бироқ, шу билан бирга у тўғридан-тўғри премьер-министрга чиқиши мумкин.

Контрразведка хизмати - MI-5 1909 йилда ички хавфсизликни таъминлаш билан шуғулланувчи махфий хизматлар Бюросининг ички департаменти сифатида тузилган.

Ҳукумат алоқа маркази Буюк Британиянинг махсус хизматлар тизимида радиоайғоқчилик учун жавоб беради. Марказ ТИВ таркибига киритилган бўлиб, ходимларининг сони ва ахборотни топиш ҳажми бўйича мамлакатнинг йирик идораларидан бири ҳисобланади.

Германиянинг ахборотни ҳимоялаш тизими. Ахборот оқимларининг хавфсизлигини таъминлашга масъул координацияловчи ҳукумат органи бўлиб 1991 йилда ташкил этилган Федерал хавфсизлик хизмати (BSI) ҳисобланади. Бу хизмат ахборот техникаси соҳасидаги хавфсизликни таъминлайди. Ҳозирги вақтда BSI фаолиятининг умумий концепцияси НАТО ва ЕС билан яқин ҳамкорликда қуйидаги функцияларни бажарилишини кўзда тутади:

- ахборот технологияларни жорий этишдаги эҳтимолий хавфни баҳолаш;

- миллий коммутация тизимларининг ҳимоялаш даражасини баҳолаш учун критериялар, усуллар ва синов воситаларини ишлаб чиқиш;

- ахборот тизимларининг ҳимояланиш даражасини текшириш ва мувофиқлик сертификатларини бериш;

- муҳим давлат объектларига ахборот тизимларини жорий этиш учун рухсатнома бериш;

- давлат органлари, полиция ва бошқа идораларда ахборот алмашинишда махсус хавфсизлик чораларини амалга ошириш;

- саноат вакилларига маслаҳатлар бериш.

Хавфсизликни таъминловчи бошқа давлат органлари:

- Германиянинг федерал разведка хизмати (Bundesnachrichtendienst -BND). BND федерал канцлер бошқармасига бўйсунадиган бўлинма ҳисобланади. BNDнинг штат таркиби 7000 кишидан зиёдни ташкил этади, улардан 2000га яқини бевосита хорижда разведка маълумотларини йиғиш билан банд. Ходимлар орасида тахминан 70 та турли соҳа вакиллари: ҳарбий хизматчилар, ҳуқуқшунослар, тарихчилар, муҳандислар ва техник мутахассислар мавжуд.

- Конституцияни ҳимоялаш федерал бюроси (Verfassungsschutz - BfV). Ушбу бюро BND ва BSI билан бир қаторда мамлакатнинг учта махсус хизматларидан бири ҳисобланади ва у Германиянинг ички ишлар вазирлигига бўйсинади. Барча федерал ерларда маҳаллий ички ишлар вазирлигига бўйсинадиган ўзининг мос хизматлари мавжуд. Ҳар йили тўпланган ахборотлар асосида Конституцияга риоя этилганлиги доирасидаги иш ҳолати ҳақида ҳукуматга ҳисобот тақдим этилади, унда хулосалар ва тавсиялар қилинади. Ҳукумат, ўз навбатида, аниқ чораларни амалга ошириш кераклиги ҳақида қарор қабул қилади. Ахборотнинг ярмидан кўпини махсус хизмат очиқ манбалардан: оммавий ахборот воситаларида чоп этилган нашрлар, Интернет, мажлис ва митингларда иштирок этиш орқали йиғади. Ахборотнинг бир қисми айрим кишилардан ва бошқа идоралардан келиб тушади.

Францияда ахборотни ҳимоялаш тизими. Франция кибермайдонда ўзининг фуқароларини назорат қилиш бўйича тузилма ташкил этган. Французлар «Эшелон» номли Америка тизимига ўхшаш ўз тизимини яратдилар. У деярли барча хусусий глобал коммуникацияларни тутиб қолишга йўналтирилган.

Миллий хавфсизликни таъминлаш бўйича сиёсатнинг стратегик йўналишларини ишлаб чиқиш билан CLUSIF (Club de la securite informatique francaise) бирлашмаси шуғулланади. У ўзининг статуси бўйича информатика соҳасида ишловчи юридик ва физик шахслар-

нинг очиқ ассоциацияси ҳисобланади. CLUSIF давлат томонидан тўлиқ қўллаб қувватланади ва махсус хизматлар билан яқин алоқага эга.

Францияниng махсус хизмати структураси. Франция разведка уюшмасининг умумий штати, учта ҳар хил вазирликка бўйсинувчи хизматларда ишлайдиган 13 мингга яқин ходимлардан иборат. Учта хизмат Ташқи хавфсизликнинг Бош дирекцияси (DGSE); Ҳарбий разведка бошқармаси (DRM) ва Ҳарбий контрразведка бошқармаси (DPSD) Мудофаа вазирлиги ҳимоясида фаолият олиб боради. Махсус хизматларга жандармерияни (Gendarmerie) ҳам киритиш мумкин. Унинг вазифаларидан бири бўлиб разведка фаолиятини юритиш ҳисобланади – жандармериянинг хар бир қисмида разведка бўлими мавжуд. Иккита махсус хизмат: контрразведка (DST) ва Бош разведка хизмати (RG) Ички ишлар вазирлигига бўйсунган.

Россия Федерацияси (РФ)нинг ахборот хавфсизлигини таъминловчи давлат органлари структураси. Ахборот хавфсизлигининг давлат сиёсатини ишлаб чиқиш, қонунлар, норматив-норматив ҳужжатлар тайёрлаш, ахборотни муҳофаза қилишни таъминлаш бўйича ўрнатилган меъёрларни бажарилиши устидан назоратни давлат органлари амалга оширадилар.

РФ Президенти ахборот хавфсизлигини таъминловчи давлат органларига бошчилик қилади. У Хавфсизлик кенгашини бошқаради ва давлатда ахборот хавфсизлигини таъминлашга доир фармонларни тасдиқлайди.

Мамлакатнинг давлат хавфсизлигига оид бошқа масалалар билан бир қаторда ахборот хавфсизлиги тизимининг умумий бошқарувини РФ Президенти ва Ҳукумати амалга оширади.

РФ Президенти ҳузуридаги Хавфсизлик Кенгаши давлат хавфсизлиги масалалари билан бевосита шуғулланувчи ҳокимият органи ҳисобланади. Хавфсизлик Кенгаши таркибига Ахборот хавфсизлиги бўйича идоралараро комиссия киради. Комиссия давлатнинг ахборот хавфсизлиги соҳасида Президент фармонларини тайёрлайди, қонун чиқариш ташаббуси билан чиқади, вазирлик ва идоралар раҳбарларининг фаолиятини мувофиқлаштиради.

Ахборот хавфсизлиги бўйича идоралараро комиссиянинг ишчи органи бўлиб РФ Президенти ҳузуридаги Давлат техник комиссияси ҳисобланади. Бу комиссия қонун лойиҳаларини тайёрлашни амалга оширади, норматив ҳужжатларни ишлаб чиқади, ахборотни муҳофаза

қилиш воситаларини (криптографик воситалардан ташқари) сертификатлаштиришни ташкил этади, ҳимоя воситаларини ишлаб чиқиш соҳасидаги фаолиятни лицензиялаштиради ва ахборотни муҳофаза қилиш бўйича мутахассисларни ўқитади. Ахборотни муҳофаза қилиш соҳасида изланишлар олиб борувчи давлат илмий-тадқиқот ташкилотлари фаолиятини мувофиқлаштиради. Бу комиссия Давлат сирини ҳимоялаш бўйича идоралараро комиссия ишини ҳам таъминлайди.

Давлат сирини ҳимоялаш бўйича идоралараро комиссиясига давлат сирини ташкил этадиган маълумотлардан фойдаланиш, ахборотни муҳофаза қилиш воситаларини яратиш ҳамда давлат сирини ҳимоялаш бўйича хизмат кўрсатиш билан боғлиқ корхона, муассаса ва ташкилотларни лицензиялашни бошқариш вазифаси юклатилган.

Назорат учун саволлар

- Ахборотни муҳофаза қилишнинг давлат тизими нима?
- Ахборотни муҳофаза қилишнинг давлат тизими иш юритиши қандай қонун, норматив-норматив ҳужжатлар асосида амалга оширилади?
- Ахборотни муҳофаза қилишнинг давлат тизимида кўзланган мақсад нима?
- Ахборотни муҳофаза қилишнинг давлат тизимида кўзланган мақсадни амалга оширишда қандай вазифаларни бажариш керак?
- «Лицензия» ва «Лицензиялаш» тушунчалари нимани англатади ва уларнинг таърифи қайси қонунда берилган?
- Ахборотни криптографик муҳофаза қилиш соҳасидаги фаолият қандай лицензияланади?
- Ахборотни муҳофаза қилишш соҳасидаги фаолиятни лицензиялаш тизимининг норматив-ҳуқуқий базаси нималардан иборат?
- Сертификациялашнинг миллий тизими нима?
- Сертификациялаш нима мақсадда амалга оширилади?
- Ахборот хавфсизлиги соҳасида мутахассисларни тайёрлаш бўйича қандай ишлар олиб борилмоқда?
- Ахборот қуроли қандай амалларни бажаришга йўналтирилган?
- Ахборот қуролидан ҳимояловчи амалий тадбирларга нималар киради?
- АҚШ ва Буюк Британиядаги ахборотни ҳимоялаш тизими ҳақида нималарни биласиз?
- Германия, Франция ва Россияда ахборотни ҳимоялаш тизими қандай ташкил қилинган?

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

Ўзбекистон Республикасининг Конституцияси. – Т., 2014.

Каримов И.А. Хавфсизлик ва барқарор тараққиёт йўлида. Т. 6. – Т., 1998.

Каримов И.А. Хавфсизлик ва тинчлик учун курашмоқ керак. Т. 10. – Т., 2002.

Каримов И.А. Тинчлик ва хавфсизлигимиз ўз куч-қудратимизга, ҳамжиҳатлигимиз ва қатъий иродамизга боғлиқ. Т. 12. – Т., 2004.

Каримов И.А. Мамлакатимизда демократик ислоҳотларни янада чуқурлаштириш ва фуқаролик жамиятини ривожлантириш концепцияси. – Т., 2011.

Каримов И.А. Она юртимиз бахту иқболи ва буюк келажаги йўлида хизмат қилиш – энг олий саодатдир. – Т., 2015.

Ўзбекистон Республикасининг 560-II-сонли «Ахборотлаштириш тўғрисида»ги 2003 йил 11 декабрь қонуни // Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2004. – № 1–2. – 10-м.

Ўзбекистон Республикасининг 848-XII-сонли «Давлат сирларини сақлаш тўғрисида»ги 1993 йил 7 май қонуни // Ўзбекистон Республикаси Олий Кенгашининг ахборотномаси. – 1993. – № 5 – 232-м.

Ўзбекистон Республикасининг 1060-XII-сонли «Электрон ҳисоблаш машиналари учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси тўғрисида»ги 1994 йил 6 май қонуни // Ўзбекистон Республикаси Олий Кенгашининг ахборотномаси. – 1994. – № 5. – 136-м.

Ўзбекистон Республикасининг 1006-XII сонли «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги 1993 йил 28 декабрь қонуни // Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – Т., 1994. – №2. – 50-м.; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2000. – №7-8. – 217-м.; 2003. – №5. – 67-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2006. – №14. – 113-м.; 2006. – №41. – 405-м.; 2013. – №41. – 543-м.; 2014. – №50. – 588-м.; 2016. – №3(I). – 32-м.

Ўзбекистон Республикасининг 71-II-сонли «Фаолиятнинг айрим турларини лицензиялаш тўғрисида»ги 2000 йил 25 май қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2000. №5-6. – 142-м.; 2003. – №1. 8-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – №14. – 110-м.; 2006. – №41. – 405-м.; – 2011. – №36. – 363-м.; – 2013. – №18. – 233-м.; – 2014. – №50. – 588-м.; – 2015. – №33. – 439-м. – №52., – 645-м.

Ўзбекистон Республикасининг 439-II-сонли «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги 2002 йил 12 декабрь қонуни // Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2003. – № 1. – 2-м.

Ўзбекистон Республикасининг 562-II-сонли «Электрон рақамли имзо тўғрисида»ги 2003 йил 11 декабрь қонуни // Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2004. – № 1–2. – 12-м.

Ўзбекистон Республикасининг 611-II-сонли «Электрон ҳужжат айланиши тўғрисида»ги 2004 йил 29 апрель қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2004. – № 20. – 230-м.

Ўзбекистон Республикасининг ЎРҚ–30-сонли «Автоматлаштирилган банк тизимида ахборотни муҳофаза қилиш тўғрисида»ги 2006 йил 4 апрель қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – № 14. – 112-м.

Ўзбекистон Республикасининг ЎРҚ-137-сонли «Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга хилоф ҳаракатлар содир этганлиги учун жавобгарлик кучайтирилгани муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартириш ва қўшимчалар киритиш тўғрисида»ги 2007 йил 25 декабрь қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – № 52. – 532-м.

Ўзбекистон Республикасининг ЎРҚ-342-сонли «Норматив-ҳуқуқий ҳужжатлар тўғрисида»ги (янги таҳрир) 2012 йил 24 декабрь қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. –2012. –№ 52. –583-м.

Ўзбекистон Республикасининг ЎРҚ-373-сонли «Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгартиш ва қўшимчалар киритиш тўғрисида»ги 2014 йил 4 сентябрь қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2014. – № 36. 452-м.

Ўзбекистон Республикасининг ЎРҚ–395-сонли «Электрон ҳукумат тўғрисида»ги 2015 йил 9 декабрь қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2015. – 49-сон. – 611-м.

Ўзбекистон Республикаси Президентининг ПФ-3080-сонли «Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникация технологияларини жорий этиш тўғрисида»ги 2002 йил 30 май фармони // Ўзбекистон Республикаси Олий Мажлисининг ахборотномаси. – 2002. – № 4–5. – 98-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – № 28–29. – 262-м.

Ўзбекистон Республикаси Президентининг ПФ-4702-сонли «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигини ташкил этиш тўғрисида»ги 2015 йил 4 февраль фармони // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2015. – №5. –52-м.

Ўзбекистон Республикаси Президентининг ПҚ-91-сонли «Ахборот технологиялари соҳасида кадрлар тайёрлаш тизимини такомиллаштириш тўғрисида»ги 2005 йил 2 июнь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2005. – № 22. – 157-м.

Ўзбекистон Республикаси Президентининг ПҚ-614 сонли «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги 2007 йил 3 апрель қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – № 14. – 140-м.

Ўзбекистон Республикаси Президентининг ПҚ-1730-сонли «Замонавий ахборот-коммуникация технологияларини янада жорий этиш ва ривожлантириш чора-тадбирлари тўғрисида»ги 2012 йил 21 март қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2012. – № 13.– 139-м.

Ўзбекистон Республикаси Президентининг ПҚ-2042-сонли «Мамлакатимизнинг дастурий таъминот воситалари ишлаб чиқувчиларини рағбатлантиришни янада кучайтириш чора-тадбирлари тўғрисида»ги 2013 йил 20 сентябрь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2013. – № 39. – 508-м.

Ўзбекистон Республикаси Президентининг ПҚ-2155-сонли «Тошкент шаҳрида Инха университетини ташкил этиш тўғрисида»ги 2014 йил 24 март

қарори // Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси – www.lex.uz

Ўзбекистон Республикасида Вазирлар Маҳкамасининг 215-сонли «Электрон рақамли имзодан фойдаланиш соҳасида норматив ҳуқуқий базани такомиллаштириш тўғрисида»ги 2005 йил 26 сентябрь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2005. – № 39. – 297-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 27-сонли «Давлат ахборот ресурслари ҳамда уларни шакллантириш, улардан фойдаланиш ва уларни қўллаб-қувватлаш учун масъул бўлган давлат органлари рўйхатини тасдиқлаш тўғрисида»ги 2006 йил 20 февраль қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – № 8. – 51-м.; 2007. – № 7–8. – 65-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 87-сонли «Давлат ахборот ресурслари ҳамда уларни шакллантириш, улардан фойдаланиш ва уларни қўллаб-қувватлаш учун масъул бўлган давлат органлари рўйхатига ўзгартириш ва қўшимчалар киритиш тўғрисида»ги 2008 йил 7 май қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2008. – № 19. – 159-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 296-сонли «Ўзбекистон Республикаси Президентининг ПҚ-1572-сонли «Миллий ахборот ресурсларини муҳофаза қилишга доир қўшимча чора-тадбирлар тўғрисида»ги 2011 йил 8 июль қарорини амалга ошириш чора-тадбирлари ҳақида»ги 2011 йил 7 ноябрь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2011. – № 45-46. – 472-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 250-сонли «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ҳузуридаги «Электрон ҳукумат» тизимини ривожлантириш маркази ҳамда Ахборот хавфсизлигини таъминлаш маркази фаолиятини ташкил этиш чора-тадбирлари тўғрисида»ги 2013 йил 16 сентябрь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2013. – №38. – 492-м.; – 2015. – №26. – 338-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 355-сонли «Ўзбекистон Республикасида ахборот-коммуникация технологиялари ҳолатини баҳолаш тизимини жорий этиш чора-тадбирлари тўғрисида»ги 2013 йил 31 декабрь қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2014. – № 2. – 17-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 87-сонли «Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги тўғрисидаги низомни тасдиқлаш ҳақида»ги 2015 йил 10 апрель қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2015. – №15. – 178-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг 365-сонли «Жисмоний ва юридик шахслар марказий маълумотлар базаларини шакллантириш ва «Электрон ҳукумат» тизими фойдаланувчиларини идентификациялашнинг ягона ахборот тизимини жорий этиш чора-тадбирлари тўғрисида»ги 2015 йил 17 декабрь қарори //Ўзбекистан Республикаси қонун ҳужжатлари тўплами. – 2015. – №50. – 628-м.

Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В.Кондрашин, М.В. Рудановский. – Брянск, 2007.

*Алферов А. П., Зубов А. Ю., Кузьмин А. С, Черемушкин А. В.*Основы криптографии: Учебное пособие . – М., 2002.

Безбогов А.А. Методы и средства защиты компьютерной информации: Учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов, 2006.

Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлари хавфсизлиги. – Т., 2008.

Гришина Н.В. Организация комплексной системы защиты информации. – М.: 2007.

Гуде С.В., Ревин С.Б. Информационные системы. РЮИ МВД России. 2002.

Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.

Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.

Кабулов Р.К., Абдурахманов Э.С. Ахборот технологиялари соҳасидаги жиноятлар: Ўқув қўлланма. – Т., 2009.

Karimov I.M. va boshqalar. Axborot texnologiyalari: Darslik. – T., 2011.

Karimov I.M. va boshqalar. Informatika: Darslik. – T., 2012.

Каримов И.М., Тургунов Н.А., Кадиров Ф., Самаров Х.К., Иминов А.А., Джаматов М.Х. Ахборот хавфсизлиги асослари: Маърузалар курси. – Т., 2013.

Каримов И.М., Тургунов Н.А. Ахборот технологияларидан амалий машқлар: Ўқув қўлланма. – Т., 2011.

Каримов И.М., Тургунов Н.А. Ахборот хавфсизлиги асослари фанидан амалий машқлар: Ўқув қўлланма. – Т., 2014.

Каторина Ю.Р. Защита информации техническими средствами: Учебное пособие. – СПб., 2012.

Қосимов С.С. Ахборот технологиялари. – Т., 2006.

Левин М. Безопасность в сетях Internet и Intranet. – М., 2001.

Мельников В.П. Информационная безопасность: Учебое пособие. – М., 2005.

Миродова Ш. Проблемы обеспечения информационной безопасности в Республике Узбекистан в условиях глоболизации. – Т., 2008.

Мухаммадиев Ж. Ў. Ахборот хавфсизлиги: муаммо ва ечимлар: Монография. – Т., 2011.

Новые информационные технологии в судебной экспертизе: Учебное пособие / Э.В.Сысоев и др. – Тамбов, 2006.

Общие вопросы технической защиты информации // http://www.intuit.ru.

Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособ. – М.: Гелиос АРВ, 2005.

Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие. – М., 2002.

Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М., 2000.

Соколов А., Степанюк О. Защита от компьютерного терроризма. – СПб., 2002.

Технологии защиты информации в компьютерных сетях // http://www.intuit.ru

Цирлов В. Л. Основы информационной безопасности автоматизированных систем. – М., 2008.

Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. –М., 2004.

Интернет сайтлар ва даврий нашрлар:

http://akadmvd.uz (Ўзбекистон Республикаси ИИВ Академияси)

http://lex.uz (Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси)

http://eduportal.uz (Мультимедия умумтаълим дастурларни ривожлантириш маркази)

http://www.connect.uz (Ўзбекистон умумтаълим портали)

http://uzsci.net (Илмий таълим тармоғи)

http://www.ziyonet.uz (Ахборот таълим тармоғи)

http://www.uzscience.uz (Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги Фан ва технологияларни ривожлантиришни мувофиқлаштириш қўмитаси)

http://www.nuu.uz (Мирзо Улуғбек номидаги Ўзбекистон миллий Университети)

http://www.tsil.uz (Тошкент Давлат Юридик Университети)

http://www.tuit.uz (Тошкент Ахборот технологиялари Университети)

http://www.mitc.uz (Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларни ривожлантириш вазирлиги)

http://**www.infocom.uz** ("Ўзбекистон ахборот технологиялари" журнали).

http://www.cert.uz (Ўзбекистонда компьютер ҳодисаларига чора кўриш хизмати)

http://**www.infosec.uz** (Ахборот хавфсизлигини таъминлаш маркази).

http://www.egovernment.uz (Электрон ҳукумат тизимини ривожлантириш маркази)

http://www.intuit.ru (Интернет-Университет Информационных Технологий).

http://www.twirpx.com/files/informatics/protection/ (Информатика и вычислительная техника/Защита информации)

http://www.crime-research.ru (Центр исследования компьютерной преступности)

http://www.cyber-crimes.ru (Федеральный правовой портал: Компьютерные преступления: квалификация, расследование, профилактика)

МУНДАРИЖА

Каримов Исраил Мирзаевич,
физика-математика фанлари номзоди, катта илмий ходим;

Тургунов Нозимжон Абдуманнопович,
физика-математика фанлари номзоди, доцент

АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ

Дарслик

Муҳаррир **С.С.Қосимов**

Техник муҳаррир **Д. Р. Джалилов**

Босишга рухсат этилди 16. 12. 2016. Нашриёт ҳисоб табағи 6,0.
Адади 30 нусха. Буюртма № . Баҳоси шартнома асосида.

Ўзбекистон Республикаси ИИВ Академияси,
100197, Тошкент шаҳри, Интизор кўчаси, 68.