ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ИЧКИ ИШЛАР ВАЗИРЛИГИ

А К А Д Е М И Я

АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ

(Маърузалар курси)

Тошкент – 2013

Ўзбекистон Республикаси ИИВ Академиясининг
Таҳририят-ноширлик ҳайъатида маъқулланган

Муаллифлар жамоаси:

физика-математика фанлари номзоди, катта илмий ходим **И. М. Каримов;**
физика-математика фанлари номзоди, доцент **Н. А. Тургунов;**
техника фанлари номзоди, доцент **Ф. Кадиров;**
техника фанлари номзоди, доцент **Х.К. Самаров**
физика-математика фанлари номзоди **А. А. Иминов;**
физика-математика фанлари номзоди **М. Х. Джаматов**

Тақризчилар:

Тошкент Ахборот технологиялари университети ахборот хавфсизлиги кафедраси мудири, техника фанлари номзоди **С.Ю. Юсупов;**

Ўзбекистон Республикаси ИИВ Ахборот маркази бошлиғи **А.Х.Хакимов**

А-95 **Ахборот хавфсизлиги асослари:** Маърузалар курси / физика-математика фанлари номзоди, катта илмий ходим И.М.Каримовнинг умумий таҳрири остида. – Т.: Ўзбекистон Республикаси ИИВ Академияси, 2013. – 131 б.

Маърузалар курси ахборот хавфсизлигини таъминлашнинг назарий асослари, асосий тушунчалари, ташкилий ва бошқарув тамойиллари тўғрисидаги билимларни шакллантириш, Ўзбекистон Республикасида ахборотни муҳофаза қилишнинг давлат тизимининг ташкилий асослари ва вазифаларини ўрганиш, тингловчиларга ахборот хавфсизлиги ва маълумотларни муҳофаза қилиш соҳасидаги халқаро тажриба, ахборот хавфсизлигини таъминлашнинг усул ва воситалари ҳамда маълумотларни муҳофаза қилишнинг комплекс тизимлари билан таништириш, шахс, жамият ва давлатнинг ахборот хавфсизлиги, давлат органларининг ахборот хавфсизлигини таъминлаш соҳасидаги асосий фаолият йўналишлари, ахборот хавфсизлигининг объектлари, таҳдидлар ва уларнинг манбалари, ахборотларни криптографик ва техник ҳимоялаш асослари, ахборотларни муҳофаза қилишнинг ташкилий чора-тадбирлари, маълумотларни муҳофаза қилиш ва ахборот хавфсизлигини таъминлашнинг усул ва воситалари, маълумотларнинг чиқиб кетиш каналлари ва уларнинг олдини олиш йўллари ҳақида назарий билимларни чуқурлаштириш имконини беради.

ИИВ Академияси тингловчиларига, профессор-ўқитувчиларга, тадқиқотчиларга ҳамда ҳуқуқни муҳофаза қилиш идоралари ва бошқа турдош соҳаларда фаолият юритаётган мутахассисларга мўлжалланган.

ББК 73я73

«*Фуқароларнинг ахборот соҳасидаги ҳуқуқ ва эркинликларини таъминлаш масаласи инсоннинг ахборот олиш, ахборотни ва ўз шахсий фикрини тарқатиш ҳуқуқи ва эркинлигини ўзида мужассам этган бўлиб, бу Ўзбекистонда демократик жамият асосларини барпо этишнинг муҳим шарти, таъбир жоиз бўлса, тамал тоши ҳисобланади*»[1].

Ислом Каримов

КИРИШ

Маълумки, ҳар қандай давлатнинг ахборот ресурслари унинг иқтисодий ва ҳарбий салоҳиятини белгиловчи омилларидан бири ҳисобланади. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантирилишини таъминлайди. Бундай жамиятда, ахборот алмашинув тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот-коммуникациялар технологияларини қўллаш кенг кўламда амалга оширилади.

Ахборотлашган жамият тезлик билан шаклланиб бормоқда. Ахборот дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда.

Ҳудудий жойлашишидан қатъи назар, кундалик ҳаётимизга турли хилдаги ахборотлар Internet халқаро компьютер тармоғи орқали кириб келди. Шунинг учун ҳам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва ўзгартириш, йўқотиш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди.

Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳон

---

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

тамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратишга қаратилган[1].

«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»[2]. Дарҳақиқат, 2002 йил 12 декабрда қабул қилинган бу қонунда[3] ахборот хавфсизлигини таъминлаш соҳасидаги давлат сиёсати ахборот соҳасидаги ижтимоий муносабатларни тартибга солишга қаратилган бўлади ҳамда шахс, жамият ва давлатнинг ахборот борасидаги хавфсизлигини таъминлаш соҳасида давлат ҳокимияти ва бошқарув органларининг асосий вазифалари ҳамда фаолият йўналишларини белгилайди деб белгиланган.

Компьютер тизимлари ва тармоқларида ахборотни муҳофаза қилиши деганда, узатилаётган, сақланаётган ва қайта ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш мақсадида турли восита ва усулларни қўллаш, чораларни кўриш ва тадбирларни амалга оширишни тушуниш қабул қилинган.

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

Ушбу маърузалар курси тингловчилар ва ҳуқуқни муҳофаза қилиш идоралари ходимларига ахборот хавфсизлигини таъминлашга оид назарий билимларни, ахборот тизимларида ахборотни муҳофаза қилишни ташкил этишнинг ташкилий, ҳуқуқий, техник, криптографик, аппарат-дастурий усулларини қўллашга оид зарур билимларни эгаллаш имконини беради.

---

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

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

[3] Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2003. – №1. – 2-м.

I. АХБОРОТ ХАВФСИЗЛИГИ ВА АХБОРОТНИ МУҲОФАЗА ҚИЛИШ

1.1. Ахборотни муҳофаза қилиш, ахборот хавфсизлиги ва унинг замонавий концепцияси.

1.2. Ахборот хавфсизлигига таҳдид ва унинг турлари.

1.3. Ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича меъёрий-ҳуқуқий ҳужжатлар. Ахборотни муҳофаза қилиш соҳасида халқаро стандартлар.

Ҳар қандай тараққий этган жамият ҳаётида ахборотнинг аҳамияти узлуксиз ортиб бормоқда. Узоқ ўтмишдан давлатнинг ҳарбий-стратегик аҳамиятига молик бўлган маълумотлар қатъий сир тутилган ва ҳимояланган. Ҳозирги вақтда ишлаб чиқариш технологияларига ва маҳсулотларни сотишга тегишли ахборот товар кўринишига эга бўлиб, ички ва ташқи бозорда унга бўлган талаб ортиб бормоқда. Ахборот технологиялари автоматлаштириш ва ахборотни муҳофаза қилиш йўналишларида мунтазам мукаммаллашиб бормоқда.

Замонавий ахборот технологияларининг тараққиёти саноат шпионажи, компьютер жиноятчилиги, конфеденциал маълумотларга рухсатсиз кириш, ўзгартириш, йўқотиш каби салбий ҳодисалар билан биргаликда кузатилмоқда. Шунинг учун ахборотни муҳофаза қилиш ҳар қандай мамлакатда муҳим давлат вазифаси ҳисобланади. Ўзбекистонда ахборотни муҳофаза қилишнинг зарурияти ахборотни муҳофаза қилишнинг давлат тизими яратилишида ва ахборот хавфсизлигининг ҳуқуқий базасини ривожлантиришда ўз ифодасини топмоқда. «Ахборотлаштириш тўғрисида», «Давлат сирларини сақлаш тўғрисида», «Электрон ҳисоблаш машиналари дастурлари ва маълумотлар базаларини ҳуқуқий ҳимоя қилиш тўғрисида» ва бошқа қонунлар ҳамда бир қатор Ҳукумат қарорлари қабул қилинди ва амалга татбиқ этилди.

Ахборотни муҳофаза қилиш ахборотни ихтиёрий кўринишда йўқотишда (ўғирлаш, бузиш, қалбакилаштириш) кўриладиган зарарнинг олдини олишни таъминлаши лозим. Ахборотни муҳофаза қилиш чоралари ахборот хавфсизлигига оид амалдаги қонун ва меъёрий ҳужжатлар асосида ва ахборотдан фойдаланувчиларнинг манфаатларига кўра ташкил этилиши зарур. Юқори даражада

ахборотни муҳофаза қилишни кафолатлаш учун мунтазам равишда мураккаб илмий-техник вазифаларни ҳал этиш ва ҳимоя воситаларини такомиллаштириш талаб этилади.

1.1. Ахборотни муҳофаза қилиш, ахборот хавфсизлиги ва унинг замонавий концепцияси

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги №439-II сонли «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонунида[1] ахборот ва унинг турлари тўғрисида қуйидаги таърифлар келтирилган:

ахборот – манбалари ва тақдим этилиш шаклидан қатъи назар шахслар, предметлар, фактлар, воқеалар, ҳодисалар ва жараёнлар тўғрисидаги маълумотлар;

ахборотни муҳофаза этиш – ахборот борасидаги хавфсизликка таҳдидларнинг олдини олиш ва уларнинг оқибатларини бартараф этиш чора-тадбирлари;

оммавий ахборот – чекланмаган доирадаги шахслар учун мўлжалланган ҳужжатлаштирилган ахборот, босма, аудио, аудиовизуал ҳамда бошқа хабарлар ва материаллар;

ҳужжатлаштирилган ахборот – идентификация қилиш имконини берувчи реквизитлари қўйилган ҳолда моддий жисмда қайд этилган ахборот;

махфий ахборот – фойдаланилиши қонун ҳужжатларига мувофиқ чеклаб қўйиладиган ҳужжатлаштирилган ахборот. Ушбу таъриф Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Ўзбекистон Республикаси Президентининг «Миллий ахборот ресурсларини муҳофаза қилишга доир қўшимча чора-тадбирлар тўғрисида» 2011 йил 8 июлдаги ПҚ–1572-сон қарорини амалга ошириш чора-тадбирлари ҳақида»ги 2011 йил 7 ноябрь 296-сонли қарорида қуйидагича ифодаланган: *махфий ахборот* – Ўзбекистон Республикаси қонун ҳужжатларига мувофиқ фойдаланиш чекланган, давлат сирларига мансуб ахборот мавжуд бўлмаган ҳужжатлаштирилган ахборот[2].

---

[1] Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2003. – №1. – 2-м.

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2011. – №45-46. – 472-м.

Конфеденциал ахборот – ҳужжатлаштирилган ахборот, ундан фойдаланиш қонун ҳужжатларига мувофиқ чегараланади[1].

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, конфеденциал ёки номахфий бўлиши мумкин.

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 тоифалари 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».

---

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

[2] Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – Т., 1993. – №5. – 232-м.

Ахборот хавфсизлиги тушунчаси, унинг ташкил этувчилари тавсифи. Ахборот хавфсизлиги деганда табиий ёки сунъий характердаги тасодифий ёки қасддан қилинган таъсирлардан ахборот ва уни қўллаб-қувватлаб турувчи инфрастуктуранинг ҳимояланганлиги тушунилади. Бундай таъсирлар ахборот соҳасидаги муносабатларга, жумладан, ахборот эгаларига, ахборотдан фойдаланувчиларга ва ахборотни муҳофаза қилишни қўллаб қувватловчи инфраструктурага жиддий зарар етказиши мумкин.

Ўзбекистон Республикасининг 2002 йил 12 декабрдаги №439-II сонли «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонунида[1] ахборот хавфсизлиги *ахборот борасидаги хавфсизлик* деб белгиланган ва у ахборот соҳасида шахс, жамият ва давлат манфаатларининг ҳимояланганлик ҳолатини англатади.

Ахборот соҳасида *шахс манфаатлари* фуқароларнинг ахборотдан фойдаланишга доир конституциявий ҳуқуқларини амалга ошишида, қонунда тақиқланмаган фаолият билан шуғулланишида ҳамда жисмоний, маънавий ва интеллектуал ривожланишда ахборотлардан фойдаланишларида, шахсий хавфсизликни таъминловчи ахборот ҳимоясида намоён бўлади.

Ахборот соҳасида *жамият манфаатлари* бу соҳада шахс манфаатларини таъминлашда, демократияни мустаҳкамлашда, ижтимоий ҳуқуқий давлатни қуришда, ижтимоий ҳамжиҳатликни қўллаб-қувватлашда ўз аксини топади.

Ахборот соҳасида *давлат манфаатлари* миллий ахборот инфраструктурасининг ривожланишига шароитлар яратишда, ахборот олиш соҳасида шахс ва фуқароларнинг конституциявий ҳуқуқ ва эркинликларини амалга ошишида, Ўзбекистоннинг ҳудудий бирлигини, суверенитетини ва конституциявий тузумининг мустаҳкамлигини, сиёсий, иқтисодий ва ижтимоий барқарорлигини таъминлаш мақсадида ахборотдан фойдаланишда, қонунийлик ва ҳуқуқ тартиботни қатъий амалга ошишида, ўзаро тенглик ва ўзаро манфаатдорликдаги халқаро ҳамкорликни ривожлантиришда ифодаланади.

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

---

[1] Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2003. – №1. – 2-м.

Бугунги кунда ахборот хавфсизлигини таъминлайдиган учта асосий тамойил мавжуд:

– *маълумотлар бутунлиги* – ахборотни йўқотилишига олиб келувчи бузилишлардан, шунингдек маълумотларни муаллифлик ҳуқуқи бўлмаган ҳолда ҳосил қилиш ёки йўқ қилишдан ҳимоя қилиш;

– ахборотнинг *конфеденциаллиги*. Ахборот ва унинг ташувчисининг ҳолатини белгилайди ва унда ахборот билан рухсатсиз танишишнинг ёки уни рухсатсиз ҳужжатлаштиришнинг (нусха кўчиришнинг) олдини олиш таъминланган бўлади;

– фойдаланиш ҳуқуқларига (муаллифликка) эга барча фойдаланувчилар ахборотдан *фойдалана олишлик*лари.

Таъкидлаш жоизки, айрим фаолият соҳалари (банк ва молия институтлари, ахборот тармоқлари, давлат бошқарув тизимлари, мудофаа ва махсус тузулмалар) уларда кўриладиган масалаларнинг муҳимлиги ва характерига кўра, уларнинг ахборот тизимлари фаолияти ишончлилигига нисбатан юқори талаблар ва хавфсизлик бўйича махсус чоралар кўрилишини талаб этади.

Ахборот хавфсизлигининг миллий хавфсизлик тизимидаги ўрни. XXI асрда шахс, жамият ва давлат тараққиётида ахборот ресурслари ва технологияларининг ролини ортиши натижасида Ўзбекистонда 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, балки хавфсизлик соҳасидаги барча хавфсизлик объектларининг асосий элементлари ҳамдир;

– 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 бутунликка бириктиради. Бу эса ахборот хавфсизлигининг роли ва унинг мамлакат миллий хавфсизлиги тизимидаги мавқеини белгилайди. Ахборот соҳасидаги Ўзбекистоннинг миллий манфаатларини, уларга эришишнинг 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 ҳамда 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 рухсатсиз 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 ҳимояланганлиги;

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

Ахборотни муҳофаза қилиш – ахборот хавфсизлигининг (маълумотларнинг бутунлиги, фойдалана олиш ва зарур бўлганда, маълумотларни киритиш, сақлаш, қайта ишлаш ва узатишда фойдаланилувчи ахборот ва унинг захиралари конфеденциаллиги) муҳим жиҳатларини таъминлашга йўналтирилган тадбирлар мажмуидир.

Хавфсиз тизимда тегишли аппарат ва дастурий воситалардан фойдаланиб, ахборотни ўқиш, ёзиш, ҳосил қилиш ва ўчириш ҳуқуқига эга шахслар ёки улар номидан амалга оширадиган жараёнлар орқали ахборотдан фойдалана олиш бошқарилади.

Маълумки, абсолют хавфсиз тизимлар мавжуд эмас, лекин «ишониш мумкин бўлган тизим» маъносидаги ишончли тизимлардан фойдаланилади. Етарлича аппарат ва дастурий воситалардан фойдаланиб, бир вақтнинг ўзида турли махфийлик даражасидаги маълумотларни фойдаланувчилар гуруҳи томонидан фойдаланиш ҳуқуқларини бузмаган ҳолда қайта ишлаш имконини берувчи тизим ишончли ҳисобланади.

Ишончлиликни баҳоловчи асосий мезонлар – бу хавфсизлик сиёсати ва кафолатланганлик.

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.

Кафолатланганлик ҳимоянинг пассив қисми бўлиб, тизимдан фойдаланишда унга бўлган ишонч даражасини ифодалайди.

Ишончли тизимда хавфсизликка тааллуқли барча жараёнлар рўйхатга олиб борилиши керак.

Ахборотни муҳофаза қилиш тушунчаси ахборот хавфсизлиги тушунчаси билан чамбарчас боғлиқ.

Тор маънода ахборотни муҳофаза қилиш деганда ахборотни йиғиш, узатиш, қайта ишлаш ва сақлаш жараёнида унинг хавфсизлиги (конфеденциаллиги ва бутунлиги)ни таъминлашга қаратилган тадбирлар ва ҳаракатлар мажмуи тушунилади. Бу таъриф ахборотни муҳофаза қилиш ва ахборот хавфсизлиги тушунчаларининг бир-бирига яқин эканлигини билдиради.

Ахборот хавфсизлиги – бу узатилувчи, йиғилувчи ва сақланувчи ахборотнинг хусусияти (ҳолати) бўлиб, унинг ташқи муҳит (инсон ва табиат) ва ички таҳдидлардан ҳимояланганлик даражасини характерлайди.

Ахборотни муҳофаза қилиш кенг маънода ахборот хавфсизлигига таҳдидни олдини олиш ва уларнинг асоратларини йўқ қилишга

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

қаратилган ташкилий, ҳуқуқий ва техник чоралар комплексини билдиради.

Ахборотни муҳофаза қилиш ахборотга бўлган салбий таъсир манбаларини ҳамда сабаб ва шароитларни аниқлаш ва бартараф этиш маъносини англатади. Бу манбалар ахборот хавфсизлигига таҳдидларни ташкил этади.

Ахборотни муҳофаза қилиш қуйидагиларга йўналтирилган:

– ахборот хавфсизлигини таъминлаш бўйича таҳдидларнинг олдини олиш;

– тизимли таҳлил ва назорат орқали реал ва эҳтимоли катта бўлган таҳдидларни аниқлаш ва уларни ўз вақтида олдини олиш чоралари;

– аниқ таҳдидлар ва жиноий ҳаракатларни аниқлаш мақсадида таҳдидларни топиш;

– жиноий ҳаракатларни бартараф этиш, шунингдек аниқ жиноий ҳаракатларни ҳамда таҳдидларни йўқ қилиш бўйича чоралар кўриш;

– таҳдид ва жиноий ҳаракатларнинг оқибатларини йўқ қилиш ва мавқеини сақлаш.

Ушбу барча усулларнинг мақсади ахборот ресурсларини ноқонуний таҳдидлардан ҳимоя қилиш ва қуйидагиларни таъминлашдан иборат:

– конфеденциал ахборотларнинг тарқаб кетишини олдини олиш;

– конфеденциал ахборот манбаларига ноқонуний киришни тақиқлаш;

– ахборотнинг бутунлиги, тўлиқлиги ва ундан фойдалана олишни сақлаш;

– ахборот конфеденциаллигига риоя қилиш;

– муаллифлик ҳуқуқларини таъминлаш.

Юқоридагиларни эътиборга олиб, ахборотни муҳофаза қилиш деганда давлат, жамият ва шахсларнинг ахборот хавфсизлигини таъминлашга йўналтирилган усул, восита ва чоралар мажмуини тушуниш мумкин.

1.2.Ахборот хавфсизлигига таҳдид ва унинг турлари

Ахборотни муҳофаза қилишнинг мақсади ва концептуал асослари. Умуман олганда *ахборотни муҳофаза қилишнинг мақсади*ни қуйидагича ифодалаш мумкин:

– ахборотни тарқаб кетиши, ўғирланиши, бузилиши, қалбакилаштирилишини олдини олиш;

– шахс, жамият, давлатнинг хавфсизлигига таҳдидни олдини олиш;

– ахборотни йўқ қилиш, модификациялаш, бузиш, нусха олиш, блокировка қилиш каби ноқонуний ҳаракатларнинг олдини олиш;

– ахборот ресурслари ва ахборот тизимларига ноқонуний таъсир қилишнинг бошқа шаклларини олдини олиш, ҳужжатлаштирилган ахборотга шахсий мулк объекти сифатида ҳуқуқий режимни таъминлаш;

– ахборот тизимида мавжуд бўлган шахсий маълумотларнинг махфийлигини ва конфеденциаллигини сақлаш орқали фуқароларнинг конституциявий ҳуқуқларини ҳимоялаш;

– давлат сирларини сақлаш, қонунчиликка асосан ҳужжатлаштирилган ахборотлар конфеденциаллигини таъминлаш;

– ахборот жараёнларида ҳамда ахборот тизимлари, технологиялари ва уларни таъминлаш воситаларини лойиҳалаш, ишлаб чиқиш ва қўллашда субъектларнинг ҳуқуқларини таъминлаш.

Ахборотни муҳофаза қилишнинг самарадорлиги унинг ўз вақтидалиги, фаоллиги, узлуксизлиги ва комплекслиги билан белгиланади. Ҳимоя тадбирларини комплекс тарзда ўтказиш ахборотни тарқаб кетиши мумкин бўлган хавфли каналларни йўқ қилишни таъминлайди. Маълумки, биргина очиқ қолган ахборотни тарқаб кетиш канали бутун ҳимоя тизимининг самарадорлигини кескин камайтириб юборади.

Ахборотни муҳофаза қилиш соҳасидаги ишлар ҳолатининг таҳлили шуни кўрсатадики, муҳофаза қилишнинг тўлиқ шаклланган концепцияси ва тузилиши ҳосил қилинган, унинг асосини қуйидагилар ташкил этади:

– саноат асосида ишлаб чиқилган, ахборотни муҳофаза қилишнинг ўта такомиллашган техник воситалари;

– ахборотни муҳофаза қилиш масалаларини ҳал этишга ихтисослаштирилган ташкилотларнинг мавжудлиги;

– ушбу муаммога оид етарлича аниқ ифодаланган қарашлар тизими;

– етарлича амалий тажриба ва бошқалар.

Бироқ, хорижий матбуот хабарларига кўра маълумотларга нисбатан жиноий ҳаракатлар камайиб бораётгани йўқ, аксинча барқарор ўсиш тенденциясига эга бўлиб бормоқда.

Ҳимояланган ахборотга таҳдидлар тушунчаси ва унинг тузилиши. Умумий йўналишга кўра ахборот хавфсизлигига таҳдидлар қуйидагиларга бўлинади:

– Ўзбекистоннинг маънавий равнақи соҳаларида, маънавий ҳаёт ва ахборот фаолиятида фуқароларнинг конституциявий ҳуқуқлари ва эркинликларига таҳдидлар;

– мамлакатнинг ахборотлаштириш, телекоммуникация ва алоқа воситалари индустриясини ривожланишига, ички бозор талабларини қондиришга, унинг маҳсулотларини жаҳон бозорига чиқишига, шунингдек маҳаллий ахборот ресурсларини йиғиш, сақлаш ва самарали фойдаланишни таъминлашга нисбатан таҳдидлар;

– Республика ҳудудида жорий этилган ҳамда яратилаётган ахборот ва телекоммуникация тизимларининг меъёрида ишлашига, ахборот ресурслари хавфсизлигига таҳдидлар.

Ахборот ҳисоблаш тизимларида ахборот хавфсизлигини таъминлаш нуқтаи назаридан ўзаро боғлиқ бўлган учта ташкил этувчини кўриб чиқиш мақсадга мувофиқ:

1) ахборот;

2) техник ва дастурий воситалар;

3) хизмат кўрсатувчи персонал ва фойдаланувчилар.

Ҳар қандай ахборот ҳисоблаш тизимларини ташкил этишдан мақсад фойдаланувчиларнинг талабларини бир вақтда ишончли ахборот билан таъминлаш ҳамда уларнинг конфеденциаллигини сақлаш ҳисобланади. Бунда ахборот билан таъминлаш вазифаси ташқи ва ички рухсат этилмаган таъсирлардан ҳимоялаш асосида ҳал этилиши зарур.

Ахборот тарқаб кетишига конфеденциал маълумотнинг ушбу ахборот ишониб топширилган ташкилотдан ёки шахслар доирасидан назоратсиз ёки ноқонуний тарзда ташқарига чиқиб кетиши сифатида қаралади.

Таҳдиднинг учта кўриниши мавжуд.

1. Конфеденциалликнинг бузилишига таҳдид шуни англатадики, бунда ахборот унга рухсати бўлмаганларга маълум бўлади. Бу ҳолат конфеденциал ахборот сақланувчи тизимга ёки бир тизимдан иккинчисига узатилаётганда ноқонуний фойдалана олишликни қўлга киритиш орқали юзага келади.

2. Бутунликни бузишга таҳдид ҳисоблаш тизимида ёки бир тизимдан иккинчисига узатилаётганда ахборотни ҳар қандай қасддан ўзгартиришни ўзида мужассамлайди. Жиноятчилар ахборотни қасддан ўзгартирганда, бу ахборот бутунлиги бузилганлигини билдиради. Шунингдек, дастур ва аппарат воситаларнинг тасодифий хатоси туфайли ахборотга ноқонуний ўзгаришлар киритилганда ҳам ахборот бутунлиги бузилган ҳисобланади. Ахборот бутунлиги – ахборотнинг бузилмаган ҳолатда мавжудлигидир.

3. Хизматларнинг издан чиқиш таҳдиди ҳисоблаш тизими ресурсларида бошқа фойдаланувчилар ёки жиноятчилар томонидан атайлаб қилинган ҳаракатлар натижасида фойдалана олишлиликни блокировка бўлиб қолиши натижасида юзага келади. Ахборотдан фойдалана олишлилик – ахборот айланувчи, субъектларга уларни қизиқтирувчи ахборотларга ўз вақтида қаршиликларсиз киришини таъминлаб берувчи ҳамда ихтиёрий вақтда мурожаат этилганда субъектларнинг сўровларига жавоб берувчи автоматлаштирилган хизматларга тайёр бўлган тизимнинг хусусиятидир.

Ахборот хавфсизлигига таҳдидларнинг тоифаланиши. Ахборот хавфсизлигига таҳдидлар даражасига кўра қуйидагича тоифаланиши мумкин:

а) шахс учун:

– ахборотларни қидириш, олиш, узатиш, ишлаб чиқиш ва тарқатиш бўйича фуқароларнинг конституциявий ҳуқуқлари ва эркинликларини бузилиши;

– фуқароларни шахсий ҳаёт дахлсизлиги ҳуқуқидан маҳрум қилиш;

– ғайриихтиёрий зарарли ахборотлардан фуқароларнинг ўз соғлиқларини ҳимоя қилиш ҳуқуқлари бузилиши;

– интеллектул мулк объектларига таҳдид.

б) жамият учун:

– ахборотлаштирилган жамиятни қуришга тўсиқлар;

– жамиятнинг маънавий янгиланиш, унинг маънавий бойликларини сақлаш, фидойилик ва холислик, мамлакатнинг кўп асрлик маънавий анъаналарини ривожлантириш, миллий, маданий меросни тарғиб қилиш, ахлоқ меъёрлари ҳуқуқларидан маҳрум қилиш;

– замонавий телекоммуникация технологияларини тараққий этиши, мамлакат илмий ва ишлаб чиқариш потенциалини ривожлантириш ва сақлаб қолишга қаршилик қилувчи муҳитни яратиш.

в) давлат учун:

– шахс ва жамият манфаатлари ҳимоясига қарши ҳаракатлар;

– ҳуқуқий давлат қуришга қаршилик;

– давлат бошқарув органлари устидан жамоат назорати институтларини шакллантиришга қарши ҳаракатлар;

– шахс, жамият ва давлат манфаатларини таъминловчи давлат бошқарув органлари томонидан қарорларни тайёрлаш, қабул қилиш ва татбиқ этиш тизимини шакллантиришга қаршилик;

– давлат ахборот тизимлари ва давлат ахборот ресурслари ҳимоясига тўсиқлар;

– мамлакат ягона ахборот муҳити ҳимоясига қарши ҳаракатлар.

Ахборот ҳимоясига методологик ёндашув – бу конфеденциал ахборотларни сақлаш вазифасини турли босқичларда ечиш бўйича асос бўлувчи ғоялар, муҳим тавсиялардир. Улар ахборотни меъёрий ҳимоя қилиш базаларини яратишда инобатга олинади. Шунингдек, қонун ва қонуности актларини қабул қилишда меъёр сифатида татбиқ қилинади ҳамда уларни бажариш мажбурий характерга эга бўлади.

Ахборотни муҳофаза қилиш тамойилларини учта гуруҳга бўлиш мумкин: ҳуқуқий, ташкилий ҳамда техник разведкадан ҳимояланишда ва ҳисоблаш техникаси воситаларида ахборотга ишлов беришда ахборотни муҳофаза қилишдан фойдаланиш.

Ахборотни муҳофаза қилиш тизимларидан фойдаланиш амалиёти шуни кўрсатмоқдаки, фақатгина комплекс ахборотни муҳофаза қилиш тизимлари самарали бўлиши мумкин. Унга қуйидаги чора-тадбирлар киради:

1. Қонунчилик. Ахборот ҳимояси соҳасида юридик ва жисмоний шахсларнинг, шунингдек давлатнинг ҳуқуқ ва мажбуриятларини қатъий белгиловчи қонуний актлардан фойдаланиш.

2. Маънавий-этик. Объектда қатъий белгиланган ўзини тутиш қоидаларининг бузилиши кўпчилик ходимлар томонидан кескин салбий баҳоланиши жорий этилган муҳитни ҳосил қилиш ва қўллаб қувватлаш.

3. Физик. Ҳимояланган ахборотга бегона шахсларнинг киришини тақиқловчи физик тўсиқлар яратиш.

4. Маъмурий. Тегишли махфийлик режими, кириш ва ички режимларни ташкил этиш.

5. Техник. Ахборотни муҳофаза қилиш учун электрон ва бошқа ускуналардан фойдаланиш.

6. Криптографик. Ишлов берилаётган ва узатилаётган ахборотларга ноқонуний киришни олдини олувчи шифрлаш ва кодлашни татбиқ этиш.

7. Дастурий. Фойдалана олишлиликни чегаралаш учун дастур воситаларини қўллаш.

Физик, аппаратли, дастурли ва ҳужжатли воситаларни ўз ичига олувчи барча ахборот ташувчиларга комплекс ҳолда *ҳимоя объекти* сифатида қаралади.

Одатда, сўнгги вақтларда ахборотдан фойдаланиш, сақлаш, узатиш ва қайта ишлашда турли кўринишдаги ахборот тизимларида амалга оширилмоқда.

Ахборот тизими – бу одатда матнли ёки график ахборотларни йиғиш, сақлаш, қидириш ва қайта ишлашга мўлжалланган амалий дастурий, баъзан эса аппарат-дастурий нимтизимдир.

Маълумотларнинг ахборот тизимида мавжуд бўлишининг моддий асоси бу электрон ва электрон-механик қурилмалар, шунингдек ахборот ташувчилардир.

Ахборот ташувчилари сифатида қоғоз, магнит ва оптик ташувчилар, электрон схемалар фойдаланилиши мумкин.

Демак, қурилма ва нимтизимларни ҳамда ахборот ташувчиларини ҳимоя қилиш зарур.

Турли ахборот тизимларида фойдаланувчилар хизмат кўрсатувчи персонал ҳисобланиб, ахборот манбаи ва ташувчилари бўлиши мумкин.

Шунинг учун ҳимоя объекти тушунчаси кенг маънода талқин этилади. Ҳимоя объекти деганда нафақат ахборот ресурслари, аппарат ва дастурий воситалар, хизмат кўрсатувчи персонал ва фойдаланувчилар, балки бино ҳамда у жойлашган ҳудуд ҳам тушунилади.

Ахборотни муҳофаза қилишнинг асосий *объектлари*га қуйидагилар киради:

– давлат сирлари билан боғлиқ ва конфеденциал маълумотларни ўзида сақловчи ахборот ресурслари;

– воситалар ва ахборот тизимлари (ҳисоблаш техникаси воситалари, тармоқлар ва тизимлар), дастурий воситалар (операцион тизимлар, маълумотлар базаларини бошқариш тизимлари, амалий дастурий таъминот), автоматлаштирилган бошқарув тизимлари, алоқа ва маълумотларни узатиш тизимлари, рухсати чегараланган ахборотни қабул қилиш, узатиш ва қайта ишлаш техник воситалари (овоз ёзиш, овоз кучайтириш, овоз эшитиш, сўзлашув ва телевизион қурилмалар, ҳужжатларни тайёрлаш, кўпайтириш воситалари ҳамда бошқа график, матн ва ҳарфли-рақамли маълумотларни қайта ишлаш воситалари), конфеденциал ва давлат сирлари тоифасига оид бевосита қайта ишловчи тизим ва воситалар. Бундай тизим ва воситаларни кўпинча ахборотларни қабул қилиш, қайта ишлаш ва сақлаш техник воситалари (АҚИТВ) деб аташади.

АҚИТВ таркибига кирмайдиган, бироқ конфеденциал маълумотлар қайта ишланувчи ҳудудга жойлашган техник восита ва тизимлар ҳам мавжуд. Бундай техник восита ва тизимлар ёрдамчи техник восита ва тизимлар (ЁТВТ) деб аталади. Уларга қуйидагилар киради: телефон, алоқа овоз кучайтиргич техник воситалари, ёнғин ва қўриқлаш сигнализацияси тизимлари, радиоалоқа тизимида маълумотларни узатиш воситалари, назорат-ўлчов қурилмалари, хўжалик электр асбоблари ва бошқалар, шунингдек улар жойлашган бино.

АҚИТВга стационар жиҳозлар, периферия қурилмалари, улаш линиялари, тақсимловчи ва коммуникацион қурилмалар, электр манба тизимларини ўзига бириктирган тизим сифатида қараш мумкин. Конфеденциал маълумотларни қайта ишлашга мўлжалланган техник воситалар, шунингдек улар жойлашган бино ҳам АҚИТВ объектини ифодалайди.

Ахборот хавфсизлигини таъминлашга йўналтирилган ҳимоя ҳаракатлари қатор катталиклар билан тавсифланиши мумкин: таҳдид характери, ҳаракат усуллари, унинг тарқалганлиги, ўраб олиш масштаби кабилар.

Таҳдид характерига кўра ҳимоя ҳаракатлари маълумотларни ошкор бўлиши, чиқиб кетиши ва ноқонуний киришдан ҳимоя қилишга йўналтирилади. Ҳаракат усулларига кўра уларни камомад ёки бошқа зарарларни: огоҳлантириш, аниқлаш, олдини олиш ва тиклаш кабиларга тақсимлаш мумкин. Ўраб олиш бўйича ҳимоя ҳаракатлари ҳудудга, бинога, иншоатга, қурилмаларга ёки уларнинг алоҳида элементларига йўналтирилган бўлиши мумкин. Ҳимоя тадбирларининг масштаби эса объект, гуруҳ ёки индивидуал ҳимоя бўйича тавсифланади.

Ахборот ҳимояси турлари икки асосий белгига кўра таснифланади:

биринчидан, ахборот хусусийлиги, аниқроғи қўриқланадиган сирлар турига кўра;

иккинчидан, ахборот ҳимояси учун қўлланилувчи кучлар, воситалар ва усуллар гуруҳлари бўйича.

Биринчи гуруҳга қуйидаги асосий йўналишлар киритилиши мумкин: давлат сирларини ҳимоя қилиш, давлатлараро махфий маълумотларни ҳимоя қилиш, тадбиркорлик сирларини ҳимоя қилиш, хизмат сирларини ҳимоя қилиш, мутахассислик сирларини ҳимоя қилиш ва хусусий маълумотларни ҳимоя қилиш.

Иккинчи гуруҳга қуйидаги асосий йўналишлар киради: ахборотларни ҳуқуқий ҳимоялаш, ахборотларни ташкилий ҳимоялаш, ахборотларни муҳандислик-техник ҳимоялаш.

Ҳуқуқий ҳимоялаш – бу ҳуқуқий асосда ахборот ҳимоясини таъминловчи махсус қонунлар, бошқа меъёрий ҳужжатлар, қоидалар, жараёнлар ва тадбирлар.

Ташкилий ҳимоя – бу бажарувчиларга етказилиши мумкин бўлган ихтиёрий зарарни бартараф этувчи ёки енгиллаштирувчи, бажарувчиларнинг меъёрий-ҳуқуқий асосдаги ўзаро муомаласи ва ишлаб чиқариш фаолиятини қатъий белгилаш.

Муҳандислик-техник ҳимоя – бу фаолиятга етказилувчи зарарларга қаршилик қилувчи турли техник воситалардан фойдаланишдир.

Ахборот ҳимояси воситаларини ва усулларини таснифлаш. Ахборотни муҳофаза қилишда фойдаланилувчи асосий усуллар

қуйидагилар ҳисобланади: яшириш, ранжирлаш, нотўғри маълумот бериш, бўлаклаш, суғурта қилиш, ҳисобга олиш, кодлаш ва шифрлаш.

Яшириш – ахборотни муҳофаза қилиш усули сифатида амалиётда маълумотларни ҳимоялашнинг асосий ташкилий усулларидан бири ҳисобланади, махфий маълумотларга рухсат этилган шахслар сонини чегаралайди. Яшириш ахборотларни ҳимоя қилишда жуда кенг қўлланилувчи усуллардан бири ҳисобланади.

Ранжирлаш ахборот ҳимоя усули сифатида, биринчидан, махфий маълумотларни махфийлик даражаси бўйича тақсимлайди, ва иккинчидан ҳимояланган ахборотга рухсатни чегаралайди.

Нотўғри маълумот бериш – ахборот ҳимоя усулларидан бири бўлиб, бирор объект ҳақидаги ҳақиқий маълумот ўрнига атайин ёлғон маълумот тарқатишни англатади.

Ахборотни бўлаклаш усули ахборотни бўлакларга бўлиб, унинг бирор қисми орқали тўлиқ маълумот олиб бўлмасликни англатади. Бу усул ҳарбий техника ва қуролланиш воситаларини ишлаб чиқаришда, шунингдек янги маҳсулотларни ишлаб чиқаришда кенг қўлланилади.

Суғурта қилиш – ахборотни муҳофаза қилиш усули сифатида эндигина тан олинмоқда. Унинг маъноси ахборот эгаси ҳуқуқлари ва манфаатларини ёки ахборот воситаларини анъанавий таҳдидлар ва ахборот хавфсизлиги таҳдидларидан ҳимоя қилишни билдиради. Ушбу усул тижорат сирларини сақлашда кўпроқ қўлланилиши эҳтимоли мавжуд. Ахборотни суғурта қилишда у дастлаб, аудиторлик текширувидан ўтиши ва хулосага эга бўлиши талаб этилади.

Ахборотларни маънавий-маърифий ҳимоялаш усули ахборотни муҳофаза қилишда жуда муҳим рол ўйнайди. Айнан инсон, у корхона ёки ташкилот ходими, махфий маълумотлардан воқиф бўлиб, ўз хотирасида кўплаб маълумотларни жамлайди ва баъзи ҳолларда ахборот чиқиб кетиши манбаига айланиши мумкин ҳамда унинг айби билан ўзгалар ушбу ахборотга ноқонуний эга бўладилар. Ахборотларни маънавий-маърифий ҳимоялаш усули қуйидагиларни назарда тутади:

– ходимни тарбиялаш, у билан маълум сифатларни, қарашларни шакллантиришга йўналтирилган махсус ишларни олиб бориш (ватанпарварлик, ахборотни муҳофаза қилиш унинг шахсан ўзи учун ҳам қандай аҳамият касб этишини тушунтириш);

– ходимни ахборотни муҳофаза қилиш қоидалари ва усулларига ўргатиш, конфеденциал ахборот ташувчилар билан амалий ишлаш кўникмаларини шакллантириш.

Ҳисобга олиш ахборотни муҳофаза қилишнинг муҳим усулларидан бири бўлиб, конфеденциал маълумотлар ташувчиларнинг ҳамда ундан фойдаланувчиларнинг ихтиёрий вақтда қаерда жойлашганлиги ҳақида маълумот олиш имконини беради. Ушбу усулсиз ҳимоя муаммосини ҳал этиш жуда қийин. Сир сақланувчи ахборотларни ҳисобга олиш тамойиллари:

– ҳимояланувчи ахборотларни ташувчиларнинг барчасини рўйхатга олиш мажбурийлиги;

– муайян ахборот ташувчини рўйхатга олиш бир марта бўлишлигини (такрорланмаслигини) таъминлаш;

– рўйхатда конфеденциал маълумот ташувчининг айни вақтда қайси манзилдалигини кўрсатиш;

– ҳар бир ҳимояланган ахборот ташувчининг сақланишига ягона жавобгарлик ва ҳисобда ушбу ахборотни ишлатган фойдаланувчи ҳақида маълумотни акс эттириш.

Кодлаш – ҳимояланувчи ахборотни рақибдан яшириш мақсадида, ахборотни канал орқали узатиш жараёнида ўзгалар томонидан тутиб олиниши хавфи мавжуд бўлганда, уни кодлаш усули ёрдамида очиқ матнни шартли ахборотга айлантириш усулидир. Кодлаш учун одатда белгилар тўплами (белгилар, рақамлар ва бошқалар), шунингдек ахборотни тушунарсиз белгилар тўплами кўринишига айлантириш имконини берувчи маълум қоидалар тизими фойдаланилади. Бу ахборотни ўқиш учун эса уни яна ўз холига келтириш, яъни кодни очиш (калит) керак бўлади. Ахборотни кодлаш техник воситалар ёрдамида ёки қўлда амалга оширилиши мумкин.

Шифрлаш – ахборотни муҳофаза қилиш усули бўлиб, кўпинча ахборотларни радиоқурилмалар воситасида узатишда, рақиб томонидан тутиб олиш хавфи бўлганда қўлланилади. Ахборотни шифрлаш, уни ўзгалар томонидан тутиб олинганда ҳам калитсиз маъносини тушуниб бўлмайдиган ҳолатга ўтказишни англатади.

Ахборотни муҳофаза қилиш воситалари – бу ахборотни муҳофаза қилиш масалаларини ҳал этиш учун фойдаланилувчи муҳандислик-техник, электр, электрон, оптик ва бошқа қурилма воситалар тўпламидир.

Ахборотни муҳофаза қилишнинг кадр ва ресурс таъминоти. Давлат сирларини ташкил этувчи ахборотни муҳофаза қилишни ташкил этувчи кадрлар тайёрлаш тизимига қуйидагилар киради:

1. Ташкилот ва бўлинма раҳбарлари.

2. Ахборотни муҳофаза қилиш бўйича махсус комиссиялар.

3. Ягона хавфсизлик хизмати таркибига кирувчи ихтисослашган бўлинмалар.

Бошқа соҳалар каби ахборотни муҳофаза қилиш соҳаси ҳам кадрлар тайёрлашдан ташқари моддий, иқтисодий ва ахборот ресурслари билан таъминланиши керак.

Моддий ресурслар ахборотни муҳофаза қилишда махсус аҳамиятга эга. Унга махсус ажратилган бино, махсус қурилмалар, қабул қилинган меъёрлар асосида аттестация қилинган компьютер ва оргтехника, аппарат воситалари, дастур воситалари, ахборотни муҳофаза қилиш воситалари ва бошқалар.

Ахборот ресурслари – бу ташкилот миқёсида ахборотни муҳофаза қилиш бўйича оптимал бошқарув ечимлари қабул қилинадиган ахборот. Унга қуйидагилар киради:

– ҳуқуқий ахборот (хавфсизлик муаммолари бўйича меъёрий база),

– тижорат ахборотлари (ишлаб чиқариладиган маҳсулот ва унда ахборотни муҳофаза қилиш бўйича кўрсатиладиган хизматлар ҳақида ахборот),

– илмий-техник ахборот (хавфсизлик бўйича мамлакат ва чет эл давлатлари сиёсати ҳақида ахборот),

– ишлаб чиқариш технологияси жараёнлари бўйича ахборот;

– ташкилотнинг ахборот хавфсизлиги ҳолати, унга таҳдидлар бўйича ахборот-таҳлилий фаолият натижасида олинган таҳлилий ахборот.

Моддий ресурслар. Ахборотни муҳофаза қилишни лойиҳалаштиришни, уни ишга туширишни моддий таъминотсиз амалга ошириб бўлмайди. Бу иш мураккаб шароитларда амалга оширилади: хавфсизлик соҳасида рақобатчилик, хизмат кўрсатувчининг кам харажат қилиб кўп фойда олиш истаги, хавфсизлик бўйича сифатсиз ишларни амалга ошириши ва ҳоказо.

Ахборот хавфсизлиги унинг эгалари томонидан ҳимояланувчи ахборотнинг тарқаб кетиш, бузилиш, йўқ қилиш ва модификация қилишни олдини олиш мақсадига йўналтирилган комплекс чора-тадбирларни ифодалайди.

Ахборотни муҳофаза қилиш тизими деганда давлат ахборотни муҳофаза қилиш тизимини ҳамда муайян объектлардаги ҳимоя тизимларини тушуниш керак.

Давлат ахборотни муҳофаза қилиш тизимига қуйидагилар киради:

– давлат меъёрий ҳужжатлари, стандартлар, бошқарув ҳужжатлари ва талаблари;

– ахборотни муҳофаза қилиш бўйича концепция, талаблар, меъёрий-техник ҳужжатлар ва илмий-услубий тавсияларни ишлаб чиқиш;

– давлат мулки бўлган ахборотни муҳофаза қилишга йўналтирилган чора-тадбирларнинг ташкил этилиши, бажарилиши ва амал қилиниши тартиби, шунингдек жисмоний ва юридик шахслар ихтиёрида бўлган ахборотни муҳофаза қилиш бўйича тавсиялар;

– ахборотни муҳофаза қилиш воситаларини синаш ва сертификациялашни ташкиллаштириш;

– ахборотни муҳофаза қилиш учун ташкилот ва соҳавий координацион тузилмаларни ташкил этиш;

– ахборотни муҳофаза қилишни ташкил этиш бўйича ишларни назорат қилиш;

– чет эл фуқаролари бўлган юридик ва жисмоний шахсларнинг давлат мулки бўлган ахборотдан ёки давлат томонидан ахборотни тарқатишга чегара қўйилган юридик ва жисмоний шахслар маълумотларидан фойдалана олиш тартибини аниқлаш.

Ахборотлаштиришнинг муайян объектларида ахборотни муҳофаза қилишнинг мақсадлари эҳтимоли бўлган таҳдидларнинг рўйхати билан белгиланади.

Ҳар қандай ахборотни муҳофаза қилиш тизими ўзининг хусусиятига эга бўлиш билан бирга умумий талабларга жавоб бериши керак. Ахборотни муҳофаза қилишга кўпроқ қўйиладиган умумий талаблар қуйидагилардир:

Ахборотни муҳофаза қилиш тизими

– бир бутунликда бўлиши;

– ахборотнинг, ахборот воситаларининг хавфсизлигини ва ахборот муносабатидагилар манфаатларининг ҳимоясини таъминлаши;

– тизимнинг ичида унинг элементлари орасида ахборот алоқасини таъминлаши;

– ахборот фаолиятининг технологик комплексини ўзига қамраб олиши;

– фойдаланиш воситалари бўйича турли, ахборотдан фойдалана олишлилик бўйича кўп даражали иерархик кўринишда бўлиши;

– ахборот хавфсизлиги чораларини ўзгартириш ва тўлдиришга очиқ бўлиши;

– ностандарт бўлиши (ҳимоя воситаларини танлашда бузғунчининг ҳимоя имкониятлари билан таниш эмаслигига ишонишмаслик);

– техник хизмат кўрсатишга оддий ва фойдаланиш учун қулай бўлиши;

– ишончли бўлиши керак (техник воситалардаги ихтиёрий бузилиш ахборотнинг тарқаб кетиш канали бўлиб қолиши мумкин).

Бошқа тизимлар каби ахборотни муҳофаза қилиш тизими ўз таъминотининг маълум турларига эга бўлиши керак. Шу сабабли бу тизим қуйидагиларга эга бўлиши мумкин:

– *ҳуқуқий таъминот* (бунга бажарилиши мажбурий бўлган меъёрий ҳужжатлар, кўрсатмалар, йўриқномалар, талаблар киради);

– *ташкилий таъминот* (бунда ахборотни муҳофаза қилиш маълум бир тузилмавий бирликлар орқали қўлланилиши назарда тутилади: ҳужжатлар ҳимояси хизмати; қўриқлаш, киришга рухсат бериш хизмати; техник воситалар ёрдамида ахборотни муҳофаза қилиш хизмати; ахборот-таҳлилий фаолият ва бошқалар);

– *аппарат таъминоти* (бунда ахборотни муҳофаза қилиш ҳамда муҳофаза қилиш тизими фаолиятини таъминлаш учун техник воситалардан кенг миқёсда фойдаланиш назарда тутилади);

– *ахборот таъминоти* (ушбу таъминот таркибига тизимнинг фаолиятини таъминловчи вазифаларни ҳал ётувчи маълумотлар, ахборотлар, кўрсаткичлар, катталиклар киради. Шунингдек, унга хавфсизлик таъминоти хизмати фаолияти билан боғлиқ бўлган турли характердаги кўрсаткичлар: рухсат бериш, рўйхатга олиш, сақлаш кабилар ҳам киради);

– *дастурий таъминот* (бунга конфеденциал ахборот манбаларига ноқонуний кириш йўллари ҳамда ахборотни чиқиб кетиш каналлари мавжудлигига баҳо берувчи турли ахборот, ҳисобга олиш, статистик ва ҳисоблаш дастурлари киради);

– *математик таъминот* (бу ҳимоя учун зарур бўлган ҳар хил ҳисобларни амалга оширишда, бузғунчилар техник воситаларининг хавфи томонидан меъёрлар, ҳудудларга баҳо берувчи математик усулларни қўллашни назарда тутади);

– *лингвистик таъминот* (ахборотни муҳофаза қилиш соҳасида мутахассислар ва фойдаланувчилар томонидан қўлланилувчи махсус тил воситаларининг тўплами);

– *меъёрий-услубий таъминот* (бунга ахборотни муҳофаза қилишни таъминловчи органлар, хизматлар, воситалар фаолияти меъёрлари ва регламентлари, ахборотни муҳофаза қилиш қаттиқ талаб этиладиган шароитларда фойдаланувчилар томонидан ўз вазифаларини бажаришда фаолиятни таъминловчи турли услублар киради).

1.3.Ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича меъёрий ҳуқуқий ҳужжатлар. Ахборотни муҳофаза қилиш соҳасида халқаро стандартлар

Меъёрий-ҳуқуқий ҳужжат тушунчаси. 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 таҳрири)»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».

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

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

Меъёрий ҳуқуқий ҳужжатлар белгилари:

– меъёрий характер

– ҳуқуқий акт

– ҳуқуқ ижодкорлиги натижаси ҳисобланади

– умуммажбурийлик

– расмий ҳужжат кўринишида тузилади

– ҳуқуқ меъёрларини гуруҳлашда маълум бир тартибга риоя қилинади.

Меъёрий ҳуқуқий ҳужжатлар турлари. Ўзбекистон Республикасининг 2012 йил 24 декабрдаги «*Норматив-ҳуқуқий ҳужжатлар тўғрисида*»ги қонунининг 5-моддаси меъёрий ҳуқуқий ҳужжатларнинг турларини аниқлайди.

---

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

Қуйидагилар меъёрий ҳуқуқий ҳужжат ҳисобланади:

– Ўзбекистон Республикаси Конституцияси;

– Ўзбекистон Республикаси қонунлари;

– Ўзбекистон Республикаси Олий Мажлиси палаталари қарорлари;

– Ўзбекистон Республикаси Президенти фармонлари;

– Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари;

– Вазирликлар, давлат комитетлари ва ташкилотлари ҳужжатлари;

– Давлат ҳокимиятининг жойлардаги органлари қарорлари.

Меъёрий ҳуқуқий ҳужжатлар қонунчилик ҳужжатлари ҳисобланади ва Ўзбекистон Республикаси қонунчилигини ташкил этади.

Ўзбекистон Республикаси Конституцияси, Ўзбекистон Республикаси Қонунлари, Ўзбекистон Республикаси Олий Мажлиси палаталари қарорлари қонунчилик ҳужжатлари ҳисобланади.

Ўзбекистон Республикаси Президенти Фармонлари, Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари, Вазирликлар, давлат комитетлари ва ташкилотлари актлари, давлат ҳокимиятининг жойлардаги органлари қарорлари қонуности ҳужжатлари ҳисобланади (ушбу қонуннинг 6-моддаси).

Ахборот хавфсизлигини таъминлашда меъёрий-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 меъёрий-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.

Ўзбекистон Республикасида ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича меъёрий ҳуқуқий ҳужжатлар. 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.

Бизнинг мамлакатимизда бундай меъёрий ҳужжатларга Конституция, Ўзбекистон Республикаси Қонунлари, Ҳукумат қарорлари, фуқаролик, маъмурий ва жиноят кодексларида келтирилган тегишли моддалар киради. Ташкилот меъёрий ҳужжатларига эса ушбу ташкилот доирасида амал қилинувчи буйруқ, йўриқнома, кўрсатма кабилар киради.

Ахборот хавфсизлиги ва маълумотларни ҳимоялаш соҳасида меъёрий ҳуқуқий ҳужжатларни қабул қилиш ва амал қилишда тизимли кетма-кетлик. Хавфсизликни 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).

Меъёрий-ҳуқуқий ҳужжатларни қабул қилиш ва қўллашнинг тизимли кетма-кетлиги

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 ***Олов ранг 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 ГФР 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* ГФР, 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.

ITSEC Оқ китобда хавфсизлик критерияларининг қуйидаги асосий қисмлари келтирилган:

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.

ITSEC Европа критерияларига кўра ахборот хавфсизлиги олти асосий элемент ва унинг қисмларини ўз ичига олади:

1. Ахборот конфеденциаллиги (ахборотни ноқонуний олишдан ҳимоялаш).

2. Ахборот бутунлиги (ахборотни ноқонуний ўзгартиришдан ҳимоялаш).

3. Ахборотдан фойдалана олишлилик (ахборот ва тизим ресурсларини ноқонуний ёки тасодифий ушлаб қолишлардан ҳимоялаш).

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

5. Ахборот хавфсизлиги функцияларининг 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.

Оқ китобда «тизим» ва «маҳсулот» ўртасида фарқ ифодаланади.

«Тизим» деганда маълум бир мақсадда ва маълум бир доирада қўлланилувчи аниқ аппарат-дастурий конфигурация тушунилади. «Маҳсулот» деганда эса, ўз хоҳишига кўра сотиб олиб ихтиёрий «тизим»га ўрнатилиши мумкин бўлган аппарат-дастурий пакет тушунилади. «Тизим» ва «Маҳсулот»нинг критерияларини умумлаштириш мақсадида **ITSEC**да ягона – «объект» атамаси киритилган. «Объект»ни ишончли деб қабул қилиш учун, хавфсизликни кафолатловчи маълум бир даражадаги ишонч керак бўлади. У эса самарадорлик ва аниқликни ўз ичига олади. Баъзи манбаларда кафолатланганликни ҳимоя воситаларининг адекватлиги деб ҳам номланади.

Ҳимоянинг самарадорлигини текширишда конфеденциаллик, бутунлик, ахборотга рухсат этилганлик бўйича хавфсизлик вазифаларининг ўзаро мослиги таҳлил қилинади. Шунингдек, ҳуқуқбузарлар томонидан ҳимоянинг қалтис жойларидан фойдаланиш оқибатлари ўрганиб чиқилади. Бундан ташқари, «самарадорлик» тушунчасига ҳимоя механизмларининг қуввати деб номланувчи тўғридан-тўғри ҳужумлар бўлгандаги қобилиятлари ҳам киради. **ITSEC**да ҳимоя механизмлари қувватининг учта даражаси (базавий, ўрта, юқори) келтирилган.

ITSEC бўйича тизим хавфсизлигини умумий баҳолаш икки қисмдан иборат – кафолатланган хавфсизлик механизмларининг даражасини баҳолаш ва уларнинг кафолатланган аниқлиги даражасини баҳолаш.

Тизимнинг хавфсизлиги умуман олганда «тизим» ва «маҳсулот»ни алоҳида баҳолаш билан амалга оширилади. Унинг ҳимояланганлиги хавфсизлик механизмларининг муҳим бўлакларидан юқори бўла олмайди.

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 ларга 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 бутунлигина 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.

Канада ўзининг **CTCPEC** номли критерияларини, АҚШ эса янги Федерал Критериялар (Federal Criteria)ни ишлаб чиқди. Ушбу критериялар ўзаро мослаша олмаслиги сабабли, уларни ўзаро мувофиқлаштириб (бирлаштириб), улар ҳимояланганликни баҳоловчи **CommonCriteria** (CC) номли тўплам яратишга қарор қабул қилинди. Критетерияларнинг умумий тўплами ҳимояланганликни баҳолаш бўйича қуйидагиларни аниқлайди:

– функционал имкониятлар ва кафолатларга талаблар;

– фойдаланувчи сўраши мумкин бўлган ишончнинг 7 даражаси (баҳолашда кафолат даражалари). Бунда EAL1 даража тизимнинг конкретлилига унча юқори бўлмаган ишончни таъминласа, EAL7 даража жуда юқори кафолатларни беради;

– икки тушунча: Ҳимоя профили (PP) ва хавфсизлик мақсади (ST).

Юқорида қайд этилган стандартларнинг аналоги сифатида Россияда «Автоматлаштирилган тизимлар. Ахборотни ноқонуний киришдан ҳимоялаш. Автоматлаштирилган тизимларни таснифлаш ва ахборот ҳимоясига талаблар» номли Давлат техника комиссиясининг Бошқарув ҳужжати ишлаб чиқилган.

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

Ҳар қандай ташкилот фаолияти ахборот технологияларидан фойдаланиш оқибатида кўплаб таҳдидлардан ҳоли бўлмаганлиги сабабли таҳдидларни бошқариш номли янги функция пайдо бўлди. У ўз ичига икки фаолиятни олади: таҳдидларни баҳолаш (ўлчаш) ва самарали ва тежамкор ҳимоя бошқарувчисини ташлаш.

Таҳдидларни бошқариш жараёнини қуйидаги босқичларга бўлиш мумкин:

1. Таҳлил қилинувчи объектларни танлаш ва уларни кўриб чиқишда батафсиллик даражаси.
2. Таҳдидларни баҳолаш методологиясини танлаш.
3. Активларни идентификациялаш.
4. Таҳдид ва унинг оқибатлари таҳлили, ҳимоянинг заифликларини аниқлаш.
5. Таҳдидларни баҳолаш.
6. Ҳимоя чораларини танлаш.
7. Танланган чораларни қўллаш ва текшириш.
8. Қолдиқ таҳдидни баҳолаш.

Ушбу муносабатларни ҳуқуқий бошқариш аввало, ахборот таҳдидларидан суғурта қилиш орқали амалга оширилиши мумкин ва зарур.

Мустақил тайёргарлик учун саволлар

1. Ахборот хавфсизлиги тушунчаси нимани англатади?

2. Ахборот хавфсизлигининг қандай ташкил этувчилари мавжуд?

3. Ахборот хавфсизлиги миллий хавфсизлик тизимида қандай ўрин тутади?

4. Ахборот хавфсизлигининг замонавий концепцияси нима?

5. Ахборот хавфсизлигига таҳдид деганда нима тушунилади?

6. Ахборотни муҳофаза қилишнинг қандай усуллари ва турлари мавжуд?

7. Ахборотни муҳофаза қилиш қандай объектларга эга?

8. Ахборотни муҳофаза қилиш воситаларига нималар киради?

9. Ахборотни муҳофаза қилиш тизимлари қандай вазифани бажаради?

10. Ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича қандай меъёрий-ҳуқуқий ҳужжатлар мавжуд?

11. Ахборотни муҳофаза қилиш соҳасида қандай халқаро стандартлар мавжуд?

II. АХБОРОТЛАРНИ ТЕХНИК ҲИМОЯЛАШ

2.1. Техник воситалар билан ҳимояланадиган ахборотларнинг турлари.

2.2. Ахборот чиқиб кетиш техник каналларининг таснифи ва таркиби.

2.3. Объектларни кузатиш, сигналларни эшитиш ва тутиб олишнинг асосий усул ва тамойиллари.

2.4. Ахборотларни инженер-техник ҳимоялаш.

Ҳозирги кунда маълумотларни техник ҳимоялаш масаласи долзарб вазифалардан бирига айланган.

Маълумотларни ҳимоялашнинг техник воситаларига механик, электромеханик, электрон-механик, оптик, акустик, лазер, радио, радиолокацион ва бошқа қурилмалар ҳамда ҳимояланадиган объектга бориш йўлини тўсишга мўлжалланган тизим ва бинолар киради.

Маълумотлар ва объектларни ҳимоялаш учун мураккаб ва такомиллашган усулларидан фойдаланилади.

Ташкилотлардаги маълумотларни электрон қайта ишлаш марказлари кучли электромагнит нур манбаи бўлган объектлардан узоқда жойлашган бўлиши ва атрофи девор билан ўралиши керак. Назорат зонасини кузатиш телевизион, радиолокацияли, лазерли, оптик, акустик ва бошқа умумий пультга уланган тизим орқали амалга оширилиши мумкин.

Ахборот хавфсизлиги муаммоси ташкилий чора-тадбирлар ва талаблар, ахборот тизимларидан фойдаланиш ва лойиҳалаш босқичларида ҳал қилинади. Улар орасида ҳимояланаётган ахборот тизими жойлашган объектни қўриқлаш муҳим ўринни эгаллайди. Бунда ҳисоблаш техника воситаларидаги маълумотларни ўғирлашни олдини оладиган ва қийинлаштирадиган, ахборот ташувчилар, шунингдек алоқа линияларидан ва ахборот тизимидан рухсат берилмаган фойдаланишни ман этадиган тегишли қўриқлаш постлари, техник воситалар ўрнатилади.

2.1. Техник воситалар билан ҳимояланадиган ахборотларнинг турлари

Ахборотларни муҳофаза қилишнинг техник воситалари – объектнинг ниқобловчи (маскировкаловчи) белгилари очилишини бартараф этиш ёки камайтириш, ёлғон аломатларни яратиш ҳамда техник воситалар орқали ахборотга рухсатсиз киришга тўсқинлик қилишга мўлжалланган техник воситалардир.

Маълумотларни рухсатсиз олишнинг объектлари, усуллари ва воситалари қуйидагилар бўлиши мумкин:

– бино, иншоат ва қурилиш конструкциялари (деворлар, томлар, поллар, дераза ва эшиклар, дераза ойналари, иситиш ва сув билан таъминлаш тизимлари, ҳаво тозалаш қувурлари); конфеденциал музокара ва мажлисларни ўтказишда акустик тебраниш каналлари бўйича маълумотларни рухсатсиз олиш;

– ҳаракатланувчи объектлар (автомобиль, темир йўл, сув ва ҳаво йўллари транспортлари); конфеденциал суҳбатлар олиб боришда – акустик тебраниш каналлари бўйича;

– кучсиз ток техника воситалари (алоқа қурилмалари, овоз кучайтиргичлар, аудио- ва телеқурилмалар, электр соатлар, радио эшиттиришлар, ёнғин ва қўриқлаш сигнализация қурилмалари, электр ёзув машинкалари, кондиционерлар ва улардан фойдаланилганда ҳамда бу воситалар ёпиқ таснифли тадбирларни ўтказишга мўлжалланган бинога жойлашганда – электроакустик ўзгаришлар бўйича ва ёндош электромагнит нурланишлар ва наводкалар (ЁЭМНН-ПЭМИН) ҳисобига;

– ҳисоблаш техникаси воситалари (монитордаги тасвир эфир орқали маълум бир масофага узатилади) – ЁЭМНН ҳисобига;

– электр манбаси ва ерга уланган ўтказгичлар тизими (бу занжир орқали овоз кучайтириш, компьютерда котиба билан алоқа ва шу кабиларни амалга оширувчи қурилмаларда қайта ишланадиган маълумотларни тутиб олиш мумкин) – ЁЭМНН ҳисобига;

– бино, автомашина ва бошқалардаги акустика (сўз, товушлар) – радиоканал ва симларда акустик радиомикрофонлар («жучоклар») бўйича ҳамда лазер қурилмалари орқали қўлга киритиш ҳисобига;

– телефонда сўзлашувлар – радиоканал ва симлар орқали телефон «жучоклар» ҳисобига;

– факс орқали маълумотлар – ёндош нурланишлар ва наводкалар ҳамда алоқа линияси орқали қўлга киритиш ҳисобига;

– «жучоклар» ўрнатилган «совға» ва «сувенирлар», мебеллар;

– йўналтирилган микрофонлар ёрдамида масофадаги шахс акустикаси (сўзи);

– уяли алоқа тармоғи орқали радиосўзлашувлар.

Ҳимоянинг техник 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.

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.

*Объектни топиш*да техник разведка воситаларининг фаолият кўрсатиш жараёнида объектнинг техник демаскировка белгилари аниқланади ва унинг мавжудлиги ҳақида хулоса қилинади.

Демаскировка белгилари қуйидагилар билан фарқ қилади:

– жойлашуви – бошқа объектлар ва атрофдаги предметлар орасида объект жойлашувини аниқлаб берадиган белги;

– таркибий кўриниш – объектнинг тузилиши ва тўлалигича кўринишини акс эттирадиган катталикларини (таркиби, сони ва алоҳида объектларнинг жойлашуви, шакли ва геометрик ўлчамлари) аниқловчи белгилар;

– фаолияти – объектнинг физик фаолият юритиши орқали уни очиб берувчи белгилар.

Техник демаскировка белгиларини икки тоифага бўлиш мумкин:

– тўғридан-тўғри демаскировка белгилари – ҳимоя объектининг фаолияти ва унинг физик майдонлари (электромагнит, акустик, радиацион ва бошқалар) билан боғлиқ бўлган, ҳимоя қилинадиган

ахборотга боғлиқ бўлмаган атроф-муҳитнинг физик майдони фонидан фарқ қиладиган белгилар;

– билвосита демаскировка белгилари – объектнинг фаолият кўрсатиши натижасида атроф-муҳитдаги ўзгаришлар натижасида юзага келадиган белгилар (фаолиятнинг оптик-визуал белгилари, геометрик ўлчамлар, ёритилганликнинг кескин фарқ қилиниши, ишлаб чиқариш фаолиятидан қолган излар ва ҳоказо).

Ахборотни муҳофаза қилишнинг самарадорлик кўрсаткичи ҳимоя объектининг техник демаскировка белгилари катталиги бўлиб, унга нисбатан ахборотни муҳофаза қилиш самарадорлигининг меъёрлари белгиланади.

Хавфли сигнал, объект белгисининг кўрсаткичи бўлиб, ундан конфеденциал маълумотларни олиш учун техник разведкада (ТР) фойдаланилади. Объектни аниқлаш – ТР воситаларининг фаолияти бўлиб, натижада объект демаскировка белгиларининг катталиклари аниқланади ва унинг тавсифи ҳақида хулоса қилинади (классификациялаш амалга оширилади). Аниқланган объектга маълум бир тоифа берилади. Ихтиёрий объектда бир қанча белгилар бўлиши мумкин, бироқ объектни аниқлашда бу белгиларнинг маълум тўпламидан фойдаланилади.

Ҳимоя объектларининг демаскировка белгилари. Объектларнинг демаскировка белгиларига қуйидагилар киради:

– фаолият белгилари: транспорт машиналарининг ҳаракати, овозлар, оловлар, чақнашлар, тутун, чанг;

– махсус қурилмаларда қайд қилинадиган турли нурланишларни (электромагнит, инфрақизил, иссиқлик) қайтариш ва чиқариш қобилияти;

– фаолият излари: сўқмоқ ва қатнов йўллари, ишлаб чиқариш материалларининг қолдиқлари, маиший чиқиндилар ва ҳоказо;

– тавсифловчи кўриниши (шакли), объектни ўлчами ва жойлашувининг муҳим томонлари;

– объект сиртининг ранги, айрим ҳолларда унинг ялтираши (ойнанинг ялтираши, металнинг товланиши);

– объектнинг ўзидан тушадиган ва унинг сиртига тушадиган соя.

Техник воситалар билан ҳимояланадиган маълумотларнинг манбаси ва ташувчилари:

– объект таркибининг физик хусусиятларини тавсифловчи белгилар (иссиқлик ва электр ўтказувчанлиги, таркиби, қаттиқлиги ва ҳоказо);

– объект томонидан ҳосил бўладиган физик майдонни тавсифловчи белгилар (элетромагнит, радиацион, акустик, гравитацион ва ҳоказо);

– объектнинг шакли, ранги, ўлчами ва элементларини тавсифловчи белгилар;

– объектнинг фазовий координаталарини (ҳаракатланадиган объектларнинг тезлигини) тавсифловчи белгилар;

– объектлар ва уларнинг элементлари ўртасидаги маълум бир алоқалар мавжудлигини тавсифловчи белгилар;

– объект фаолияти натижасини (тутун чиқариш, чангитиш, объектнинг тупроқдаги изи, сув ва ҳавони ифлослантириш ва шу каби) тавсифловчи белгилар.

Объектни аниқлаш унинг демаскировка белгилари бўйича амалга оширилади. Бу белгилар *кўриниши, фаолият белгиси ва жойлашуви* бўйича учта гуруҳга бўлинади.

Кўриниши бўйича демаскировка белгиларга объектнинг физик (оптик ва радиолакацион диапазонли нурланиш тўлқинларини қайтариш қобилияти, иссиқлик диапазонида энергияга эга бўлган нурланиш чиқариши) ва геометрик (объект шакли ва унинг алоҳида ташкил этувчиларининг ўлчамлари) хусусиятлари киради.

Фаолиятнинг демаскировка белгилари объект таъсири (ҳаракатланиш, атроф-муҳитнинг ўзгариши ва шу кабилар) натижасида намоён бўлади.

Жойлашув белгилари объектнинг атрофдаги предметларга нисбатан жойлашув ҳолати билан аниқланади.

Объектнинг кўринадиган электромагнит спектр диапазонидаги демаскировка белгилари. Объект ва атроф-муҳитнинг оптик катталиклари разведкада ҳамда разведканинг техник воситаларидан самарали ҳимоя қилишда муҳим роль ўйнайди. Объектларнинг оптик тасвири ва уларнинг алоҳида ташкил этувчилари фонга нисбатан ёркинлиги, ўлчами, шакли ва ранги билан фарқ қилади. Кўринадиган тўлқин диапазонида объектнинг тасвири унинг ёркинлиги билан аниқланади. Объект билан фон орасидаги ранг ёркинлигининг фарқи қўшимча маълумот ҳисобланади. Объект билан фон орасидаги ёркинлик фарқи, уларнинг ёруғлик қайтариш қобилиятининг турличалиги натижасида пайдо бўлади.

Объектнинг электромагнит инфрақизил спектр диапазонидаги демаскировка белгилари. Бу белгиларга қизиган жисмнинг ўзидан чиқарган нури (табиий) ва объектлардан қайтган (сунъий)

инфрақизил нурлар киради. Табиий инфрақизил нурлар манбаси ер устидаги (тупроқ, ўрмон ва ҳоказо), атмосферадаги (булут, газлар) ва космосдагидан (қуёш, ой, юлдузлар) иборат бўлади. Табиий инфрақизил нурлар объектни аниқлашни қийинлаштирувчи фон нурлари ҳисобланади. Объект ва фоннинг иссиқликни нурлаш қобилиятидаги фарқ ҳисобига объектни аниқлаш мумкин.

Радиоэлектрон воситаларни демаскировка белгилари. Радиоэлектрон қурилмаларни демаскировка белгилари радиодиапазондаги электромагнит тўлқин нурланишлари билан боғлиқ. Электромагнит тўлқинлар техник восита ва тизимларнинг вазифаси ҳамда тавсифлари ҳақидаги маълумотларни ташиши мумкин. Нурланиш асосий ва ёрдамчи воситалардан, назорат-ўлчаш қурилмаларидан, тренажёрлардан, имитатордан ва бошқалардан чиқиши мумкин.

Радионурланиш билан боғлиқ бўлган барча демаскировка белгилари радиосигналнинг техник тавсифлари билан аниқланади. Уларни *частотали, вақтли, энергетик, спектрли, фазо-энергетик, фазоли, поляризацияли* гуруҳларга ажратиш мумкин.

Радионурланишнинг техник аломатини *гуруҳли, индивидуал ва тезкорга* ажратиш мумкин.

Гуруҳли техник белгилар радиоэлектрон тизим (РЭТ)ни бирор синфга тааллуқли эканлигини аниқлаш имконини беради. Улар аниқ РЭТ турига мос келувчи тавсиф ёки тавсифлар мажмуи билан аниқланади. Унга қуйидагилар киради:

– фазовий кўриш соҳасининг тавсифи;

– антеннанинг айланиш тезлиги;

– нурланиш тури;

– частотани қайта созлаш тартиби ва чегараси;

– модуляция қилинувчи сигналнинг тури ва ўзгариш қонунияти;

– сигнал катталикларининг қийматлари (ташувчи частоталар, импульс давомийлиги, импульснинг чиқиш частотаси ва бошқалар).

Индивидуал демаскировка белгилари РЭТ тўпламидаги бирор турга оид ва аниқ намуна ҳақидаги маълумотлардан иборат бўлади. РЭТда ўзига хос демаскировка белгилари сигнал катталикларининг технологик ва ишлатишдаги тарқоқлиги натижасида намоён бўлади.

2.2. Ахборот чиқиб кетиш техник каналларининг таснифи ва таркиби

Маълумот майдон ёки модда орқали узатилади. Бу ё акустик тўлқин (товуш), ё электромагнит нурланиш ё матн ёзилган бир варақ

қоғоздир. Бироқ, на узатилган энергия, на фойдаланилган модда ўз-ўзича ҳеч қандай қийматга эга эмас, улар фақат маълумот ташувчи ҳисобланади, холос.

Физик табиатига кўра қуйидагилар маълумот ташувчи воситалар ҳисобланади:

– ёруғлик нури;

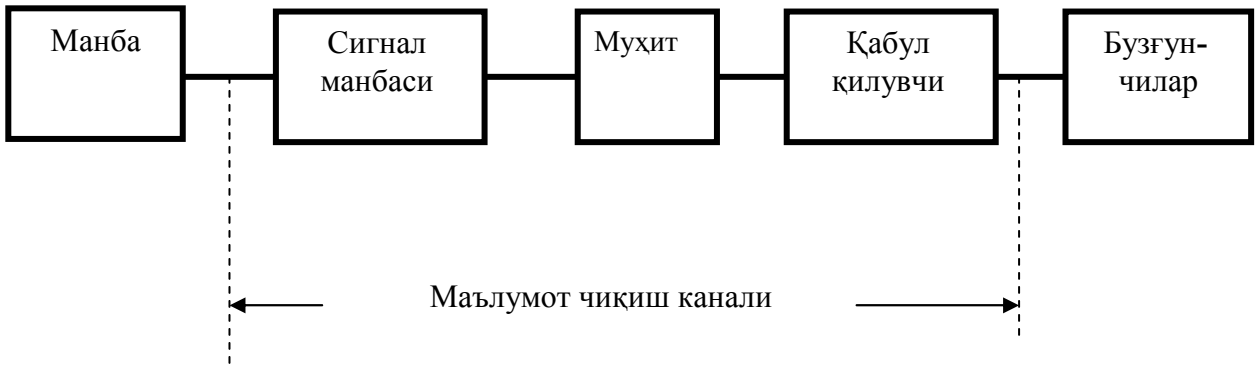
– товуш тўлқинлари;

– электромагнит тўлқинлар;

– материал ва моддалар.

Табиатда маълумотларни ташиш учун булардан бошқалари мавжуд эмас.

Ўз манфаатларига қараб инсонлар у ёки бу физик майдондан фойдаланиб ўзаро маълумот узатишнинг бирор тизимини яратадилар. Бундай тизимларни *алоқа тизими* деб номлаш қабул қилинган. Ихтиёрий *алоқа тизими (маълумот узатиш тизими)* маълумотлар манбаи, узатгич, маълумот узатиш канали, қабул қилгич ва қабул қилиб олувчи ҳақидаги маълумотдан ташкил топади. Бу тизимлар кундалик ҳаётда бирор мақсад учун фойдаланилади ва маълумот узатишнинг расмий воситаси ҳисобланади. Унинг фаолияти ишончлиликни, аниқлиликни ва маълумот узатиш хавфсизлигини таъминлаш мақсадида назорат қилинади. Бу эса рақобатчиларнинг тизимга рухсатсиз киришни олдини олади. Бироқ, маълум шароитлар мавжудки, унда бир жойдан бошқасига маълумот узатиш тизими объект ва манбанинг хоҳишига боғлиқ бўлмайди. Бундай ҳолларда, албатта, бундай канал ўзини очиқча намоён қилмаслиги керак. Маълумотлар узатиш канали сингари бундай канал *маълумот чиқиб кетиш канали* деб аталади. У ҳам сигнал манбаи, уни тарқатувчи физик муҳит ва ёвуз ниятли шахслар (бузғунчилар) томонидаги қабул қилувчи қурилмалардан ташкил топади. Қуйидаги расмда маълумот чиқиб кетиш каналининг тузилиши келтирилган.



Маълумотлар чиқиб кетиш канали деб конфеденциал маълумотлар манбасидан ёвуз ниятли шахсгача бўлган физик йўл тушунилади. Бу йўл орқали маълумот чиқиб кетиши ёки сақланаётган маълумотга рухсатсиз кириш мумкин. Маълумотлар чиқиб кетиш каналининг вужудга келиши (пайдо бўлиши, ўрнатиш) учун маълум фазовий, энергетик ва вақтдаги шароит ҳамда ёвуз ниятли шахсда уларга мос маълумотларни қабул қилиш ва қайд қилиш воситалари мавжуд бўлиши керак.

Физик хусусиятларини инобатга олган ҳолда маълумотлар чиқиб кетиш каналининг пайдо бўлишини қуйидаги гуруҳларга ажратиш мумкин:

– визуал-оптик;

– акустик;

– электромагнит (магнит ва электрик майдонни ўз ичига олади);

– материал-буюмли (қоғоз, фото, магнитли ташувчилар, турли кўринишдаги қаттиқ, суюқ, газ ҳолатидаги саноат чиқиндилари).

Визуал-оптик каналлар – бу бевосита ёки узоқдан (жумладан телевизион) кузатишдир. Маълумот ташувчи бўлиб, конфеденциал маълумот манбаси чиқарадиган ёки ундан қайтувчи кўринадиган, инфрақизил ва ультрафиолет диапазондаги ёруғлик хизмат қилади.

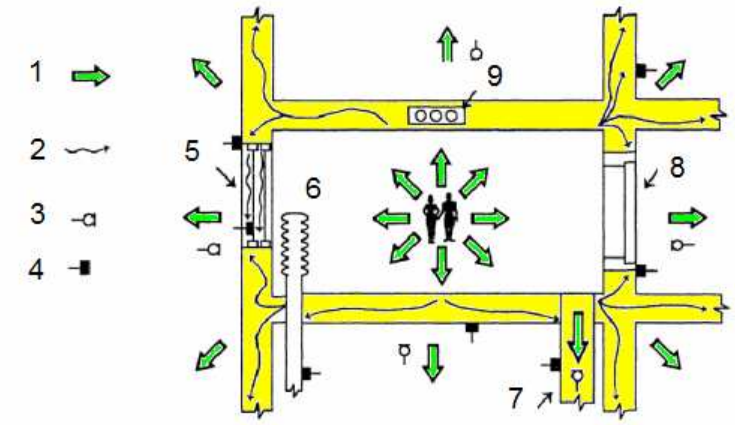
Акустик каналлар. Инсон учун маълумотларни эшитиш қобилияти кўришдан кейин иккинчи ўринда туради. Шу сабабли маълумот чиқиб кетиши каналининг энг кўп тарқалгани акустик канал ҳисобланади. Акустик каналда маълумот ташувчиларга ультра

(20000 Гц дан юқори), эшитиш ва инфратовуш диапазондаги тўлқинлар киради. Инсон эшитадиган товуш частотаси 16 дан 20000 Гц гача ва инсон гапиргандаги 100 дан 6000 Гц гача бўлади.

Ҳавода акустик тўлқин тарқалганда ҳаво зарралари тебранади ва бунинг натижасида биридан-бирига энергия узатилади. Агар товуш йўлида тўсиқ бўлмаса, у ҳамма томонга бирдай тарқалади. Агар товуш тўлқинлари йўлида девор, ойна, эшик, том ва каби бошқа тўсиқлар бўлса, товуш тўлқини уларга маълум даражада босим беради ҳамда уларни ҳам тебрантиради. Товуш тўлқинларининг бундай таъсири акустик маълумот чиқиб кетиши каналининг пайдо бўлишига асосий сабаб бўлади.

Муҳитга қараб товуш тўлқинларининг тарқалиши фарқ қилади. Бу товушнинг ҳаво бўшлиғида тўғри тарқалиши, қаттиқ муҳитда (таркибий товуш) тарқалишидир. Бундан ташқари, товушнинг бино ва иморатларга босим билан таъсири қилиши уларнинг тебранишига сабаб бўлади.

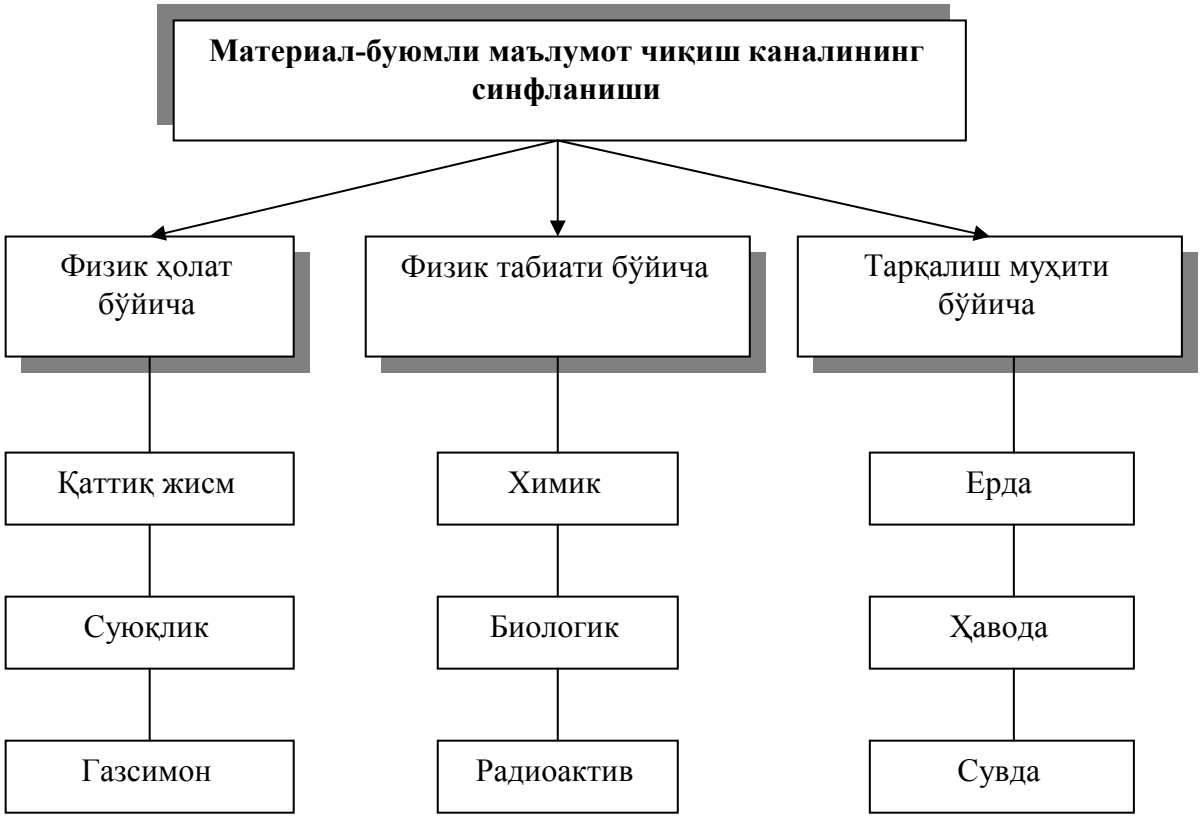
Қуйидаги расмда акустик ва вибрацион тебранишлар орқали маълумотлар чиқиб кетиш каналларининг чизмаси келтирилган бўлиб, унда акустик тебраниш ва товушларнинг қаттиқ муҳитда, метал буюмларда ва бинонинг бошқа элементларида тарқалиши тасвирланган.



1. Акустик тебранишларнинг тарқалиши
2. Вибрацион тебранишларнинг тарқалиши
3. Эшитиш микрофони
4. Эшитиш вибродатчиги
5. Дераза
6. Иситгич батареялари
7. Ҳаво тозалагич
8. Эшик
9. Кабеллар учун жой

Электромагнит каналлар. Бундай ҳолларда маълумот ташувчи, ўта узун тўлқин узунлигидан (10000 м – частотаси 30 Гц дан кичик) субмиллиметрлигача (1-0,1 мм – частотаси 300дан 3000 ГГц гача) бўлган диапазондаги электромагнит тўлқинлар ҳисобланади. Бу кўринишдаги ҳар бир электромагнит тўлқин тарқалишнинг фазо ва узоқлиги бўйича ўзига хос хусусиятига эга. Масалан, узун тўлқинлар жуда узоқ масофаларга, миллиметрлилар эса аксинча, фақат тўғри йўналишда бир ва бир неча ўн километрга тарқалади. Бундан ташқари, турли телефон ва алоқа симлари ҳамда кабеллари ўз атрофида магнит ва электр майдонини ҳосил қилади. Яқин масофада булар ҳам маълумотларнинг чиқиб кетиши элементларига киради.

Материал-буюмли маълумот чиқиб кетиши каналига қаттиқ, суюқ ва газсимон ёки корпускуляр (радиоактив элементлар) кўринишдаги моддалар киради. Булар, жуда кўп ҳолларда, саноатнинг турли чиқиндилари, сифатсиз моллар, хомаки материаллар ва бошқалар бўлиши мумкин. Шундай экан ҳар бир конфеденциал маълумот манбаи у ёки бу даражадаги маълумот чиқиб кетиши каналига эга бўлиши мумкин.



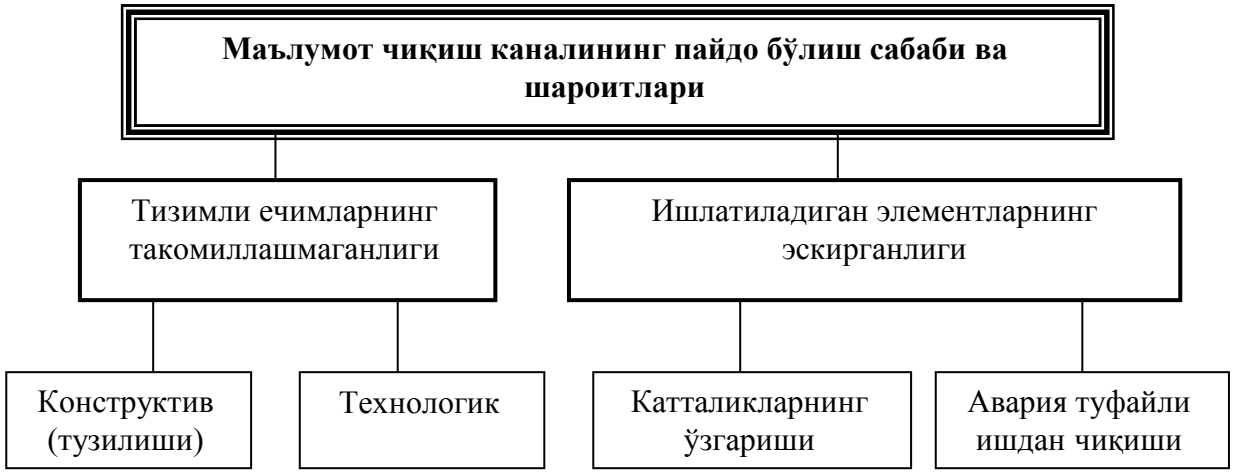
Ишлаб чиқаришда, илмий фаолиятларда ва ахборотларни автоматик қайта ишлашда турли техник таъминот воситаларидан кенг фойдаланиш деб ном олган маълумотлар чиқиб кетиши *техник* каналлари гуруҳининг пайдо бўлишига олиб келди. Уларда маълумотларни ташувчи бўлиб, турли хил тоифадаги ёндош электромагнит нурланишлар ва наводкалар (ЁЭМНН): акустик-ўзгартириладиган, нурланувчан ҳамда зарарли алоқа ва наводкалар ҳисобланади. ЁЭМНН ихтиёрий электрон қурилмага, тизимларга, табиий хусусиятларга эга бўлган маҳсулотларга хосдир.

Хавфли нурланишга асос бўлувчи физик ҳодисалар турли хил тавсифларга эга. Шунинг билан бирга, бундай нурланиш ҳисобига бўладиган умумий кўринишидаги маълумотлар чиқиб кетишини, ҳимояланадиган маълумотларнинг бирор «қўшимча» алоқа тизими орқали узатилиши деб қараш мумкин.

Шуни таъкидлаш жоизки, техник восита ва тизимлар нафақат қайта ишланадиган ахборотлардан иборат бўлган сигналларни фазога тарқатади, балки ўзининг микрофон ёки антеннаси ёрдамида акустик ёки магнит (электромагнит) нурланишларни қабул ҳам қилади, уларни электр сигналига айлантиради ва ўз алоқа линияси орқали, одатда назоратсиз, жўнатади. Бу эса маълумот чиқиб кетиши хавфини янада орттиради.

Алоҳида техник воситалар ўз таркибида «микрофон» ва «антенна» каби қурилмалардан ташқари юқори частотали ёки импульсли генераторларга ҳам эга бўлади. Уларнинг нурланиши конфеденциал маълумотларга эга бўлган турли сигналларга мослаштирилган бўлиши мумкин.

Хавфли «микрофон эффект»и (зарарли электр сигналларининг пайдо бўлиши) айрим телефон қурилмаларида, ҳатто телефон трубкаси қўйилган ҳолда бўлишига қарамасдан ҳам пайдо бўлади. Электромагнит нурланишлар товуш чиқарувчи ва товуш кучайтирувчи қурилмаларнинг радиочастоталарида ўз-ўзидан пайдо бўлишида ҳам ҳосил бўлиши мумкин.



ЁЭМННнинг пайдо бўлиш манбасининг шароити ва сабабининг таҳлили шуни кўрсатадики, унинг пайдо бўлишига маълум тоифадаги техник воситаларнинг ишлаш схемасини такомиллашмаганлигини, элементларнинг ишлатилиши натижасида эскирганлигини ва шу кабилар асос бўлади.

Техник канал бўйича маълумотлар чиқиб кетишидан ҳимоялашда, одатда қуйидаги амалларнинг бажарилиши талаб этилади**:**

1. Мумкин бўлган маълумотлар чиқиб кетиши каналларини ўз вақтида аниқлаш.

2. Назорат зонаси (ҳудуди, кабинети) чегарасида маълумот чиқиб кетиши каналининг энергетик тавсифларини аниқлаш.

3. Ёвуз ниятли шахслар томонидан канални назорат қилиш воситаларининг имкониятларини баҳолаш.

4. Ташкилий, ташкилий-техник ёки техник чора ва воситалар ёрдамида маълумот чиқиб кетиши каналларининг энергетикасини йўқ қилиш ёки заифлаштириш.

2.3. Объектни кузатиш, эшитиш ва сигнални тутиб олишнинг асосий усуллари ва тамойиллари

Маълумотларни визуал-оптик канал бўйича чиқиб кетишидан ҳимоялаш – конфеденциал маълумотларнинг ёруғлик энергияси ҳисобига назорат зонасидан чиқиб кетишини бартараф этиш ёки камайтириш бўйича комплекс тадбирлардир.

Маълумотларни визуал-оптик канал бўйича чиқиб кетишидан ҳимоялаш мақсадида қуйидагилар тавсия этилади:

– ҳимоя объекти шундай жойлаштириладики, ундан қайтадиган ёруғлик ёвуз ниятли шахслар жойлашган томонга тушмаслиги керак (фазовий тўсиқ);

– ҳимоя объектининг ёруғлик қайтариш хусусиятини камайтириш;

– ҳимоя объектининг ёруғлигини камайтириш (энергетик чегаралаш);

– атрофини ўраш воситалари (экранлар, пардалар, қорайтирилган ойна, ниқоб, тўсиқлар ва турли чегараловчи воситалар)дан фойдаланиш ёки қайтган ёруғликни иложи борича сусайтириш;

– ҳимоя қилиш ва ёвуз ниятлиларни чалғитиш мақсадида яшириш (маскировка), имитация ва бошқа воситаларни қўллаш;

– ҳимоя объектини ёруғлик қайтариш хусусияти ва фон ёркинлигини ўзгартириш орқали маскировкани амалга ошириш;

– назоратсиз тарқалаётган чиқувчи ёки қайтувчи нурлардан манбани ҳимоялашда фаол ва пассив ҳимоя воситаларидан фойдаланиш;

– объектни маскировка қилишда аэрозол парда, маскировкаловчи сетка, бўёқ кабиларни қўллаш.

Яширишнинг тезкор воситалари сифатида аэрозол пардалари кенг қўлланилади. Улар турли моддаларнинг газда сузиб юрувчи майда зарралари бўлиб, ўлчами ва агрегат ҳолатига қараб тутун, туман, қурум ҳосил қилади ва ҳимоя объектидан қайтган ёруғликни тўсади. Тутунсимон моддалар ёруғликни яхши ютиш хусусиятига эга.

Кузатув ва фото суратга олишдан ҳимояланишда қуйидагилар тавсия этилади:

– ҳужжатлаштириш, кўпайтириш ва маълумотларни тасвирлаш воситалари (компьютер монитори, умумфойдаланишга мўлжалланган экран ва бошқалар)ни тўғридан-тўғри ёки масофадан кузатишнинг олдини олиш учун уларни оптимал жойлаштириш;

– ёруғлик ўтказмайдиган ойналардан, пардалардан, плёнкалардан ва бошқа ҳимоялаш ашёларидан (решетка, дераза эшиклари ва ҳоказо) фойдаланиш;

– деразалари хавфсиз зонага (йўналишга) қаратилган хоналарни танлаш;

– маълум бир вақтдан кейин компьютер монитори ва умумфойдаланиш экранларини ўчирувчи воситалардан фойдаланиш (вақт бўйича ишлаш режими).

Кузатувдан ва жойларда фото суратга олишдан ҳимоялашда маскировка чораларини кўриш, жойлашиш рельефидан фойдаланиб объектни яшириш ва объект фаолиятини яширишни таъминловчи қўриқлаш режимини ташкил этиш керак.

Қийинроқ шароитларда фаол яшириш воситалари (маскировкаловчи тутун, аэрозоллар ва бошқа воситалар)ни қўллаш мумкин.

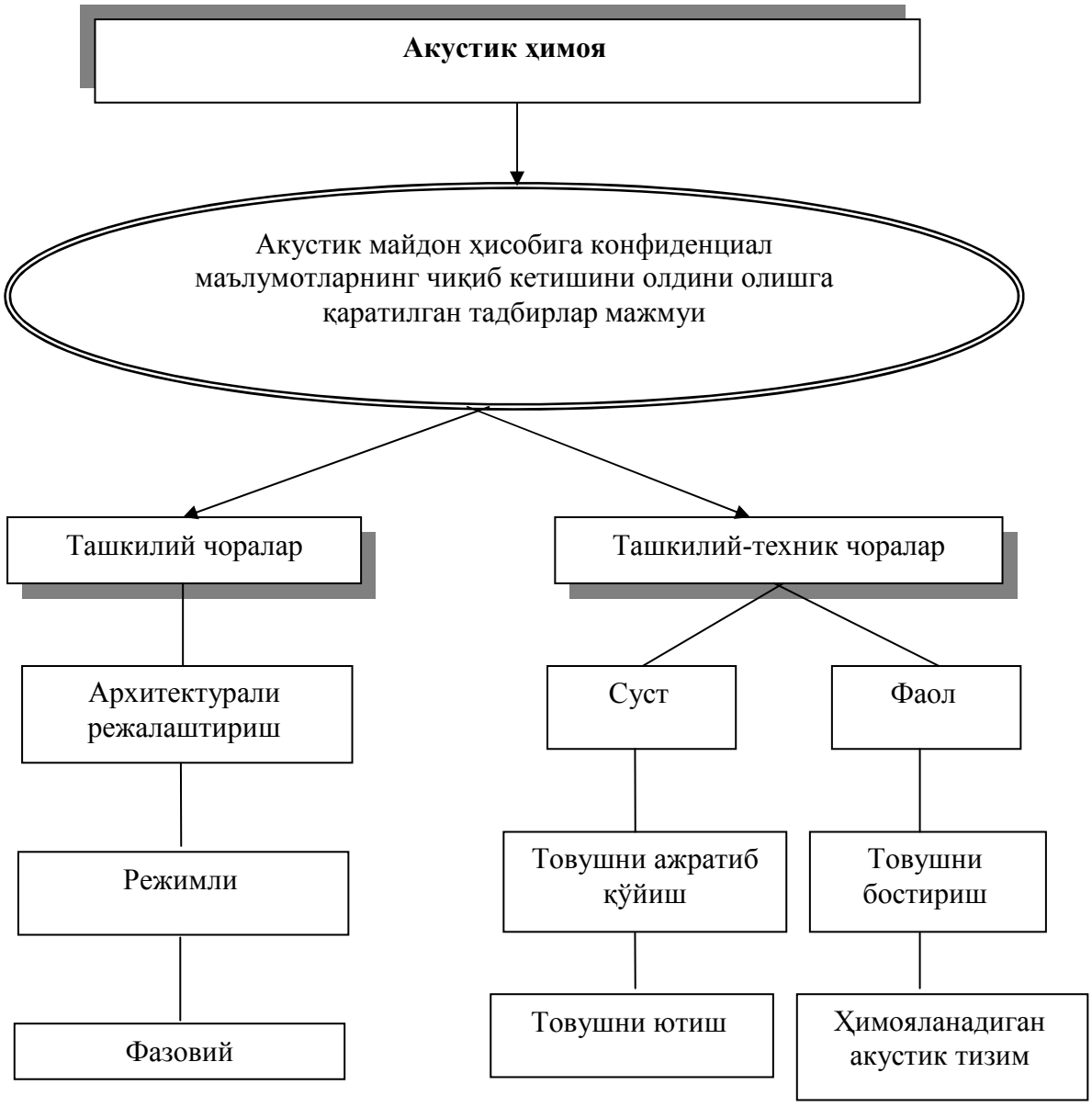
Маълумотни акустик канал орқали чиқиб кетишидан ҳимоялаш – бу конфеденциал маълумотларни акустик майдон ҳисобига назорат зонасидан чиқиб кетишини бартараф этиш ёки камайтириш бўйича комплекс тадбирлардир.

Ҳимоянинг бу туридаги асосий тадбирларга ташкилий ва ташкилий-техник чоралар киради.

Ташкилий чоралар архитектурали режалаштириш, фазовий ва режимли тадбирларни ўтказишни кўзда тутса, *ташкилий-техник чоралар* – суст (товушни ўтказмайдиган қилиш, товушни ютиш) ва фаол (товушни бостириш) тадбирлардан ташкил топади. Техник тадбирларни конфеденциал сўзлашувларни махсус ҳимояланган воситалардан фойдаланиш ҳисобига ўтказиш мумкин.

Товушни ўтказмайдиган қилиш билан ҳимоялашнинг самарадорлигини аниқлаш учун шовқин ўлчагичлар ишлатилади. *Шовқин ўлчагич* – товуш босими тебранишларини товуш босими даражасига мос кўрсаткичларга айлантирувчи ўлчов асбобидир. Одам товушини акустик ҳимоя қилиш соҳасида аналогли шовқин ўлчагичлардан фойдаланилади.

Аниқлик даражаси бўйича шовқин ўлчагичлар тўрт синфга ажратилади. Нолинчи синфдаги шовқин ўлчагичлар лабораториядаги ўлчашларда, биринчиси – табиий шароитдаги ўлчашларда, иккинчиси – умумий мақсадлардаги ўлчашларда, учинчиси – йўналтирилган ўлчашларда ишлатилади. Амалиётда акустик каналнинг ҳимояланганлик даражасини баҳолаш учун шовқин ўлчагичларнинг иккинчи синфи, кам ҳолларда биринчи синфидан фойдаланилади.



Яширинча эшитиш – разведка ва саноат айғоқчилигини олиб бориш усули бўлиб, айғоқчилар, кузатувчилар, пинҳона эшитишнинг махсус постлари, барча разведка бўлинмалари томонидан қўлланилади. Алоқанинг техник воситалари орқали узатиладиган сўзлашувлар ва хабарларни ҳам яширинча эшитиш амалга оширилиши мумкин.

Маълумки, эшитиш бевосита бўлиши мумкин, яъни гапирувчининг акустик тебранишлари тўғридан-тўғри ёки бино ва иншоатларнинг элементлари орқали эшитувчига етиб боради.

Аммо турли техник воситалар: микрофонлар, лазерлар, радиозакладка, юқори частотали тебранишлардан фойдаланиб сўзлашувларни эшитиш кенг тарқалган.

Маълумотларни электромагнит канал орқали чиқишдан ҳимоялаш – бу конфеденциал маълумотларни ёндош таснифга эга электромагнит майдон ва наводкалар ҳисобига назорат зонасидан чиқиб кетишини бартараф этиш ёки камайтириш бўйича комплекс тадбирлардир.

Маълумот чиқишининг қуйидаги электромагнит каналлари мавжуд:

– электрон схемалар элементларининг микрофон эффекти;

– юқори ва паст частотали электромагнит нурланишлар;

– паразит кучайтиргичларнинг юзага келиши;

– электрон схемаларнинг манба занжирлари ва ерга уланиш занжирлари;

– алоқа линияси ва симларнинг ўзаро таъсири;

– юқори частотали боғланишлар;

– оптик-толали тизимлар.

Электромагнит каналлардан маълумотлар чиқиб кетишини ҳимоялаш учун умумий ҳимоялаш усуллари ва айнан шу турдаги каналга мўлжалланган махсус ҳимоялаш усуллари қўлланилади. Бундан ташқари, ҳимоя чораларини конструктор-технологик ечимлар ва эксплуатацион (фойдаланиш) синфларига ажратиш мумкин.

Конструктор-технологик ечимларда маълумотларнинг чиқиб кетиши эҳтимоли мавжуд бўлган каналларнинг пайдо бўлиши бартараф этилади. Эксплуатацион ҳимояда ишлаб чиқариш ва меҳнат фаолияти шароитида турли хил техник воситаларни қўллаш орқали чиқиб кетиш каналлари тўсилади.

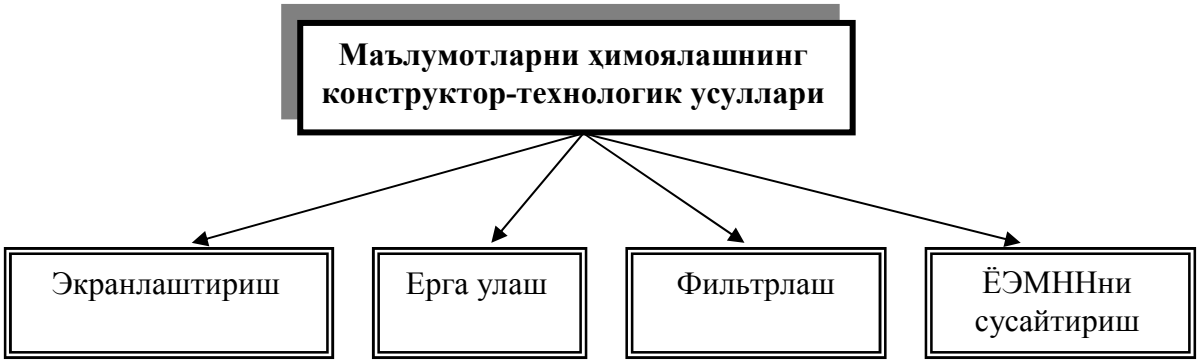
Маълумотларга ишлов берувчи ва узатувчи техник воситалардаги ЁЭМНН ҳисобидан пайдо бўлиши мумкин бўлган маълумотлар чиқиб кетиш каналини олдини олиш бўйича конструктор-технологик тадбирлар мақбул конструктор-технологик ечимларни қабул қилишга олиб келади. Унга қуйидагилар киради:

– қурилма элемент ва узелларини экранлаштириш;

– элементлар ва ток ўтказувчи симлар орасидаги электромагнит, ҳажмли, индуктив алоқаларни сусайтириш;

– манба ва ерга уланиш занжирларидаги сигналларни фильтрлаш ва ЁЭМННни сусайтириш ёки бартараф этиш каби тадбирлар.

Экранлаштириш элементларни кераксиз акустик ва электромагнит сигналлардан ва ўзининг электромагнит майдон нурланишидан ҳимоялаш имконини беради ҳамда ташқи нурланишларнинг зарарли таъсирини сусайтиради (ёки бартараф этади).



Қурилма ва унинг элементларини ерга улаш ҳамда сиртларини металл пуркаб қоплаш йўналтирилган сигналларни ерга ўтказиб юбориш, алоҳида занжирлар орасидаги зарарли алоқаларни сусайтиришнинг ишончли воситасидир.

Турли мақсадларга мўлжалланган фильтрлар пайдо бўлган ёки тарқаладиган сигналларни камайтириш ёки сусайтиришга ҳамда ахборотларни қайта ишлаш қурилмаларининг манба тизимини ҳимоя қилиш учун хизмат қилади.

Тутиб олиш – бу радиодиапазондаги электромагнит сигналларни қабул қилиш ҳисобига конфеденциал маълумотларни рухсатсиз олишдир.

Конфеденциал маълумотларни рухсатсиз олиш шаклидан бири бўлган радио тутиб олиш жиҳатларига эга:

– криминал қизиқишли объект билан бевосита боғланмасдан амалга оширилади;

– турли диапазондаги радиотўлқинларнинг тарқалиш чегараси билан аниқланадиган катта масофа ва фазода ўринли;

– йил ва куннинг ихтиёрий вақтида ва турли об-ҳавода узлуксиз таъминланади;

– маълумот айнан манбадан чиққани учун ишончли маълумотлар билан таъминлайди;

– турли статистик ва тезкор таснифдаги маълумотларни олиш имконини беради;

– қизиқтирган маълумотларни аниқ вақтда, амалга ошириладиган воқеаларни (у ёки бу амалларни бажариш ҳақидаги буйруқларни тутиш орқали) олиш имконини беради;

– яширинча амалга оширилади, чунки маълумот манбаси, одатда, рухсатсиз кирилганликни аниқлай олмайди.

Турли диапазондаги радиотўлқин нурланиш манбалари:

– мобиль ва стационар тизимлар, жумладан йўлдошлар, радиорелели ва бошқалар учун мўлжалланган радиоалоқа воситалари;

– уяли радиоалоқа воситалари;

– пейджингли алоқа воситалари;

– тезкор хизмат радиоалоқа воситалари;

– радиотелефон узайтиргич сигналлари;

– радиомикрофон сигналлари;

– техник восита ва тизимларнинг сигналлари (радиолокацион, радионавигация тизимлар, электрон-ҳисоблаш машиналари воситаларининг сигналлари);

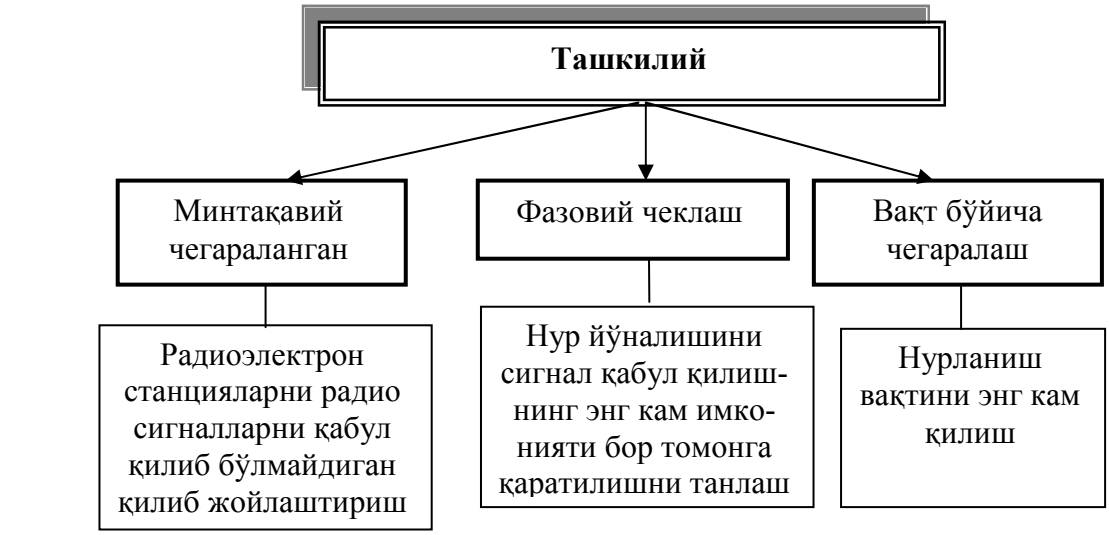
– алоқа ва технологик таснифдаги радиосигналлар очиқ нурланишининг бошқа тизимлари (масалан, самолётлар учишини таъминловчи воситалар, сувда қутқариш воситалари ва бошқалар).

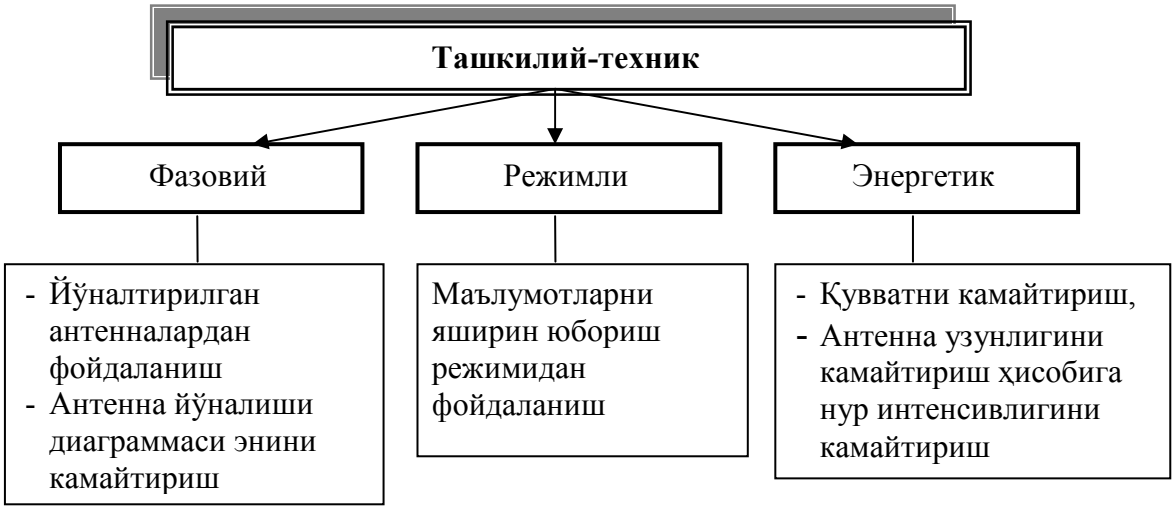
Тутиб олишдан ҳимоялаш усуллари:

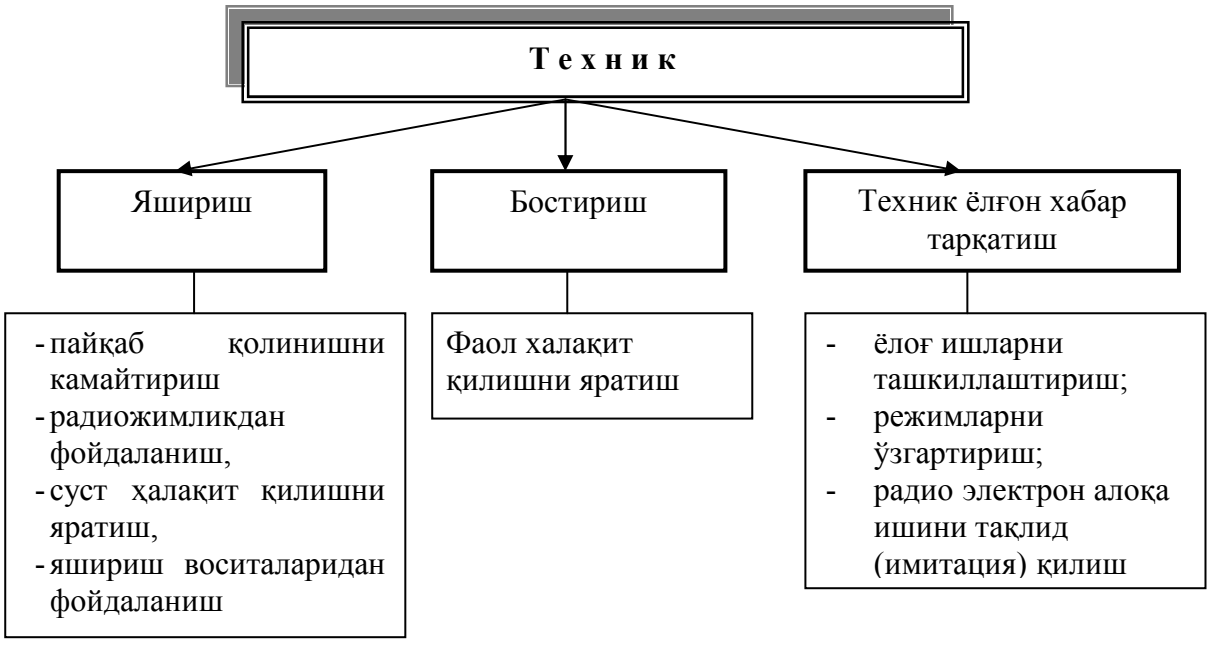
– ташкилий;

– ташкилий-техник;

– техник.


Ташкилий
Минтақавий чегараланган
Фазовий чеклаш
Вақт бўйича чегаралаш
Радиоэлектрон станцияларни радио сигналларни қабул қилиб бўлмайдиган қилиб жойлаштириш
Нур йўналишини сигнал қабул қилишнинг энг кам имконияти бор томонга қаратилишни танлаш
Нурланиш вақтини энг кам қилиш


Ташкилий-техник
Фазовий
Режимли
Энергетик
- Йўналтирилган антенналардан фойдаланиш
- Антенна йўналиши диаграммаси энини камайтириш
Маълумотларни яширин юбориш режимидан фойдаланиш
- Қувватни камайтириш,
- Антенна узунлигини камайтириш ҳисобига нур интенсивлигини камайтириш


Т е х н и к
Яшириш
Бостириш
Техник ёлғон хабар тарқатиш
- пайқаб қолинишни камайтириш
- радиожимликдан фойдаланиш,
- суст ҳалақит қилишни яратиш,
- яшириш воситаларидан фойдаланиш
Фаол халақит қилишни яратиш
- ёлоғ ишларни ташкиллаштириш;
- режимларни ўзгартириш;
- радио электрон алоқа ишини тақлид (имитация) қилиш

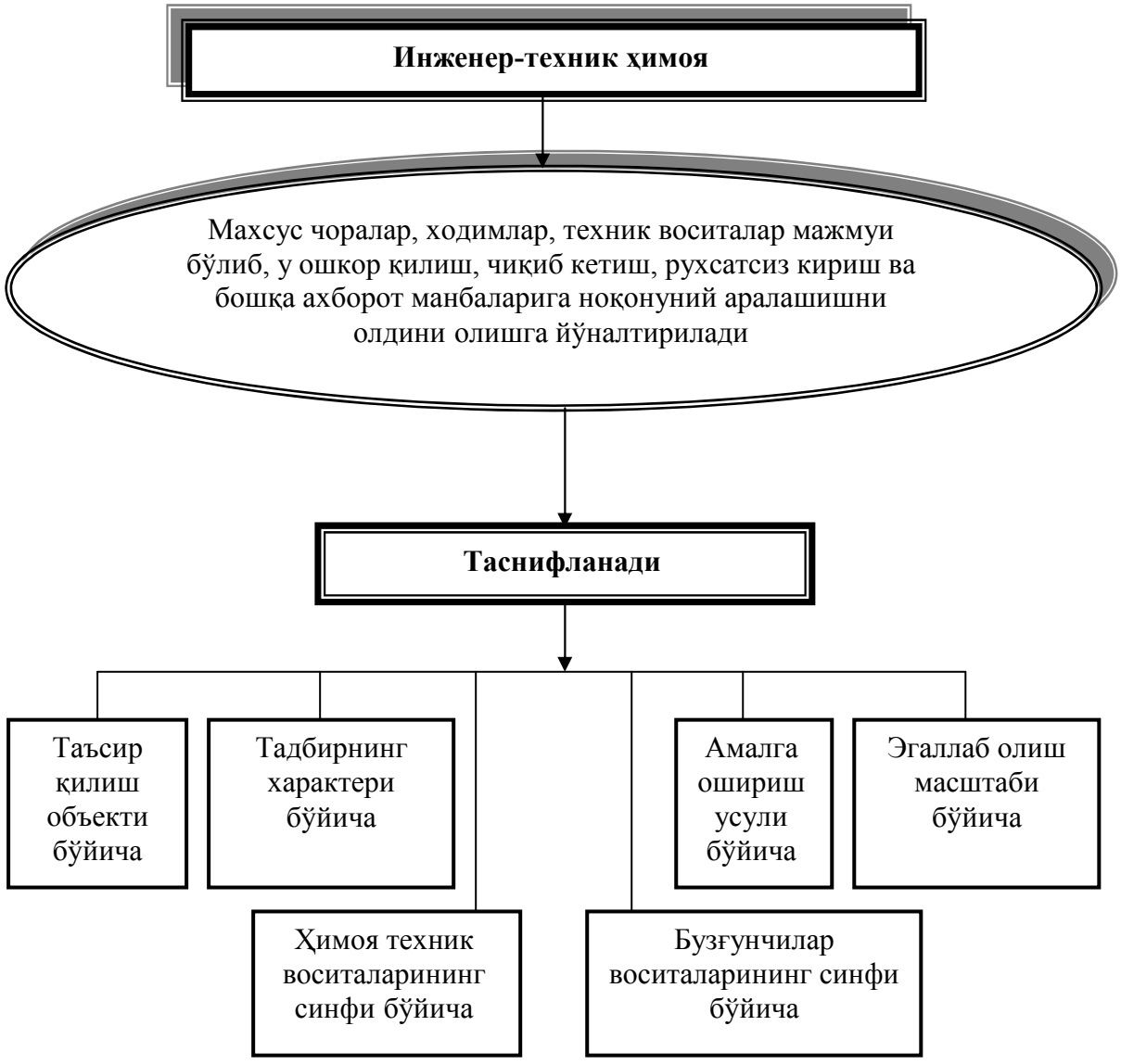
2.4. Ахборотларни инженер-техник ҳимоялаш

Инженер-техник ҳимоянинг таснифи – бу конфеденциал маълумотларни ҳимоялашга қаратилган махсус идоралар, техник воситалар ва тадбирлар мажмуидир.

Мақсад, вазифа, ҳимоя объектлари ва ўтказиладиган тадбирларнинг турличалиги кўриниш, йўналганлик ва бошқа тавсифлар бўйича воситаларнинг синфланиш тизимини қараб чиқишни тақозо этади.

Масалан, ҳимоянинг инженер-техник воситаларини таъсир қилиш объектлари бўйича қараш мумкин. Шу маънода улар инсонларни, моддий бойликларни, молияни, маълумотларни ҳимоялаш учун қўлланилиши мумкин.

Қуйидаги расмда инженер-техник ҳимоянинг тахминий синфланиш тузилиши келтирилган:



Классификация тавсифларининг турличалиги инженер-техник воситаларни таъсир объекти, тадбир тавсифи, амалга ошириш усули, эгаллаш масштаби, ёвуз ниятлилар воситаларининг синфи бўйича қараш имконини беради. Уларга қарши фаолиятни хавфсизлик хизмати кўрсатади.

Функционал вазифаси бўйича инженер-техник ҳимоя воситаларини гуруҳларга ажратиш мумкин:

– *физик воситалар*. Улар ҳимоя объектларига ва конфеденциал маълумотли моддий ташувчиларга ёвуз ниятлиларни киришига (ёки фойдаланишига) тўсқинлик қиладиган турли восита ва иншоатлардан ташкил топади ва ходимларга, моддий бойликларга, молия ҳамда ахборотларга ноқонуний таъсир қилишдан ҳимоялашни амалга оширади;

– *аппарат воситалари.* Бунга ахборотларни ҳимоя қилиш учун ишлатиладиган асбоблар, жиҳозлар, ускуналар ва бошқа техник воситалар киради. Ташкилотларнинг иш фаолиятида жуда кўп қурилмалар, телефон аппаратларидан тортиб автоматлаштирилган тизимларгача ишлатилади. Аппарат воситаларининг асосий вазифаси – ишлаб чиқариш фаолиятидаги техник воситалар орқали маълумотларнинг ошкора бўлиши, чиқиб кетиши ва уларга рухсатсиз киришдан қатъий ҳимоя қилишдир;

– *дастурий воситалар*. Улар махсус дастурлардан, дастурий комплекслардан ва турли мақсадларга йўналтирилган ахборот тизимларидаги ва маълумотларни қайта ишлаш воситаларидаги ҳимоя тизимларидан иборат;

– *криптографик воситалар* – бу маълумотларни ҳимоялашнинг махсус математик ва алгоритмик воситаларидир. Маълумотлар тизим ва алоқа тармоғи орқали узатилишида, компьютерда сақланишида ва қайта ишланишида турли шифрлаш усуллардан фойдаланилади.

Ҳимоянинг аппарат воситалари ва усуллари кенг тарқалган. Бироқ, улар етарлича ўзгарувчанликка эга бўлмаганлиги сабабли ҳимояланган ишлаш принципларининг ошкора бўлиши улардан кўпинча келажакда фойдаланишни йўққа чиқаради.

Ҳимоянинг дастурий воситалари ва усуллари ишончли бўлиб, уларнинг кафолатли ишлатилиши аппарат воситаларга нисбатан анча кенг.

Криптографик усул муҳим аҳамиятга эга бўлиб, маълумотлар ҳимоясини узоқ вақтга сақлашни таъминлайдиган восита ҳисобланади.

Маълумотларни ҳимоялаш воситаларининг бундай тақсимлаш шартли ҳисобланиб, амалиётда улар кўпинча: бир-бирини тўлдиради, комплекс (маълумотларни беркитиш алгоритмларидан кенг фойдаланувчи аппарат-дастурий модуль) шаклда намоён бўлади.

Ҳимоя тизимини ишлаб чиқиш босқичлари.

Биринчи босқичда (ҳимоя объектини таҳлили) нимани ҳимоя қилиш аниқланади:

– ҳимоялаш керак бўлган маълумотни аниқлаш;

– ҳимояланадиган маълумотнинг муҳим элементларни ажратиш;

– ҳимояланадиган маълумот муҳим элементининг яшаш муддатини аниқлаш (рақобатчи томонидан қўлга киритилган маълумотни очиш учун вақт);

– ҳимояланаётган маълумотларни тавсифини акс эттирувчи калит элементларни (индикаторларни) аниқлаш;

– корхонанинг фаолият зонаси (ишлаб чиқариш – технологик жараёнлари, ишлаб чиқаришнинг моддий-техник таъминоти тизими, бошқарув бўлинмалари) бўйича индикаторларини классифи-кациялаш.

Иккинчи босқич хавфни аниқлашдан иборат:

– ҳимояланадиган маълумот билан ким қизиқиши мумкинлиги аниқланади;

– рақобатдошларнинг маълумотни олиш учун фойдаланадиган усуллари баҳоланади;

– маълумот чиқиши мумкин бўлган каналлар аниқланади;

– рақобатдош ёки ихтиёрий бузғунчиларнинг ҳаракатини чегаралаш бўйича тадбирлар тизими ишлаб чиқилади.

Учинчи босқичда қабул қилинган ва доимий ишлатиладиган хавфсизликни таъминлаш тизимининг самарадорлигини таҳлил қилиш (ҳужжатларнинг физик хавфсизлиги, ходимларнинг ишончлилиги, конфеденциал маълумот юбориладиган алоқа каналининг хавфсизлиги ва бошқалар) амалга оширилади.

Ҳимоя объекти ва маълумот чиқиб кетиш техник каналини моделлаштириш асослари. Зарар келтирувчи кўп сонли манбаларни, объектларни ва таъсирларни таҳлил қилиш учун моделлаштириш усулларидан фойдаланиш мақсадга мувофиқдир. Чунки бунда реал ҳолатларни «ўрнини босувчи» моделлардан фойдаланилади. Модель оригиналга нисбатан содда ҳисобланади. Шу билан бирга, реал ҳолатни, унинг мураккаб томонларини ҳисобга олган ҳолда тасвирлаш учун етарлича умумий бўлиши керак.

Ахборот хавфсизлиги концептуал моделининг ташкил этувчилари қуйидагилар бўлиши мумкин:

– хавф-хатар объектлари;

– хавф-хатарлар;

– хавф-хатарлар манбаи;

– ёвуз ниятлилар томонидан бўладиган хавф-хатарларнинг мақсади;

– маълумотлар манбаи;

– конфеденциал маълумотларни қонунга хилоф равишда эгаллаш усуллари (кириш усуллари);

– маълумотларни ҳимоялаш йўллари;

– маълумотларни ҳимоялаш усуллари;

– маълумотларни ҳимоялаш воситалари.

Ҳозирги кунда барча ташкилотларда маълумотларни ҳимоялаш долзарб вазифалардан бирига айланган. Бу эса ўз навбатида маълумотлар хавфсизлигини физик сатҳда ҳам таъминлаш заруратини келтириб чиқаради.

Маълумотларни ҳимоялашнинг техник воситаларига, ҳимоя объектига бориш йўлига тўсиқларни ҳосил қилишга мўлжалланган, маълумотларни ҳимоялашни мустақил ёки бошқа воситалар билан комплексда амалга оширувчи механик, электромеханик, электрон-механик, оптик, акустик, лазер, радио, радиолокацион ва бошқа қурилмалар ҳамда тизим ва бинолар киради.

Маълумотларни ҳимоялаш муаммоси пайдо бўлганга қадар ҳимоянинг физик воситалари мавжуд эди. Улар банк, дўкон, музей ва шу кабиларни анчадан бери маълум бўлган қўриқлаш воситаларидан деярли фарқ қилмайди. Маълумотлар сақланадиган ва уларга ишлов бериладиган объектларни ва маълумотларнинг ўзини ҳимоялаш учун мураккаб ва такомиллашган усулларидан фойдаланилади.

Физик воситалар маълумотлар ва ҳисоблаш тизими элементлари ҳимоясининг биринчи чизиғи ҳисобланади. Шунинг учун ҳам бундай тизим ва қурилмаларнинг физик бутлигини таъминлаш маълумотлар ҳимоясининг зарурий шарти ҳисобланади. Ривожланган хорижий давлатларда ҳимоянинг физик воситалари қўлланишига ва такомиллашувига катта эътибор қаратилмоқда.

Физик ҳимоя воситаларининг асосий вазифалари:

1. Ҳудудни қўриқлаш.
2. Асбоб-ускуналар ва маълумот ташувчиларни қўриқлаш.
3. Ички хоналарни қўриқлаш ва уларни кузатиш.

4. Назорат зоналарига назоратли ўтишни жорий қилиш.
5. Наводка ва нурланишларнинг таъсирини йўқотиш.
6. Визуал кузатувларга тўсқинлик қилиш.
7. Ёнғинга қарши ҳимоя.
8. Бузғунчи шахсларнинг ҳаракатини блокировка қилиш.

Ташкилотлардаги маълумотларни электрон қайта ишлаш марказлари кучли электромагнит нур манбаи бўлган объектлардан узоқда жойлашган бўлиши ва атрофи девор билан ўралиши керак. Назорат зонасини кузатиш телевизион, радиолокацион, лазерли, оптик, акустик ва бошқа умумий пультга уланган тизим орқали амалга оширилиши мумкин.

Объектлар хавфсизлигини таъминлаш тизимларининг умумий тузилиши қуйидаги расмда келтирилган. Аниқ ҳолатлар учун схеманинг айрим элементлари бўлмаслиги ёки айрим элементлар қўшилиши мумкин.

Одатда, объектнинг хавфсизлигини таъминлаш қуйидаги тамойилларга асосланади:

– объектга бўлган хавф-хатарни аниқлаш ва баҳолаш;

– адекват (мос) ҳимоя чораларини ишлаб чиқиш ва уларни қўллаш.

Адекват ҳимоялашда қуйидаги ва чоралари чоралар кўзда тутилади:

– объект ҳудуди, бино ва хоналарига рухсатсиз киришни умумий назорат қилиш;

– «ёпиқ» бино ва хоналарга кирувчи одамларни чеклаш ва назорат қилиш ҳамда назорат натижаларини ҳужжатлаштириш;

– ёвуз ниятли шахсларни олдига қўйган мақсади томон ҳаракатининг бошланғич босқичида аниқлаш;

– вазиятни баҳолаш;

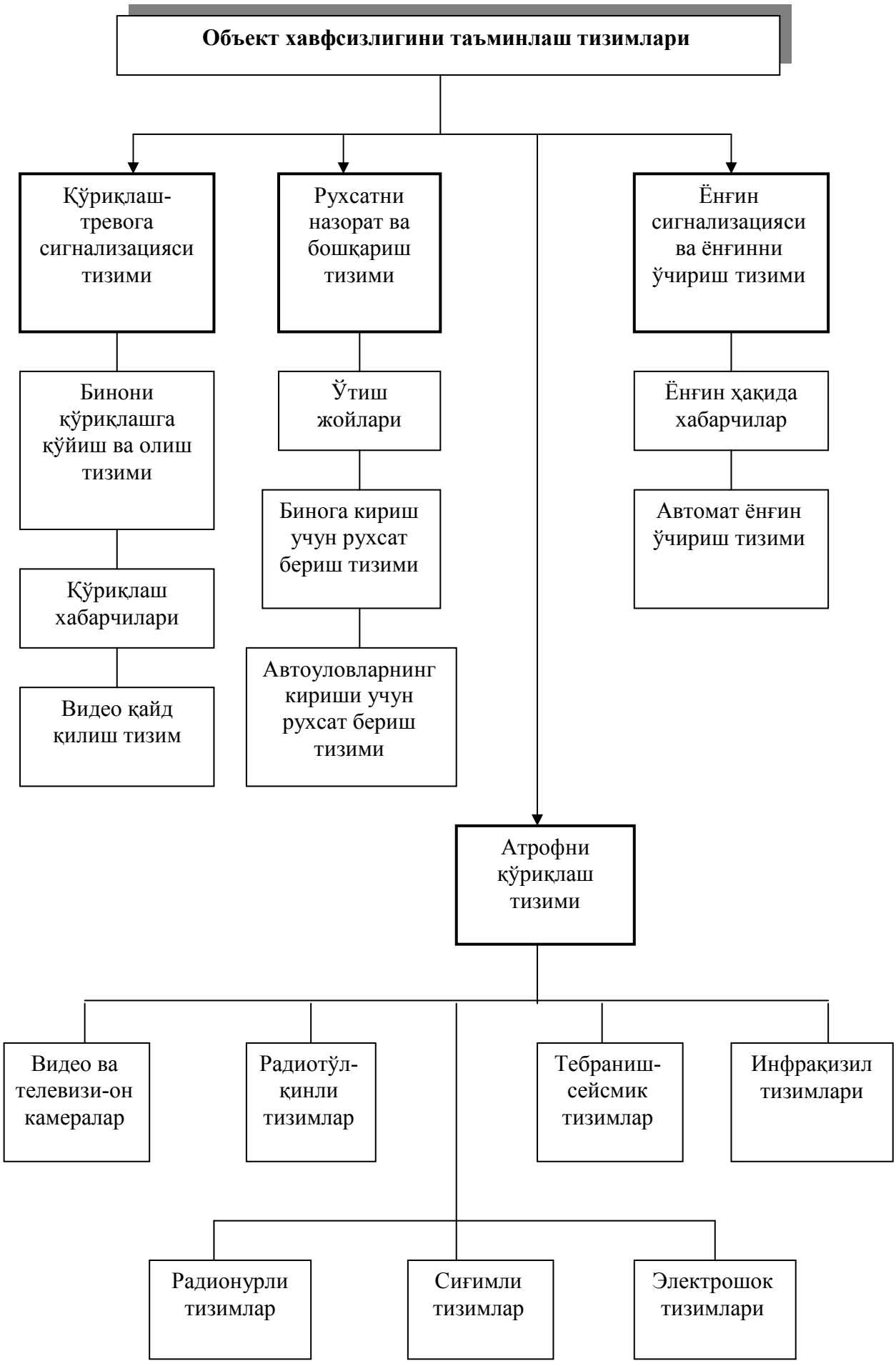
– тартиббузарни ушлаш учун қўриқловчилар томонидан унинг йўналишини физик тўсиқлар орқали тўсиш;

– ёвуз ниятли шахслар ҳаракатини тўхтатиш учун тезкор чораларни қўллаш;

– объектнинг ўта муҳим участкаларидаги ходимлар ҳаракатини видеоҳужжатлаштириш.

Қўриқлаш-огоҳлантириш сигнализация тизими (ҚОС):

– биноларни қўриқлашни қабул қилади ва топширади;


Объект хавфсизлигини таъминлаш тизимлари
Қўриқлаш-тревога сигнализацияси тизими
Рухсатни назорат ва бошқариш тизими
Ёнғин сигнализацияси ва ёнғинни ўчириш тизими
Бинони қўриқлашга қўйиш ва олиш тизими
Ўтиш жойлари
Ёнғин ҳақида хабарчилар
Қўриқлаш хабарчилари
Бинога кириш учун рухсат бериш тизими
Автомат ёнғин ўчириш тизими
Видео қайд қилиш тизим
Автоуловларнинг кириши учун рухсат бериш тизими
Атрофни қўриқлаш тизими
Видео ва телевизи-он камералар
Радиотўл-қинли тизимлар
Тебраниш-сейсмик тизимлар
Инфрақизил тизимлари
Радионурли тизимлар
Сиғимли тизимлар
Электрошок тизимлари

– ёпилган ва қўриқлашга топширилган бинога бегона шахсларнинг рухсатсиз киришларида ёки киришга ҳаракат қилишларида тревога сигналини беради;

– интеграллашган хавфсизлик тизимининг автоматлаштирилган иш жойида қўриқланаётган бинонинг ҳолатини бу бино плани бўйича график режимда кузатади ҳамда планда тревога сигналини ёки носозликларни график, матн ва товуш шаклида акслантиради;

– компьютер хотирасида ҚОС тизимининг ҳолати ҳақида баённома юритади ҳамда уни кўриш ва чоп этиш имконини беради;

– стандарт ва ностандарт ҳолатларда оператор фаолиятини қайд этувчи электрон журнални юритади.

Киришни назорат қилиш ва бошқариш тизими (КНБТ) рухсат этилган ходимларга ташкилот ҳудудига, кириш чекланган хона ва зоналарга киришига ҳамда рухсати йўқларга тўсиқ бўлишга йўналтирилган комплекс тадбирларни бажариш учун мўлжалланган.

Ёнғин ҳақида сигнал бериш тизими:

– бинода аниқланган ёнғин манбаси жойидаги датчиклардан келаётган хабарларни қўриқлаш пости хонасига юбориш (ҳар бир датчик «диққат» ва «ёнғин» деган хабарларни бериши учун алоҳида сезгирлик бўйича созланиши ҳамда бу созлашлар кундузги ва кечки режимлар учун ҳар хил бўлиши керак);

– носоз датчик манзилини кўрсатувчи хабар қўриқлаш постига юбориш;

– одамларга ёнғин ҳақида хабар бериш ва вентиляция тизимлари орқали ҳаво оқими келишини тўсиб қўйиши

– автомат равишда ёнғин ўчириш қурилмаларини бошқариш;

– юқоридаги талабларни бажаришда автоном режимда ишлаши;

– ёнғин содир бўлганлиги ҳолати ва вақтини қайд этиш ҳамда ҳодиса ҳақидаги хабарнинг операторлар иш жойидаги мониторларда акс эттириш;

– интеграллашган хавфсизлик тизимининг автоматлаштирилган иш жойида қўриқланаётган бинонинг ҳолатини бу бино плани бўйича график режимда кузатиш ҳамда планда «ёнғин» сигналини ёки носозликларни график, матн ва товуш шаклида тасвирлаш;

– компьютер хотирасида ёнғин тизимининг ҳолати ҳақида баённома юритилиш ҳамда уни кўриш ва чоп этиш имконини бериш;

– стандарт ва ностандарт ҳолатларда оператор фаолиятини қайд этувчи электрон журнални юритиш учун мўлжалланади.

Объектни периметри бўйича қўриқлашни ташкил этишда унинг

ички ҳудуди (қўриқланадиган майдон) шартли равишда: аниқлаш, кузатиш, тўхтатиб қолиш, нишонга олиш каби бир неча функционал зоналарга бўлиб, ҳар бир зонада ўзига хос техник воситалар жойлашиши керак.

Мустақил тайёргарлик учун саволлар

1. Ахборотларни муҳофаза қилишнинг техник воситалари тушунчаси нимани англатади?

2. Маълумотларни рухсатсиз олишнинг объектлари, усуллари ва воситалари нималардан иборат?

3. Маскировкаловчи белгиларнинг очилиши тушунчасини нимани билдиради?

4. Демаскировка белгилари нималар билан фарқ қилади?

5. Ҳимоя объектларининг демаскировка белгиларига нималар киради?

6. Техник воситалар билан ҳимояланадиган маълумотларнинг манбалари ва ташувчилари нималардан иборат?

7. Объектнинг демаскировка белгилари қандай гуруҳларга бўлинади?

8. Объектнинг кўринадиган ва инфрақизил электромагнит спектр диапазонларидаги демаскировка белгилари нималардан иборат?

9. Радиоэлектрон воситаларнинг қандай демаскировка белгилари мавжуд?

10. Нималар маълумот ташувчи воситалар ҳисобланади?

11. Маълумотлар чиқиш канали деб нимага айтилади?

12. Маълумотлар чиқиб кетиш канали қандай гуруҳларга ажратилади?

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

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

15. Маълумотларни визуал-оптик канал бўйича чиқиб кетишидан ҳимоялаш қандай амалга оширилади?

16. Акустик канал орқали маълумот чиқишидан ҳимоялашда қандай чоралар кўрилади?

17. Маълумот чиқишининг қандай электромагнит каналлари мавжуд?

18. Маълумотларни ҳимоялашнинг қандай конструктор-технологик усуллари бор?

19. Тутиб олишдан ҳимоялашнинг қандай усуллар мавжуд?

20. Инженер-техник ҳимоя тушунчаси нимани билдиради?

21. Функционал вазифаси бўйича инженер-техник ҳимоя воситалари қандай гуруҳларга ажратилади?

22. Ҳимоя тизимини ишлаб чиқиш босқичлари нималардан иборат?

23. Физик ҳимоя воситаларининг асосий вазифаларига нималар киради?

24. Объект хавфсизлигини таъминлаш тизимлари нималардан иборат?

III. АХБОРОТЛАРНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

3.1. Криптография: унинг асосий тушунчалари ва қисқача тарихи.

3.2. Содда шифрлар ва уларнинг хоссалари.

3.3. Очиқ ва ёпиқ калитлар билан шифрлаш тизими.

Криптография ахборотни муҳофаза қилиш усулларидан бири ҳисобланади. Криптография ахборот (маълумотлар)ни ўзгартириш тамойиллари, воситалари ва усулларини тадқиқ этади. Бундан мақсад ахборот мазмунидан рухсат этилмаган фойдаланишдан муҳофазалаш ва уни бузишни бартараф қилиш. Криптография маълумотларни алоқа каналлари орқали узатишда ёки сақлашда конфеденциалликни ёки ҳақиқийликни таъминлаш усуллари билан шуғулланади.

Шу билан бирга криптография маълумотларни хабардор бўлмаган шахслар учун тушуна олмайдиган қилиш мақсадида ўзгартириш усули ҳамдир. Маълумотлар хавфсизлиги тизимининг муҳим таркибий бўлаги. Унинг моҳияти маълумотларни узатишдан олдин маъносиз белгилар ёки сигналлар йиғмасига айлантириш ва маълумотларни олувчи қабул қилиб олгандан сўнг, уларни дастлабки шаклига қайта тиклашдир.

3.1. Криптография: асосий тушунчалари ва қисқача тарихи

Инсоният ахборотни ҳимоя қилиш муаммоси билан ёзув пайдо бўлгандан бери шуғулланади. Бу муаммо ҳарбий ва дипломатик маълумотларни яширинча узатиш заруратидан келиб чиққан. Масалан, антик спарталилар ҳарбий маълумотларни шифрлашган. Хитойликлар томонидан оддий ёзувни иерогрифлар кўринишида тасвирлашлари уни хорижийлардан яшириш имконини берган.

«Криптография» атамаси грек тилидан таржима қилинганда «яшириш, ёзувни беркитиб қўймоқ» маъносини билдиради. Атаманинг маъноси криптография керакли маълумотни яширин сақлаш ва ҳимоялаш мақсадида кўлланишини англатади.

Криптография ахборотни ҳимоялаш воситаси, шунинг учун у ахборот хавфсизлигини таъминлашнинг бир тармоғи ҳисобланади.

Криптологиянинг (крипто – яширин, логия – фан, билим) ривожланишини *учта босқич*га ажратиш мумкин. *Биринчи босқич* – криптологияни фан сифатидан эътироф этилмаган даври, тор доирадаги қизиқувчиларга хос фаолият тури бўлган. *Иккинчи босқич* 1949 йилдан бошланиб, К.Шеноннинг «*Махфий тизимларда алоқа назарияси*» номли рисоланинг чоп этилиши билан боғланади. Бу рисолада шифрлашнинг фундаментал илмий тадқиқоти ва унинг мустаҳкамлиги ёритиб берилган. Бу китобнинг чоп этилиши криптология амалий математиканинг таркибий қисми сифатида шаклланишига асос бўлди. Ва, ниҳоят *3-босқич* 1976 йилда У.Диффи ва М.Хеллман томонидан «*Криптографиянинг янги йўналишлари*» номли асарнинг чоп этилиши билан белгиланади. Унда махфий алоқа, ёпиқ калитни аввалдан бермасдан ҳам, амалга ошириш мумкинлиги баён этилган. Ушбу санадан бошлаб то ҳозирги кунгача анъанавий классик криптография билан бир қаторда очиқ калитли криптографиянинг интенсив ривожланиши давом этмоқда.

Бир неча асрлар давомида ёзувнинг пайдо бўлишини ўзи ахборотни ҳимоялаш сифатида эътироф этилар эди, чунки ёзувни ҳамма ҳам тушунмас эди.

Эрамиздан олдинги XX аср. Месопатамияда ўтказилган қазилмалар вақтида энг қадимий шифрланган матнлар топилган. Лойдан ясалган тахтачага қозиқчалар билан ёзилган матн ҳунармандларнинг сопол буюмларини қоплаш учун тайёрланадиган бўёқнинг рецепти бўлиб, у тижорат сири ҳисобланган. Қадимги мисрликларнинг диний ёзувлари ва тиббиёт рецептлари ҳам маълум.

Эрамиздан олдинги IX асрнинг ўрталари. Плутарх берган маълумотларига кўра, ана шу даврда шифрловчи қурилма – скиталь, қўлланилган бўлиб, у ўрин алмаштиришлар орқали матнни шифрлаш имконини берган. Матнни шифрлашда сўзлар бирор диаметрли цилиндрга (скиталга) ўралган энсиз лентага ёзилган. Лента ёйилганда унда очиқ матн ҳарфларининг ўринлари алмаштирилган ҳолати ҳосил бўлган. Бунда калит сифатида цилиндрнинг диаметри хизмат қилган. Бундай матнни шифрдан ечиш усулини Аристотел таклиф этган. У лентани конусга ўраган ва ўқилиши мумкин бўлган сўз ёки сўзнинг бир қисмини кўрсатувчи жой цилиндрнинг диаметри деб ҳисоблаган.

Эрамизнинг 56 йили. Ю.Цезарь галлар билан уруш вақтида ширфлашнинг алмаштириш турини қўллаган. Очиқ матн алфавити

остига цикл бўйича (Цезарда учта позицияга) силжитиш орқали шу алфавит ёзилган. Шифрлашда очиқ матндаги алфавитлар, 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. Алфавит квадрат жадвал кўринишида тасвирланади. Шифрлашда очиқ матн ҳарфи жадвалдаги иккита сонга алмаштирилган – мос тушувчи ҳарфнинг жойлашган устун ва қатор рақамларига. Алфавитни жадвалда ихтиёрий тарзда жойлаштириш ва у орқали қисқа хабарни шифрлаш замонавий қарашлар нуқтаи назари бўйича ҳам мустаҳкам шифрлаш ҳисобланади. Бу ғоя биринчи жаҳон урушида мураккаб шифрлашларда амалга оширилган.

*V аср*да Рим империясининг емирилиши фан ва санъат, шулар қаторида криптография ривожланишининг тўхташига сабаб бўлди. У пайтларда черков махфий белгилар билан ёзилган хатни таъқиб қилган ва уни афсунгарлик ва жодугарлик деб ҳисоблаган. Чунки маълумотларни шифрлаш черков томонидан уларни назорат қилиш имконини бермас эди.

Француз роҳиби ва файласуфи Р.Бэкон (1214–1294) махфий ёзувнинг еттита тизимини баён этган. У даврларда кўпгина шифрлар илмий ахборотларни яшириш учун қўлланилган.

XV асрнинг иккинчи ярми. Ватиканда ишлаган, архитектор ва математик, шифрлар тўғрисидаги китоб муаллифи Леон Батиста Альберта иккита концентрик айлана асосида алмаштириш шифрини баён қилган. Биринчи айланага очиқ матннинг алфавити жойлаштирган бўлса, иккинчисига шифрловчи алфавит ёзилган. Бу шифрловчи алфавитдаги ҳарфлар кетма-кет жойлаштирилмаган. Матнда ҳарфларнинг турли даражада қайтарилиш хусусиятини Альберта биринчи бўлиб шифрни ечиш учун қўллаган. Шунингдек, шифрлашнинг мустаҳкамлигини ошириш учун бошқа шифрлаш тизимлари ёрдамида қайта шифрлашни таклиф этган.

Тарихдан маълумки, 1546 йилда Франция қироли Франциск I фуқароларига шифрлашни тақиқловчи фармон эълон қилган. Ваҳоланки, у даврдаги шифрлар оддий бўлишига қарамай, уларни очиб бўлмас эди.

Германиялик Иоганн Тритемий (1462–1516) 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, 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).

Италиялик математик, механик, врач Джироламо Кардано (1506–1576) Кардано панжараси деб номланган шифрлаш тизимини ихтиро қилган. Иккинчи жаҳон уруши вақтида Буюк Британия ҳарбий-денгиз қўшинларининг мустаҳкам шифрларидан бири шу тизим асосида яратилган. Панжаралар чизилган картон бўлагида ихтиёрий тартибда номерланган тешикчалар қилинган. Шифрланган матнни ҳосил қилиш учун, картон бўлагини қоғозни устига қўйиб, картоннинг тешиклари бўлган жойларига танланган тартибда ҳарфлар ёзиб чиқилган. Картон олиб ташлангандан сўнг, ёзилган ҳарфларнинг оралари псевдомазмунли жумлалар билан тўлдирилган, шу орқали шифрланган хабар яратилган. Агар ҳарфлар орасидаги масофалар катта бўлиб, сўзлар узунлиги кичик бўлса (масалан инглиз тилидаги сўзлар), яшириш осон амалга оширилган.

XVI аср. 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.

XVII аср. Франция қироли Людовик XIII ҳузуридаги вазир кардинал Ришелье дунёда биринчи бўлиб шифрлаш хизматини ташкил этган.

Лорд Френсис Бэкон (1562–1626) 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.

XVII асрда луғатли шифрлар ихтиро этилган. Шифрлашда очиқ матн ҳарфлари иккита сон билан белгиланган. Бунда кенг тарқалган китоблардан бири олиниб, шифрланувчи ҳарф китобнинг маълум бетидаги қатор номери ва ҳарф номерига алмаштирилган. Бу тизим мустаҳкам шифрлаш усули ҳисобланади, лекин ундан фойдаланиш

қулай эмас. Шу билан бирга, китоб рақиб қўлига тушиб қолиши эҳтимолидан ҳоли эмас.

Маълумки, криптографик воситалар ҳозирги вақтгача асосан давлат сирларини ҳимоя қилишга қаратилган эди, шунинг учун бу воситалар махсус органлар томонидан яратилган. Бунда юқори криптомустаҳкамликка эга бўлган криптотизимлар қўлланилган, бу эса катта харажатларни талаб қилган. Охирги йилларда маълумотларни криптографик ўзгартиришнинг янги усуллари интенсив ишлаб чиқилмоқда, улар анъанавий қўлланишига қараганда кенгроқ соҳаларга татбиқ этилмоқда.

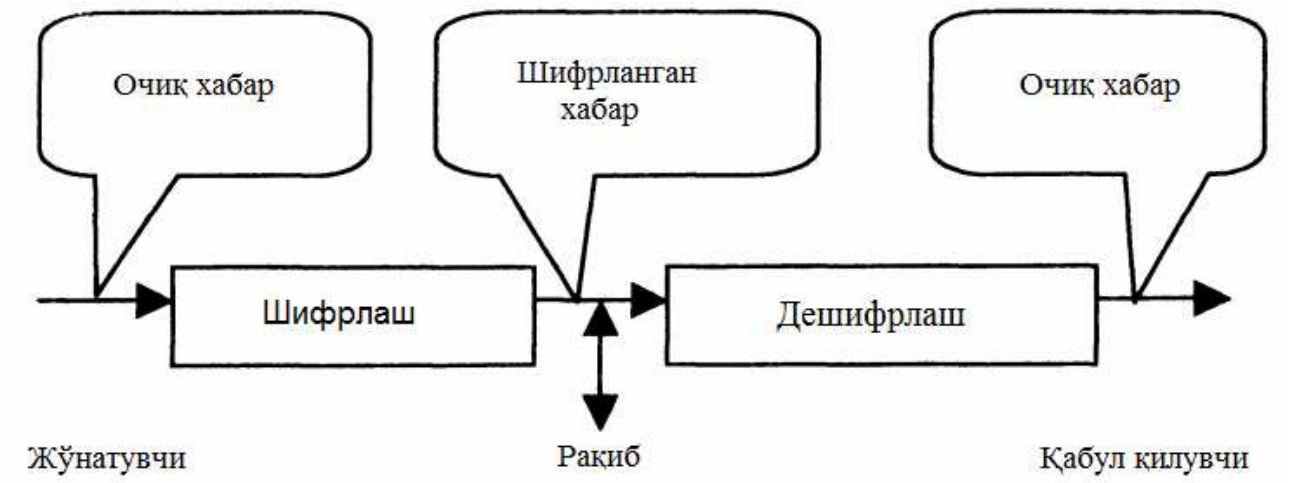
Автоматлаштирилган тизимларда маълумотлар ҳимоясининг криптографик усуллари ҳисоблаш техникаси воситаларида қайта ишланаётган ёки ҳар хил турдаги сақлаш қурилмаларида сақланаётган маълумотларни ҳимоялашда, шунингдек алоқа линиялари орқали тизим элементларига узатилаётган маълумотларни ҳимоялашда қўлланилади. Ҳозирги вақтда кўплаб ҳар хил шифрлаш усуллари ишлаб чиқилган ва уларни қўллашнинг назарий ва амалий асослари яратилган.

Ахборот тизимларида криптографик усуллар кенг қўлланилмоқда. Чунки компьютер тармоқлари, жумладан Интернет жадал ривожланмоқда. Тармоқ орқали давлат, ҳарбий, тижорат ва хусусий таснифга эга катта ҳажмдаги маълумотлар узатилмоқда. Бу маълумотларга бегона шахсларнинг кириши мумкин эмас. Шу билан бирга, юқори қувватли компьютерларнинг, тармоқ ва нейрон ҳисоблаш технологияларининг пайдо бўлиши аввал ўта мустаҳкам, амалда ечими йўқ деб ҳисобланган криптографик тизимларни обрўсизлантирди. Бу эса замонавий криптографик усуллардан фойдаланиш ўта долзарб эканлигини англатади.

Замонавий криптография ахборот хавфсизлигининг *конфеденциаллик*, *бутунлик*, *аутентификация* ва *томонларнинг муаллифликни инкор этолмасликлари* муаммоларини ҳал этувчи билим соҳаси ҳисобланади.

*Конфеденциаллик*ни таъминлаш деганда ахборот билан танишиш ҳуқуқи бўлмаган шахслардан бу ахборотни ҳимоялаш тушунилади.

Рақиб томонидан назоратда бўлган алоқа канали орқали узатиладиган хабарнинг конфеденциаллигини таъминлаш муаммоси криптографиянинг анъанавий масалаларидан ҳисобланади. Оддий ҳолда бу муаммо учта субъект (томонлар)нинг ўзаро муносабати сифатида баён этилади. Ахборот эгаси (жўнатувчи), рақибдан ҳимоя



қилиш мақсадида, очиқ канал орқали қабул қилувчига юборилаётган очиқ маълумотни ўзгартиради, яъни шифрлайди.

Узатилаётган хабар маъноси билан танишиш ҳуқуқи йўқ субъект рақибни англатади. Дешифрлаш билан шуғулланувчи крипто-таҳлилчи ҳам рақиб сифатида қаралиши мумкин. Олинган хабарни ҳақиқий қабул қилувчи *дешифрлайди*. Рақиб эса ҳимояланган хабарга эгалик қилмоқчи бўлади, унинг ҳаракати *ҳужум* ҳисобланади. Ҳужум *фаол* ёки *суст* бўлиши мумкин. *Суст* ҳужум яширин эшитиш, трафикни таҳлил қилиш, шифрланган хабарни қўлга киритиш, *дешифровка қилиш*, яъни ҳимояни «синдириш»га қаратилган ҳаракатлар ҳисобланади. *Фаол* ҳужумда рақиб хабарни узатиш жараёнини тўхтатиб қўйиши, қалбаки хабарлар юбориши ёки шифрлаб узатилаётган хабарни модификация қилиши мумкин. Бу фаол ҳаракатлар мос равишда имитация қилишга ва алмаштириб қўйишга уриниш ҳисобланади.

Калит шифрлашнинг асосий элементи бўлиб, берилган хабарни шифрлашдаги алмаштиришлар у орқали амалга оширилади. Одатда, калит ҳарф ва сонларнинг бирор-бир кетма-кетлигидан иборат бўлади.

Ҳар бир алмаштириш калит билан бир қийматли аниқланади ва бирор криптографик алгоритм орқали амалга оширилади. Шифрлашда бир криптографик алгоритм ҳар хил режимларда қўлланиши мумкин. Шу тарзда ҳар хил шифрлаш усуллари (оддий алмаштириш, гаммалаш ва бошқалар) амалга оширилади. Ҳар бир режимнинг афзаллик ва камчилик томонлари мавжуд. Шунинг учун режимни танлаш конкрет ҳолатга боғлиқ. Дешифрлашдаги криптографик алгоритм, умумий ҳолда, шифрлашдаги алгоритмдан фарқ қилиши мумкин. Бу ҳолатда шифрлашдаги ва дешифровка

қилишдаги калитлар ҳам мос тушмаслиги мумкин. Шифрловчи ва дешифровка қилувчи алгоритмлар жуфтлигини криптотизим, бу алгоритмларни амалга оширувчи қурилмани шифровчи техника дейилади.

Барча ҳолатларга мос ягона шифр йўқ. Шифрлаш усулини, яъни криптографик алгоритм ва ундан фойдаланиш режимини танлаш узатилаётган ахборотнинг хусусиятига (қийматига, ҳажмига, тасвирлаш усулига, зарурий узатиш тезлигига ва бошқалар) ҳамда ахборот эгасининг ахборотни ҳимоя қилиш имкониятига (қўлланилаётган техник воситаларининг нархига, қўллашининг қулайлигига, ишлашининг ишончлигига ва бошқалар) боғлиқ. Ҳимояланадиган ахборот турли-туман шаклларга (матнли, товушли, расмли ва бошқалар) эга бўлиши мумкин. Ҳар бир шаклнинг ўзига хос хусусиятлари мавжуд бўлиб, шифрлаш усулини танлашда уни инобатга олиш керак. Шифрланган ахборотнинг ҳажми, уни талаб этилган тезликда узатиш ҳамда алоқа каналининг ҳар хил халақит берувчи шовқинлардан ҳимояланганлиги катта аҳамиятга эга. Буларнинг барчаси криптографик алгоритмни танлашда ва ҳимояланган алоқани ташкил этишда муҳим роль ўйнайди.

Бутунликни таъминлаш деганда ахборотни рухсатсиз ўзгартириб бўлмаслигининг кафолати тушунилади. Бутунликни кафолатлаш учун маълумотлар бўйича бирон-бир ўзгартиришларни амалга оширишни аниқлайдиган содда ва ишончли мезон бўлиши керак. Бу ўзгартиришлар матнни ўчириш, алмаштириш, янгисини қўйиш орқали амалга оширилиши мумкин.

*Аутентификация*лашни таъминлаш ахборотли ўзаро муносабат жараёнида ахборотнинг ўзини ва томонларнинг ҳақиқийлигини тасдиқлаш усулларини ишлаб чиқишни англатади. Алоқа канали орқали узатилаётган ахборот манбаси, яратилган санаси, ташкил этувчи маълумотлари, узатиш санаси ва шу кабилар билан аудитенфикация қилиниши керак.

*Муаллифликни инкор этолмаслик*ни таъминлаш бу субъектлар томонидан амалга оширилган ҳаракатларни тан олмаслик ҳолати мумкинлигини олдини олади.

Криптографик фаолиятнинг таснифи. Кўпгина криптографик ҳимоя усулларини қўллашда бирор-бир ахборот алмашиш зарурияти вужудга келади. Масалан, ахборот-телекоммуникация тизими объектларини аудитентификация қилиш идентификацияловчи ва аутентификацияловчи ахборотлар алмашинуви орқали амалга ошади.

Умумий ҳолда, бундай тизимлар объектлари (субъектлари)нинг ўзаро муносабати маълум бир келишувлар (*протоколлар*)га риоя этилган ҳолда бўлади. Объект (субъект)ларнинг маълум бир мақсадга эришиш учун кетма-кет бажарадиган амалини формал жиҳатдан протокол дейиш мумкин. Қўйилган мақсад протоколнинг тузилишини ва қўллаш хусусиятини белгилайди.

Криптология икки йўналишдан: криптография ва крипто-таҳлилдан иборат. Криптотаҳлил криптографияга тескари бўлиб, унда калитни билмасдан туриб ахборотни дешифрлаш амалга оширилади.

3.2. Содда шифрлар ва уларнинг хоссалари

Анъанавий (классик) шифрлаш усулларига ўринларини алмаштириш шифрлари, оддий ва мураккаб алмаштириш шифрлари ва уларнинг комбинациялари ва модификациялари киради. Таъкидлаш жоизки, ўринларини алмаштириш шифрлари ва алмаштириш шифрларининг комбинациялари амалиётда қўлланилаётган ҳар хил турдаги симметрик шифрларни ташкил этади.

Ўринларини алмаштириш шифрларида шифрланадиган матннинг ҳарфлари шу матн блоки ичида маълум қоидалар бўйича ўрин алмаштирилади. Ўринларини алмаштириш шифрлари энг содда ва энг қадимий ҳисобланади.

Шифрловчи жадваллар. Тикланиш (XIV аср охирлари) даврининг бошларида ўринларини алмаштириш шифрларида шифрловчи жадваллардан фойдаланилган. Шифрловчи жадвалларнинг калити сифатида: жадвалнинг ўлчами; ўрин алмаштиришни белгиловчи сўз ёки жумла; жадвал тузилишининг хусусияти бўлган.

Калит сифатида жадвалнинг ўлчами берилиши энг содда жадвалли шифрлаш ҳисобланади. Қуйидаги матн берилган бўлсин:

ОБЪЕКТ БЕЛГИЛАНГАН ЖОЙГА БОРАДИ

Ушбу ахборот устун бўйича кетма – кет жадвалга киритилади:

О	К	Л	А	Н	Г	Р
Б	Т	Г	Н	Ж	А	А
Ъ	Б	И	Г	О	Б	Д
Е	Е	Л	А	Й	О	И

Натижада, 4х7 ўлчовли жадвал ташкил қилинади.

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

ОКЛА НГРБ ТГНЖ АААЪБ ИГОБ ДЕЕЛ АЙОИ

Бу ерда калит сифатида жадвал ўлчовлари хизмат қилади.

Табиийки, узатувчи ва қабул қилувчи калит жадвал ўлчами бўлишлигини ўзаро келишиб олишлари керак. Дешифрлашда тескари амал бажарилади.

Энди, калит бўйича оддий ўрнини алмаштириш шифрини кўриб чиқайлик. Бу усул олдингисига нисбатан дешифровка қилиш учун анча мураккабдир. Бу усулда жадвал устунлари калит бўлувчи сўз, ибора, жумла орқали ўрин алмаштирилади.

Мисол тариқасида УЧРАШУВ СОАТ БЕШДА ХИВА КИНОТЕАТРИДА матнини ТЕГИРМОН сўзини калит сифатида қабул қилиб, ўрнини алмаштириш шифрини қўллаб шифрлайлик. Матнда 32 та ва калитда 8 та ҳарфлар борлиги учун 8х4 жадвал тузамиз.

У	Ш	О	Е	Х	К	Т	Р
Ч	У	А	Ш	И	И	Е	И
Р	В	Т	Д	В	Н	А	Д
А	С	Б	А	А	О	Т	А

Энди калит орқали 8х6 жадвал тузиб калитдаги ҳарфларни алфавит бўйича рақамлаб чиқамиз.

Т	Е	Г	И	Р	М	О	Н
8	2	1	3	7	4	6	5
У	Ш	О	Е	Х	К	Т	Р
Ч	У	А	Ш	И	И	Е	И
Р	В	Т	Д	В	Н	А	Д
А	С	Б	А	А	О	Т	А

Рақам бўйича устунлар ўзгартирилади.

Г	Е	И	М	Н	О	Р	Т
1	2	3	4	5	6	7	8
О	Ш	Е	К	Р	Т	Х	У
А	У	Ш	И	И	Е	И	Ч
Т	В	Д	Н	Д	А	В	Р
Б	С	А	О	А	Т	А	А

Қатор бўйича 4 тадан блокларга бўлиб, символлар кетма-кетлигидаги шифрланган матнни оламиз. Шуни эътиборга олиш керакки, агар қаторда кетма-кет иккита бир хил ҳарф келса, чап тарафдан келаётган ҳарф биринчи рақамланади, кейин эса иккинчиси рақамланади ва шифрланган матн ҳосил қилинади. Натижада қуйидаги шифрланган матн ҳосил бўлади:

ОШЕК РТХУ АУШИ ИЕИЧ ТВДН ДАВР БСАО АТАА

Шифрни очишда тескари жараён амалга оширилади.

Шифрланган матннинг очилишини янада мураккаблаштириш учун у қайтадан шифрланиши мумкин. Бу усул *икки томонлама ўрин алмаштириш* шифри дейилади. Бу усулда калит сифатида устун ва қатордаги ҳарфлар тартибидаги сонлардан фойдаланилади. Аввалам бор калит символларига қараб жадвал тузилади ва очиқ матн жойлаштирилиб чиқилади. Сўнгра рақамлар навбатма – навбат тартибланиб, аввал устун, кейин қаторлар ўрни алмаштирилади ва жадвалдаги маълумот қатор бўйича ўқилиб, шифрланган матнга эга бўлинади. Масалан: «**ОБЪЕКТ БУГУН КАСАЛ**» очиқ матни шифрлаш талаб этилсин. Бу ерда калит бўлиб **1342** ва **2341**хизмат қилади.

4х4 жадвал яратиб, очиқ матн қатор бўйича ёзилади:

	2	**3**	**4**	**1**
1	**О**	**Б**	**Ъ**	**Е**
3	**К**	**Т**	**Б**	**У**
4	**Г**	**У**	**Н**	**К**
2	**А**	**С**	**А**	**Л**

K_2

K_1

Энди қатор ва устунлар тартиб бўйича ўринлари алмаштирилади.

	2	3	4	1
1	О	Б	Ъ	Е
2	А	С	А	Л
3	К	Т	Б	У
4	Г	У	Н	К

	1	2	3	4
1	Е	О	Б	Ъ
2	Л	А	С	А
3	У	К	Т	Б
4	К	Г	У	Н

Охирги жадвалга асосан шифрланган матнни ёзамиз ва блокларга бўлиб чиқамиз.

ЕОБЪ ЛАСА УКТБ КГУН

Икки томонлама алмаштиришда жадвал катталигига қараб вариантлар ҳам ортиб боради. Жадвал ўлчамининг катталиги шифр чидамлилигини оширади: 3х3 жадвалда 36 та вариант, 4х4 жадвалда 576 та вариант, 5х5 жадвалда 14400 вариант.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб натурал сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал бўйича сонлар йиғиндиси битта сонга тенг бўлган квадрат шаклидаги жадвалга айтилади.

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

Мисол тариқасида 4х4 ўлчовли сеҳрли квадратни оламиз, бунда сонларнинг 880 та ҳар хил комбинацияси мавжуд. Квадратни қуйидагича тўлдирамиз:

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

Бошланғич матн сифатида қуйидаги **ТОВАР ОЛТИДА КЕЛДИ** матнини оламиз ва жадвалга жойлаштирамиз:

И	**В**	**О**	**Е**
Р	**Д**	**А**	**Т**
И	**О**	**Л**	**К**
А	**Д**	**Л**	**Т**

Шифрланган матн жадвал элементларини сатрлар бўйича ўқиш натижасида ташкил топади:

ИВОЕ РДАТ ИОЛК АДЛТ

Ўрта ва катта ўлчамдаги сеҳрли квадратлар ёрдамида, у даврларда мустаҳкам шифрлашни амалга ошириш мумкин бўлган. Чунки дешифровка қилишда барча вариантларни қўлда амалга ошириб бўлмас эди.

Оддий алмаштириш орқали шифрлаш

Шифрланадиган матннинг ҳарфлари берилган қоида бўйича шу ёки бошқа алфавитдаги ҳарфларга алмаштирилади. Оддий алмаштириш шифрида берилган матннинг ҳар бир ҳарфи шу алфавитдаги унга мос қўйилган бошқа ҳарфга алмаштирилади. Одатда, бу шифрлаш усули бир алфавитли алмаштириш шифри деб аталади.

Цезарнинг шифрлаш тизими. Цезарнинг шифрлаш усули оддий алмаштириш шифрининг хусусий ҳолидир. Бу усулда алфавитнинг ҳар бир ҳарфи К сонга сурилган ҳарфга алмаштирилган. Сурилиш алфавит охирига етганда, унинг бошидан бошланган. Цезарь К=3 бўлган силжитишни қўллаган. Қуйидаги жадвалда бу силжитишдаги лотин графикасидаги ҳарфларининг мослиги келтирилган:

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

F	I	O	R	X	A
G	J	P	S	Y	B
H	K	Q	T	Z	C
I	L	R	U		

Цезарнинг «келдим, кўрдим, ютдим» мазмундаги хабари VENI VIDI VICI, у таклиф этган усулда шифрланганда YHQL YLGL YLFL кўринишни олади.

Цезарь усулининг камчилиги бу бир хил ҳарфларнинг ўз навбатида, бир хил ҳарфларга алмашишидир. Криптотаҳлилда ҳарфларнинг такрорланиш частотаси ёрдамида бу усулда шифрланган матн тезгина расшифровка қилиниши мумкин.

Калит сўзли Цезарь тизими. Цезарнинг калит сўзли шифрлаш тизими битта алфавитли алмаштириш тизими ҳисобланади. Бу усулда калит сўзи орқали ҳарфларнинг суришда ва тартибини ўзгартиришда фойдаланади.

Мисол тариқасида калит сўзи сифатида DIPLOMAT сўзи ва суриш 5 га тенг қилиб олинган бўлсин. Калит сўзи алфавит остига 5 та ҳарфга сурилган ҳолда ёзилади:

0	1	2	3	4	5					10					15					20					25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
					D	**I**	**P**	**L**	**O**	**M**	**A**	**T**													

Алфавитнинг қолган алфавит кетма-кетлигида калит сўздан кейин ёзилади.

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	**D**	**I**	**P**	**L**	**O**	**M**	**A**	**T**	B	C	E	F	G	H	J	K	N	Q	R	S	U

Натижада, берилган матннинг ҳарфларига мос алмаштирувчи ҳарфлар аниқланади. Агар очиқ матн TOVAR KELDI бўлса, шифрлашдан сўнг JCNVG MZAYL матнига айланади.

*Вижинернинг шифрлаш тизими***.** XVI асрда француз дипломати Вижинер томонидан яратилган шифрлаш тизими 1586 йилда чоп этилган. У машҳур кўп алфавитли тизим ҳисобланади. Вижинер тизими Цезарь шифрлаш тизимига қараганда мукаммалроқ ҳисобланиб, унда калит ҳарфдан ҳарфга алмаштирилади. Бундай кўп алфавитли алмаштириш шифрини шифрлаш жадвали орқали ифодалаш мумкин. Қуйидаги жадвалларда рус ва лотин алфавитлари

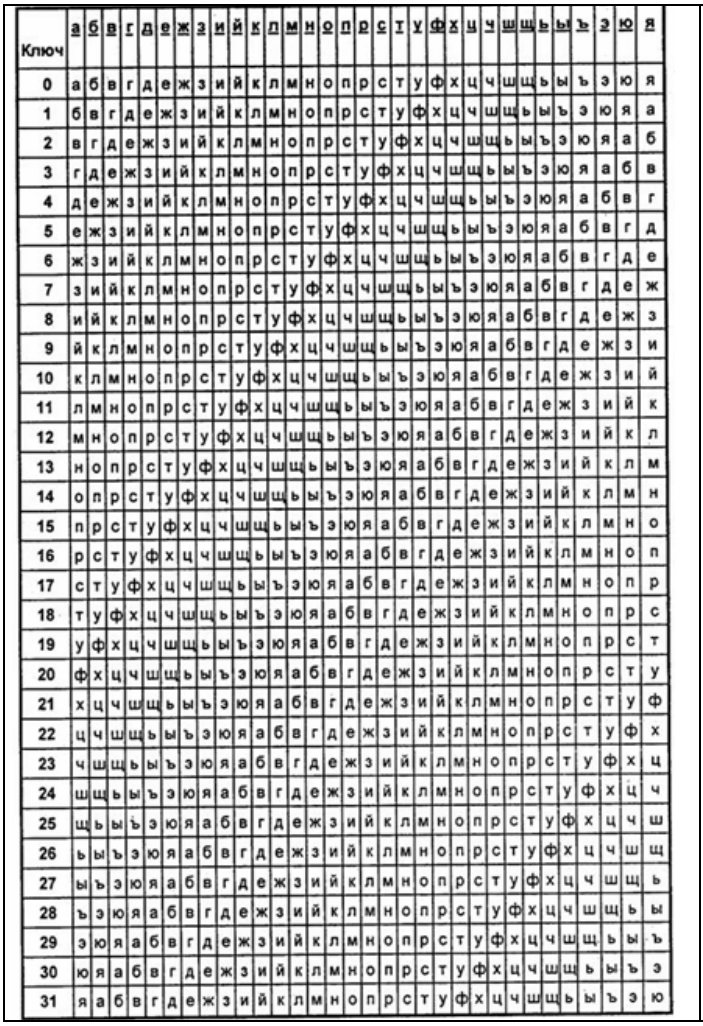
учун мос келувчи жадваллар кўрсатилган. Бу жадваллардан матнни шифрлаш ва уни очиш учун фойдаланилади. Жадвалнинг иккита кириши бўлиб:

– юқори қатордаги ҳарфлардан кирувчи очиқ ёзув учун фойдаланилади.

– чап устунда эса калит сўзи жойлашади.

Очиқ матнни шифрлашда бу матн бир сатрга ёзилади. Унинг остидаги сатрга калит сўз жойлаштирилади. Агар калит сўзнинг узунлиги қисқа бўлса, бу сўз очиқ матннинг охирги ҳарфигача такрорлаб ёзилади. Шифрлаш жараёнида жадвалнинг юқори қисмида жойлашган очиқ матннинг ҳарфи топилади ва чап қисмдан калит сўзнинг ҳарфи танланади. Сатр ва устун кесишган катакдаги ҳарф берилган ҳарфни алмаштиради.

Хабар	Б	А	Й	Р	А	М	К	У	Н	И
Калит	В	А	З	А	В	А	З	А	В	А
Шифрматн	Г	А	Р	Р	В	М	С	У	П	И



3.3. Очиқ ва ёпиқ калитлар билан шифрлаш тизими

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

Хабарларни шифрлаш учун фойдаланилган калит шифрни очиш калитидан олинган ва акси ўринли 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 жиноятчига калит маълум бўлса, ҳеч қандай қаршиликсиз барча тутиб олинган маълумотлар шифрини очиш имкони яратилади. Демак танланган калитни бегоналардан сир сақлаш зарур.

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 компьютер алгоритмларида, одатда, блок узунлиги 64 битни ташкил этади.

Симметрияли тизимларда қуйидаги иккита муаммо мавжуд:

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

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Симметрик калит билан шифрлаш схемасини қуйидаги мисолда кўриб чиқамиз. Али (А) ва Вали (В) номли корреспондентлар бир-бири билан хабар алмашишмоқчи. Корреспондентларнинг ҳар бири ўзининг махфий калитига эга, бу калитдан хабарни тармоқ орқали юборишдан аввал маълумотларни шифрлашда фойдаланиши мумкин. Шифрлаш схемасини кўримлироқ тасвирлаш учун, калитни оддий калит, шифрланган хабарни эса конвертга солинган ҳужжат кўринишида тасвирлаймиз. Шифрлаш ва қайта шифрлаш жараёни қуйидаги расмда тасвирланган.

Симметрик калит ёрдамида шифрлаш тизими

Фойдаланувчи А ўзининг махфий калити билан хабарни шифрлайди ва хабарни тармоқ орқали жўнатади, қабул қилувчи В (худди шундай махфий калитдан фойдаланиб) хабарни қайта тиклайди. Расмда схеманинг симметрик эканлиги кўриниб турибди. Чап ва ўнг томондаги фойдаланувчилар бир хил (симметрик) калитлардан фойдаланишмоқда, шунинг учун бундай турдаги шифрлаш симметрик калит ёрдамида шифрлаш деб юритилади.

Махфий калит ёрдамида шифрлаш усули маълум камчиликлардан ҳоли эмас. Биринчи навбатда, симметрик шифрлаш аутентификация-лаш муаммосини ҳал қилиб бермайди. Масалан, Али (А) Соли (С)га хат ёзиб юбориши, лекин бу хатни Вали (В) ёзган деб тан олмаслиги мумкин. Бундан ташқари, симметрик калит хабар юборилишидан олдин хабар жўнатувчи ва қабул қилувчи компьютерларда ўрнатилган бўлиши керак. Табиийки, Интернетда хавфсиз мулоқот қилиш учун шифрлаш, корреспондентларнинг шахсан учрашишлари шарт бўлмаган ҳолатда маънога эга. Муаммо махфий калитни узатишда юзага келади. Ҳақиқатда, агар жўнатувчи Али қабул қилувчи Валига калитни шифрламасдан узатса, калитни тутиб олишлари мумкин. Агар калит шифрланган кўринишда жўнатилса, унда қабул қилувчи Вали уни оча олмайди. Бир нечта корреспондентлар билан ёзишмалар олиб бориш учун, ҳар бир қабул қилувчи учун алоҳида калитлар бўлиши лозим, бу эса ноқулайликни туғдиради. Бу муаммони ечимини топиш учун асимметрик шифрлаш (очиқ (оммавий) калит ёрдамида шифрлаш) схемаси таклиф этилган.

Очиқ калитли шифрлаш ёки шифрлашнинг асимметрик алгоритмлари деб аталувчи алгоритмларда шифрлаш учун ишлатиладиган калит шифрни очиш учун ишлатиладиган калитдан фарқ қилади. Бундан ташқари, шифрлаш калитини билган ҳолда, шифрни очиш учун зарур калитни жуда катта муддат ичида ҳисоблаб топиш имкони бўлмайди. Ихтиёрий фойдаланувчи шифрлаш калити ёрдамида хабарни шифрлаши мумкин, лекин бу калитга мос шифрни очиш калитига эга шахсгина бу хабарни ўқий олади. Шифрлаш

калитини очиқ (оммавий) калит, шифрни очиш калитини эса ёпиқ (махфий, хусусий) калит дейилади. Хабарни ёпиқ ёки очиқ калит ёрдамида шифрлаш мумкин, қайта тиклаш эса иккинчи калит ёрдамида амалга оширилади. Яъни, ёпиқ калит ёрдамида шифрланган матн фақат очиқ калит ёрдамида қайта тикланиши мумкин ва аксинча. Ёпиқ калит фақат эгасига маълум, ва у ҳеч кимга берилмайди, очиқ калит эса очиқ тарқатилади ва у ҳаммага маълум бўлиши мумкин. Иккита калитни аутентификациялаш масаласининг ечимини топиш учун ҳамда конфеденциалликни таъминлашда қўллаш мумкин.

Агар биринчи калит ёпиқ бўлса, у ҳолда у электрон имзо сифатида ишлатилади ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг бутунлигини таъминлаш имкони пайдо бўлади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

– фойдаланувчини аутентификациялаш, яъни компьютер тизими ресурсларига киришга кирмоқчи бўлган фойдаланувчини аниқлаш;

– тармоқ абонентлари алоқасини ўрнатиш жараёнида уларни ўзаро аутентификациялаш.

Қуйидаги схемага мувофиқ, фойдаланувчи Али (А) олдиндан очиқ калитни Вали (В) ва Соли (С) номли корреспондентларга жўнатади, кейин эса ёпиқ калит билан шифрланган матнни юборади.

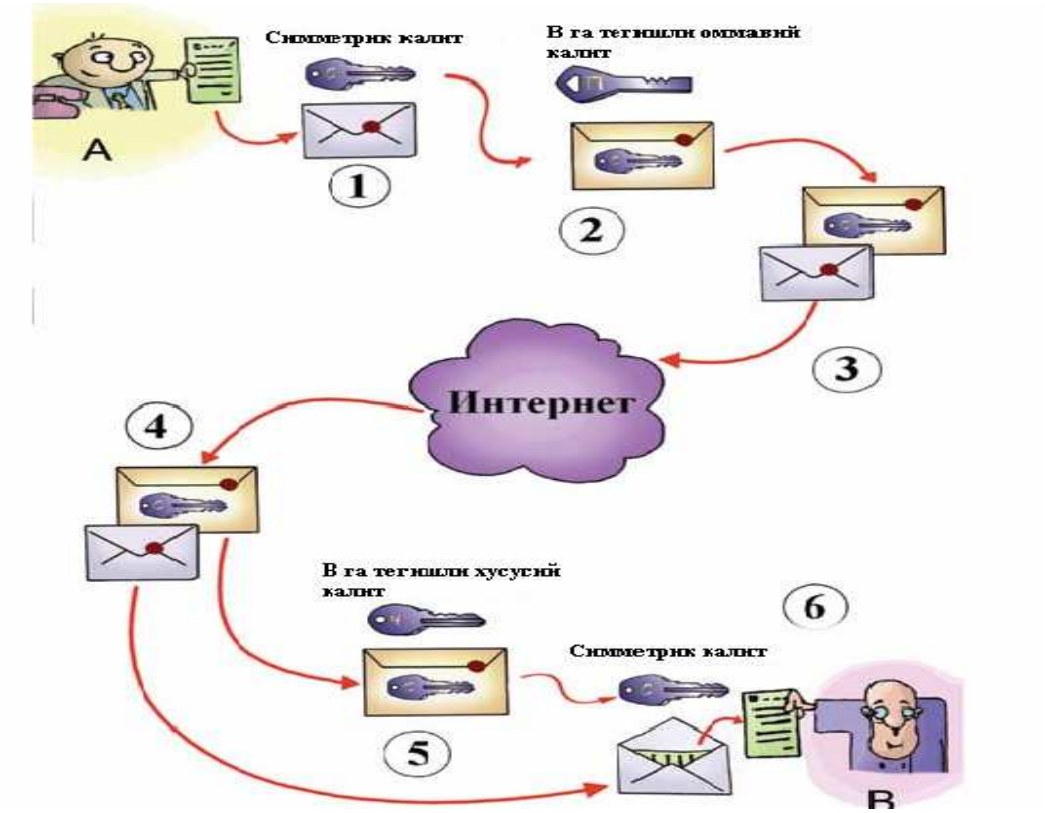
Хабарни фақат Али (А) жўнатиши мумкин (ёпиқ калит унга тегишли), бунда аутентификация муаммоси ечилган. Лекин, масалан Вали (В)нинг унга йўлланган хатни Соли (С) ўқимаганлигига аниқ ишончи йўқ. Демак, конфеденциаллик таъминланмаган.

Конфеденциалликни таъминлаш схемаси қуйидаги расмда тасвирланган.

Хабарни фақат Али (А) ўқиши мумкин, чунки у хабарни қайта тиклаш имконини берувчи ёпиқ калитга эга, хабарни конфеденциаллиги таъминланган. Лекин, Али (А) хабарни Соли (С) юбормаганига аниқ ишончи йўқ, чунки у Вали (В) номидан хабарни юбориши ҳам мумкин. Демак, аутентификациялаш таъминланмаган. Иккита шахс орасида хабар алмашишда конфеденциалликни таъминлаш учун иккита калит бўлиши шарт.

Жуфт калит билан шифрлашда Али (А) томонидан ҳаммага очиқ калит жўнатилиши шарт эмас. Очиқ калит тармоқдаги очиқ фойдаланишни имконини берувчи серверга жойлаштирилиши мумкин.

Симметрик ва асимметрик калит ёрдамида шифрлаш. Шуни таъкидлаш лозимки, асимметрик шифрлаш алгоритмида маълумотларни шифрлаш ва қайта тиклаш учун симметрик шифрлашга қараганда кўп вақт талаб қилинади, шунинг учун замонавий шифрлаш тизимларида асимметрик шифрлаш ва анъанавий симметрик шифрлашнинг комбинациялари қўлланилади. Очиқ калит ёрдамида шифрлаш симметрик калитни узатишда фойдаланилади, бу калит ёрдамида узатиладиган ахборот шифрланади. Бу схемани ишлаш қоидаси қуйидаги расмда келтирилган.



Аввал Али (А) бошланғич файлни симметрик калит ёрдамида шифрлайди (1-пункт). Кейин (2-пункт) Али очиқ манбалардан Вали (В)га тегишли бўлган очиқ калитни олади ва бу калит ёрдамида ўзининг симметрик калитини шифрлайди. Сўнгра (3-пункт) иккала объект (шифрланган файл ва шифрланган симметрик калит) Интернет орқали Вали (В)нинг манзилига жўнатилади. Вали иккала объектни қабул қилиб олади (4-пункт). Симметрик калит Валига тегишли бўлган ёпиқ калит ёрдамида қайта тикланади (5-пункт) ва қайта тикланган симметрик калит ёрдамида бошланғич файл шифрдан ечилади (6-пункт).

Кимдир, сизнинг ёпиқ калитингиз ёрдамида шифрланган хабарни олса, у сиздан хабар келганига ишонч ҳосил қилади. Яъни, бу ҳолатда, шифрлаш имзо қўйганга эквивалент бўлади. Демак, рақамли (электрон) имзо – бу жўнатувчи ёки имзо муаллифини аутентификациялаш усули бўлиб, ҳужжат мазмуни ўзгартирилмаганлигини тасдиқлайди[1]. Рақамли имзо шифрланган ҳолда ёки очиқ шифрланмаган ҳолда юборилиши мумкин.

[1] Ўзбекистон Республикасининг «Электрон рақамли имзо тўғрисида»ги 2003 йил 11 декабрь қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2004. – № 1-2. – 12-м.

Рақамли сертификатлар. Очиқ калитли ширфлаш схемасидан фойдаланганда очиқ калитни мижозларга тарқатиш ёки тармоқдаги серверга ўрнатмоқ керак. Лекин рақиб сизнинг номингиз билан ўзини танитиши ва очиқ калитни сизнинг номингиздан тарқатиши мумкин. Оммавий калитни ҳақиқий эгаси кимлигини аниқлаш учун, ҳамма корреспондентлар ишонч билдирадиган учинчи томонга эҳтиёж пайдо бўлади. Бу масала сертификатлаштириш марказлари (Certification Authority) орқали ҳал этилади. Улар томонидан сертификатлар – эгасини идентификациялайдиган очиқ калит ва ахборотнинг мослигини тасдиқлайдиган рақамли маълумотлар, кафолатчи имзолаган рақамли имзо берилади. Сертификатда оммавий калит, калитнинг эгаси ҳақидаги маълумот, сертификатлаштириш марказининг номи, сертификатни амал қилиш муддати каби маълумотлар бўлади. Сертификатнинг ҳар бир нусхасига сертификат берган ташкилотнинг рақамли имзоси бириктирилади, шунинг учун ким сертификат олган бўлса, унинг ҳақиқийлигига ишонч ҳосил қилиши мумкин. Сертификат шахсни кимлигини тасдиқловчи ҳужжатнинг аналогидир. Шахсни идентификация қилиш муаммоси (паспорт, ҳайдовчилик гувоҳномаси ва ҳоказо) учрашув пайтида юзага келади. Тармоқда шерикни кўрмасдан туриб мулоқот қилишда, шахснинг кимлигини билиш янада муҳимроқдир.

Шифрлашнинг криптографик мустаҳкамлиги. Ҳимояланган ахборотнинг хавфсизлиги биринчи навбатда калит билан аниқланади. Шифрга ҳужум (криптотаҳлил) калит ва шифрлаш алгоритми номаълум бўлган ҳолатда шифрланган ахборотнинг шифрини ечиш жараёнини билдиради. Одатда, шифрлаш алгоритми рақибга маълум ва аввалдан таҳлил этилиши мумкин деб ҳисобланади. Фақат шифрлашни амалга оширувчи калит яширин сақланади. Рақибнинг асосий мақсади бу калитни қўлга киритишдир.

Криптомустаҳкамлик шифрнинг таснифи бўлиб, у калитни билмасдан туриб шифрни ечишга бўлган мустаҳкамликни билдиради. Шифрлаш орқали ахборотни ҳимоялашнинг самарадорлиги калитнинг яширин сақланишига ва шифрнинг криптомустаҳкамлигига боғлиқ.

Шифрлашга қўйиладиган асосий талаблар. Замонавий шифрлаш усуллари қуйидаги асосий талабларга жавоб бериши керак:

– шифрнинг мустаҳкамлиги шифрлаш алгоритмининг махфийлиги билан эмас, калитнинг сир сақланиши билан таъминланади;

– фақат барча мумкин бўлган калитларни бирма-бир тўлиқ кўриб чиқиш орқалигина шифрни ечиш мумкинлиги;

– калитларни бирма-бир тўлиқ кўриб чиқишдаги чекли амаллар сонига замонавий компьютерларда эришиб бўлмаслик;

– шифрланган матн ҳажм жиҳатдан берилган матндан жуда ҳам катта бўлмаслиги;

– шифрлаш жараёнида кетма-кет ишлатилаётган калитлар оддий ва тезкор аниқланадиган боғлиқликда бўлмаслиги;

– шифрлаш жараёнидаги хатолик ахборотнинг бузилиши ва йўқолишига олиб келмаслиги керак;

– шифрлаш жуда ҳам кўп меҳнат талаб қилмаслиги ва унинг қиймати ҳимояланувчи ахборотнинг қиймати билан мос келиши керак.

Ушбу талабларга шифрлаш усулларидан: ўринларини алмаштириш; алмаштириш; гаммалаштириш; аналитик ўзгартириш кабилари жавоб беради.

Кенг тарқалган шифрлаш алгоритмлари. Ахборотни криптографик ҳимоялаш стандартлари, хэш функция.

AES [advanced encryption standard (AES)] – АҚШда маълумотларни шифрлаш стандарти бўлиб, симметрик шифртизимларда фойдаланиш учун қўлланади. Блок ўлчами 128 бит, калит узунлиги 128, 192 ёки 256 битдан иборат бўлган базавий блокли шифрлаш алгоритмига асослаган. 2002 йилдан бери амалда қўлланилмоқда.

DES [data encryption standard] шифрлаш стандарти Америка стандарт шифрлаш тизими бўлиб, симметрик шифртизимларда фойдаланиш учун мўлжалланган. Дунёда шифрлашнинг биринчи очиқ расмий стандарти сифатида 1977 йилдан 1997 йилгача амал қилган. Блок катталиги 64 бит, калит узунлиги 56 битга тенг бўлган базавий блокли шифрлаш алгоритми асосида қўлланилган. Шифрлашнинг 4 режими ва хабарни ҳақиқийлигини аниқлаштирувчи кодни шакллантиришнинг 2 режимига эга.

DES-алгоритми қўллашининг асосий соҳалари:

1) компьютерда маълумотларни сақлаш (пароль ва файлларни шифрлаш);

2) хабарларни аутентификациялаш (хабар ва назорат гуруҳига эга бўлиб, хабарни ҳақиқийлигига ишонч ҳосил қилиш қийинчилик туғдирмайди);

3) электрон тўлов тизимларида (кўп сонли мижозлар ва банклар ўртасидаги операцияларда);

4) тижорат хабарларни электрон алмашинувида (харидор, сотувчи ва банк ходими ўртасида маълумотлар алмашинувида ўзгартиришлар киритиш ва ушлаб қолишлардан ҳимояланган).

ГОСТ 28147-89 шифрлаш стандарти – Россия шифрлаш стандарти бўлиб, симметрик шифртизимларда фойдаланиш учун мўлжалланган. Блок катталиги 56 бит, калит узунлиги 256, 512 битга тенг бўлган базавий блокли шифрлаш алгоритмига асосланган. Шифрлашнинг 4 режимига эга.

Кўп сонли турли очиқ калитли криптотизимлар ичида кенг тарқалгани 1977 йилда ихтиро қилинган ва унинг муаллифлари Рон Ривест, Ада Шамир ва Леонард Эйдельман номига қўйилган **RSA** криптотизимидир. Улар, катта туб сонларни аниқлаш, ҳисоблаш жиҳатдан оддий эканлигидан ҳамда шундай иккита катта сонларнинг кўпайтмаси бўлган сонни кўпайтувчиларга ажратиш жудаям қийин, амалда мумкин эмаслигидан фойдаланишган. **RSA** шифрини очиш шундай кўпайтувчиларга ажратишга тенглиги исботланган (Рабин теоремаси). Шунинг учун калит узунлиги қандай бўлишидан қатъи назар шифрни очиш учун талаб қилинадиган амалларнинг қуйи чегарасини баҳолаш, замонавий компьютерларнинг тезлигини билган ҳолда шифрни очиш учун керак бўладиган вақтни ҳам аниқлаш мумкин. RSA алгоритмининг ҳимояланганлик кафолатини аниқлаш имконияти, унинг бошқа очиқ калитли алгоритмлар орасида машҳур бўлишининг сабаби ҳисобланади. Шунинг учун RSA алгоритмидан банк компьютер тизимларида фойдаланилмоқда, айниқса узоқ масофадаги мижозлар билан ишлашда (кредит карточкаларга хизмат кўрсатишда) қўлланилмоқда.

Хабар хеш-функцияси – қиймати кириш кетма-кетлигининг, яъни иккилик саноқ тизимида берилган хешловчи соннинг ҳар бир битига ёки хешловчи дастлабки матннинг ҳар бир рамзига боғлиқ бўлган функция[1]. Хешлаш алгоритми кириш матнидан бир хил узунликда натижа чиқаради. Бунда узунлик деганда, иккилик саноқ тизимида берилган ифодадаги битлар сони назарда тутилади. Масалан, кириш матни «АКТ луғати» бўлса ва хеш-функция қиймати «1011011101010010 1»га тенг чиқса, хеш-функция қиймати узунлиги 17 битга тенг бўлади. Чиқиш узунлиги 128, 192, 256 бит бўлган хеш-функциялар ҳам мавжуд. Хеш-функция самарали бўлиши учун кириш

[1] Ахборот-коммуникация технологиялари изоҳли луғати (иккинчи нашр). – Т., 2010.

хабари учун натижа ноёб бўлиши лозим. Одатда, хеш-функциялар бир томонли функциялардир. Чунки, чиқиш қиймати асосида дастлабки матнни ҳисоблаб топиш жуда қийин. Хеш-функциялар ахборот узатиш ва сақлашда унинг хавфсизлигини муҳофаза қилиш учун қўлланилади.

Электрон рақамли имзо ва очиқ калитлар структураси. Электрон рақамли имзони қўллашдан мақсад, биринчидан электрон ҳужжатдаги ахборот асл нусха эканлигини тасдиқлаш, иккинчидан учинчи тарафга (арбитр, судга ва бошқаларга) ҳужжатни 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 имзоланганлигини аниқлаш учун таклиф этилган.

Ҳозирги пайтда рақамли имзо кенг қўлланилмоқда (узатиладиган ёки сақланадиган шифрланган матнга бириктирилган рақам, бу ахборотнинг бутунлигини ва муаллифни ҳақиқийлигини текшириш имкониятини кафолатлайди). Симметрик шифрлаш алгоритмларига асосланган рақамли имзо моделлари ҳам мавжуд.

Мустақил тайёргарлик учун саволлар

1. *Криптография нима?*
2. *Криптография ривожланишининг қандай босқичлари мавжуд?*

3. Замонавий криптография қанақа муаммоларни ҳал этувчи билим соҳаси ҳисобланади?

4. Ахборотларни содда шифрлашни қандай усуллари бор?

5. Цезарнинг шифрлаш усули қандай амалга оширилади?

6. Вижинернинг шифрлаш тизими нима?

7. Калит деганда нима тушунилади?

8. Симметрик шифрлаш қандай амалга оширилади?

9. Асимметрик шифрлаш нима?

10. Симметрик ва асимметрик калит ёрдамида шифрлаш қандай амалга оширилади?

11. Рақамли сертификатлар нима?

12. Криптотомустаҳкамлик нимани билдиради?

13. Шифрлашга қанақа талаблар қўйилади?

14. Қайси шифрлаш алгоритмлари кенг тарқалган?

15. Электрон рақамли имзо нима мақсадда ишлатилади?

IV. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АППАРАТ-ДАСТУРИЙ ВОСИТАЛАРИ

4.1. Асосий тушунчалар. Фойдаланиш ҳуқуқини чеклашнинг усул ва воситалари.

4.2. Дастурларни ўзгартиришлардан ҳимоялаш ва бутунликнинг назорати.

4.3. Маълумотларни узатиш тармоғида ахборот хавфсизлигининг аппарат-дастурий воситалари.

Ахборотни муҳофаза қилишнинг аппарат-дастурий воситалари – ахборотни муҳофаза қилиш функцияларини (фойдаланувчиларни идентификациялаш ва аутентификация қилиш, ресурслардан фойдалана олишни чеклаш, воқеаларни қайд қилиш, ахборотни криптографик ҳимоялаш ва шу кабилар) бажарадиган (мустақил ёки бошқа воситалар билан биргаликда) турли электрон қурилмалар ва махсус дастурлардир.

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

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

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

Тармоқнинг хавфсизлиги ундаги барча компьютерларнинг ва тармоқ қурилмаларининг хавфсизлиги билан аниқланади. Бузғунчи тармоқнинг бирор-бир ташкил этувчисининг ишини бузиш орқали бутун тармоқни обрўсизлантириши мумкин.

Ҳамма фойдаланаётган тармоқдан келиб чиқаётган таҳдидларни блокировкалаш учун «тармоқлараро экран» (**Firewall**) деб номланувчи дастурий ва аппарат-дастурий воситалардан фойдаланилади.

4.1. Асосий тушунчалар. Фойдаланиш ҳуқуқини чеклашнинг усуллари ва воситалари

Ахборотларни ҳимоялашнинг аппарат воситаларига, компьютернинг техник воситаларига тааллуқли бўлган, ахборот хавфсизлигини таъминлашнинг айрим функцияларини мустақил равишда ёки дастурий воситалар билан бир мажмуа таркибида бажарадиган электрон ва электрон-механик мосламалари киритилади. Бундай қурилмаларни маълумотларни ҳимоялашнинг инженер-техник воситаларига эмас, балки аппарат воситаларига киритишнинг асосий шарти, уларни компьютернинг техник воситалари таркибида киритилиши билан белгиланади.

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 халақит 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 деганда, фақатгина ахборотлар хавфсизлигини таъминлашга мўлжалланган ва компьютер воситаларининг дастурий таъминоти таркибига киритилган махсус дастурлар тушунилади.

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 тизимла-

рини ва ҳоказо) ноқонуний ўзгартиришлардан, фойдаланишлардан ва кўпайтиришлардан ҳимояловчи дастурлар.

Компьютер тизимларида ахборот хавфсизлигини таъминлашга тааллуқли маънода идентификациялаш атамаси компьютер тизимлари субъектининг уникал номини бир қийматли таниб олишни билдиради. Аутентификациялаш эса тақдим этилган номни ушбу субъектга мослигини тасдиқлашни англатади (субъектнинг асллигини тасдиқлаш).

Ахборотларни муҳофаза қилишнинг ёрдамчи дастурий воситаларига мисол қилиб қуйидагиларни келтириш мумкин:

– қолдиқ ахборотларни (тезкор хотира блокидаги, вақтинчалик файллардаги ва ҳоказо) йўқ қилувчи дастурлар;

– компьютер тизимларининг хавфсизлиги тизимига боғлиқ бўлган турли воқеа ва ҳодисаларни тиклаш ҳамда шундай воқеа ва ҳодисалар рўй берганини исботлаш учун фойдаланиладиган аудит дастурлари (қайд қилиш журналларини юритиш);

– қоидабузар билан ишлашни имитацияловчи дастурлар (қоидабузарни гўёки ёпиқ ахборотларни олган деб чалғитиш);

– компьютер тизимларининг ҳимояланганлигини синовдан ўтказувчи назорат дастурлар ва бошқалар.

Ахборотларни муҳофаза қилишнинг дастурий воситаларининг афзалликларига қуйидагилар киради:

– кўпайтиришнинг осонлиги;

– мосланувчанлик (турли шароитларда қўлланиладиган муайян компьютер тизимларини, ахборот хавфсизлигига таҳдиднинг ўзига хослигини ҳисобга олиб, созлаш имконияти);

– қўллашнинг қулайлиги – бир хил дастурлар, масалан шифрловчи дастурлар «шаффоф» (фойдаланувчига кўринмайдиган) режимда ишлайди, бошқалари фойдаланувчидан ҳеч қандай қўшимча янги (бошқа дастурлари билан таққослаганда) кўникмалар талаб қилмайди;

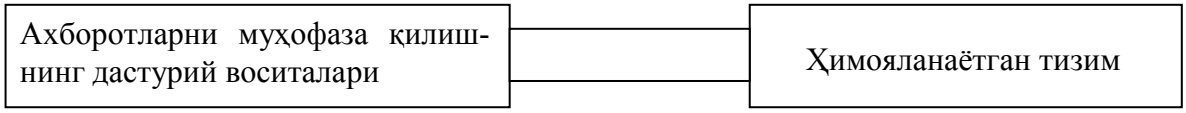
– уларни ахборот хавфсизлигига янги таҳдидлар ҳисобини юритиш учун ўзгартиришлар киритиш йўли билан такомиллашувининг амалдаги чек-чегарасиз имкониятлари мавжудлиги.

Ахборотларни муҳофаза қилишнинг дастурий воситаларининг камчиликларига қуйидагилар киради:

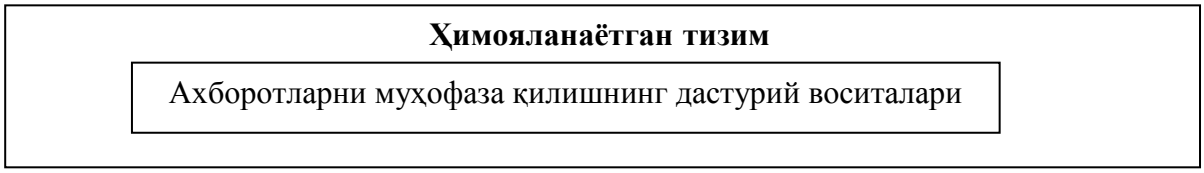
– ҳимояловчи дастурларнинг фаолияти компьютер тизимлари ресурсларидан фойдаланиш ҳисобига бўлгани учун бу тизимлар самарадорлигининг сусайиши;

– жуда паст унумдорлик (худди шундай вазифани бажараётган аппарат воситалар билан таққослаганда, масалан шифрловчи қурилма);

– ахборотларни ҳимояловчи кўпгина дастурий воситаларнинг компьютер дастурий таъминотига бевосита ўрнатилмагани (қуйидаги расмлар), бу ҳолат қоидабузарнинг ушбу дастурларни четлаб ўтишига принципиал имкониятлар яратади;



Ахборотларни муҳофаза қилиш дастурининг дастурий таъминотга уланиш чизмаси



Дастурий таъминот таркибидаги ахборотларни муҳофаза қилиш дастури чизмаси

– компьютер тизимларидан фойдаланиш жараёнида ахборотларни ҳимоялашнинг дастурий воситаларини қасддан ўзгартириш имконияти.

Компьютер тизимларидан фойдаланиш ҳуқуқини чеклашнинг усул ва воситалари. Ахборот хавфсизлигини таъминлашнинг асосий концепциясини турли алоқа ва хавфсизликни таъминлаш нимтизимлари, умумий техник воситалар, алоқа каналлари, дастурий таъминот ва маълумотлар базаларига эга ягона тизимга интеграциясига асосланган комплекс ёндашув ташкил этади.

Комплекс хавфсизлик – вужудга келиши мумкин бўлган барча турдаги таҳдидлар (ноқонуний фойдаланиш, маълумотларни тутиб олиш, терроризм, ёнғин, табиий офатлар ва ҳоказолар)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.

Объектнинг ахборот хавфсизлигини таъминлаш тизимининг самарадорлиги муҳим аҳамият касб этади. Компьютер тизимлари учун ушбу самарадорликни, ҳисоблаш тизимида қўлланилаётган аппарат-дастурий воситаларни танланганлиги билан баҳолаш мумкин. Бундай самарадорликни баҳолаш, хавфсизликни таъминлаш даражаси фойдаланиш ҳуқуқига бўлган назоратни кучайтирилишига боғлиқликни кўрсатувчи ўсувчи эгри чизиқ орқали амалга оширилиши мумкин.

Қурилмадан, жумладан компьютердан фойдалана олиш деганда, субъектга ушбу қурилмадан фойдаланиб, унга муайян рухсат этилган ҳаракатларни бажара олиш имконини бериш тушунилади. Масалан, компьютер фойдаланувчисига компьютерни ишга тушириш ва ўчириш, дастурлар билан ишлаш, маълумотларни киритиш ва чиқаришга рухсат этилади. Хизмат кўрсатувчи шахс эса ўрнатилган тартибда компьютерни текширади, ишдан чиққан блокларни алмаштиради ва тиклайди.

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 инденти-фикаторлар ичидан, одатда, қуйидагиларидан фойдаланилади:

– пароллар;

– ечиб олинадиган ахборот ташувчилар;

– электрон жетонлар;

– пластик карточкалар;

– механик калитлар.

Конфеденциал 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 хешланган ҳолатда компьютернинг қаттиқ дискида сақланади. Паролларни таққослаш операцион тизим (ОТ) томонидан фойдаланувчи ҳуқуқига мос имкониятлар юклангунга қадар амалга оширилади. Лекин, компьютернинг ОТдан фойдаланишда 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.

Атрубутивли идентификаторлардан (пароллардан ташқари) рухсат берилиш ва қайд қилиш чоғида фойдаланилиш мумкин ёки улар иш вақти тугагунга қадар ишлатилаётган қурилмага доимий уланган ҳолда бўлиши шарт. Қисқа вақтга бирор жойга чиқилганда

ҳам идентификатор олиб қўйилади ва қурилмадан фойдаланиш блокировка қилинади. Бундай аппарат-дастурий воситалар нафақат қурилмалардан фойдаланишни чеклаш масалаларини ҳал қила олади, шу билан бирга ахборотлардан ноқонуний фойдаланишдан ҳимоялашни таъминлайди. Бундай қурилмаларнинг ишлаш принципи қурилмага ўрнатилган ОТ функцияларини кенгайтиришга асосланган.

Аутентификациялаш жараёни компьютер тизимлари билан рухсат этилган субъект орасида амалга ошириладиган диалогни 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.

Кўпинча содда идентификатор сифатида механик калитлардан фойдаланилади. Механик қулф қурилмага ток етказиб берувчи қурилмага ўрнатилган бўлиши мумкин. Қурилманинг асосий бошқарув органлари жойлашган жойни беркитувчи қопқоғи қулфланган ҳолда бўлиши мумкин. Қопқоқни очмасдан қурилмани ишлатишнинг имкони йўқ. Бундай қулфнинг мавжудлиги, бузғунчининг қурилмадан ноқонуний фойдаланишни амалга ошириши йўлида қўшимча тўсиқ бўлиб хизмат қилади.

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 конфеденциал 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.

Ҳимояловчи аппарат-дастурий комплексларнинг кўпчилиги максимал сондаги ҳимоялаш механизмларидан фойдаланилади. Бу механизмларга қуйидагилар киради:

– фойдаланувчиларни идентификациялаш ва аутентификациялаш;

– файллар, папкалар, дисклардан фойдаланишга рухсатни чеклаш;

– дастурий воситалар ва ахборотлар бутунлигини назорат қилиш;

– фойдаланувчи учун функционал ёпиқ муҳитни яратиш имконияти;

– ОТни юкланиш жараёнини ҳимоялаш;

– фойдаланувчи йўқлигида компьютерни блокировка қилиш;

– маълумотларни криптографик ўзгартириш;

– ҳодисаларни қайд қилиш;

– хотирани тозалаш.

Фойдаланишни чеклаш воситалари ёрдамида ноқонуний фойдаланишдан ҳимоялаш (НФҲ)нинг усул ва воситаларидан ташқари компьютерни ҳимоялаш учун қуйидаги услуб ва воситалар қўлланилади:

– қурилмаларни ноқонуний улаб олишга қарши ҳаракатлар;

– бошқарув ва уланишларни, ички монтажни ноқонуний аралашувлардан ҳимоялаш;

– фойдаланиш жараёнида дастур тузилишининг бутунлигини ва ҳимоясини назорат қилиш.

Компьютер тизимларига (КТ) қурилмаларни ноқонуний улаб олишга қарши ҳаракатларни ташкил этишда, бу уланиш КТнинг техник тузилишини ноқонуний ўзгартириш имконини берувчи йўллардан бир эканлигини назарда тутиш лозим. Ушбу ўзгартиришлар рўйхатдан ўтказилмаган қурилмаларни улаш ёки компьютер тизимларининг таркибий воситаларини алмаштириш орқали амалга оширилади.

Бунда таҳдидларни олдини олиш учун қуйидаги усуллардан фойдаланилади:

– қурилманинг ўзига хос хусусиятларини текшириш;

– қурилмаларни идентификациялашдан фойдаланиш.

Компьютер тизимларининг хотира қурилмаларида, одатда тизим конфигурацияси ҳақидаги маълумотлар сақланади. Бундай маълумотларга: қурилманинг (блокларнинг) тури ва уларнинг тавсифлари, ташқи қурилмаларнинг сони ва уланиш сабабларини ўзига хос хусусиятлари, иш режимлари ва бошқаларни киритиш мумкин. Конфигурциянинг муайян тузилиши компьютер тизимларининг ва ОТнинг турига қараб аниқланади. Ҳар қандай ҳолатда ҳам дастурий воситалар ёрдамида КТ конфигурацияси

ҳақидаги маълумотларни йиғиш ва таққослашни ташкил этиш мумкин. Агар компьютер тармоқда ишлаётган бўлса, ҳеч бўлмаганда уни тармоққа улаш пайтида компьютернинг конфигурацияси назоратдан ўтказилади.

Назоратнинг янада ишончли ва тезкор усули, қурилманинг махсус код – идентификаторидан фойдаланиш ҳисобланади. Бу код қурилма воситаларида ҳосил қилинади ва хотира қурилмасида сақланиши мумкин. Генератор назорат қилувчи қурилмага қурилманинг уникал рақамларини узатишни амалга оширади. Хотира қурилмасидаги код, КТ администраторининг воситалари ёрдамида даврий равишда ўқиб ва таҳлил қилиб борилади. Конфигурациянинг ўзига хос хусусиятларини таҳлил қилиш усулларидан комплекс фойдаланиш ва қурилмаларни идентификациялашдан фойдаланиш, ноқонуний уланиш ёки алмаштириб қўйиш учун амалга оширилган уринишларни пайқаш эҳтимоллигини оширади.

4.2. Дастурларни ўзгартиришлардан ҳимоялаш ва бутунликнинг назорати

Компьютер вирусларидан ва бошқа дастурлар таъсиридан ва ўзгартиришлардан ҳимояланиш, компьютер тизимларида ахборотларни қайта ишлаш жараёнини ҳимоялашнинг мустақил йўналишларидан ҳисобланади. Ушбу хавфга етарлича баҳо бермаслик фойдаланувчиларнинг ахборотлари учун жиддий салбий оқибатларни келтириб чиқариши мумкин. Вирусларнинг таъсир механизмларини, уларга қарши кураш усуллари ва воситаларини билиш вирусланишга қарши ҳаракатларни самарали ташкил этиш, уларнинг таъсиридан зарарланиш эҳтимоллигини ва талафатларни минимумга келтириш имконини беради.

Компьютер вируслари – бу КТда тарқалиш ва ўзини ўзи ишлаб чиқиш хусусиятига эга бўлган кичик ҳажмдаги бажарилувчи дастурлар. Вируслар КТда сақланаётган дастурий воситалар ёки маълумотларни йўқ қилиши ёки ўчириб юбориши мумкин. Тарқалиш жараёнида вируслар ўзини модификациялаши мумкин.

Вирусларнинг оммавий тарқалиб кетиши ва уларнинг КТ ресурсларига таъсири оқибатларининг жиддийлиги, махсус антивирус воситаларини ва уларни қўллаш усулларини яратиш ва фойдаланиш заруриятини келтириб чиқарди. Антивирус воситалари қуйидаги масалаларни ҳал этиш учун қўлланилади:

– КТда вирусларни топиш;

– вирус – дастурлар ишини блокировка қилиш;

– вируслар таъсирининг оқибатларини бартараф қилиш.

Вирусларни топишни, уларни жойлашиб олиш босқичида ёки ҳеч бўлмаганда вируснинг бузғунчилик функцияларини бошлагунга қадар амалга оширган мақсадга мувофиқ. Шуни таъкидлаш жоизки, барча турдаги вирусларни топишни кафолатловчи антивирус воситалар мавжуд эмас.

Вирус топилган ҳолатда, унинг тизимга келтириши мумкин бўлган зарарли таъсирини минималлаштириш мақсадида дарҳол вирус-дастурнинг ишини тўхтатилиш лозим.

Вируснинг таъсир оқибатларини бартараф қилиш икки йўналишда олиб борилади:

– вирусни ўчириш;

– файлларни, хотира соҳаларини тиклаш.

Тизимни қайта тиклаш вирус турига, уни аниқланган ҳамда зарарловчи таъсирини бошлаган вақтига боғлиқ. Вируслар тизимга кириш жараёнида, ўзини сақлайдиган жойдаги маълумотларни ўчириб юборса ҳамда зарарловчи таъсири натижасида маълумотларни ўзгартириш назарда тутилган бўлса, захирага олинган маълумотларсиз йўқолган маълумотларни тиклаб бўлмайди.

Вирусларга қарши курашда аниқ бир кетма-кетлик ва комбинацияда қўлланилувчи, вирусларга қарши курашиш усулларини ҳосил қилувчи дастурий ва аппарат-дастурий воситалардан фойдаланилади.

КТнинг хавфсиз ишлашининг асосий шартларидан бири, амалда синовдан ўтказилган ва ўзининг юқори самара беришини кўрсатган бир қатор қоидаларга[1] риоя қилиш ҳисобланади.

Биринчи қоида – қонуний расмий йўл билан олинган дастурий маҳсулотлардан фойдаланиш. Дастурий таъминотнинг қароқчилик йўли билан кўпайтирилган нусхаларида, расмий йўл билан олинганларига нисбатан вирусларнинг мавжудлик эҳтимоли жуда юқори.

Иккинчи қоида – ахборотлар захирасини ҳосил қилиш. Аввало дастурий таъминотнинг дистрибутивлари ёзилган ташувчиларни сақлаш зарур. Бунда ташувчиларга маълумотларни ёзиш имкони

[1] *Мельников В.П. и др.* Информационная безопасность и защита информации: Учебое пособие. – М., 2008.

берилган бўлса, имкон қадар уни блокировка қилиш зарур. Ишга тааллуқли маълумотларни сақланишига жиддий ёндашиши зарур. Мунтазам ишга тааллуқли файлларнинг захира нусхаларини яратиб бориш ва уларни ёзишдан ҳимояланган ечиб олинувчи ташувчиларда сақлаш керак. Агар бундай нусхалар ечиб олинмайдиган ташувчиларда яратилаётган бўлса, уларни бутунлай бошқа компьютернинг доимий хотирасида яратиш мақсадга мувофиқ. Бунда ёки файлнинг тўлиқ нусхаси ёки киритилаётган ўзгаришларнинг нусхалари сақланади.

Учинчи қоида – антивирус воситаларидан мунтазам фойдаланиш. Антивирус воситалари мунтазам янгиланиб турилиши лозим.

Тўртинчи қоида – янги ечиб олинадиган ахборот ташувчилардан ва янги файллардан фойдаланилганда эҳтиёткорликка риоя қилиш. Янги ечиб олинадиган ташувчилар олинганда, албатта, юкланувчи ва файл вируслари мавжудлигига, олинган файллар эса файл вируслари мавжудлигига текширилиши лозим. Текширув, сканерловчи – дастурлар ва эвристик таҳлилни амалга оширувчи дастурлар ёрдамида амалга оширилиши керак. Олинган ҳужжатлар ва жадваллар билан ишлашда, ушбу файллар тўлиқ текширилгунга қадар, матн ва жадвал муҳаррирларига ўрнатилган макрокомандаларнинг бажарилишини тақиқлаш зарур.

Бешинчи қоида – тизимга, айниқса тақсимланган тизимларга ёки жамоа бўлиб фойдаланиладиган тизимларга, киритилаётган файлларни ва ечиладиган ахборот ташувчиларни махсус ажратилган компьютерларда текшириш. Уни тизим администратори ёки маълумотлар хавфсизлигига масъул бўлган шахснинг автоматлаштирилган иш жойидан амалга оширилиши мақсадга мувофиқ. Диск ва файлларни ҳар томонлама антивирус текширувидан ўтказилувидан сўнг уларни тизимдан фойдаланувчиларга тақдим этиш мумкин.

Олтинчи қоида – агар ахборотларни ташувчиларга ёзиш назарда тутилмаган бўлса, бундай амалларни бажарилишини блокировка қилиш.

Юқорида келтирилган тавсияларга доимий риоя қилиниши вирус дастурлар билан зарарланиш эҳтимолини анча камайтиради ва фойдаланувчини ахборотларни қайтиб тиклаб бўлмайдиган йўқотишлардан сақлайди.

КТдан фойдаланиш босқичларида тизимдаги ахборотларнинг бутунлиги ва улардан фойдаланиш ҳуқуқи қуйидагилар орқали таъминланади:

– КТда мавжуд ахборотларнинг бутунлиги;

– КТнинг рад этишга барқарорлигини ошириш;

– тизимнинг қайта юкланиши ва «осилиб қолиши»ни бартараф этиш;

– ахборот захираларини яратиш;

– қатъий белгиланган дастурлар мажмуидан фойдаланиш;

– техник хизмат кўрсатиш ва кам-кўстини тўлдириш жараёнларининг ўзига хос тартибига риоя қилиш;

– антивирус тадбирлари комплексини ўтказиш.

Ахборотнинг бутунлиги ва фойдаланишга қулайлиги аппарат воситалар захирасини яратиш, фойдаланувчиларнинг хато ҳаракатларини блокировка қилиш, компьютер тизимларининг ишончли элементларидан ва барқарор ишловчи тизимлардан фойдаланиш йўли билан амалга оширилади. Тизим элементларини қасддан ортиқча ишлатиш таҳдидлари бартараф этилади. Бунинг учун бажариладиган дастурларга буюртмаларни келиб тушиш интенсивлигини ўлчаш механизмларидан ва бундай буюртмаларни беришни чеклаш ёки блокировка қилиш механизмларидан фойдаланилади. Бундай ҳолларда маълумотларни узатиш ёки дастурларни бажартиришга бўлган буюртмалар оқимининг бирданига кескин ошиб кетишини аниқлаш имкони ҳам олдиндан назарда тутилган бўлиши керак.

КТда ахборотларнинг бутунлиги ва фойдаланишга қулайлигини таъминлашнинг асосий шартларидан бири уларнинг захираларини ҳосил қилишдан иборат. Ахборотлар захирасини яратиш стратегияси ахборотнинг муҳимлигини, КТнинг узлуксиз ишлашига бўлган талабларни, маълумотларни тиклашдаги қийинчиликларни ҳисобга олган ҳолда танланади.

Ҳимояланган КТда фақатгина рухсат этилган дастурий таъминотдан фойдаланилиши лозим. Фойдаланишига расман рухсат этилган дастурларнинг рўйхати, уларнинг бутунлигини назорат қилишнинг усуллари ва даврийлиги КТни эксплуатация қилишидан олдин аниқланиши керак.

Дастурлар бутунлигини назорат қилишнинг содда усулларидан бири назорат йиғиндилари усули ҳисобланади. Назорат йиғиндиси – маълумотлар блокининг охирига ёзиладиган битлар кетма-кетлиги. Назоратдаги файлга киритилган ўзгартиришни, назорат йиғиндини тузатиб қўйиш билан, беркитишни истисно қилиш мақсадида назорат йиғиндини шифрланган ҳолда сақлаш ёки назорат йиғиндини ҳисоблашнинг махфий алгоритмидан фойдаланиш зарур.

Ахборот бутунлигини назорат қилишнинг кўпроқ мақбул бўлган методларида бир хеш-функциядан фойдаланиш ҳисобланади. Хэш-функциянинг қийматини унинг калитини билмасдан туриб қалбакилаштириб бўлмайди, шу сабабли хешлаш калитини шифрланган кўринишда ёки жиноятчининг «қўли етмайдиган» жойдаги хотирада сақлаш керак.

Ахборот хавфсизлигини таъминлашнинг дастурий ва аппарат-дастурий воситалардан фойдаланишга қўйиладиган асосий талаблар. Хавфсизлик моделини тўғри танлаш ОТ мутахассисларинигина эмас, хавфсизлик бўйича мутахассисларнинг асосий вазифаси ҳисобланади. Ҳозирда мавжуд стандартлар моделларнинг мажбурий рўйхатини фақат икки модель, яъни фойданиш ҳуқуқини бошқаришнинг *дискрет* ва *мандатли* турлари билан чеклайди. Кўп ҳолларда ушбу икки моделнинг қўлланилиши етарли ҳисобланади.

ОТда ахборот хавфсизлигини самарали таъминлаш учун қуйидаги тавсияларни[1] бажариш лозим:

1. Хавфсизлик моделини тўғри жорий этиш.

2. Объектлар ва субъектларнинг ишончли идентификациялаш ва аутентификациялашдан ўтказиш. Ушбу муаммо техник характерга эга. Ҳозирда, ишончли идентификациялашни ва берилган аниқликда аутентификциялашни таъминлашлайдиган тизимлар мавжуд. Идентификациялашнинг ишончлилиги фойдаланилаётган белгиларнинг ноёблиги (уникаллиги) билан, аутентификациялашники эса – қалбакилаштиришнинг қийинлиги билан таъминланади. Фойдаланувчиларни идентификациялаш ва аутентификациялашни ишончли алгоритмларини қўллаш учун махсус аппарат воситалар – магнит карталар, фойдаланувчининг физиологик катталиклари (бармоқ излари, кўз тўр пардаси ва ҳоказо)ни ўқувчи қурилмалар зурур. Ушбу усулларни дастурий жиҳатдан ихтиёрий мавжуд тизимларга жорий этиш мумкин. Субъектлар ва объектларнинг дастурий (инсон иштирокисиз) идентификациялаш ва аутенфикациялаш учун кейинги пайтлар кенг қўлланилаётган электрон имзодан фойдаланилмоқда. Идентификациялаш ва аутенфикациялашнинг муайян бир механизми, қурилмаси ва воситасини танлаш муайян тизимга қўйиладиган талаблардан келиб чиқади ва ахборот хавфсизлигини таъминлашда қўлланилаётган бошқа қарорларга боғлиқ бўлмаган ҳолда амалга оширилиши мумкин.

---

[1] *Мельников В.П. и др.* Информационная безопасность и защита информации: Учебое пособие. – М., 2008.

3. Хавфсизликни таъминлаш тизимини дастурий амалга ошириш-даги хатоликларни камайтириш ёки тўлиқ бартараф этилишига эришиш. Бошқа дастурий таъминотлар сингари ҳимоялашнинг усул ва воситалари ҳам жорий этиш хатоликларидан ҳоли эмас. Ҳимоя тизимининг ихтиёрий ташкил этувчисидаги бирор хатолик бутун тизимнинг хавфсизлигини шубҳа остида қолдириши табиийдир. Шу сабабли хавфсизликка жавобгар бўлган дастурий таъминотдаги хатоликлар нафақат ўз вазифани бажара олмай қолади, балки бутун тизимни издан чиқаради. Ушбу муаммони ҳал этилишига қаратилган чора-тадбирлар дастурлаш технологияси ва ОТнинг ишончлик соҳасига тааллуқли бўлади.

4. Хавфсизликни таъминлаш воситаларининг бутунлигини тегишли назоратини ташкил этиш. Ушбу муаммо соф технологик характерга эга бўлиб, ҳозирда бутунликни назорат қилиш усуллари етарлича ривожланган ва ушбу масаланинг ишончли ечимлари топилган (масалан, электрон рақамли имзо орқали). Аммо, амалиётда, одатда ушбу методлар фақатгина маълумотлар бутунлигини назорат қилиш учунгина (масалан, алоқа канали орқали маълумотларни узатишда) қўлланилади. Ушбу муаммони ҳал этиш учун биринчи навбатда, хавфсизликни таъминловчи механизмлар бутунлигини назорат қилиш лозим.

5. Дастурий ва қурилмавий маҳсулотларни ишлаб чиқишнинг якуний босқичида созлаш ва тестдан ўтказиш воситаларини мавжудлигини таъминлаш. Ушбу муаммони ҳал этилиши учун ташкилий тадбирлардан фойдаланиш мумкин. Хавфсизлик ҳал қилувчи аҳамиятга эга бўлган барча тизимлар, ўзида шунга ўхшаш имкониятлар мавжуд эмаслигини тасдиқловчи сертификатларга эга бўлиши лозим. Табиийки, ушбу талабни бажарилиши учун тўлиқ жавобгарликни ишлаб чиқарувчи ўз зиммасига олади.

6. Администрациялашдаги хатоликларни минимумга келтириш. Ушбу муаммо инсон фактори билан боғлиқлиги сабабли соф техник воситалар ёрдамида ҳал этила олмайди. Шу каби хатоликларни вужудга келиш эҳтимоллигини камайтириш учун хавфсизликни бошқариш ва фойдаланишга рухсат беришни назорат қилиш воситаларини қулай ва ишлашга осон бўлган интерфейс билан таъминлаш лозим ҳамда имкониятга қараб бошқарувнинг автоматлаштирилган тизимидан фойдаланган маъқул. Бундан ташқари, ҳисоблаш тизими конфигурациясини администра-циялашнинг адекват эмаслигини текширадиган верификацияловчи воситаларнинг қўлланилиши ҳам назарда тутилиши мумкин.

Маълумотларни базасини бошқариш тизими (МББТ)да маълумотларни қайта ишлаш жараёнини ҳимоялаш. Маълумотлар базасида ахборотларни қайта ишлаш жараёнини ҳимоялаш, файлдаги маълумотларни ҳимоялашдан фарқ қилади ва қуйидаги ўзига хос хусусиятларга эга:

– танланган ҳимоя механизмида маълумотлар базасини бошқариш тизимини ишлай олишини ҳисобга олиш зарурияти;

– базадаги маълумотлардан фойдаланишга рухсат беришни чеклашни файл сатҳида эмас, маълумотлар базасининг қисмлари сатҳида амалга ошириш лозимлиги.

Маълумотлар базасида маълумотларни қайта ишлаш жараёнини ҳимоялаш воситаларини яратишда, ушбу воситаларнинг нафақат ОТ билан, балки МББТ билан биргаликда ишлай олишини ҳисобга олиш керак.

Замонавий маълумотлар базасида маълумотлардан фойдаланишга рухсат беришни чеклаш, маълумотларнинг физик бутунлигини ва мантиқий сақланганлик масаласи етарли даражада муваффақиятли ҳал этилган. Ҳозирда фойдаланувчи томонидан маълумотлар базаси ёзувларидан ва ёзув майдонларидан фойдаланишга рухсатни чеклаш алгоритмларидан унумли фойдаланилмоқда, ушбу ҳимояни жиноятчи зарарловчи дастурларни жорий этиш ёки фойдаланувчи ҳуқуқларини қалбакилаштириш ёрдамида енгиб ўтиши мумкин. Маълумотлар базаси файлидан ва базанинг қисмларидан фойдаланишга рухсат бериш МББТ томонидан, фойдаланувчининг ҳуқуқларини белгилаб бериш ва рухсат берилиши керак бўлган объектлардан фойдаланишга рухсат бериш ҳуқуқларини назорат қилиш йўли билан амалга оширилади.

Фойдаланувчи ҳуқуқлари МББТ администратори томонидан белгиланади. Одатда, фойдаланувчининг стандарт идентификатори бўлиб, шифрланган кўринишда узатиладиган пароль ҳисобланади. Тақсимланган КТда фойдаланувчининг ҳақиқийлигини тасдиқлаш жараёни, масофавий жараёнларни ўзаро аутентификациялаш каби махсус процедура билан тўлдирилади.

4.3. Маълумотларни узатиш тармоғида ахборот хавфсизлигининг аппарат-дастурий воситалари

Тармоқ технологиясининг кенг кўламда қўлланиши натижасида умумий ресурслардан фойдаланиш имконини берувчи локал

тармоққа компьютерлар бирлаштирилди. Клиент-сервер технологиясининг татбиқ этилиши эса бу тармоқни тақсимланган ҳисоблаш муҳитига айлантирди. Тармоқнинг хавфсизлиги ундаги барча компьютерларнинг ва тармоқ қурилмаларининг хавфсизлиги билан аниқланади. Бузғунчи тармоқнинг бирор-бир ташкил этувчисининг ишини бузиш орқали бутун тармоқни обрўсизлантириши мумкин.

Замонавий телекоммуникация технологиялари локал тармоқларни глобал тармоққа – Интернетга улаш имконини берди. Интернетнинг ривожланиши хавфсизликни таъминлашни долзарб масалага айлантирди ва Интернетга уланган тармоқ ва тизимларда, қандай маълумотларга ишлов берилишидан қатъий назар, хавфсизлик воситалари бўлишини тақозо этади. Чунки, Интернетнинг имкониятларидан фойдаланиб, бузғунчи хавфсизликни бузишни глобал масштабда олиб бориши мумкин. Интернетга уланган компьютер тажовуз объекти бўлса, ҳужумни амалга ошираётган шахсга унинг қаерда (қўшни хонада ёки бошқа континентда) жойлашгани катта аҳамиятга эга эмас.

Ҳамма фойдаланаётган тармоқдан келиб чиқаётган таҳдидларни блокировкалаш учун «тармоқлараро экран» (Firewall) деб номланувчи дастурий ва аппарат-дастурий воситалардан фойдаланилади. Одатда, алоҳида ажратилган ва ҳимояланган КТ «тармоқлараро экран» орқали ҳамма фойдаланадиган тармоққа уланади.

Тармоқлараро экран ҳимояланган КТга келиб тушаётган ва ундан чиқиб кетаётган ахборотларни назорат қилиш учун қўлланилади.

Тармоқлараро экран қуйидаги тўртта функцияни бажаради:

– маълумотларни фильтрлаш;

– экранловчи агентлардан фойдаланиш;

– манзилларни трансляциялаш;

– ҳодисаларни қайд қилиш.

Тармоқлараро экраннинг асосий вазифаси (кираётган ёки чиқаётган) трафикни фильтрлашдан иборат. Корпоратив тармоқнинг ҳимояланганлик даражасига қараб фильтрлашнинг турли қоидалари ўрнатилиши мумкин. Фильтрлаш қоидалари фильтрлар кетма-кетлигини танлаш орқали амалга оширилади. Ушбу фильтрлар ўзидан кейинги фильтрга ёки протокол сатҳига маълумотларни узатилишига рухсат беради ёки тақиқлайди.

Тармоқлараро экран фильтрлашни каналлар, тармоқлар, транспорт ва амалий сатҳларда амалга оширади. Экран қанча кўп сатҳни ўз ичига олса, шунча такомиллашган ҳисобланади.

Тармоқлараро экранда, дастурий воситачи вазифани бажарувчи ва субъект ва объект орасида уланишни таъминловчи, сўнгра ахборотни қайд қилиш ва назоратини амалга ошириб жўнатувчи, *экранловчи агентлардан* (proxy-серверлар) фойдаланилади. Экранловчи агентларнинг қўшимча вазифаси фойдаланишга рухсат берилган субъектдан ҳақиқий объектни яширишдан иборат. Экранловчи агентларнинг ўзаро алоқа иштирокчиларига таъсири йўқ.

Тармоқлараро экраннинг манзилларни *трансляциялаш* функцияси ҳақиқий ички манзилларни ташқи абонентлардан яшириш учун мўлжалланган. Бу тармоқ топологиясини яшириш ва агар ҳимояланган тармоқ учун етарли миқдорда манзиллар ажратилмаган бўлса, янада кўпроқ сондаги манзиллардан фойдаланишга имкон яратади.

Тармоқлараро экран махсус журналларда *ҳодисаларни қайд* қилиб боради. Бирор аниқ талаб бўйича экранни созлаш орқали журналларни юритиш имконияти назарда тутилган. Ёзувлар таҳлили ўрнатилган қоидаларни бузишга бўлган бузғунчиларнинг уринишларини қайд қилиш ва уларни аниқлаш имконини беради.

Экран симметрик эмас. У «ташқи» ва «ички» тушунчаларини фарқлай олади. Экран ички соҳани назоратсиз ва адоватли бўлган ташқи муҳитдан ҳимоясини таъминлаб беради. Шу билан бирга экран ҳимояланган тармоқ субъектлари томонидан оммавий тармоқ объектларидан фойдаланишни чеклашни ҳам таъминлайди. Фойдаланишга рухсат берилган субъектнинг ваколатлари бузилган ҳолатда унинг иш фаолияти блокировка қилинади ва барча керакли маълумотлар журналга ёзиб қўйилади.

Тармоқлараро экранларга қуйидаги замонавий талаблар қўйилади:

1. Асосий талаблар – бу ички тармоқнинг хавфсизликни таъминлаш ва ташқаридан уланишлар ва алоқа сеансларини тўлиқ назорат қилиш.

2. Экранловчи тизим ташкилотнинг хавфсизлик сиёсатини оддий ва тўлиқ юритиш учун қувватли ва мосланувчан бошқариш воситаларига эга бўлмоғи даркор.

3. Тармоқлараро экран локал тармоқ фойдаланувчиларига сездирмасдан ишлаши ва улар томонидан рухсат этилган амалларни бажаришларига халақит бермаслиги лозим.

4. Тармоқлараро экран кўп миқдордаги мурожаатлар билан блокировка қилиб қўйишни ва ишдан чиқишининг олдини олиш учун, унинг процессори тез ишлай олиш, пик режимларида кирувчи

ва чиқувчи оқимларни етарли даражада самарали қайта ишлай олишга улгуриши лозим.

5. Хавфсизликни таъминлаш тизими ҳар қандай ташқи ноқонуний таъсирлардан ҳимояланган бўлиши лозим, чунки бу таъсирлар ташкилотнинг конфеденциал маълумотларини очиш калити бўлиши мумкин.

6. Экранни бошқарув тизими олисдаги филиаллар учун ҳам ягона хавфсизлик сиёсатини юритишни марказлашган ҳолда таъминлаш имкониятига эга бўлмоғи лозим.

7. Тармоқлараро экран фойдаланувчиларнинг ташқи уланишлари орқали фойдаланишга рухсат беришнинг муаллифлаштириш воситаларига эга бўлмоғи керак. Бу ташкилот ходимларини хизмат сафарида ҳам тармоқдан фойдаланишларига имкон яратади.

Мустақил тайёргарлик учун саволлар

1. Ахборотларни муҳофаза қилишнинг асосий ва ёрдамчи аппарат воситаларига нималар киради?

2. Ахборотларни муҳофаза қилишнинг дастурий воситалари қандай дастурлардан иборат?

3. Ахборотларни муҳофаза қилишнинг дастурий воситаларининг афзалликлари ва камчиликлари нималардан иборат?

4. Компьютер тизимларидан фойдаланиш ҳуқуқини чеклашнинг қандай усул ва воситалари мавжуд?

5. Қандай атрибутивли индентификаторларни биласиз ва улар қандай тартибда ишлайди?

6. Ҳимояловчи аппарат-дастурий комплексларда ҳимоялаш механизмлари нималардан иборат?

7. Компьютер вируслари нима?

8. Компьютер тизимларининг хавфсиз ишлаши учун қандай қоидаларга риоя этилиши талаб этилади?

9. Тизимдаги ахборотларнинг бутунлиги қандай таъминланади?

10. Ахборот хавфсизлигини таъминлашнинг дастурий ва аппарат-дастурий воситалардан фойдаланишга қандай талаблар қўйилади?

11. Маълумотларни базасини бошқариш тизимида маълумотлар қандай муҳофаза қилинади?

12. Тармоқда ахборот хавфсизлигини таъминловчи қандай аппарат-дастурий воситалар мавжуд?

13. Тармоқлараро экран қандай функцияларни бажаради?

14. Тармоқлараро экранларга қандай талаблар қўйилади?

V. ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА АХБОРОТНИ МУҲОФАЗА ҚИЛИШНИНГ ДАВЛАТ ТИЗИМИ

5.1. Ахборотни муҳофаза қилишнинг давлат тизими.

5.2. Ахборотни муҳофаза қилиш соҳасида лицензиялаш ва сертификациялаш.

5.3. Етакчи чет эл мамлакатларида ахборотни муҳофаза қилиш тизимлари.

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 меъёрий 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.

5.1. Ахборотни муҳофаза қилишнинг давлат тизими

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, кадрларни тайёрлаш, махсус алоқа тизимлари, илмий-тадқиқот ва тажриба-конструкторлик ишларини ташкиллаштириш тизимларини ўз ичига олувчи мураккаб тизимдир.

Ахборотни муҳофаза қилишнинг давлат тизими иш юритиши қуйидаги қонун, меъёрий ҳужжатлар асосида амалга оширилади:

– Ўзбекистон Республикасининг Конституцияси;

– «Давлат сирларини сақлаш тўғрисида»ги қонун;

– «Ахборотлаштириш тўғрисида»ги қонун;

– «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги қонун;

– «Фаолият 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;

– 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 зарарни 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 идоралари 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 меъёрий-методик ва ахборий таъминлаш.

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;

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.

---

[1] Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – Т., 2000. –№5-6. – 142-м.

Ўзбекистон Республикаси Вазирлар Маҳкамаси ваколатлари жумласига қуйидагилар киради (5-модда):

– лицензияловчи органларни ва фаолиятнинг айрим турларини лицензиялаш тартибини белгилаш, қонунда назарда тутилган ҳоллар бундан мустасно;

– Ўзбекистон Республикаси ҳудудида лицензиялар реестрини юритиш тартибини белгилаш;

– фаолиятнинг айрим турларини лицензиялаш соҳасидаги қонун ҳужжатларига лицензияловчи органларнинг риоя этишларини назорат қилиш;

– лицензиялашнинг айрим турларини амалга ошириш.

Лицензияловчи органларнинг ваколатлари жумласига қуйидагилар киради (6-модда):

– фаолиятнинг айрим турларини қонун ҳужжатларига мувофиқ лицензиялаш;

– қонунда назарда тутилган ҳолларда фаолиятнинг тегишли турларини лицензиялаш тартиби тўғрисидаги низомларни тасдиқлаш;

– лицензия талаблари ва шартларига лицензиатлар риоя этишини назорат қилиш;

– лицензияларни қайта расмийлаштириш;

– лицензияларнинг амал қилишини тўхтатиб туриш, қайта тиклаш;

– лицензияларнинг амал қилишини тугатиш;

– лицензияларни бекор қилиш;

– лицензиялар реестрини юритиш.

Фаолиятнинг лицензияланадиган турлари жумласига (7-модда) амалга оширилиши фуқароларнинг ҳуқуқлари ва қонуний манфаатларига, соғлиғига, жамоат хавфсизлигига зарар етказиши мумкин бўлган ҳамда тартибга солиб турилиши лицензиялашдан ташқари усуллар билан амалга оширилиши мумкин бўлмаган фаолият турлари киради.

Амалга оширилиши учун лицензия талаб қилинадиган фаолият турлари қонунлар билан белгиланади.

Лицензия олиш учун лицензия даъвогари тегишли лицензияловчи органга қуйидагиларни тақдим этади (14-модда):

– лицензия бериш тўғрисидаги ариза – унда: юридик шахс учун – юридик шахснинг номи ва ташкилий-ҳуқуқий шакли, жойлашган ери (почта манзили), банк муассасасининг номи ва банк муассасасидаги ҳисоб рақами; жисмоний шахс учун – фамилияси, исми ва отасининг

исми, фуқаронинг шахсини тасдиқловчи ҳужжатнинг маълумотлари; юридик ёки жисмоний шахс амалга оширишни мўлжаллаган фаолиятнинг лицензияланаётган тури (унинг бир қисми), шунингдек қонун ҳужжатларида назарда тутилган ҳолларда фаолиятнинг мазкур тури;

– юридик шахслар учун – юридик шахс давлат рўйхатидан ўтказилганлиги тўғрисидаги гувоҳноманинг нотариал тасдиқланган нусхаси; жисмоний шахслар учун – якка тартибдаги тадбиркор давлат рўйхатидан ўтказилганлиги тўғрисидаги гувоҳноманинг нусхаси;

– лицензияловчи орган лицензия даъвогарининг аризасини кўриб чиқиши учун лицензия даъвогари йиғим тўлаганлигини тасдиқловчи ҳужжат;

– фаолиятнинг айрим турига лицензия олиш учун қўйиладиган талаблар ва шартларни лицензия даъвогари бажариши мумкинлигини тасдиқловчи ҳамда қонун ҳужжатларида белгилаб қўйиладиган бошқа ҳужжатлар.

Лицензия даъвогарининг аризасини барча зарур ҳужжатлар билан бирга олган кундан эътиборан ўттиз кундан ошмаган муддат ичида лицензияловчи орган намунавий (оддий) лицензия бериш ҳақида ёки беришни рад этиш тўғрисида қарор қабул қилади ва лицензияловчи орган лицензия даъвогарини қабул қилинган қарор тўғрисида уч кун ичида хабардор қилиши шарт (16-модда).

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 лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва криптографик ҳимоя воситаларини қўллаш киради.

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

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

– Ўзбекистон Республикасининг 2007 йил 17 июлдаги 102-сонли қонуни[1] «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[2] билан тасдиқланган Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилиш тўғрисидаги Низом;

---

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

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 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 бўлим 24 бандига мувофиқ давлат идораларининг ахборот тизимида қўлланиладиган ахборотни ҳимоялаш дастурий-техник воситалари лицензияланган ва сертификатлаштирилган бўлиши керак.

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

СМТ фаолиятини регламентация қилувчи асосий меъёрий-ҳуқуқий акт бўлиб Ўзбекистон Республикасининг 1993 йил 28 декабрь кунидаги «Маҳсулотлар ва хизматларни сертификат-лаштириш 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;

маҳсулотларни сертификатлаштириш (матнда бундан кейин *сертификатлаштириш* деб юритилади) – маҳсулотларнинг белги-ланган талабларга мувофиқлигини тасдиқлашга оид фаолият;

мувофиқлик сертификати – сертификатланган маҳсулотнинг белгиланган талабларга мувофиқлигини тасдиқлаш учун сертификат-лаштириш тизими қоидаларига биноан берилган ҳужжат;

---

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

[2] Ўзбекистон Республикасининг қонун ҳужжатлари тўплами. – Т., 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. – Т., 2000. – №7-8. – 217-м.; 2003. –№5. – 67-м.; Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2006. – №14. – 113-м.; 2006. – №41. – 405-м.

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 идоралар;

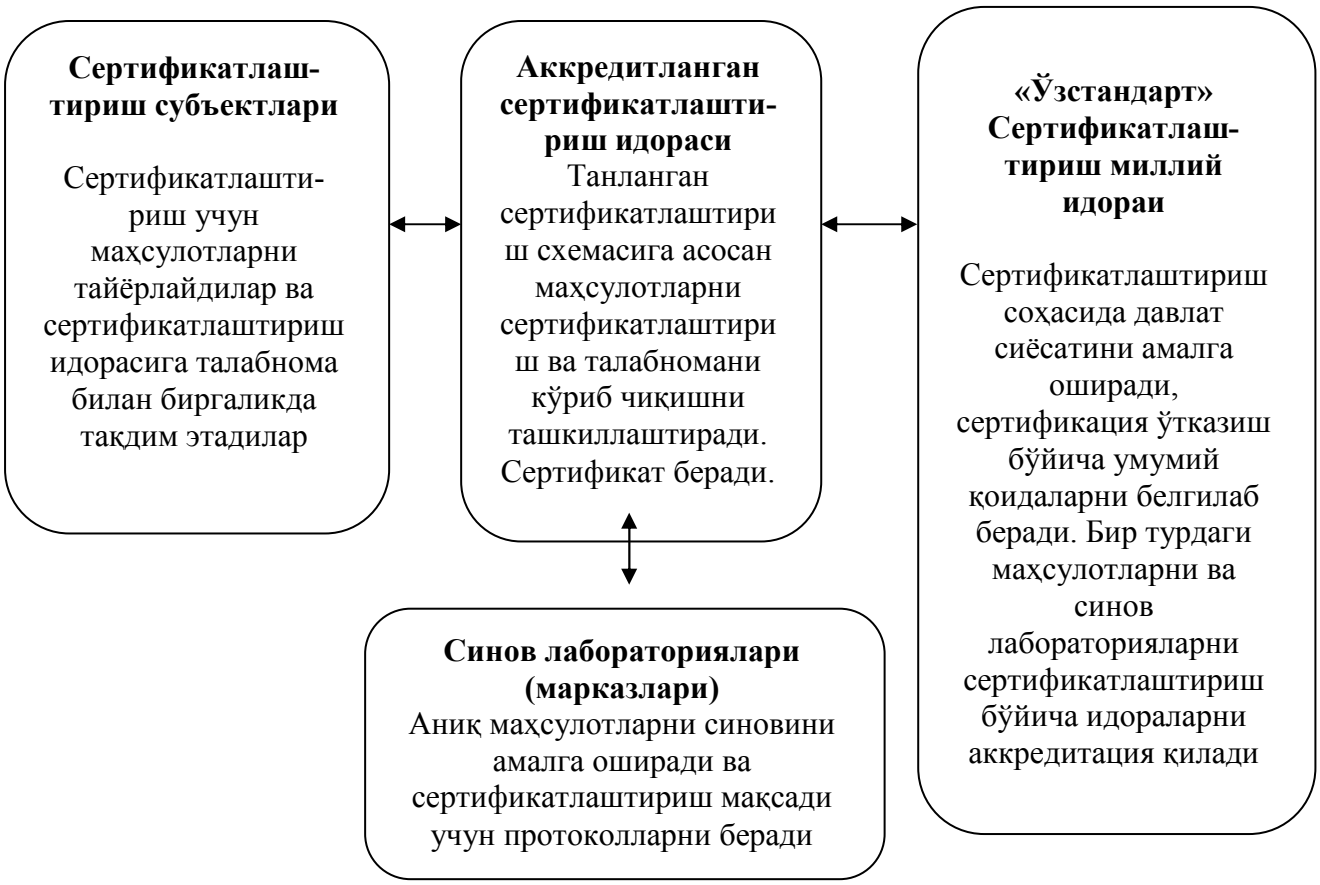
– синов лабораториялари (марказлари).

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.

СМТда маҳсулотлар (хизматлар)ни сертификатлаштиришнинг умумий тартиби:



Ўзбекистон Республикаси ҳудудида мажбурий сертификатлаштирилиши лозим бўлган маҳсулотлар номлари «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.

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

[2] Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – Т., 2011. – №18. – 178-м.

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 нашрлар эркин тарқатилади (мисол учун ёшлар орасида оммалашган «Хакер» ва «Спецхакер» журналларини келтириш мумкин). Ҳозирги кунда ихтиёрий ўспирин арзимаган пулга ахборот тизимларига ҳужум қилишнинг элементар усулларини ўргатувчи китобни сотиб олиши мумкин. Китобда баён этилган усулларни ўзлаштирган бундай ўспирин компьютер тизимлари 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 (очиқ) 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 ахлоқ-одобни 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 идораларда ва судларда компьютер соҳасидаги жиноятчиликка қарши курашиш бўйича мутахассисларни тайёрлаш лозим.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Тошкент ахборот технологиялари университети фаолиятини ташкил этиш тўғрисида»ги 2002 йил 7 ноябрь 385-сонли қарорига[1] мувофиқ бу университет республиканинг алоқа ва ахборот технологиялари соҳасида кадрлар тайёрлаш, қайта тайёрлаш ва мутахассислар малакасини ошириш бўйича базавий олий таълим муассасаси ҳисобланади.

Ўзбекистон Республикаси Президентининг «Миллий ахборот-коммуникация тизимларининг компьютер хавфсизлигини таъминлаш борасидаги қўшимча чора-тадбирлар тўғрисида»ги 2005 йил 5 сентябрь 167-сонли қарорига мувофиқ компьютер ва ахборот технологияларини ривожлантириш ҳамда жорий этиш маркази «Ўзинфоком» ҳузурида «Компьютер ҳодисаларига чора кўриш хизмати» ташкил этилган.

Ушбу Хизматнинг асосий вазифаларига қуйидагилар киради:

– компьютер хавфсизлигини таъминлашда халқаро тажрибани ўрганиш ва умумлаштириш асосида ахборот тизимларига ноқонуний кириш ҳаракатларини олдини олишни таъминловчи эффектив дастурий-аппаратли воситаларни қўллаш бўйича миллий фойдаланувчиларга тавсиялар ишлаб чиқиш, уларга консультатив хизматлар ва техник ёрдам бериш;

– эҳтимолий хавфни баҳолаш, ахборот тизимларида ва давлат корхона ҳамда ташкилотларда компьютер хавфсизлиги ҳолати бўйича миллий фойдаланувчиларга консультатив хизматлар ва техник ёрдам бериш, инцидент оқибати ва сабабларини таҳлил қилишда кўмаклашиш, компьютер тизимларини ҳимоялаш учун механизмларни қидириш;

– компьютер тизимини хавфсизлигини таъминлаш масалалари бўйича миллий ахборот тизимларига хизмат кўрсатувчи давлат корхоналари, операторлар ва провайдерлар мутахассислари учун ўқитиш ва тренинг машғулотларини ўтказишни ташкил этиш.

---

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

5.3. Етакчи чет эл 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 эҳтиёжини 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 ҳолда миллий ва корпоратив тармоқларни жаҳон очиқ тармоғларига уланишини таъминловчи ахборот технологияларни такомиллаштирувчи давлат дастурини ишлаб чиқиш.

3. Жаҳон ахборот тармоқларида ишлаш учун оммавий фойдаланувчиларни ва ахборот хавфсизлиги бўйича мутахассисларни тайёрлаш ва малакасини ошириш комплекс тизимини ташкил қилиш.

4. Очиқ жаҳон тармоқлари фойдаланувчиларининг масъулиятлари ва мажбуриятлари, регламент ҳуқуқи ва ахборот ресурслари билан фойдаланиш қоидаларининг миллий қонунчилик қисмини ишлаб чиқиш. Жаҳон очиқ тармоқлари ишлашининг меъёрий-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 ҳисобланади. 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 экспертлар комиссияси ахборот уруши ҳодисасига қарши ҳарбий телекоммуникация ва компьютер тармоқлари хавфсизлигини таъминловчи шошилинч чораларни қабул қилиш лозимлиги ҳақида доклад тайёрлади. Пентагон ҳарбий автомат-лаштирилган 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 парламент комитети Британия махсус хизматлари устидан назорат идораси сифатида 1994 йилда ташкил этилган. Бу комитет «Разведка хизматлари тўғрисида»ги қонунга мувофиқ учта махсус хизмат: Махфий хизмат (MI5), SIS разведкаси ва Ҳукумат алоқа маркази томонидан бюджет маблағларининг сарфланишини, бу хизматларнинг бошқарилишини ва уларнинг олиб бораётган сиёсатини назорат қилиш учун тузилган.

Secret Intelligence Service/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 – Military Intelligence-5 (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 идораси 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 мезонлар, 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 идоралари, полиция ва бошқа идораларда ахборот алмашинишда махсус хавфсизлик чораларини амалга ошириш;

– саноат вакилларига маслаҳатлар бериш.

Хавфсизликни таъминловчи бошқа давлат идоралари:

– Германиянинг федерал разведка хизмати (Bundesnachrichten-dienst /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 бўйсунади. Барча федерал ерларда маҳаллий ички ишлар вазирлигига бўйсунадиган 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 шахсларнинг очиқ ассоциацияси ҳисобланади. CLUSIF давлат томонидан тўлиқ қўллаб қувватланади ва махсус хизматлар билан яқин алоқага эга.

Франциянинг махсус хизмати структураси. Франция разведка уюшмасининг умумий штати, учта ҳар хил вазирликка бўйсунувчи

хизматларда ишлайдиган 12779 га 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 ҳар 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 идоралари структураси. Ахборот хавфсизлигининг давлат сиёсатини ишлаб чиқиш, қонунлар, норматив-меъёрий ҳужжатлар тайёрлаш, ахборотни муҳофаза қилишни таъминлаш бўйича ўрнатилган меъёрларни бажарилиши устидан назоратни давлат идоралари амалга оширадилар.

РФ Президенти ахборот хавфсизлигини таъминловчи давлат идораларига 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 идораси 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 идораси бўлиб РФ Президенти ҳузуридаги Давлат техник комиссияси ҳисобланади. Бу комиссия қонун лойиҳаларини тайёрлашни амалга оширади, норматив меъёрий 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.

РФ вазирлик ва идораларида ахборот хавфсизлиги сиёсатининг мос даражаларини бошқаришни таъминловчи иерархияга асосланган тузилмалар мавжуд. Бу тузилмалар, турли-хил номлангани билан ўхшаш функцияларни бажарадилар.

Мустақил тайёргарлик учун саволлар

1. *Ахборотни муҳофаза қилишнинг давлат тизими нима?*
2. *Ахборотни муҳофаза қилишнинг давлат тизими иш юритиши қандай қонун, норматив-меъёрий ҳужжатлар асосида амалга оширилади?*
3. *Ахборотни муҳофаза қилишнинг давлат тизимида кўзланган мақсад нима?*
4. *Ахборотни муҳофаза қилишнинг давлат тизимида кўзланган мақсадни амалга оширишда қандай вазифаларни бажариш керак?*
5. *«Лицензия» ва «лицензиялаш» тушунчалари нимани англатади ва уларнинг таърифи қайси қонунда берилган?*
6. *Ахборотни криптографик муҳофаза қилиш соҳасидаги фаолият қандай лицензияланади?*
7. *Сертификациялашнинг миллий тизими нима?*
8. *Сертификациялаш нима мақсадда амалга оширилади?*
9. *Ахборотни муҳофаза қилиш воситаларини сертификатлаштириш қандай амалга оширилади?*
10. *Ахборот хавфсизлиги соҳасида мутахассисларни тайёрлаш бўйича қандай ишлар олиб борилмоқда?*
11. *Ахборот қуроли қандай амалларни бажаришга йўналтирилган?*
12. *Ахборот қуролидан ҳимояловчи амалий тадбирларга нималар киради?*
13. *АҚШ ва Буюк Британиядаги ахборотни ҳимоялаш тизими ҳақида нималарни биласиз?*
14. *Германия, Франция ва Россияда ахборотни ҳимоялаш қандай ташкил қилинган?*

ХУЛОСА

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 бутунликка 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.

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 долзарб масалалардан биридир.

Амалиёт шуни кўрсатадики, ахборотни муҳофаза қилишда етарли даражадаги ютуқларга эришиш учун ҳуқуқий, ташкилий ва техник чораларни биргаликда амалга ошириш зарур. Бу ҳимояланадиган ахборотнинг конфеденциаллиги, таҳдиднинг таснифи ва ҳимоя воситаларининг мавжудлиги билан белгиланади. Умумий ҳолда хавфсизликни таъминлашнинг комплекс чораларига:

- рухсатсиз фойдаланишдан комплекс ҳимоя қилиш воситалари;
- аппарат-дастурий воситалар;
- криптографик муҳофаза қилишнинг комплекс воситалари;
- инженер-техник тадбирлар;
- техник каналларни блокировкалаш комплекс воситалари;
- объектларни жисмоний қўриқлашни киритиш мумкин.

Бу чораларнинг ҳар бири бошқасини тўлдиради, бироита усулнинг йўқлиги ёки етишмаслиги етарли даражадаги ҳимоянинг бузилишига сабаб бўлиши мумкин.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

Ўзбекистон Республикасининг Конституцияси. – Т., 2012.

Каримов И.А. Ўзбекистон: миллий истиқлол, иқтисод, сиёсат, мафкура. Т.1. – Т., 1996.

Каримов И.А. Биздан озод ва обод Ватан қолсин. Т. 2. – Т., 1996.

Каримов И.А. Ватан саждагоҳ каби муқаддасдир. Т. 3. – Т., 1996.

Каримов И.А. Бунёдкорлик йўлидан. Т.4. – Т., 1996.

Каримов И.А. Янгича ишлаш ва фикрлаш – давр талаби. Т. 5. – Т., 1997.

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

Каримов И.А. Биз келажагимизни ўз қўлимиз билан қурамиз. Т. 7. –Т., 1999.

Каримов И.А. Озод ва обод Ватан, эркин ва фаровон ҳаёт – пировард мақсадимиз . Т.8. –Т., 2000.

Каримов И.А. Ватан равнақи учун ҳар биримиз масъулмиз. Т. 9. – Т., 2001.

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

Каримов И.А. Биз танлаган йўл – демократик тараққиёт ва маърифий дунё билан ҳамкорлик йўли. Т. 11. – Т., 2003.

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

Каримов И.А. Ўзбек халқи ҳеч қачон, ҳеч кимга қарам бўлмайди. Т. 13. – Т., 2005.

Каримов И.А. Инсон, унинг ҳуқуқ ва эркинликлари – олий қадрият. Т.14. – Т., 2006.

Каримов И.А. Жамиятни эркинлаштириш, ислоҳатларни чуқурлаштириш, маънавиятимизни юксалтириш ва халқимизнинг ҳаёт даражасини ошириш – барча ишларимизнинг мезони ва мақсадидир. Т.15. – Т., 2007.

Каримов И.А. Мамлакатимизни модернизация қилиш ва иқтисодиётимизни барқарор ривожлантириш йўлида. Т.16. – Т., 2008.

Каримов И.А. Юксак маънавият – енгилмас куч. – Т., 2008.

Каримов И.А. Ватанимизни босқичма-босқич ва барқарор ривожлантириш бизнинг олий мақсадимиз. Т.17. – Т., 2009.

Каримов И.А. Жаҳон молиявий-иқтисодий инқирози, Ўзбекистон шароитида уни бартараф этиш йўллари ва чоралари. – Т., 2009.

Каримов И.А. Жаҳон инқирозининг оқибатларини енгиш, мамлакатимизни модернизация қилиш ва тараққий топган давлатлар даражасига кўтариш сари. Т.18. – Т., 2010.

Каримов И.А. Демократик ислоҳотларни янада чуқурлаштириш ва фуқаролик жамиятини шакллантириш – мамлакатимиз тараққиётининг асосий мезонидир. Т.19. – Т., 2011.

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

Каримов И.А. Ўзбекистон мустақилликка эришиш остонасида. – Т., 2011.

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

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

Ўзбекистон Республикасининг «Маҳсулотлар ва хизматларни сертификатлаштириш тўғрисида»ги 1993 йил 28 декабрь 1006-XII сон қонуни // 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.

Ўзбекистон Республикасининг «Фаолиятнинг айрим турларини лицензиялаш тўғрисида»ги 2000 йил 25 май 71-II-сон қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2000. – №5-6. – 142-м.

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

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

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

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

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

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

Ўзбекистон Республикасининг «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»ги 2007 йил 17 июль ЎРҚ-102-сон қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №29-30. – 295-м.

Ўзбекистон Республикасининг «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 ЎРҚ-137-сон қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №52. – 532-м.

Ўзбекистон Республикасининг ««Фаолиятнинг айрим турларини лицензиялаш тўғрисида»ги Ўзбекистон Республикаси қонунига ўзгартиш ва қўшимчалар киритиш ҳақида»ги 2011 йил 7 сентябрь ЎРҚ-292-сон қонуни // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2011. – №36. – 363-м.

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

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

Ўзбекистон Республикаси Президентининг «Ахборот-коммуникация технологияларини янада ривожлантиришга оид қўшимча чора-тадбирлар тўғрисида»ги 2005 йил 8 июль ПҚ-117-сон қарори // Ўзбекистон Республикаси қонун хужжатлари тўплами. – 2005. –№27. – 189-м.

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

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

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникация технологияларини жорий этиш чора-тадбирлари тўғрисида»ги 2002 йил 6 июнь 200-сон қарори // Ўзбекистон Республикаси қонун хужжатлари тўплами. – 2002. – №11–12. – 91-м., 2003. – №24. – 241-м. – 2004. – №19. – 420-м., 2006. – №40. – 396-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Халқаро компьютер тармоқларидан фойдаланишни марказлаштиришдан чиқариш тўғрисида»ги 2002 йил 10 октябрь 352-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2002. – №19. – 149-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Ахборотлаштириш соҳасида норматив ҳуқуқий базани такомиллаштириш тўғрисида»ги 2005 йил 22 ноябрь 256-сон қарори // Ўзбекистон Республикаси Ҳукуматининг қарорлари тўплами. – 2005. – №47-48. – 355-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Ziyonet ахборот тармоғини янада ривожлантириш тўғрисида»ги 2005 йил 28 декабрь 282-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2005. – №389. – 389-м.

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

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «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 27-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2006. – №8. – 51-м., 2007. – №7-8. – 65-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Давлат ва хўжалик бошқаруви, маҳаллий давлат ҳокимияти органларининг ахборот-коммуникация технологияларидан фойдаланган ҳолда юридик ва жисмоний шахслар билан ўзаро ҳамкорлигини янада такомиллаштириш чора-тадбирлари тўғрисида»ги 2007 йил 23 август 181-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №33-34. – 348-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Ахборотнинг криптографик ҳимоя воситаларини лойиҳалаштириш, тайёрлаш, ишлаб чиқариш, реализация қилиш, таъмирлаш ва улардан фойдаланиш фаолиятини лицензиялаш тўғрисидаги Низомни тасдиқлаш ҳақида»ги 2007 йил 21 ноябрь 242-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2007. – №46-47. – 471-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «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 87-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2008. – №19. – 159-м.

Ўзбекистон Республикаси Вазирлар Маҳкамасининг «Давлат ва хўжалик бошқаруви, маҳаллий давлат ҳокимияти органлари ходимларининг малакаси ва кўникмаларини оширишга доир қўшимча чора-тадбирлар ҳамда уларни ишда компьютер техникаси ва ахборот-коммуникация технологияларидан фойдаланиш юзасидан аттестациядан ўтказиш тартиби тўғрисида»ги 2011 йил 27 октябрь 289-сон қарори // Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2011. – №43-44. – 465-м.

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

Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.

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

Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.

Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.

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. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.

Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.

Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.

Казиев В.М. Введение в правовую информатику. – http://www. intuit.ru.

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

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

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 Республике Узбекистан в условиях глоболизации. – Т., 2008.

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

Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М., 2005.

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

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

Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М., 1999.

Семененко В.А. Информационная безопасность: Учебное пособие. – М., 2008.

Серго А.Г. Интернет и право. – М., 2003. http://Cyber-Crimes.ru.

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

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

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

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

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

www.twirpx.com / Информатика и вычислительная техника / Защита информации (ЗИ).

Тошкент ахборот технологиялари университети қошидаги радиоэлектрон тизимлар ва ахборот технологиялари Марказининг презентация материаллари.

М У Н Д А Р И Ж А

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

ТУРГУНОВ Нозимжон Абдуманнопович
физика-математика фанлари номзоди, доцент;

КАДИРОВ Фахриддин
техника фанлари номзоди, доцент;

САМАРОВ Хусниддин Камариддинович
техника фанлари номзоди, доцент;

ИМИНОВ Абдурасул Абдулатипович
физика-математика фанлари номзоди;

ДЖАМАТОВ Мустафа Хатамович
физика-математика фанлари номзоди

АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ

Маърузалар курси

Муҳаррир **С. С. Қосимов**
Техник муҳаррир **Д. Х. Ҳамидуллаев**

Босишга рухсат этилди 01.01.2013. Нашриёт ҳисоб табоғи 8,0.
Адади 50 нусха. Буюртма . Баҳоси шартнома асосида.

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