O‘ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI

AKADEMIYA

KARIMOV I. M., TURGUNOV N. A.

# AXBOROT XAVFSIZLIGI ASOSLARI

*Darslik*

Toshkent–2016

*O‘zbekiston Respublikasi IIV Akademiyasining*
*Tahririyat-noshirlik hay’atida ma’qullangan*

*T a q r i z c h i l a r :*

Toshkent Axborot texnologiyalari universitetining axborot xavfsizligi kafedrasi dotsenti, texnika fanlari nomzodi **A.A. Ganiyev;**

Toshkent shahar IIBB Axborot markazi boshlig‘i, texnika fanlari nomzodi **M. Rajabov**

**Karimov I. M.**

**K-23** **Axborot xavfsizligi asoslari:** Darslik / I. M. Karimov, N. A. Turgunov. – T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2016. – 91 b.

Darslikda axborot xavfsizligi va tashkil etuvchilari, axborotni muhofaza qilish, himoyalangan axborotga tahdidlar, axborotlarni muhofaza qilishga kompleks yondashuv va uni amalga oshirish chora-tadbirlari; axborotni muhofaza qilishning asosiy obyektlari, O‘zbekiston Respublikasida axborot xavfsizligi va ma’lumotlarni muhofaza qilishga oid normativ-huquqiy hujjatlar, axborot himoyasi sohasida xalqaro standartlar, ma’lumotlarni ruxsatsiz olishning obyektlari, usullari va vositalari, himoyaning texnik vositalari, ma’lumotlar chiqib ketish texnik kanallari tasnifi, ma’lumotlarni tutib olish, kriptografiya va kriptotahlil, shifrlar va ularning xossalari, shifrlovchi dasturlar, elektron raqamli imzo, ma’lumotlarni himoyalashning apparat-dasturiy vositalari, axborotni muhofaza qilishning davlat tizimi, uni amalga oshiruvchi qonun, normativ hujjatlar, yetakchi chet el mamlakatlarida axborot xavfsizligini ta’minlash tizimlariga oid ma’lumotlar keltirilgan. Ushbu ma’lumotlar bilan tanishish orqali kitobxonlar axborot xavfsizligi va ma’lumotlarni himoyalash bo‘yicha o‘z nazariy bilimlarini shakllantirib, uning tashkil etuvchilari imkoniyatlari haqida batafsil tushunchalarga ega bo‘ladilar.

IIV Akademiyasi tinglovchilari, kursantlari, huquqni muhofaza qilish idoralari xodimlari va boshqa turdosh sohalarda faoliyat yuritayotgan mutaxassislarga mo‘ljallangan.

**BBK 73ya73**

# KIRISH

Axborot-kommunikatsiya texnologiyalari shiddat bilan rivojlanib borayotgan hozirgi davrda har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi muhim omillardan biri hisoblanadi. Mazkur resurslardan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirilishini ta'minlaydi. Bunday jamiyatda axborot almashinuv tezligi yuksalib, axborotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanish bo'yicha ilg'or axborot-kommunikatsiyalar texnologiyalarini qo'llash keng ko'lamda amalga oshiriladi.

Bugungi kunda axborotlashgan jamiyat jadal suratlar bilan shakllanib, axborotlar dunyosida davlat chegaralari degan tushuncha yo'qolib bormoqda. Global kompyuter tarmog'i jahon davlatlarining ijtimoiy-iqtisodiy, siyosiy, ma'naviy va madaniy hayotida alohida ahamiyat kasb etmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi bo'lib hisoblanadi. O'zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimini yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o'z ifodasini topdi. Bu borada O'zbekiston Respublikasining «Davlat sirlarini saqlash to'g'risida»gi, «Axborotlashtirish to'g'risida»gi va boshqa qonunlar qabul qilindi hamda amalda tatbiq etib kelinmoqda.

Mamlakatimizda axborotlashtirish sohasidagi davlat siyosati axborot resurslari, axborot texnologiyalari va axborot tizimlarini rivojlantirish hamda takomillashtirishning zamonaviy jahon tamoyillarini hisobga olgan holda milliy axborot tizimini yaratishga qaratilgan[1].

O'zbekiston Respublikasining Birinchi Prezidenti Islom Karimov bugungi kunda jamiyat taraqqiyotida axborot texnologiyalarining ahamiyatiga to'xtalib, quyidagilarni ta'kidlagan: «Bugungi sharoitda, Internet va elektronika davrida iqtisodiyot tarmoqlarida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish, «Elektron hukumat» tizimi faoliyatini yanada rivojlantirish ustuvor ahamiyatga egadir.

---

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

Jahon tajribasi shundan dalolat beradiki, ayni paytda global iqtisodiyotda kompyuter va telekommunikatsiya texnologiyalari, dasturiy ta’minot mahsulotlarini ishlab chiqarish va ular asosida keng turdagi interfaol xizmatlar ko‘rsatishni o‘z ichiga olgan axborot-kommunikatsiya texnologiyalari sohasining roli va ahamiyati tobora ortib bormoqda.

Axborot-kommunikatsiya texnologiyalarining rivojlanishi mamlakatning raqobatdoshlik darajasiga ta’sir ko‘rsatishi, katta hajmda axborot to‘plash va uni umumlashtirish imkonini berishi, boshqarishni strategik darajada tashkil etish uchun keng imkoniyatlar ochib berishini unutmasligimiz zarur».[1]

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida[2] axborot xavfsizligini ta’minlash sohasidagi davlat siyosati axborot sohasidagi ijtimoiy munosabatlarni tartibga solishga qaratilgan hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashdan iborat deb belgilangan. ««Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi Qonunning qabul qilinishi har kimning axborotni erkin va moneliksiz olish hamda foydalanish huquqlarini amalga oshirishda, shuningdek, axborotning muhofaza qilinishi, shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashda muhim ahamiyat kasb etdi»[3].

---

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

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

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

# I. AXBOROT XAVFSIZLIGI VA AXBOROTNI MUHOFAZA QILISH

## 1.1. Axborot xavfsizligi va axborotni muhofaza qilish tushunchalari

**Axborot xavfsizligi** – ko‘p qirrali faoliyat sohasi bo‘lib, unga faqat tizimli, kompleks yondashuv muvaffaqiyat keltirishi mumkin. Ushbu muammoni hal etish uchun huquqiy, ma’muriy, protsedurali va dasturiy-texnik choralar qo‘llaniladi.

Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborotni muhofaza qilish esa davlatning birlamchi masalalariga, davlat siyosati darajasiga aylanmoqda.

*Axborot xavfsizligining milliy xavfsizlik tizimidagi o‘rni.* XXI asrda shaxs, jamiyat va davlat taraqqiyotida axborot resurslari va texnologiyalarining rolini ortishi natijasida O‘zbekiston Respublikasida fuqarolik jamiyatini axborotlashtirilgan jamiyat sifatida qurish masalasini hal etish bilan birga quyidagi omillar milliy xavfsizlikni ta’minlash tizimida axborot xavfsizligining yetakchi o‘rin egallashini belgilaydi:

– milliy manfaatlar, ularga tajovuz va ularni bu tajovuzlardan himoyalash axborot va axborot sohasi orqali ifodalanadi, amalga oshiriladi;

– inson va uning huquqlari, axborot va axborot tizimlari hamda ularga egalik qilish – bu nafaqat axborot xavfsizligining asosiy obyektlari, shu bilan birga jami xavfsizlik sohalaridagi xavfsizlik obyektlarining asosiy elementlaridir;

– axborot yondashuvidan asosiy ilmiy-amaliy usul sifatida foydalanish orqali milliy xavfsizlik masalalarini hal etish mumkin;

– milliy xavfsizlik muammosi yaqqol ajralib turuvchi axborot tavsifiga ega.

Axborot xavfsizligi tizimi davlatning axborot sohasidagi siyosatini mamlakatda milliy xavfsizlikni ta’minlash davlat siyosati bilan chambarchas bog‘laydi. Bunda axborot xavfsizligi tizimi davlat siyosatining asosiy tashkil etuvchilarini yaxlit bir butunlikka biriktiradi. Bu esa axborot xavfsizligining roli va uning mamlakat milliy xavfsizligi tizimidagi mavqeini belgilaydi. Axborot sohasidagi O‘zbekistonning milliy manfaatlarini,

ularga erishishining strategik yo‘nalishlarini va ularni amalga oshirish tizimlarini o‘zida aks ettiruvchi maqsadlar yaxlitligi davlat axborot siyosatini anglatadi. Shu bilan birga davlat axborot siyosati mamlakatning tashqi va ichki siyosatining asosiy tashkil etuvchisi hisoblanadi va jamiyatning barcha jabhalarini qamrab oladi.

*Axborot xavfsizligining zamonaviy konsepsiyasi* axborot xavfsizligini ta’minlovchi maqsadlar, vazifalar, tamoyillar va asosiy yo‘nalishlar bo‘yicha rasmiy nuqtai nazarlar majmuini bildiradi.

Quyida axborot xavfsizligining asosiy tashkil etuvchilari va jihatlari keltirilgan:

– axborotni muhofaza qilish (shaxsiy ma’lumotlarni, davlat va xizmat sirlarini va boshqa turdagi tarqatilishi chegaralangan ma’lumotlarni qo‘riqlash ma’nosida);

– kompyuter xavfsizligi yoki ma’lumotlar xavfsizligi – kompyuter tarmoqlarida ma’lumotlarning saqlanishini, foydalanishga ruxsat etilganligini va konfedensialligini ta’minlovchi apparat va dasturiy vositalar to‘plami, axborotdan mualliflashtirilmagan foydalanishdan himoya qilish choralari;

– axborot egalariga yoki axborotdan foydalanuvchilarga hamda uni qo‘llab quvvatlovchi infratuzilmaga zarar yetkazishi mumkin bo‘lgan tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan ta’sir etishlardan axborot va uni qo‘llab quvvatlovchi infratuzilmaning himoyalanganli;

– fuqarolar, alohida guruhlar va ijtimoiy qatlamlar, umuman olganda aholining yashash faoliyati, ta’lim olish va rivojlanishlari uchun zarur bo‘lgan sifatli axborotga bo‘lgan talablarining himoyalanganligi.

*Xavfsizlik siyosati* – xavfsizlik obyektlari va subyektlarining berilgan ko‘pligining xavfsizligini ta’minlash protseduralari va mexanizmlarini belgilovchi qoidalar to‘plami[1]. Tizim xavfsizligini ta’minlashning aniq mexanizmlarini tanlash qabul qilingan xavfsizlik siyosatiga muvofiq amalga oshiriladi.

O‘zbekiston Respublikasi Prezidentining 2015-yilning 4-fevral kuni e’lon qilingan “O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligini tashkil etish to‘g‘risida”gi Farmoniga[2] ko‘ra “Axborot xavfsizligini ta’minlash va kommunikatsiya tarmoqlari, dasturiy mahsulotlar, axborot tizimlari va resurslarini himoya

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

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

qilishning zamonaviy texnologiyalarini tatbiq etish chora-tadbirlarini amalga oshirish, axborot resurslarini himoya qilish bo‘yicha texnik infratuzilmani yanada rivojlantirish” ustuvor vazifalardan biri sifatida qayd etilgan.

**Axborot xavfsizligi** deganda tabiiy yoki sun’iy xarakterdagi tasodifiy yoki qasddan qilingan ta’sirlardan axborot va uni qo‘llab-quvvatlab turuvchi infratuzilmaning himoyalanganligi tushuniladi. Bunday ta’sirlar axborot munosabatlariga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni ta’minlovchi infratuzilmaga jiddiy zarar yetkazishi mumkin.

O‘zbekiston Respublikasining 2002-yil 12-dekabrdagi «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonunida[1] axborot xavfsizligi *axborot borasidagi xavfsizlik* deb belgilangan va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi.

Konfidensiallik, butunlik va ruxsat etilganlik axborot xavfsizligini ta’minlash borasida uchta muhim xususiyat hisoblanadi.

– **axborotning konfidensialligi** – axborotning holati bo‘lib, bunda axborotga ruxsat, faqat tegishli huquqqa ega bo‘lgan subyektlargagina beriladi.

– **axborotning butunligi** – axborotda hech qanday o‘zgartirishlar bo‘lmagan yoki o‘zgartirishlar faqat alohida huquqqa ega bo‘lgan subyektlar tomonidan amalga oshiriladigan axborotning holati.

– **axborotning ruxsat etilganligi** – axborotga ruxsat etilgan subyektlarning, uni amalga oshirishga to‘siqlar mavjud bo‘lmagan holati.

Ruxsat etilganlik huquqiga axborotni yoki uning resurslarini o‘qish uchun, o‘zgartirish, nusxa olish, axborotni yo‘q qilish huquqlari kiradi.

**Axborotni muhofaza qilish –** bu axborot himoya tizimini yaratish bilan bog‘liq jarayon. Axborot himoya tizimi hech qachon yuz foizlik himoyani ta’minlay olmasligini anglash muhimdir. Bu esa axborotni mumkin bo‘lgan darajadagi o‘zgartirish, o‘g‘irlash yoki yo‘q qilish tavakkalchiligiga asoslangan axborot xavfsizligi haqida fikr yuritishni taqozo etadi.

Amalga oshirilish usullariga ko‘ra barcha axborot himoyasi choralarini quyidagi turlarga ajratish mumkin:

– huquqiy;

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

– ma’naviy-etik;
– texnologik;
– tashkiliy;
– fizik;
– texnik (qurilmaviy va dasturiy).

Yuqorida qayd etilganlar himoya turlari orasida asosiylari huquqiy, tashkiliy va texnik himoya hisoblanadi.

**Huquqiy himoya** – axborotni himoyalash bo‘yicha subyektlarning munosabatlarini tartibga soluvchi, amalda joriy etuvchi hamda ularning bajarilishini nazorat qiluvchi qonunchilik va normativ-xuquqiy hujjatlar asosida axborotni huquqiy usullar bilan himoyalashdir. Axborotni huquqiy himoyalash choralariga O‘zbekiston Respublikasining mazkur sohadagi qonunlari, Prezident farmonlari va qarorlari, Vazirlar Mahkamasining qaror va farmoyishlari va boshqa normativ-huquqiy hujjatlar kiradi. Axborotga murojaat qilish qoidalari, axborot munosabati qatnashchilari, ularning huquqlari va majburiyatlari, shuningdek, qonunchilik talablari buzilgan hollarda javobgarlik qonunchilik darajasida ko‘rib chiqiladi va tartibga solinadi.

**Himoyaning tashkiliy choralari** – tashkiliy xarakterga ega bo‘lgan, axborot tizimi faoliyatini, xodimlar ishini, foydalanuvchilarning tizim bilan o‘zaro aloqalarini tashkillashtirishga mo‘ljallangan choralardir. Ushbu choralar ichidan quyidagi asosiylarini ko‘rsatish mumkin:

– xavfsizlik siyosatini shakllantirish;
– binoga kirishni tartiblash;
– xodimlarning axborot tizimidan foydalanish uchun ruxsat etishni tartiblash;
– axborot xavfsizligi talablariga rioya etmagan hollarda javobgarlikni aniqlash va ta’minlash.

Tashkiliy choralar o‘z holicha axborot xavfsizligi vazifalarini hal eta olmaydi. Ular himoyaning fizik va texnik choralari bilan birgalikda ishlashi zarur.

**Fizik himoya** nazorat qilinuvchi hududga g‘arazgo‘y kimsalarning jismoniy kirishiga qarshilik qiluvchi vositalar to‘plamini anglatadi. Ular turli ko‘rinishdagi mexanik, elektr yoki elektro-mexanik qurilmalar bo‘lishi mumkin. Korxona yoki tashkilotning axborot xavfsizligini ta’minlash odatda, aynan fizik himoyani tashkil etishdan boshlanadi.

Axborot himoyasi choralari orasida **texnik himoya** muhim ahamiyatga ega. U axborot tizimlarida ma'lumotlarni texnik, dasturiy va dasturiy-texnik vositalar yordamida himoya qilishni nazarda tutadi.

O'zbekiston Respublikasining 2002-yil 12-dekabrdagi «Axborot erkinligi prinsiplari va kafolatlari to'g'risida»gi qonunida[1] axborotni muhofaza qilish bo'yicha quyidagi ta'rif keltirilgan:

*Axborotni muhofaza etish* - axborot borasidagi xavfsizlikka tahdidlarning oldini olish va ularning oqibatlarini bartaraf etish chora-tadbirlari.

Saqlash, o'zgartirish, uzatish va ma'lum maqsadlar uchun foydalanish obyekti bo'lgan tevarak olam haqidagi ma'lumotlarni, keng ma'noda axborot deb tushunish mumkin. Bu tushunchaga ko'ra inson, uning hayot tarziga va harakatlariga ta'sir etuvchi doimiy o'zgaruvchi axborot maydoni ta'sirida bo'ladi. Axborot o'z tavsifiga ko'ra siyosiy, harbiy, iqtisodiy, ilmiy-texnik, ishlab chiqarishga yoki tijoratga oid hamda maxfiy, konfidensial yoki maxfiy bo'lmagan bo'lishi mumkin.

*Maxfiy axborot* – foydalanilishi qonun hujjatlariga muvofiq cheklab qo'yiladigan hujjatlashtirilgan axborot[2].

*Hujjatlashtirilgan axborot* esa identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan holda moddiy jismda qayd etilgan axborotdir.

*Konfidensial axborot* deganda mamlakat qonunchiligi bilan foydalanish cheklanadigan hujjatlardagi axborot tushunilib, unga xizmat, kasbiy, tijorat va boshqa turdagi axborotlar kiradi[3].

O'zbekiston Respublikasining 1993-yil 7-maydagi 848-XII-sonli «Davlat sirlarini saqlash to'g'risida»gi qonunning[4] 1-moddasida davlat sirlari tushunchasi berilgan:

«Davlat tomonidan qo'riqlanadigan va maxsus ro'yxatlar bilan chegaralab qo'yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiy-texnikaviy va o'zga xil ma'lumotlar O'zbekiston Respublikasining davlat sirlari hisoblanadi».

---

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

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

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

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

Mazkur qonunning 3-moddasida davlat sirlarining kategoriyalari keltirilgan:

«O‘zbekiston Respublikasining davlat sirlari – davlat, harbiy va xizmat sirlarini qamrab oladi.

Oshkor etilishi respublika harbiy-iqtisodiy imkoniyatlarining sifat holatiga salbiy ta’sir etishi yoki O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi, iqtisodiy va siyosiy manfaatlari uchun boshqa og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan ma’lumotlar davlat sirini tashkil etadi.

Oshkor etilishi O‘zbekiston Respublikasining mudofaa qobiliyati, davlat xavfsizligi va Qurolli Kuchlari uchun og‘ir oqibatlar keltirib chiqarishi mumkin bo‘lgan harbiy xususiyatga ega ma’lumotlar harbiy sirni tashkil etadi.

Oshkor etilishi O‘zbekiston Respublikasi manfaatlariga zarar yetkazishi mumkin bo‘lgan fan, texnika, ishlab chiqarish va boshqaruv sohasiga doir ma’lumotlar xizmat sirini tashkil etadi».

Axborotlashtirish jarayonining jadallashuvi munosabati bilan jamiyatning barcha sohalarida axborot muhofaza qilish muammosi tobora dolzarb bo‘lib bormoqda. Konfidensial axborotlar va davlat sirlariga taalluqli bo‘lgan maxfiy axborotlar muhofazaga muhtojdir.

Umuman olganda *axborot muhofaza qilish* yoki *axborot himoyasi* axborot xavfsizligi sohasi mutaxassislari va g‘arazgo‘y kimsalar orasidagi qarama-qarshilikni ifodalaydi. *G‘arazgo‘y kimsa* – noqonuniy yo‘llar bilan axborotning qonuniy foydalanuvchilaridan axborotni oluvchi, o‘zgartiruvchi yoki yo‘q qiluvchi subyektdir.

Axborot himoyasi zaif tuzilmali vazifa bo‘lib, uni quyidagicha tavsiflash mumkin:

– samarali himoyani tuzishga ta’sir ko‘rsatuvchi omillarning ko‘pligi;

– aniq dastlabki kirish ma’lumotlarining yo‘qligi;

– dastlabki ma’lumotlar to‘plami bo‘yicha aniq optimal natijalarni olish imkonini beradigan matematik usullarning yo‘qligi.

Zaif tuzilmali vazifalarni yechishda tizimli yondashuv asos bo‘lib xizmat qiladi. Shu sababli axborot himoyasi masalasini hal etishda xizmat vazifasi axborot xavfsizligini ta’minlashga qaratilgan elementlar to‘plamidan iborat bo‘lgan axborot himoya tizimini hosil qilish lozim bo‘ladi. Har qanday tizimga kirish – bu tizim holatini o‘zgartiruvchi ta’sirlardir. Axborot himoya tizimi uchun kirish ham ichki, ham tashqi tahdidlar hisoblanadi.

## 1.2. Himoyalangan axborotga tahdidlar va himoya obyektlarini toifalash

**Axborot xavfsizligiga tahdid** – axborot xavfsizligi buzilishiga olib kelishi mumkin bo‘lgan real yoki potensial xatarlarni ifodalovchi sharoit yoki omillar yig‘indisidir. Ana shunday xatarlarni amalga oshirish – hujum deyilib, ushbu vazifani bajaruvchi – g‘arazgo‘y kimsa deb ataladi.

**Axborot xavfsizligiga tahdid manbai** – bu axborot xavfsizligiga bevosita tahdidni yuzaga keltirishga sabab bo‘luvchi subyekt (jismoniy shaxs, moddiy obyekt yoki fizik hodisa). Tashkilot ichidagi texnik vositalar, tashkilot xodimlari, g‘arazgo‘y kimsalar, axborot tizimidagi yondosh fizik hodisalar *tahdid manbai* bo‘lishi mumkin. Axborot himoya tizimining kattaliklariga quyidagilarni kiritish mumkin:

– maqsad va vazifalar;

– tizimning kirish va chiqishlari;

– tizimning kirish va chiqishini o‘zgartiruvchi, tizimdagi ichki jarayonlar.

**Maqsad** – bu tizim himoyasini hosil qilishda kutilgan natija, vazifa esa – ana shu maqsadga erishish uchun qilinishi kerak bo‘lgan ishlar. Axborot himoyasining maqsadi axborot xavfsizligini ta’minlash hisoblanadi. Axborot xavfsizligi deganda nafaqat axborotning, balki uni qo‘llovchi infratuzilmaning xavfsizligini ham tushunish lozim. Agar axborotning o‘zini alohida olib qaralsa, u holda axborot xavfsizligi tushunchasi – axborotning himoyalanganlik holatini bildirib, bunda uning konfidensialligi, butunligi va ruxsat etilganligi ta’minlanadi.

*Tahdidlar va himoya obyektlarini toifalash.* Axborot ayrim simvollar (belgilar) to‘plami sifatida har xil turdagi axborot tashuvchilarda turli shakllarda mavjud bo‘lishi mumkin. Axborotlashtirish jarayonlarining jadal suratlar bilan rivojlanishi natijasida zamonaviy hisoblash vositalari asosidagi avtomatlashtirilgan tizimlarda to‘planuvchi, saqlanuvchi va qayta ishlanuvchi axborot hajmi tobora ortib bormoqda.

Avtomatlashtirilgan tizim – xodimlardan va qo‘yilgan vazifani bajarishda axborot texnologiyasini qo‘llovchi avtomatlashtirish vositalari majmuasidan iborat bo‘lgan tizimdir. Demak, avtomatlashtirilgan tizim quyidagi qismlar to‘plamidan iborat:

– ma’lumotlarni qayta ishlash va uzatish texnik vositalari;

– dasturiy ta’minot;

– turli axborot tashuvchilardagi ma’lumotlar;

– xizmat ko‘rsatuvchi xodimlar va tizim foydalanuvchilari.

Avtomatlashtirilgan tizimda axborot xavfsizligini ta’minlash muammosining asosiy yo‘nalishlaridan biri – bu axborot tizimiga mumkin bo‘lgan tahdidlarni aniqlash, tahlil qilish va toifalashdan iborat. Ahamiyati katta bo‘lgan tahdidlar ro‘yxatini tuzish, ularning ehtimolligini baholash va g‘araz niyatli kimsalar tomonidan sodir etilish modelini yaratish himoyaning optimal tizimini hosil qilishda asosiy axborot hisoblanadi.

**Axborot xavfsizligiga tahdid** – axborot xavfsizligining buzilishiga imkon beruvchi yoki real xatarlarni vujudga keltiruvchi sharoit va omillar to‘plamidir.

**Avtomatlashtirilgan tizimning axborot xavfsizligiga tahdid** – bu avtomatlashtirilgan tizimda qayta ishlanuvchi axborotga, uning konfidensialligi, butunligi va ruxsat etilganligini buzishga olib keluvchi ta’sirni amalga oshirish imkoniyati. Shuningdek, avtomatlashtirilgan tizimni zaiflashtirish, yo‘q qilish yoki izdan chiqarishga olib keluvchi, uning tarkibiy qismlariga ta’sir etish imkonidir.

**Axborot xavfsizligiga tahdid manbai –** axborot xavfsizligiga tahdidni yuzaga kelishiga bevosita sabab bo‘luvchi subyektdir.

Avtomatlashtirilgan tizimlarda xavfsizlikni buzishning asosiy manbalari quyidagilar hisoblanadi:

– avariya yoki tabiiy ofatlar (yong‘in, yer silkinishi, suv toshqini va boshqalar);

– texnik vositalarning inkor etishi va buzilishi;

– avtomatlashtirilgan tizim qismlarini loyihalash va ishlab chiqishdagi xatolar (dasturiy vositalar, ma’lumotlarni qayta ishlash texnologiyalari, qurilma vositalari va boshqalar);

– foydalanishdagi xatolar;

– tartibbuzarlarning maqsadli harakatlari.

Tahdidlarni toifalashning ko‘plab mezonlari mavjud. Ulardan keng tarqalganlari quyidagilar:

1. **paydo bo‘lish tabiatiga ko‘ra:** tabiiy va sun’iy.

Tabiiy tahdidlar – bu insonlarga bog‘liq bo‘lmagan holda obyektiv fizik jarayonlar yoki tabiiy ofatlarning avtomatlashtirilgan tizimlar va ularning qismlariga ta’siri tufayli yuzaga keluvchi tahdidlar. O‘z navbatida sun’iy tahdidlar – inson faoliyati bilan bog‘liq holda kelib chiquvchi avtomatlashtirilgan tizimlarga tahdidlardir.

2. **motivatsiya darajasiga ko‘ra:** oldindan biror maqsadni ko‘zlamagan holda (tasodifiy) va oldindan maqsadli (qasddan).

Tasodifiy tahdidlar turli xatolar bilan bog‘liq bo‘lib, bular avtomatlashtirilgan tizim qismlarini loyihalashdagi, dasturiy ta’minotdagi, xizmat ko‘rsatuvchi xodimlarning avtomatlashtirilgan tizim bilan ishlashdagi va shu kabi xatoliklar bo‘lishi mumkin. Oldindan maqsadli tahdidlar g‘araz niyatli shaxslarning g‘arazli, g‘oyali va boshqa maqsadlari bilan bog‘liq holda yuzaga keladi. Bunga sabab moddiy foyda ko‘rish, qasos, ma’naviy e’tiqod yoki boshqalar bo‘lishi mumkin.

Asosiy **tasodifiy tahdidlarga** quyidagilarni kiritish mumkin:

– tizimning me’yorda faoliyat ko‘rsatishini buzilishiga yoki to‘liq to‘xtab qolishiga olib keluvchi ataylab qilinmagan harakatlar. Bu toifaga shuningdek, tizimning qurilmalari, dasturlari hamda resurslari buzilishi ham kiradi;

– qurilmani tasodifan o‘chirib qo‘yish;

– axborot tashuvchilarni tasodifan buzib qo‘yish;

– noto‘g‘ri ishlatilganda tizimning ish faoliyatini izdan chiqarishga qodir bo‘lgan (tizimning osilib qolishi) yoki tizimni qaytarib bo‘lmas o‘zgarishlarga (fayllarni o‘chirib tashlash, formatlash va shu kabilar) olib keluvchi dasturiy ta’minotdan foydalanish;

– mansab vazifalarini bajarish uchun kerak bo‘lmagan dasturlardan foydalanish. Bularga o‘yin, ta’limiy va boshqa dasturlarni kiritish mumkin. Ularni ishlatish tizim resurslarining, xususan, protsessor va tezkor xotiraning maqsadsiz sarflanishiga olib keladi.

– kompyuterning viruslar bilan tasodifiy zararlanishi;

– ehtiyotsiz harakatlar tufayli konfidensial ma’lumotlarning oshkor bo‘lishi;

– xato ma’lumotlarni kiritish;

– parol, shifrlash kaliti, ruxsatnoma, identifikatsiyalovchi kartochka kabi identifikatorlarni yo‘qotish, boshqalarga berish yoki oshkor qilish;

– zaif joylarga ega bo‘lgan tizim yaratish, ma’lumotlarni qayta ishlash texnologiyasidan foydalanish, dasturlarni tuzish;

– xavfsizlik siyosatiga yoki tizim bilan ishlashga o‘rnatilgan qoidalarga rioya qilmaslik;

– xizmat ko‘rsatuvchi xodimlar tomonidan himoya vositalarini o‘chirib qo‘yish yoki ulardan noto‘g‘ri foydalanish;

– abonentlar bilan xato elektron manzillar orqali aloqa o‘rnatish.

Asosiy **qasddan tahdidlarga** quyidagilarni kiritish mumkin:

– tizim yoki uning alohida tashkil etuvchilari (qurilmalar, axborot tashuvchilar, xizmat ko‘rsatuvchi xodimlar)ning me’yordagi faoliyati buzilishiga, ishdan chiqishiga, xato ishlashiga olib keluvchi fizik ta’sir ko‘rsatish;

– hisoblash tizimining faoliyatini ta’minlovchi tizimostilarni o‘chirib qo‘yish yoki ishdan chiqarish (elektr manba, sovutgich va ventilatsiya, aloqa kanali va boshq.)

– tizimning me’yoriy ishlashini buzishga qaratilgan harakatlar (qurilma yoki dasturlarning ish rejimini o‘zgartirish, tizim qurilmalari ishlovchi chastotalarda faol radioshovqinlar hosil qilish va boshq.)

– xizmat ko‘rsatuvchi xodimlarni yoki alohida vakolatga ega bo‘lgan foydalanuvchilarni shantaj qilish, sotib olish yoki boshqa ta’sir yo‘llarini qo‘llash;

– masofaviy foto-, video-tasvirga olish, eshituvchi qurilmalarni qo‘llash va shu kabilar;

– aloqa kanallari orqali uzatiluvchi ma’lumotlarni tutib olish va ularni tizimga kirish qoidalarini, foydalanuvchilarni mualliflashtirish va ularni imitatsiya qilish orqali tizimga kirish yo‘llarini aniqlash maqsadida tahlil qilish;

– axborot tashuvchilar (magnit disklar, tasmalar, xotira mikrosxemalari, saqlovchi qurilmalar va butun kompyuterlar)ni o‘g‘rilash;

– axborot tashuvchilardan noqonuniy nusxa ko‘chirish;

– ishlab chiqarish chiqindilari (chop etilgan qog‘ozlar, yozuvlar, ro‘yxatdan chiqarilgan axborot tashuvchilar va boshq.)ni o‘g‘irlash;

– tashqi xotira qurilmalari yordamida tezkor xotiradagi qoldiq axborotlarni o‘qish;

– ruxsatni chegaralovchi parollarni va boshqa rekvizitlarni noqonuniy (ayg‘oqchi orqali, foydalanuvchilarning e’tiborsizligi tufayli, tanlash orqali va boshqalar) qo‘lga kiritish va ularni keyinchalik ro‘yxatdan o‘tgan foydalanuvchi sifatida qo‘llash;

– foydalanuvchilarning o‘ziga xos fizik tavsifga ega bo‘lgan terminallari (masalan, tarmoqdagi ishchi stansiya raqami, fizik manzil, aloqa tizimidagi manzil va boshqalar)dan noqonuniy foydalanish;

– axborotning kriptohimoyasi shifrini ochish;

– tizimga noqonuniy va yashirin kirish imkonini yaratuvchi “maxsus ilovalar”, “o‘rnashmalar”, “viruslar”ni kiritish va tizimda ro‘yxatdan o‘tib,

undagi ma’lumotlarni uzatish yoki ishdan chiqarish maqsadida tizim resurslariga noqonuniy ruxsatni amalga oshirish;

– aloqa kanallariga noqonuniy ulanib olish va qonuniy foydalanuvchi ishidagi to‘xtash (pauza)lar vaqtida uning nomidan yolg‘on xabarlar kiritish uzatilayotgan ma’lumotlarni modifikatsiya qilish;

– aloqa kanallariga, qonuniy foydalanuvchini tizimga kirib olganidan so‘ng uni almashtirish hisobiga noqonuniy ulanib olish va keyinchalik noto‘g‘ri ma’lumotlarni kiritish hamda yolg‘on xabarlar berish.

Ta’kidlash joizki, maqsadga erishish uchun g‘araz niyatli kimsalar yuqorida keltirilgan usullarning biridan emas, balki ularning bir nechtasidan birgalikda foydalanadilar.

Tahdidlarni toifalashning boshqa mezonlari:

3. **Nisbatan nazorat qilinuvchi soha holatiga ko‘ra**: tashqi va ichki tahdidlar. Tashqi tahdidlarga misol sifatida tizimda uzatiluvchi yoki yondosh elektromagnit nurlanishlar va navodkalar orqali ma’lumotlarni tutib olishni keltirish mumkin. Ichki tahdidlarga konfidensial axborotga ega bo‘lgan axborot tashuvchini, qurilma qismini o‘g‘rilash kabilar kiradi.

4. **Avtomatlashtirilgan tizimga ta’sir ko‘rsatish darajasiga ko‘ra**: passiv va faol tahdidlar. Passiv tahdidlar – avtomatlashtirilgan tizim tarkibi va faoliyatini buzmaydigan tahdidlardir. Ularga misol sifatida konfidensial axborotdan nusxa ko‘chirish, axborotni chiqib ketish texnik kanali orqali chiqarib yuborish, eshitish va shu kabilarni keltirish mumkin. Faol tahdid esa mos ravishda avtomatlashtirilgan tizim faoliyatini, uning tuzilishi va tarkibini buzilishiga olib keladi.

5. **Axborotning buziluvchi xususiyati turiga ko‘ra**: konfidensiallikka, ruxsat etilganlikka va butunlikka tahdidlar. Ruxsat etilganlikka tahdidlarga misol tariqasida sun’iy tahdidlar bilan bir qatorda tabiiy tahdidlar, ya’ni chaqmoq yoki qisqa tutashuv oqibatida qurilmalarning buzilishini keltirish mumkin. Hozirgi vaqtda axborotning ruxsat etilganligiga tahdid sifatida tarmoq hujumlari – DDoS (Distributed Denial of Service – xizmat ko‘rsatishda taqsimlangan rad etish) – hujumlar keng qo‘llanilmoqda.

Shuningdek, ta’kidlash joizki butunlikning buzilishiga nafaqat ma’lumotlar, balki dasturlar muhiti ham taalluqlidir. Tizimning virus bilan zararlanishi butunlikka tahdidning amalga oshirilishiga misol bo‘la oladi.

Konfidensiallikka tahdidlarga axborotga noqonuniy ruxsat bilan bog‘liq bo‘lgan ixtiyoriy tahdidni kiritish mumkin. Masalan, maxsus

dastur yordamida tarmoq orqali uzatilayotgan axborotni tutib olish yoki tanlangan paroldan foydalanib, noqonuniy ruxsatga ega bo‘lish.

6. **Tahdid yo‘naltirilgan tizimning turiga ko‘ra**: avtonom ish joyi asosidagi tizimlar va umumiy foydalanish tarmog‘iga ulangan tizimlar.

7. **Amalga oshirish usuliga ko‘ra**: himoyalanuvchi axborotga noqonuniy ruxsat (shu jumladan tasodifiy), axborotga maqsadli ta’sir ko‘rsatish, axborotni chiqib ketish texnik kanallari orqali chiqarib yuborish.

Eng keng tarqalgan va ommalashgan axborotga tahdid toifalariga: *amalga oshirish usuliga ko‘ra* hamda *axborotning buziluvchi xususiyati turiga ko‘ralar* kiradi.

## 1.3. Axborot xavfsizligi bo‘yicha normativ huquqiy hujjatlar

Ma’lumki, huquq – bu hukumat tomonidan turmushning ma’lum bir sohalariga, davlat organlari, tashkilotlari yoki aholiga nisbatan o‘rnatilgan yoki sanksiyalangan umummajburiy qoidalar va me’yorlar to‘plamidir.

O‘zbekiston Respublikasining 2012-yil 24-dekabrdagi «*Normativ-huquqiy hujjatlar to‘g‘risida (yangi tahrirda)*»gi qonunining[1] 3-moddasiga asosan «Normativ huquqiy hujjat ushbu qonunga muvofiq qabul qilingan, umummajburiy davlat ko‘rsatmalari sifatida huquqiy normalarni belgilashga, o‘zgartirishga yoki bekor qilishga qaratilgan rasmiy hujjatdir».

*Normativ huquqiy hujjat* – bu huquq ijodkorligi hujjati bo‘lib, ma’lum bir tartibda, qat’iy belgilangan subyektlar tomonidan qabul qilinadi va huquq me’yoriga ega bo‘ladi.

Normativ huquqiy hujjat huquqning asosiy manbai hisoblanadi. Normativ huquqiy hujjat (boshqa huquq manbalariga nisbatan) kafolat doirasida faqat mas’ul davlat organlari tomonidan qabul qilinadi hamda ma’lum bir ko‘rinishga, hujjat shakliga ega bo‘ladi. Normativ huquqiy hujjatlar mamlakat bo‘yicha amal qiladi va yagona tizimni hosil qiladi.

*Normativ huquqiy hujjatlar belgilari:*

– me’yoriy xarakter;
– huquqiy akt;
– huquq ijodkorligi natijasi hisoblanadi;
– umummajburiylik;
– rasmiy hujjat ko‘rinishida tuziladi;

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

– huquq me’yorlarini guruhlashda ma’lum bir tartibga rioya qilinadi.

«*Normativ-huquqiy hujjatlar to‘g‘risida*»gi qonunning 5-moddasi normativ huquqiy hujjatlarning turlarini aniqlaydi. Quyidagilar normativ huquqiy hujjat hisoblanadi:

- O‘zbekiston Respublikasi Konstitutsiyasi;
- O‘zbekiston Respublikasi qonunlari;
- O‘zbekiston Respublikasi Oliy Majlisi palatalari qarorlari;
- O‘zbekiston Respublikasi Prezidenti farmonlari, qarorlari va farmoyishlari;
- O‘zbekiston Respublikasi Vazirlar Mahkamasi qarorlari;
- vazirliklar, davlat qo‘mitalari va idoralarning buyruqlari hamda qarorlari;
- mahalliy davlat hokimiyati organlarining qarorlari.

Normativ-huquqiy hujjatlar qonun hujjatlari hisoblanadi va O‘zbekiston Respublikasi qonun hujjatlari majmuini tashkil etadi.

O‘zbekiston Respublikasining Konstitutsiyasi va qonunlari, O‘zbekiston Respublikasi Oliy Majlisi palatalarining qarorlari qonunlardir.

O‘zbekiston Respublikasi Prezidenti farmonlari, qarorlari va farmoyishlari, O‘zbekiston Respublikasi Vazirlar Mahkamasi qarorlari, vazirliklar, davlat qo‘mitalari va idoralarning buyruqlari hamda qarorlari, mahalliy davlat hokimiyati organlarining qarorlari qonun osti hujjatlari hisoblanadi (ushbu qonunning 6-moddasi).

*Axborot xavfsizligini ta’minlashda normativ huquqiy boshqaruvning zarurligi*. Huquqiy baza axborotga egalik huquqiga va uni muhofaza qilishga oid vazifalarni yechish imkonini berishi zarur. Himoyalanayotgan axborotga tahdidni aniqlashi va uni himoyalash tartibini belgilashi kerak. Huquqiy davlatda barcha tashkilot va muassasalar, rahbar shaxslar va fuqarolar faoliyati amaldagi qonunlar doirasida tashkil etilishi lozim.

Axborotni muhofaza qilish sohasiga oid normativ huquqiy hujjatlarda:

– axborotni muhofaza qilish, uning maxfiyligi va himoya uchun o‘rnatilgan qoidalar sohasida turli subyektlarning huquqlari ifodalanishi;

– himoyalanayotgan axborotga noqonuniy tahdid qilish yoki uning egasiga zarar yetkazuvchi oqibatlarni keltirib chiqarishi mumkin bo‘lgan harakatlar uchun jinoiy, ma’muriy, moddiy va ma’naviy javobgarlik belgilanishi kerak.

Axborotni huquqiy himoyalash zaxira sifatida davlat va xalqaro miqyosda tan olingan hamda xalqaro shartnoma, konvensiya va deklara-

tsiyalarda aniqlanadi. Davlat miqyosida axborotni huquqiy himoyalash davlat va tashkilot hujjatlari orqali nazorat qilinadi.

Axborot xavfsizligini ta’minlash muammosi kompleks xarakterga ega. Uni hal qilish uchun huquqiy hamda tashkiliy choralar va dasturiy-texnik ta’minotni (identifikatsiya va autentifikatsiya; ruxsatni boshqarish; protokollashtirish va audit; kriptografiya) birgalikda ko‘rish talab etiladi (misol uchun, korxona boshqaruvi miqyosida uning kompyuter axborot tarmog‘ida axborot xavfsizligini ta’minlash uchun xavfsizlik siyosatini ishlab chiqish hamda kerakli resurslar talab etiladi).

O‘zbekiston Respublikasining 2015-yil 9-dekabrda e’lon qilingan «Elektron hukumat to‘g‘risida»gi qonunining[1] 12-moddasi “Axborot xavfsizligini ta’minlash prinsipi” deb nomlanadi. Ushbu moddaga binoan elektron davlat xizmatlari ko‘rsatuvchi davlat organlari elektron davlat xizmatlari ko‘rsatishda foydalaniladigan axborot tizimlari va axborot resurslarining axborot xavfsizligini ta’minlashi shart.

Elektron davlat xizmatlari ko‘rsatuvchi davlat organlari shaxsga doir ma’lumotlar, shuningdek davlat sirlarini yoki qonun bilan qo‘riqlanadigan boshqa sirni tashkil etuvchi ma’lumotlar muhofaza qilinishini va ulardan ruxsatsiz foydalanishning oldi olinishini ta’minlash yuzasidan zarur tashkiliy-texnik choralar ko‘radi.

Elektron davlat xizmatlari ko‘rsatuvchi davlat organlarining axborot tizimlarida va axborot resurslarida saqlanadigan shaxsga doir ma’lumotlardan ular qaysi ariza beruvchiga taalluqli bo‘lsa, o‘sha ariza beruvchining roziligi bilan ularga ishlov berish, ularni uzatish va olish uchun foydalaniladi, bundan qonun hujjatlarida belgilangan hollar mustasno.

***Axborotni muhofaza qilish sohasida xalqaro standartlar.*** 1983-yil AQSH Mudofaa Vazirligi (MV) kompyuter xavfsizligi Agentligi **TSEC** (Ishonchli Tizimlarning Himoyalanganligini Baholash Kriteriylari) nomli hisobotini chop etdi. U boshqacha aytganda ***To‘q sariq rangli kitob*** (kitob rangiga ko‘ra) deb nomlandi. Unda ko‘p foydalanuvchili kompyuter tizimlarida maxfiy ma’lumotlarni himoyalash uchun xavfsizlikning 7 ta darajasi ajratilgan. Bular: Al – kafolatli himoya; Bl, B2, V3 – ruxsatni to‘liq boshqarish; Cl, C2 – ruxsatni tanlash orqali boshqarish; D – minimal xavfsizlik.

AQSH Mudofaa Vazirligi kompyuter tizimlarini baholash maqsadida AQSH MV qoshidagi kompyuter xavfsizligi Milliy Markazi **NCSC-TG-**

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

**005** va **NCSC-TG-011** nomli ***Qizil kitob*** (kitob rangiga ko‘ra) deb nomlangan qo‘llanmasini chiqardi.

Bunga javob tariqasida Germaniya axborot xavfsizligi Agentligi **Green Book** (***Yashil kitob***) ni tayyorladi. Unda xususiy hamda davlat miqyosida axborot xavfsizligini ta’minlashda vujudga keluvchi talablar kompleks tarzda o‘z aksini topgan.

1990-yilda *Yashil kitob* Germaniya, Buyuk Britaniya, Fransiya va Gollandiya davlatlari tomonidan ma’qullandi va Yevropa Ittifoqiga yuborildi. Uning asosida Yevropa standartini ifodalovchi **ITSEC** (Axborot Texnologiyalarining Himoyalanganligini Baholash Kriteriyalari) yoki ***Oq kitob*** tayyorlandi. Bu kitobda xavfsiz axborot tizimlarini tashkil etish kriteriyalari keltirilgan.

Oq kitobda xavfsizlik kriteriyalarining quyidagi asosiy qismlari berilgan:

1. Axborot xavfsizligi.
2. Tizim xavfsizligi.
3. Mahsulot xavfsizligi.
4. Xavfsizlikka tahdid.
5. Xavfsizlik funksiyasi to‘plami.
6. Xavfsizlikning kafolatlanganligi.
7. Xavfsizlikning umumiy bahosi.
8. Xavfsizlik sinflari.

Yevropa kriteriyalariga ko‘ra **ITSEC** axborot xavfsizligining olti asosiy elementi va uning qismlarini o‘z ichiga oladi:

1. Axborot konfidensialligi (axborotni noqonuniy olishdan himoyalash).
2. Axborot butunligi (axborotni noqonuniy o‘zgartirishdan himoyalash).
3. Axborotdan foydalana olishlik (axborot va tizim resurslarini noqonuniy yoki tasodifiy tutib olishlardan himoyalash).
4. Xavfsizlik maqsadlari (axborot xavfsizligi funksiyalari nima uchun kerak?).
5. Axborot xavfsizligi vazifalarining tasnifi:

– identifikatsiya va autentifikatsiya (foydalanuvchining haqiqiyligini an’anaviy tekshirishgina emas, yangi foydalanuvchilarni ro‘yxatga olish, eskilarini o‘chirish, shuningdek autentifikasiya, axborotlarini o‘zgartirish va tekshirish uchun funksiyalar, shu jumladan butunlikni nazorat qiluvchi vositalar ham tushuniladi);

– foydalanish huquqini boshqarish (shu jumladan, umumfoydalaniluvchi obyektlarning butunligini ta’minlash maqsadida ularga ruxsatni vaqtincha chegaralovchi xavfsizlik funksiyalari, ruxsat berish huquqini tarqatishni boshqarish kabilar);

- hisobot berishlilik (protokollashtirish);
- audit (mustaqil nazorat);
- obyektlardan qayta foydalanish;
- axborotning aniqligi (ma’lumot turli qismlarining o‘zaro mosligini ta’minlash (aloqa aniqligi) hamda axborotni uzatishda uni o‘zgarmasligini ta’minlash (kommunikatsiya aniqligi));
- xizmat ko‘rsatishning ishonchliligi (qisqa vaqt ichida vaqt bo‘yicha kritik harakatlar bajarilishini ta’minlovchi funksiyalar; kritik bo‘lmagan, ya’ni kerakli vaqtda ma’lumotni olish imkonini berish; xatolarni topish va ularni bartaraf etish funksiyalari; kommunikatsiya xavfsizligini ta’minlovchi rejalovchi funksiyalar);
- ma’lumot almashish.

6. Xavfsizlik mexanizmlarini ifodalash.

Yevropa kriteriyalarida xavfsizlikning 10 ta sinfi o‘rnatilgan (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-D1, F-DC, F-DX). Ularning dastlabki beshtasi Amerikaning TCSEC kriteriyasidagi Cl, C2, Bl, B2, V3 darajalarga mos keladi. F-IN sinfi axborot butunligiga bo‘lgan yuqori talabga asoslangan bo‘lib, MBBT (ma’lumotlar bazasini boshqarish tizimi)ga mos keladi hamda ruxsatning quyidagi turlari farqlanadi: o‘qish, yozish, qo‘shish, o‘chirish, hosil qilish, qayta nomlash va obyektlarni belgilash. F-AV sinfi axborot tizimlari ish qobiliyatini ta’minlash uchun yuqori talabga mo‘ljallangan. F-D1 sinfi axborot kanallari orqali uzatiluvchi ma’lumotlarning butunligiga bo‘lgan yuqori talabga mo‘ljallangan. F-DC sinfi axborot konfedensialligiga bo‘lgan yuqori talabga moslashgan. F-DX sinfi esa bir vaqtda F-D1 va F-DC sinflari talablariga nisbatan kuchaytirilgan talabga asoslangan.

Axborot himoyasining kompleks tashkil etilishiga kriptografik himoya vositalaridan foydalanish algoritmini davlat standartlariga mos ravishda ta’minlash hisobiga erishiladi.

***Nazorat uchun savollar***

- Axborot xavfsizligi tushunchasi nimani anglatadi?
- Axborot xavfsizligining qanday tashkil etuvchilari mavjud?
- Axborot xavfsizligini ta’minlashning uchta muhim xususiyati nimalardan iborat?
- Axborotni muhofaza qilish deganda nima tushuniladi?
- Axborotni muhofaza qilishning qanday usullari va turlari mavjud?
- Axborotni muhofaza qilish vositalariga nimalar kiradi?
- Axborotni muhofaza qilish tizimlari qanday vazifani bajaradi?
- Axborot xavfsizligiga tahdid deganda nima tushuniladi?
- Axborot xavfsizligi bo‘yicha normativ-huquqiy hujjatlar nimani ifodalaydi?
- Axborotni muhofaza qilish sohasida qanday xalqaro standartlar mavjud?

# II. AXBOROTLARNI TEXNIK HIMOYALASH

## 2.1. Texnik himoya obyektlari va himoya vositalari

Axborot tizimlarida ma’lumotlarni texnik himoyalash masalasi bugungi kunda dolzarb vazifalardan biri hisoblanadi.

Zamonaviy axborot tizimlarida saqlanuvchi, qayta ishlanuvchi va uzatiluvchi axborotlarni hamda obyektlarni himoyalash uchun murakkab va takomillashgan usullaridan foydalaniladi. Tahdidlar spektri kengligini inobatga olib, axborot himoyasi masalasiga kompleks yondashish talab etiladi.

Axborot himoyasi tizimining juda keng ko‘lamga ega bo‘lgan chorasi – bu texnik himoya bo‘lib, u muhim ahamiyatga ega.

**Axborotning texnik himoyasi** – amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta’minlashni inobatga oluvchi axborot himoyasidir. Shunga alohida e’tibor qaratish muhim-ki, texnik himoya deganda nafaqat texnik kanallar orqali ma’lumotning chiqib ketishini oldini olish, balki axborotni noqonuniy ruxsatlardan, matematik ta’sirlardan, zararlantiruvchi dasturlardan va boshqalardan himoya qilish ham tushuniladi. Axborotni texnik himoyalash obyektlariga quyidagilarni kiritish mumkin:

– axborotlashtirish obyekti;
– axborot tizimi;
– axborot tizimi resurslari;
– axborot texnologiyalari;
– dasturiy vositalar;
– aloqa tarmoqlari.

*Nazorat hududi* – bu qo‘riqlanuvchi (hudud, bino, ofis va boshq.) soha bo‘lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog‘ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi.

Axborot tizimlarida ta’sir etilishi mumkin bo‘lgan **obyektlarga** quyidagilarni kiritish mumkin:

– apparat ta’minoti;
– dasturiy ta’minot;

– kommunikatsiyalar (aloqa kanallari yoki kommunikatsiya qurilmalari orqali ma’lumotlarni uzatish va qayta ishlash);

– xizmat ko‘rsatuvchi xodimlar.

Axborotning konfidensialligi, butunligi va ruxsat etilganligini buzish maqsadida ta’sir ko‘rsatish obyektlariga nafaqat axborot tizimi elementlari, balki uni qo‘llab turuvchi infratuzilma (elektr, issiqlik ta’minoti, sovitish tizimlari) ham kiradi. Bundan tashqari texnik vositalarning joylashish hududiga ham e’tibor qaratish lozim, ya’ni ularni qo‘riqlanuvchi hududga joylashtirish zarur. Simsiz aloqa vositalarini o‘rnatishda, ularning amal qilish masofasi (harakat zonasi) nazorat qilinuvchi hududdan chiqib ketmasligi tavsiya etiladi.

**Texnik himoya vositalari** – bu texnik qurilmalar, komplekslar yoki tizimlar yordamida obyektni himoyalashdir. Texnik vositalarning afzalligi keng ko‘lamdagi masalalarni hal etilishda, yuqori ishonchlilikda, kompleks rivojlangan himoya tizimini yaratish imkoniyatida, ruxsatsiz foydalanishga urinishlarga mos munosabat bildirishda va himoyalash amallarini bajarish usullaridan foydalanishning an’anaviyligida namoyon bo‘ladi.

*Maskirovkalovchi (niqoblovchi) belgilarning ochilishi (demaskirovka belgilari)* deganda obyektning boshqa obyektlardan biron-bir tavsifi bilan farq qiladigan xususiyati tushuniladi. Farqlovchi tavsiflar son yoki sifatda baholanishi mumkin. *Obyektning demaskirovka belgilari* – bu himoya obyektiga xos xususiyat bo‘lib, undan texnik razvedka obyektni topishi yoki aniqlashi hamda obyekt haqida kerakli ma’lumotlarni olish uchun foydalanilishi mumkin. Axborotga egalik demaskirovka belgilarini tahlil etish orqali amalga oshiriladi. Demak, bu belgilar axborotni o‘ziga xos chiqib ketish kanali hisoblanadi. Demaskirovka belgilarni tarqatuvchilar bo‘lib to‘g‘ridan-to‘g‘ri bu belgilar bilan bog‘liq bo‘lgan fizik maydonlar hisoblanadi.

***Axborot tizimida texnik xarakterdagi tadbirlar.*** Axborot xavfsizligi tizimining injener-texnik elementi texnik razvedka vositalariga hamda ularning kompleksi asosida nazorat sohasini hosil qilishga qarshi faol va passiv qarshilik ko‘rsatish uchun mo‘ljallangan. Axborotni himoya qilishda ushbu element muhim ahamiyatga ega bo‘lib, uning tarkibiga quyidagilar kiradi:

– bino, inshoat, aloqa liniyalari joylashgan hududga begona shaxslarning kirishiga qarshi fizik himoyani tashkillashtirish;

– kompyuter qurilmalari, aloqa vositalari, modemlar, fakslar va aloqa kanali orqali ma’lumot uzatishda ishtirok etuvchi boshqa qurilmalar bilan

ishlash jarayonida vujudga keluvchi axborotning chiqib ketish texnik kanallariga qarshi texnik vositalar;

– binoni vizual usullar bilan texnik razvedka qilishdan himoyalovchi vositalar;

– kuzatish vositalari, xabar berish, signalizatsiya, axborot berish, texnik vositalarning ish faoliyati buzilganda yoki tarmoq aloqasi kattaliklari o‘zgartirilganda ularni identifikatsiya qilish;

– texnik razvedka asboblari va qurilmalari (eshitish, kuzatish, uzatish va boshq.)ni aniqlovchi vositalar;

– xizmat ko‘rsatuvchi xodimlar tomonidan ish joyidan maxsus niqoblangan (maskirovka) buyumlarni, axborot tashuvchilar, tashqi xotiralar va shu kabilarni olib chiqib ketishni oldini oluvchi nazorat texnik vositalari;

– texnik vositalarning zaxirasini yaratish, axborot tashuvchilarning nusxasini hosil qilish.

Axborot himoya tizimining asosiy elementlaridan biri – bu tizimdagi barcha elektron qurilmalarni uzluksiz ishlashi uchun ularni elektr manbai bilan ta’minlash. Ko‘pchilik axborot tashuvchilarga elektr energiyasi uzatishning to‘liq uzilishi kompyuter yoki boshqa elektron qurilmalarning ish holatiga salbiy ta’sir ko‘rsatadi degan noto‘g‘ri fikrga ega. Aksincha, elektr tarmog‘idagi oddiy ko‘z bilan ilg‘ab bo‘lmaydigan kuchlanish o‘zgarishlari yoki xalaqit berishlar tizimdagi qurilmalarga eng katta zarar keltirishi mumkin. Yuqori sezgirli elektron qurilmalar, shu jumladan kompyuter, kommutator va marshrutizatorlar elektr tarmog‘idagi kuchlanish o‘zgarishini darhol sezadi va munosabat bildiradi.

Bundan tashqari, shunga e’tibor berish kerakki, g‘arazgo‘y kimsalar obyekt (korxona, tashkilot)dagi axborot muhitida qayta ishlanayotgan ma’lumotlarni 127/220/380 V kuchlanishli elektr tarmog‘i vositasida yechib olishlari mumkin. Yondosh elektromagnit nurlanishlar darajasini kamaytirish uchun maxsus axborot himoya vositalari qo‘llaniladi. Bular:

– binoni ekranlash;

– himoya obyektlari kuchlanishini qo‘shimcha ravishda yechish (yerga ulanish);

– tarmoq shovqin-pasaytirgich filtrlar yordamida elektr manbai zanjirlarini ajratish;

– nazorat qilinuvchi sohadagi axborot zanjirlari va tashqi aloqa liniyalari orasida elektromagnit maydonini ajratish.

## 2.2. Axborotning chiqib ketish texnik kanallari tasnifi

Ma’lumki, axborot maydon yoki moddiy buyum orqali uzatiladi. Bu akustik to‘lqin yoki elektromagnit nurlanish yoki matn joylashgan qog‘oz varag‘i bo‘lishi mumkin. Boshqacha aytganda u yoki bu fizik maydonlardan foydalangan holda inson axborot uzatish tizimini yoki aloqa tizimini yaratadi. Aloqa tizimi, umuman olganda uzatkich, axborot uzatish kanali, qabul qilgich va axborotni qabul kiluvchidan tashkil topadi. Legitim aloqa tizimlari axborotni qonuniy ravishda almashish uchun hosil qilinadi va qo‘llaniladi. Biroq axborot uzatishning fizik tabiatini inobatga olganda, ma’lum bir shartlarni bajarishda aloqa tizimida axborotni jo‘natuvchi va qabul qiluvchiga bog‘liq bo‘lmagan holda axborotni uzatuvchi aloqa kanali – *axborotning chiqib ketish texnik kanali* vujudga kelishi mumkin.

**Chiqib ketish –** konfedensial ma’lumotning tashkilot yoki ma’lum bir shaxslar doirasidan nazoratsiz chiqib ketishidir.

**Texnik kanal orqali ma’lumotlarning chiqib ketishi –** fizik muhit orqali himoyalangan axborot tashuvchidan axborotni tutib oluvchi texnik vositaga axborotning nazoratsiz chiqib ketishi. Axborotning chiqib ketish texnik kanali (ACHKTK) xuddi axborotni uzatish kanali kabi signal manbai, uni tarqatuvchi fizik muhit va g‘arazgo‘y kimsaning qabul qilgich qurilmasidan tashkil topadi. Axborotning chiqib ketish texnik kanali tuzilishi 1-rasmda keltirilgan.


**1-rasm.** *Axborotning chiqib ketish texnik kanali tuzilishi.*

Axborotning chiqib ketish texnik kanallarini toifalashning asosiy belgisi sifatida axborot tashuvchining fizik tabiati olinadi. Ushbu belgiga ko‘ra ACHKTK quyidagilarga bo‘linadi:

– optik;

– radioelektron;

– akustik;

– moddiy-buyumli.

Elektromagnit maydon (fotonlar) optik kanalda axborot tashuvchi hisoblanadi. Optik to‘lqinlar diapazoni quyidagilarga bo‘linadi:

– olis infraqizil diapazon 100-10 mkm (3-30 TGs);

– o‘rta va yaqin infraqizil diapazon 10-0,76 mkm (30-400 TGs);

– ko‘rinuvchi diapazon (ko‘k-yashil-qizil) 0,76-0,4 mkm (400-750 TGs).

Axborotni chiqib ketish radioelektron kanalida axborot tashuvchi sifatida radiodiapazondagi elektr, magnit va elektromagnit maydonlar, shuningdek, metall o‘tkazgichlarda tarqaluvchi elektr toki (elektronlar oqimi) foydalaniladi. Radioelektron kanalda chastota diapazoni bir necha o‘n GGs dan tovush chastotasigacha bo‘lgan sohani egallaydi. Ushbu diapazon quyidagilarga bo‘linadi:

– past chastotali 10-1 km (30-300 kGs);

– o‘rta chastotali 1 km – 100 m (300 kGs – 3 MGs);

– yuqori chastotali 100-10 m (3-30 MGs);

– ultrayuqori chastotali 10-1 m (30-300 MGs);

– shu tartibda o‘ta yuqori chastotaligacha 10-1 sm (3-30 GGs);

Muhitda tarqaluvchi elastik akustik to‘lqinlar akustik kanalda axborot tashuvchi hisoblanadi. Unda quyidagi diapazonlar ajratiladi:

– infratovushli diapazon 1500-75 m (1-20 Gs);

– quyi tovushli diapazon 150-5 m (1-300 Gs);

– tovushli diapazon 5-0,2 m (300-16000 Gs);

– ultratovushli diapazon 16000 Gs dan 4 MGs gacha.

Moddiy-buyumli kanalda axborotning chiqib ketishi nazorat qilinuvchi sohada himoyalangan axborotga ega moddiy tashuvchilarning noqonuniy tarqalishi oqibatida yuzaga keladi. Aksariyat hollarda bunday moddiy tashuvchilar – hujjatlarning qoralanma varianti yoki nusxa ko‘chirishda foydalanilgan qog‘oz bo‘lishi mumkin.

Axborotning chiqib ketish kanallarini yana axborotlashtirilganligiga ko‘ra toifalash mumkin, ya’ni axborotlashtirilgan, kam axborotlashtirilgan va axborotlashtirilmagan. Kanalning axborotlashtirilganligi undagi uzatilayotgan axborotlarning qimmatliligiga ko‘ra baholanadi.

Paydo bo‘lish vaqtiga ko‘ra kanallar: doimiy, davriy va epizodik (har zamonda) turlariga bo‘linadi. Doimiy kanalda axborotning chiqib ketishi deyarli doimiy xarakterga ega bo‘ladi. Epizodik kanallarda bu holat tasodifiy bir martalik xarakterga ega bo‘ladi.

Axborotning chiqib ketish texnik kanallari quyidagi tahdidlarni yuzaga keltirishi mumkin:

– akustik axborotning chiqib ketish tahdidi;

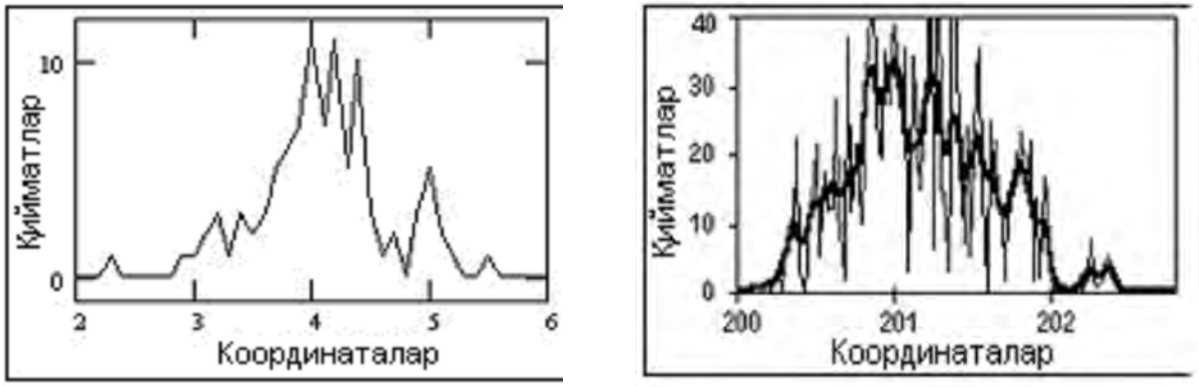
– ko‘rinuvchi axborotning chiqib ketish tahdidi;

– kanallarga yondosh bo‘lgan elektromagnit nurlanish orqali chiqib ketish tahdidi.

Uzatish qurilmasi, tarqalish muhiti va qabul qilish qurilmasidan iborat bo‘lgan axborotning chiqib ketish kanali bir kanalli hisoblanadi. Biroq, ayrim hollarda axborotning chiqib ketishi murakkabroq yo‘l bilan – bir nechta ketma-ket yoki parallel kanallar orqali amalga oshiriladi. Bunda axborotning bir tashuvchidan boshqasiga yozib olish usulidan foydalaniladi. Masalan, biror xonada maxfiy suhbat olib borilayotganda, axborotning chiqib ketishi faqatgina oyna, devor, eshik orqali akustik kanal vositasida emas, balki lazer nuri orqali oyna vositasida ma’lumotni olish – optik kanal orqali yoki xonaga radioo‘rnashma qo‘yish bilan radioto‘lqinlarni tutib olib, so‘ngra uzatish vositasida – radioelektron kanal orqali amalga oshirilishi mumkin. Keyingi ikki holatda akustik va optik yoki akustik va radioelektron kanallardan iborat bo‘lgan tarkibiy kanal hosil bo‘ladi.

**Axborot signali tushunchasi.** Turli fizik tabiatga ega bo‘lgan signallar moddiy axborot tashuvchilari bo‘lishi mumkin. Tor ma’noda signal deganda elektr toki, kuchlanishining tebranishlari – elektromagnit to‘lqinlar, mexanik tebranishlar tushuniladi. Axborot signallari ma’lum bir qonuniyatlar asosida axborot tashuvchining u yoki bu kattaliklarini o‘zgarishi orqali hosil bo‘ladi. Demak, kattaliklari uzatiluvchi axborotga bog‘liq ravishda o‘zgaruvchi ixtiyoriy fizik jarayon – axborot signali bo‘lishi mumkin.

Signalning fizik muhit orqali o‘tishida unga turli muvozanatdan chiqaruvchi omillar (faktorlar) ta’sir ko‘rsatadi. Buning oqibatida turli tabiatga ega bo‘lgan shovqinlar va xalaqit berishlar yuzaga keladi (2-rasm).




*Signal* *Signal halaqit berishlar bilan*

**2-rasm.**

Tuzilishiga ko‘ra signallar **analogli** va **raqamli** turlarga bo‘linadi. Analogli signal uzluksiz argumentning uzluksiz funksiyasi sifatida ifodalanadi. Bunday signallar vaqt davomida uzluksiz bo‘lib, ularning manbai sifatida ixtiyoriy fizik jarayonlar yoki hodisalarni olish mumkin. Raqamli signallar 0 yoki 1 ko‘rinishidagi signallar bo‘lib, ular vaqt davomida signalning bor yoki yo‘qligini anglatadi.

***Xavfli signallar va ularning manbalari.*** G‘arazgo‘y kimsalar tomonidan tutib olinib, keyinchalik ularni ochish mumkin bo‘lgan himoyalangan ma’lumotlarni uzatuvchi signallar xavfli signallar deb ataladi. Bunday signallar ikki ko‘rinishga bo‘linadi: ***funksional*** va ***tasodifiy***. Funksional signallar ma’lumotlarni qayta ishlovchi texnik vositalar tomonidan ularga qo‘yilgan vazifalarni bajarish uchun hosil qilinadi. Bunday signallarning asosiy manbalariga quyidagilar kiradi:

– aloqa tizimi manbalari;
– radiotexnik tizimlar uzatkichlari;
– o‘zidan akustik signal chiqaruvchilar;
– insonlar.

Funksional signallarning tasodifiy signallardan farqli jihati shundaki, axborot egasi ularning xavfsizligi buzilishiga tahdidlar mavjudligini oldindan biladi va ularni oldini olish yoki kamaytirish choralarini ko‘rishi mumkin.

Biroq zamonaviy axborotni qayta ishlash, saqlash va uzatish vositalari o‘zlarining ish jarayonida yondosh radio- yoki elektr signallarini hosil qilishi mumkin. Bunday signallar tasodifiy xavfli signallar deb nomlanadi. Ushbu signallar axborot egasining xohishiga bog‘liq bo‘lmagan holda hosil bo‘ladi va ularni maxsus tadqiqotlar o‘tkazmay turib aniqlab bo‘lmaydi.

Tasodifiy xavfli signallar manbai bo‘lishi mumkin bo‘lgan texnik vositalarga quyidagilar kiradi:

– o‘tkazgichli telefon aloqasi vositalari;
– mobil aloqa va radioaloqa vositalari;
– elektron pochta vositalari;
– hisoblash texnikasi vositalari;
– audioqurilmalar va tovush kuchaytirgich vositalari;
– radio qabul qiluvchi qurilmalar;
– videoqurilmalar;
– televizion vositalar;
– chiziqli radioefir vositalari.

Tasodifiy xavfli signallar quyidagi elektr jihozlari tomonidan paydo bo‘lishi mumkin:

– tizimda vaqtni elektron taqsimlash vositalari;
– qo‘riqlash signalizatsiyasi vositalari;
– yong‘in xavfsizligi signalizatsiyasi vositalari;
– orgtexnika (shu jumladan printerlar);
– sovitish va ventilatsiya tizimi vositalari;
– tarkibida akustik axborotlarni elektromagnit signallarga aylantirib beruvchi elementlarga ega bo‘lgan maishiy va boshqa texnikalar;
– nazorat qilinuvchi hududdan o‘tuvchi elektr o‘tkazuvchi aloqa inshootlari.

Texnik vositalar asosiy texnik vositalar va tizimlar (ATVT) hamda yordamchi texnik vositalar va tizimlar (YOTVT)ga bo‘linadi. Bunda e’tiborli jihati shundaki, YOTVT himoyalangan axborotni qayta ishlamaydi. Ammo ular ATVT bilan birgalikda nazorat zonasida joylashgan bo‘lishi mumkin. Ma’lum bir sharoitlarda YOTVT tasodifiy xavfli signallar manbai bo‘lib qolishi mumkin. Shuning uchun ular ham himoyaga muhtoj hisoblanadi.

***Akustik axborotlarni chiqib ketish texnik kanallari.***

**Tovush** – bu eshitish organi orqali qabul qilinuvchi, elastik muhit zarralarining mexanik tebranishi. Tovush aslida to‘lqin bo‘lganligi uchun uni xarakterlovchi kattaliklar amplituda va chastota spektri hisoblanadi. Inson 16-20000 Gs chastota diapazonidagi tovushlarni eshitadi. Undan past chastotali diapazondagi tovushlar infratovush deb nomlanadi. 20000 Gs dan 1 GGs gacha chastota oralig‘idagi tovushlar – ultratovushlar, 1 GGs dan yuqorilari esa – gipertovushlar deb ataladi.

Tashuvchisi akustik signallar bo‘lgan axborotlar akustik axborotlar deyiladi. Akustik tebranishlarning birlamchi manbai - mexanik tizimlar, masalan, insonning nutq organlari, ikkilamchi manbalari esa turli o‘zgartirgichlar, jumladan elektroakustik qurilmalar hisoblanadi.

**Tovush bosimi** – bu muhitda tovush to‘lqinlari tarqalishi bilan bog‘liq bo‘lgan o‘zgaruvchi bosim. Tovush bosimi kattaligi tovush to‘lqinining yuza birligiga ta’sir ko‘rsatish kuchi bilan baholanadi va barlarda (N/m2) o‘lchanadi.

Tovush bosimi o‘zgaruvchan bo‘lishiga sabab, u bir zarrachadan boshqasiga uzatiladi va bu holat elastik muhitda zarrachaning keskin siljishi bilan amalga oshadi, natijada ana shu joyda bosim ortishi sodir bo‘ladi. Bu jarayon keyingi qo‘shni zarrachalarga uzatiladi va shu tartibda davom etadi. Bu jarayonni elastik muhitda bosim ortishi ko‘chib yurishi bilan ifodalash mumkin. Bunda muhitda to‘lqin ko‘rinishida tarqaluvchi bosim

ortgan va kamaygan sohalar ketma-ketligi kuzatiladi. Muhitdagi har bir zarra tebranuvchi harakatni sodir etadi.

Suyuq va gazsimon muhitlarda akustik tebranishlar bo‘ylama xarakterga ega bo‘lib, unda zarrachalar tebranishi to‘lqin tarqalishi yo‘nalishiga mos tushadi. Qattiq jismlarda bo‘ylama deformatsiyadan tashqari siljish elastik deformatsiyasi ham paydo bo‘lib, uning ta’sirida ko‘ndalang to‘lqinlar ham hosil bo‘ladi. Bu holda zarrachalar to‘lqin tarqalish yo‘nalishiga perpendikular yo‘naluvchi tebranishlarni sodir etadi. Bo‘ylama to‘lqinlarning tarqalish tezligi siljish to‘lqinlarinikiga nisbatan ancha yuqori bo‘ladi.

**Tovush kuchi** – bu birlik vaqt ichida birlik yuzadan o‘tuvchi tovush energiyasi miqdori bo‘lib, u kvadrat metrdagi vattlarda o‘lchanadi (Vt/m2). Ta’kidlash kerakki, tovush bosimi va tovush kuchi o‘zaro kvadrat ko‘rinishda bog‘liq, ya’ni tovush bosimi 4 barobar oshirilsa, tovush kuchi 16 barobar ortadi.

**Tovush balandligi** – tovushni sezish intensivligi bo‘lib, u tovush kuchi va chastotasiga bog‘liq. U tovush kuchining logarifmiga proporsional bo‘lib, detsibellarda ifodalanadi. Tovush balandligining o‘lchov birligi – fon hisoblanadi.

**Dinamik diapazon** – tovush balandligi diapazoni yoki detsibellarda ifodalanuvchi tovush bosimining eng yukori va eng quyi tovushlari farqi.

***Axborotlarni chiqib ketish akustik kanali hosil bo‘lishining manbai*** – bular insonning tovush bo‘g‘ini kabi tebranuvchi jism va mexanizmlar, mashinalarning harakatlanuvchi elementlari, telefon apparatlari, tovush kuchaytirgich qurilmalar va boshqalar bo‘lishi mumkin.

Axborot signalining paydo bo‘lish fizik tabiatiga, shuningdek akustik tebranishlarning tarqalish muhiti va ularni tutib olish usuliga ko‘ra akustik axborotlarning chiqib ketish kanallarini quyidagi turlarga ajratish mumkin: havo, tebranuvchi, elektroakustik, optik-elektron va parametrli.

Axborotlarni havo akustik chiqib ketish kanalida akustik signallarni tarqalish muhiti sifatida havo qaraladi, asosiy tutib olish qurilmasi sifatida esa mikrofondan foydalaniladi. Mikrofon akustik signalni elektr signalga aylantirib beradi va yozib olish qurilmasiga yoki biror bir uzatuvchi qurilmaga ulangan bo‘ladi. Olingan signallarni g‘arazgo‘y kimsaga uzatishni esa turli kanallar: radiokanal, optik kanal, elektr tarmog‘i va boshqalar orqali amalga oshirish mumkin.

***Axborotlarni chiqib ketish optik kanallari***. Optik kanallar demaskirovka belgilariga ko‘ra eng kuchsiz hisoblanadi, ya’ni maxsus texnik

vositalar, masalan, maxsus fototasvir yordamida masofadan turib axborotni tutib olish mumkin.

Ko‘rinish tirqishi kichik bo‘lgan, murakkab tuzilishga ega va yaxshi yoritilmagan sohalarni vizual kuzatish uchun optik-tolali qurilmalar – **endoskoplar** ishlab chiqilgan. Bunday qurilma kuchli yorug‘lik manbai, yoritish svetovodi, tasvir svetovodi, yorug‘lik ravshanligini boshqaruvchi okulyar, svetovodning ishchi qismi egiluvchan sohasining manipulyatoridan tashkil topadi. Yorug‘lik manbai sifatida interferension qoplamali akslantiruvchi bilan jihozlangan galogen lampadan foydalaniladi. Yoritish svetovodi orqali yorug‘lik kuzatilishi qiyin bo‘lgan yaxshi yoritilmagan sohaga yuboriladi. Obyektiv bilan kattalashtirilgan tasvir svetovod orqali operatorga uzatiladi. Tasvir sifati ravshanlikni boshqaruvchi yordamida o‘zgartiriladi. 3-rasmda ETG seriyasidagi endoskop tasviri keltirilgan.

**3-rasm.** *ETG seriyasidagi endoskop.*

Optik kanal orqali axborotni tutib olishda, misol uchun binoning yuqori qavatlarida joylashgan xonalardagi tasvirlarni to‘g‘ridan-to‘g‘ri ko‘rish yoki kuzatish mumkin emas. Buning uchun albatta ushbu xonaga qarama-qarshi binodan turib, maxsus optik qurilma yordamidan foydalanish zarur bo‘ladi. Biroq, agar xona oynalari axborot bilan ishlash jarayonida to‘liq yopilsa, ya’ni maxsus pardalar bilan berkitilsa, u holda axborot chiqib ketishi uchun vizual optik kanalning o‘zi mavjud bo‘lmaydi. Boshqacha aytganda, bunday xonada axborotni optik tutib olish kanali hosil bo‘lmaydi. Bunga qo‘shimcha ravishda xonalar oynasini tonirovka qilish yoki ularga sirtiga maxsus ishlov berilgan oynalar o‘rnatish ham mumkin.

***Axborotni chiqib ketish radioelektron kanallari.*** Radioelektron kanallar demaskirovka belgilariga ko‘ra axborotni tutib olishning asosiy kanali hisoblanadi.

Radioelektron vositalar va elektr qurilmalari faoliyat ko‘rsatish jarayonida ular atrofida yondosh elektromagnit maydon nurlanishi yuzaga kelib, ular himoyalangan axborotni o‘zida saqlashi mumkin. Aksariyat hollarda statik va dinamik zaradlarga ega bo‘lgan elektr toki zanjirlari ana

shunday nurlanish manbalari bo‘ladi. Elektr zanjirida axborotni bevosita qayta ishlash jarayonida axborotni o‘zida aks ettiruvchi yondosh nurlanishlar vujudga keladi.

Elektromagnit maydonning nurlanish turi va uning tarqalish xususiyati maydonning tebranish chastotasi va nurlantirgich turiga bog‘liq. Bunga asoslangan holda past chastotali va yuqori chastotali xavfli nurlanishlar farqlanadi.

Tovush kuchaytiruvchi qurilmalar (mikrofon, audiomagnitofon, telefon apparati, ularni bog‘lovchi kabellar va shu kabilar)dan tarqaluvchi tovush diapazonidagi nurlanishlar past chastotali hisoblanadi.

Radioelektron vositalar zanjiridan nurlanuvchi, yuqori chastotali signallar tarqatuvchi elektromagnit maydonlar yuqori chastotali xavfli nurlanishlarga taalluqli bo‘lib, ular o‘zida himoyalangan axborotni mujassamlaydi. Audio- va videomagntofonlarning o‘chirish va magnitlash generatorlari, monitor va televizorlarning elektron-nur trubkalari, kompyuterning yuqori chastotali signallar bilan ishlovchi elementlari kabilar bunday nurlanishlarni tarqatuvchi qurilmalarga misol bo‘lishi mumkin.

Real hayotda elektromagnit to‘lqinlarning tarqalishiga to‘siqlarning ko‘pligi sababli ularning tarqalish xususiyati juda ham murakkab hisoblanib, ularni aniq bir matematik ifodalashning imkoni yo‘q.

***Radiosignallarni tutib olish vositalari.*** Elektromagnit, elektr, magnit maydonlarni hamda axborotga ega bo‘lgan elektr signallarini tutib olish radio- yoki radiotexnik razvedka deb ataladi. Uning asosiy bosqichlariga quyidagilarni kiritish mumkin:

– muhitda tarqaluvchi signallarni topish;

– signallarni kuchaytirish;

– qabul qilinayotgan signallarni tahlil qilish va ulardan axborotni yechib olish;

– signal manbai joylashgan manzilni aniqlash.

Radiosignallarni tutib olishning namunaviy kompleksiga quyidagilarni kiritish mumkin:

– qabul qiluvchi antenna;

– radiopriyemnik;

– signalning texnik xususiyatini tahlil qiluvchi qurilma – analizator;

– radiopelengator;

– ro‘yxatga oluvchi qurilma.

Radio- yoki radiotexnik razvedka vositalariga quyidagilar kiradi:

– portativ skanerlovchi priyomniklar (qabul qiluvchi qurilmalar), spektrning raqamli analizatorlari, radiotesterlar va boshq.;

– radiotelefonlar va uyali aloqa vositalarini nazorat qiluvchi maxsus vositalar;

– skanerlovchi priyomniklar asosida qurilgan dasturiy-apparat komplekslar;

– portativ radiopelengatorlar va boshqalar.

Skanerlovchi priyomniklar radiorazvedkalarni o‘tkazishda keng qo‘llanilib, ular o‘lchami va vazniga ko‘ra portativ (qo‘lda olib yuruvchi) va tashib yuriluvchi turlariga bo‘linadi. Portativ skanerlovchi priyomnik-larning vazni 150-350 grammni tashkil etib, ular avtonom tok manbaiga ega bo‘ladi. O‘zining ixchamligi va yengilligiga qaramay bunday priyom–niklar 100-500 kGs dan 1300 MGs gacha, ayrimlar hatto 2060 MGs (“HSC-050”) bo‘lgan chastota diapazonidagi razvedkani olib borish imkonini beradi. Portativ skanerlovchi priyomniklar 100 dan 1000 tagacha xotira kanallariga ega bo‘lib, bir soniyada sozlashning 50-500 Gs dan 50-1000 kGs gacha chastota qadamida 20 dan 30 tagacha kanallarni skanerlash tezligini ta’minlaydi. Bunday priyomniklarning ayrimlarini, masalan AR-2700, AR-8000, IC-R20, IC-R10 rusumlilarini kompyuter yordamida boshqarish mumkin. AR-8000 va IC-R20 rusumidagi portativ skanerlovchi priyomniklarning umumiy ko‘rinishlari 4-rasmda keltirilgan.

Icom firmasi tomonidan ishlab chiqilgan IC-R20 rusumidagi portativ skanerlovchi priyomnigi o‘zining mukammalligi bilan ajralib turadi. Ushbu priyomnik signallarni qabul qilishda yuqori sifatni kafolatlash bilan birga bir vaqtning o‘zida ikki xil chastotada kuzatish olib borish imkonini beradi. Uning og‘irligi 320 grammni tashkil etadi.

*AR-8000 rusumidagi portativ skanerlovchi priyomnik.*

*IC-R20 rusumidagi portativ skanerlovchi priyomnik.*

***4-rasm.*** *Portativ skanerlovchi priyomniklar.*

Tashib yuriluvchi skanerlovchi priyomniklar portativ skanerlovchi priyomniklardan o‘zlarining katta hajmi va og‘irligi bilan farqlanadi. Ularning og‘irligi 1,2 kg dan 6,8 kg gacha bo‘lishi mumkin. Hajm va massaning ortishi bilan priyomniklarning funksional imkoniyatlari ham ortib boradi. Tashib yuriluvchi skanerlovchi priyomniklarning deyarli barchasi kompyuter yordamida boshqarilishi mumkin. AR-3000A rusumli tashib yuriluvchi skanerlovchi priyomnikning umumiy ko‘rinishi 5-rasmda keltirilgan.

**5-rasm.** *AR-3000A rusumli tashib yuriluvchi skanerlovchi priyomnik.*

Har ikki turdagi skanerlovchi priyomniklar quyidagi rejimlardan birida ishlashi mumkin:

– berilgan chastota diapazonida avtomatik skanerlash rejimi;

– fiksirlangan chastota bo‘yicha avtomatik skanerlash rejimi;

– qo‘lda boshqarish rejimi.

Radiotexnik razvedkalarda skanerlovchi priyomniklar bilan bir qatorda spektr analizatorlaridan ham foydalanish mumkin.

Spektr analizatorlari juda keng chastota diapazonidagi signallarni qabul qilish va ularning tuzilishini tahlil qilish imkonini yaratadi. Portativ analizatorlar o‘rtacha 9,5 dan 20 kg gacha og‘irlikka ega bo‘lishi mumkin. Bunday qurilmalarning signal kattaliklarini o‘lchash aniqligi juda ham yuqori bo‘lib, sezgirligi 125-145 Db ni tashkil etadi. Shu sababli ham ular qimmatbaho hisoblanadi. Tektronix firmasi tomonidan ishlab chiqarilgan RSA5103A rusumli analizatorning umumiy ko‘rinishi 6-rasmda keltirilgan.

**6-rasm.** *RSA5103A rusumli spektr analizatori.*

## 2.3. Ma’lumotlarni tutib olish vositalari

Akustik tebranishlarning tebranuvchi kanallarda tarqalish muhiti sifatida binolar, devorlar, shiftlar, metall trubali konstruksiyalar va boshqa qattiq buyumlar bo‘lishi mumkin. Bunday axborotni tutib olish qurilmasi **stetoskoplar** bo‘lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi. Elektron stetoskoplar yordamida axborotni tutib olish uchun himoyalangan binoga ruxsat kerak emas. Portativ stetoskopning ko‘rinishi 7-rasmda keltirilgan.


**7-rasm.** *Kichik o‘lchamli kontakt mikrofoniga ega bo‘lgan PKI 2850 markali elektron stetoskop.*

PKI 2850 markali stetoskop portativ elektron stetoskoplarning vakili hisoblanadi. Uning kuchaytirgich bloki o‘lchamlari - 95x60x25 mm, mikrofoni – 50x35x15 mm ni tashkil etadi. Bunday kichik o‘lchamga ega bo‘lishiga qaramay ushbu stetoskopning kuchaytirish koeffitsiyenti 80 dB dan kam emas. Ishlash davomiyligi to‘liq zarayadlangan akkumulator bilan 800 soatni tashkil etadi.

Zamonaviy elektron stetoskoplar 80-100 dB tartibidagi kuchaytirish koeffitsiyentiga ega bo‘lib, hatto shivirlash yoki soat sekundomerining tovushi kabi kuchsiz tovush tebranishlarini ham tutib olish imkoniyatiga ega. Bunday elektron stetoskoplarni devorlarga, eshik chetidagi qobiqlarga, xona shiftiga, isitish tizimi yoki suv trubalariga, havo sovutgichlari qoplamalari ichiga joylashtirilishi va kuchaytirish bloki bilan maxsus ulangan kabel orqali ulanadi.

Axborotlarni elektroakustik chiqib ketish kanallari elektroakustik aylantirishlar, ya’ni akustik signallarni elektr signallariga aylantirish jarayonida hosil bo‘ladi. Bunday jarayonni amalga oshiruvchi qurilmalar orasida bizga yaxshi tanishlari bular - telefonlar, mikrofonlar va tovushli aloqa tizimlaridir.

**Optik-elektron kanalda** axborotni tutib olish lazer orqali amalga oshiriladi va shu sababdan ba'zida uni lazerli kanal deb ham ataladi. Tovush to‘lqinlari ta'sirida oyna yoki toshoyna kabi qaytaruvchi sirtlar tebrana boshlaydilar. Agar ularga lazer nurini yo‘naltirilsa, ular oyna sirtida modulyatsiyalanadi va sirtdan qaytgan nurlar optik nurlanishli qabul qiluvchi qurilmaga kiradi. Qabul qiluvchi qurilmada ushbu signal demodulyatsiyalanadi va kuchaytiriladi hamda undan dastlabki akustik signalni olish mumkin bo‘ladi.

**Akustik razvedka vositalari.** Umumiy holda akustik razvedka obyektning ishlab chiqarish shovqinlarini yoki nutqli axborotlarni tutib olish bilan amalga oshiriladi.

Foydalanish usuliga ko‘ra akustik axborotlarni tutib olish vositalarini ikki toifaga bo‘lish mumkin:

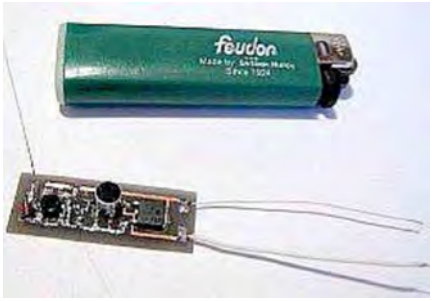
1. Himoyalangan obyektga fizik jihatdan kiritilishi talab etiluvchi vositalar:

– radioo‘rnashmalar;
– IQ-diapazondagi akustik axborotlarni uzatuvchi o‘rnashmalar;
– 220 voltli tarmoq orqali uzatuvchi o‘rnashmalar;
– telefon tarmoqlari orqali axborot uzatuvchi o‘rnashmalar;
– diktofonlar;
– o‘tkazgichli mikrofonlar;
– "telefon quloq"lari.

2. Himoyalangan obyektga fizik jihatdan kiritilishi talab etilmaydigan vositalar:

– "mikrofon effekti"dan foydalanuvchi qurilmalar;
– stetoskoplar;
– lazerli mikrofonlar;
– yo‘naltirilgan mikrofonlar.

**Radioo‘rnashmalar.** Bunday qurilmalarning vazifasi himoyalangan obyektdan akustik axborotlarni radiokanallar orqali uzatib berishdir. O‘rnashmalar alohida modul sifatida turli kundalik maishiy buyumlar (masalan zajigalka, kalkulator, avtoruchka va boshq.) ko‘rinishida tayyorlanishi mumkin. Radioo‘rnashmalarning tashqi ko‘rinishlari 8, 9, 10-rasmlarda keltirilgan.




**8-rasm.** *Zajigalka ko‘rinishidagi radioo‘rnashma.*


**9-rasm.** *Tanga ko‘rinishidagi radioo‘rnashma.*


**10-rasm.** *Oddiy ko‘rinishdagi radioo‘rnashma.*

Radioo‘rnashmalar radiodiapazondagi elektromagnit to‘lqinlar yordamida axborotlarni uzatadi. Mazkur usuldan foydalanishda albatta qabul qiluvchi qurilma kerak bo‘ladi. Bunday qabul qiluvchi qurilma sifatida oddiy maishiy buyumlar (pleyer, musiqa markazi, magnitofon kabilar)dan foydalanish mumkin. Faqatgina bu yerda radioo‘rnashmaning qaysi chastotada ishlayotganini hisobga olish kerak bo‘ladi. Bu esa g‘arazgo‘y kimsaga qo‘l kelib, uni maxsus qabul qilish qurilmasini sotib olishga majbur qilmaydi. Shuningdek, bu holda ushbu signalni boshqa kimsalar ham tutib olish ehtimolini vujudga keltiradi.

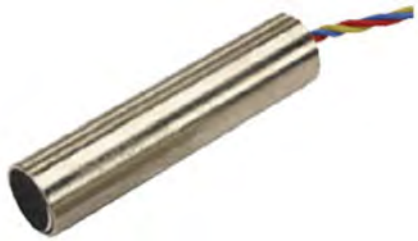
Akustik axborotlarni tutib olish texnik vositalariga diktofonlar ham kiradi. Diktofon – tovushli axborotni tasmaga, ichki xotira mikro-sxemasiga qayd qiluvchi qurilma. Turli diktofonlarning yozib olish vaqti turlicha bo‘lib, u 15 minutdan 8 soatgacha bo‘lishi mumkin.

Zamonaviy raqamli diktofonlar axborotni ichki xotiraga bir necha soat mobaynida yozib olish imkoniyatini beradi. Bu diktofonlar deyarli shovqinsiz bo‘lib, o‘z xotirasidagi ma’lumotlarni kompyuter xotirasiga o‘tkazish va keyinchalik uni qayta ishlashga sharoit yaratadi.


**11-rasm.** *Edic-Mini Tiny B21 rusumli mini-diktofon.*

Ko‘pchilik diktofonlarning elektr manbasi batareykalar bo‘lib, ularning og‘irligi o‘nlab yoki yuzlab grammlarni tashkil etadi. Shuning uchun zamonaviy diktofonlar juda ham kichik o‘lchamlarga (11-rasm) ega bo‘lib, ularni himoyalangan obyektning ixtiyoriy joyiga o‘rnatish mumkin.

Bino yoki inshoatlarni qurish yoki ta’mirlash jarayonida ularga yashirin ravishda kichik o‘lchamli mikrofonlarni o‘rnatib qo‘yish mumkin. Mikrofonlar simlar orqali signalni qabul qiluvchi qurilmaga ulanadi va ular manbadan 7-10 metr uzoqlikdagi nutqlarning o‘rtacha tovushlarini qayd qila oladi. Bunda chastota diapazoni 20 – 100 Gs dan 6 – 20 kGs gachani tashkil etadi. Bunday mikrofonlar elektr manbaining doimiy kuchlanishi 9-15 voltga teng. Odatda mikrofon kuchaytirgich bilan ta’minlanadi. Axborotni uzatish va kuchaytirgichni elektr manbai bilan ta’minlash uchun 2 yoki 3 talik simlardan foydalaniladi.



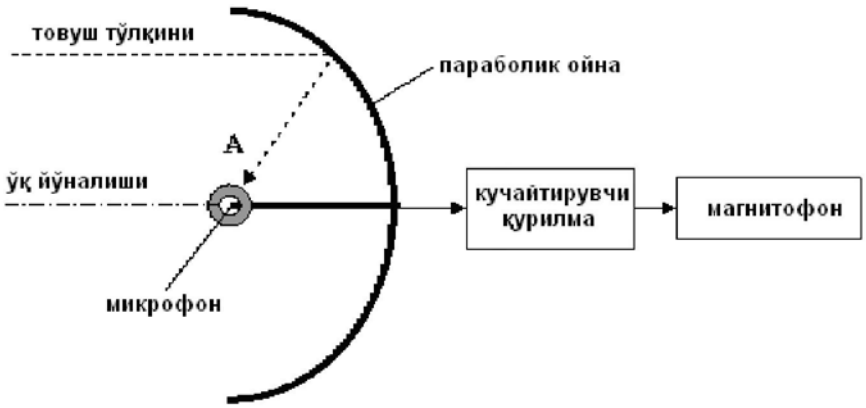
**12-rasm.** *3 ta simli Shorox-8 mikrofoni.*

Akustik axborotlarni telefon tarmog‘i orqali uzatish uchun “telefon quloq” turidagi o‘rnashmalardan foydalaniladi. Ushbu qurilma telefon korpusiga yoki telefon rozetkasiga yashirin ravishda o‘rnatiladi (13-rasm). U kuchaytiruvchi qurilma va telefon liniyasiga ulanish imkonini beruvchi maxsus qurilmaga ega bo‘lgan elektret (qutblangan dielektrik) turidagi mikrofondan iborat.

**13-rasm.** *TU-2 rusumli "Telefon quloq".*

*Himoyalangan obyektga fizik jihatdan kiritilishi talab etilmaydigan vositalar.* Agar himoyalangan binoda deraza yoki fortochka ochiq bo‘lsa, u holda undan akustik axborotlarni tutib olishda yo‘naltirilgan mikrofonlardan foydalanish mumkin. Yo‘naltirilgan mikrofonlar quyidagi turlarga ajratiladi: parabolik, trubkali, yassi va gradiyentli. Ular orasidan dastlabki uchtasi ko‘proq qo‘llaniladi.

**Parabolik mikrofon** markazida oddiy mikrofon joylashgan, parabola shaklidagi optik jihatdan yaltiroq yoki yaltiroq bo‘lmagan materialdan iborat 20-30 sm diametrga ega bo‘lgan tovushni qaytaruvchi moslamadan iborat (14-rasm).




**14-rasm.** *Parabolik mikrofon sxemasi.*

O‘q yo‘nalishidagi tovush to‘lqinlari parabolik oynadan qaytib, A fokus nuqtasida faza bo‘yicha jamlanadi. Bu yerda tovush maydonining kuchayishi sodir bo‘ladi. Parabola oynasining diametri qancha katta bo‘lsa, qurilma tovushni shuncha katta kuchaytirish imkonini beradi. Agar kelayotgan tovush to‘lqinining yo‘nalishi o‘q yo‘nalishiga mos kelmasa, u holda A nuqtaga yig‘ilayotgan signallar yig‘indisi bir fazaga jamlanmaydi va oqibatda kuchaytirish kam natija beradi. Kelayotgan tovush signali va o‘q yo‘nalishi orasidagi burchak ortib borgani sari kuchaytirish tobora kama-

yib boradi. Shunday qilib qurilmaning burchakli tanlash vaziyati yuzaga keladi. Parabolik mikrofonlarning tashqi ko‘rinishi 15-rasmda keltirilgan.

**15-rasm.** *"Super Uxo – 100" rusumli parabolik mikrofon.*

**Yassi mikrofon** tuzilishi fazalangan akustik panjara shaklida bo‘lib, uning tugunlarida mikrofonlar joylashtiriladi. Ulardan kelayotgan signallar jamlanib, kuchaytiruvchi qurilmaning kirishiga uzatiladi. Bunday qurilma kelayotgan tovush yo‘nalishiga perpendikular joylashtirilgan biror tekislikning aniq bir nuqtalarida tovush to‘lqinini qabul qilish g‘oyasiga asoslangan. Agar tovush to‘lqini o‘q yo‘nalishiga mos ravishda kelsa, ya’ni panjara sirti tekisligi tovush yo‘nalishiga perpendikular joylashsa, qabul qilinayotgan signallarning fazalari mos keladi va tovush maksimal darajada bo‘ladi. Aksincha, panjara sirti tekisligi tovush yo‘nalishiga perpendikular joylashmasa, bunda turli mikrofonlarda qabul qilinayotgan signallar fazasi orasida farq yuzaga keladi. Shu sababli, tovush yo‘nalishi va panjara sirti tekisligi orasidagi burchak qanchalik ortib borsa, signalning kuchaytirilishi shunchalik kamayib boradi.

**16-rasm.** *G.R.A.S. firmasining yassi mikrofoni.*

Akustik razvedkalar uchun mo‘ljallangan yuqoridagi kabi qurilmalardan foydalanishda g‘arazgo‘y kimsalardan alohida bilim darajasi talab etiladi. Mini-diktofon yoki mikrofonni o‘rnatib, undan yopiq bino ichida foydalanish uchun avvalo, qurilmalar ishlashining fizik mohiyatini yaxshi bilish zarur. Akustik razvedka uchun u yoki bu vositani tanlash birinchi galda egallanmoqchi bo‘lgan axborotning qiymatiga bog‘liq. Har qanday holatda ham axborot xavfsizligi bo‘yicha mutaxassis axborot himoya obyektlarini joylashishi va faoliyatini samarali tashkil etishi uchun axborotni noqonuniy egallab olishning qanday tahdidlari mavjudligini bilishi lozim.

***Nazorat uchun savollar***

– Axborotlarni muhofaza qilishning texnik vositalari tushunchasi nimani anglatadi?

– Maskirovkalovchi belgilarning ochilishi tushunchasini nimani bildiradi?

– Demaskirovka belgilari nimalar bilan farq qiladi?

– Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbalari va tashuvchilari nimalardan iborat?

– Nimalar ma’lumot tashuvchi vositalar hisoblanadi?

– Ma’lumotlar chiqish kanali deb nimaga aytiladi?

– Ma’lumotlar chiqib ketish kanalining paydo bo‘lish sabablari va sharoitlari nimalardan iborat?

– Texnik kanal bo‘yicha ma’lumotlar chiqib ketishidan himoyalashda qanday amallar bajarilishi talab etiladi?

– Tutib olishdan himoyalashning qanday usullar mavjud?

– Akustik razvedkalar uchun qanday qurilmalar mavjud?

# III. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH USULLARI

## 3.1. Kriptografiya va uning asosiy tushunchalari

Insoniyat taraqqiyotida yozuv paydo bo‘lgan davrdan boshlab axborotni himoya qilish muammosi ham yuzaga kela boshladi. Bu muammo harbiy va diplomatik ma’lumotlarni yashirincha uzatish zaruratidan kelib chiqqan. Masalan, antik spartaliklar harbiy harakatlar vaqtida ma’lumotlarni shifrlash usullaridan foydalanganlar. Xitoyliklar tomonidan esa oddiy yozuvni iyerogriflar ko‘rinishida tasvirlash usuli qo‘llanilib, bu ularga ma’lumotlarni raqiblardan yashirish imkonini bergan.

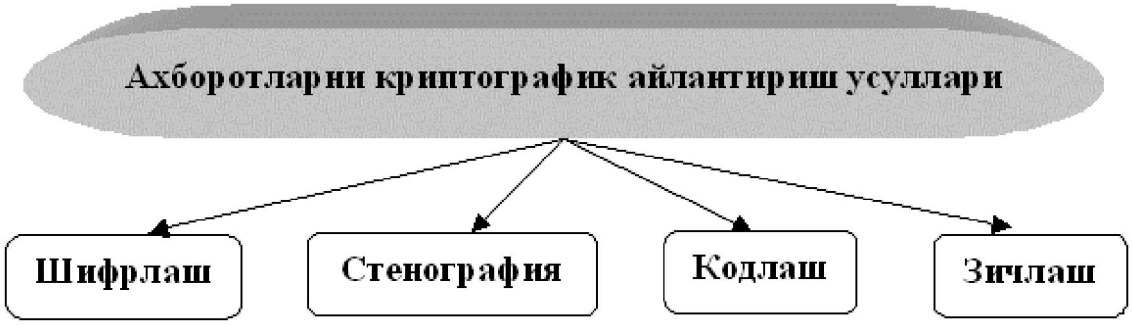
**Kriptografiya** qadimiy yunon tilida “yashirin yozaman” degan ma’noni anglatib, axborotning konfidensialligini va autentligini ta’minlash usullari haqidagi fandir. Kriptografiya ma’lumotni, g‘arazgo‘y kimsalar tomonidan egallangan taqdirda, befoyda ko‘rinishga aylantirib beruvchi usullar to‘plamini tashkil etadi. Bunday usullar axborot xavfsizligiga taalluqli ikkita asosiy masalani yechishga imkon beradi. Bular:

– konfidensiallik himoyasi;

– butunlik himoyasi.

Axborotning konfidensialligi va butunligi himoyasi muammolari bir-biri bilan uzviy bog‘liq bo‘lib, ularning birini yechimi ikkinchisi bilan bog‘liq bo‘ladi.

Axborotlarni kriptografik aylantirish usullarini toifalashga turlicha yondashishlar mavjud. Dastlabki ma’lumotlarga ta’sir etish ko‘rinishiga ko‘ra kriptografik aylantirish usullarini 4 ta guruhga bo‘lish mumkin.




**Shifrlash** jarayoni dastlabki axborotni qayta tiklash imkoni bilan matematik, mantiqiy, kombinatsion va boshqacha aylantirishlarni amalga

oshirishni o‘z ichiga oladi. Buning natijasida shifrlangan axborot harflar, raqamlar, boshqa simvollar va ikkilik kodlarining xaotik to‘plamidan iborat bo‘ladi.

Axborotni shifrlash uchun aylantirish algoritmi va kalitdan foydalaniladi. Odatda biror shifrlash usuli uchun algoritm o‘zgarmas bo‘ladi. Shifrlash algoritmi uchun dastlabki ma’lumotlar – bu shifrlanuvchi axborot va shifrlash kaliti hisoblanadi. Kalit boshqaruvchi axborotni o‘zida saqlaydi. Bunday axborot algoritmning muayyan qadamlarida qanday aylantirish tanlashnishini va shifrlashda ishlatiladigan operandlar kattaliklarini aniqlaydi. Operand – bu ustida amal bajarilayotgan dasturlash tilining konstantasi, o‘zgaruvchisi, funksiyasi, ifodasi va boshqa obyektidir.

Axborotni kriptografik aylantirishning boshqacha usullaridan farqli ravishda **stenografiya** usullari saqlanuvchi yoki uzatiluvchi axborotning nafaqat ma’nosini, balki yopiq axborotning saqlanishi va uzatilishini ham yashirish imkonini beradi. Stenografiya usullari asosida yopiq axborotni ochiq fayllar orasida niqoblash (maskirovkalash) yotadi.

Grafik va tovushli axborotlar raqamli ko‘rinishda ifodalanadi. Grafik obyektlarning eng kichik tasvir elementi bir bayt bilan kodlanishi mumkin. Tasvirning kichik razradli aniq baytlariga kriptografik aylantirish algoritmiga mos ravishda yashirish faylning bitlari joylashtiriladi. Agar aylantirish algoritmi va tasvir to‘g‘ri tanlansa, dastlabki tasvir hamda fonida yashiringan fayl joylashgan, hosil qilingan tasvir orasidagi farqni inson ko‘zi bilan ajratib bo‘lmaydi. Stenografiya vositalari yordamida matnlarni, tasvirlarni, raqamli imzolarni, shifrlangan xabarlarni niqoblash mumkin.

Yashiringan fayl ham shifrlanishi mumkin. Agar begona shaxs yashirin faylni tasodifan topib olsa, u holda shifrlangan axborot tizim faoliyatidagi xatolik sifatida qabul qilinadi. Stenografiya va shifrlashdan umumiy holda foydalanish, konfidensial axborotni topish va uni ochish vazifasi murakkabligini ko‘p karra oshirib yuboradi.

Axborotlarni **kodlash** jarayoni ma’lumot (so‘z, gap)ning dastlabki ma’nosini kodlar bilan almashtirishdan iborat. Bunda kodlar sifatida harflar, raqamlar, belgilar mosligidan foydalanish mumkin. Ma’lumotlarni kodlash va ularni qayta tiklashda maxsus jadvallar yoki lug‘atlardan foydalaniladi. Axborot tarmoqlarida ma’lumotni (yoki signalni) dasturiy-apparat vositalar yordamida kodlash uzatilayotgan axborotning ishonchliligini oshirish uchun qo‘llaniladi.

Aksariyat hollarda kodlash va shifrlashni bir-biri bilan almashtirib yuborishadi. Kodlangan axborotni qayta tiklash uchun almashtirish qoidasini bilish yetarli. Biroq shifrlangan axborotni shirfdan ochish uchun esa shifrlash qoidasidan tashqari shifrlash kalitini ham bilish talab etiladi.

Axborotni **zichlash** usulini kriptografik aylantirish usullariga ma'lum bir chetlanishlar bilan kiritish mumkin. Chunki, axborotni zichlashdan maqsad ma'lumotning hajmini qisqartirishdir. Zichlash vositalariga egalik qilish imkoniyati kengligi va ularni qayta tiklash osonligini inobatga olgan holda, bu usulga axborotni ishonchli kriptografik aylantirish vositasi sifatida qarab bo‘lmaydi. Hatto zichlash algoritmi maxfiy saqlangan holda ham ularni statistik usullar bilan nisbatan yengil ochish mumkin. Shuning uchun konfidensial axborotlarning zichlangan fayllari keyinchalik shifrlanishi lozim. Ma'lumotlarni uzatish vaqtini kamaytirish uchun zichlash va shifrlash jarayonlarini birlashtirish maqsadga muvofiq.

**Kriptotahlil** – bu kalitni bilmay turib, shuningdek, shifrlash algoritmi haqida ma'lumotlar yo‘q bo‘lgan holda yopiq axborotni shifrdan ochish jarayonidir.

**Shifrning kriptomustahkamligi –** samaradorlikning asosiy ko‘rsatkichi bo‘lib, u vaqt bilan yoki kriptotahlilchining kalit ma'lum bo‘lmagan holda shifrmatndan dastlabki ma'lumotni chiqarib olishi uchun kerak bo‘ladigan vositalar narxi bilan o‘lchanadi.

Keng qo‘llaniluvchi shifrlash algoritmlarini maxfiy saqlash mumkin emas. Shuning uchun shifrlash algoritmini yashirish zarurati yo‘q. U holda shifrlashning kriptomustahkamligi kalit uzunligi bilan belgilanadi. Chunki, yopiq axborotni shifrdan ochish uchun yo‘l faqatgina kalitni to‘g‘ri tanlashdir. Demak, kriptotahlilga ketadigan xarajat, ya'ni vaqt va mablag‘ kalitning uzunligi va shifrlash algoritmi murakkabligiga bog‘liq bo‘ladi.

## 3.2. Axborotlarni kriptografik himoyalash usullari

Axborotlarni kriptografik himoyalash usullari axborot xavfsizligi uchun kurashda samarali vosita bo‘lib, bugungi kunda ular axborot tizimlarida keng qo‘llanilmoqda.

Kriptografiya usullari – axborotning konfidensialligi va butunligini ta'minlashning kuchli qurollaridan biri hisoblanadi. Kriptografiyaning asosiy elementi – bu shifrlashdir. Ta'kidlash joizki, shifrlash usulining vujudga kelishi juda ham qadimiy tarixga ega.

Qadimiy yunon sarkardasi YU. Sezar gallar bilan urush vaqtida (eramizning 56-yili) shifrlash usullaridan biri bo‘lgan almashtirish shifrini qo‘llagan. Ochiq matn alifbosi ostiga ma’lum bir sikl bo‘yicha (Sezarda uchta tartibga) siljitish orqali yangi alifbo yozilgan. Shifrlashda ochiq matndagi alifbolar, ya’ni yuqori qismda joylashgan harflar quyi qismdagi mos harflar bilan almashtirilgan. Bu turdagi shifrlash YU.Sezargacha ma’lum bo‘lgan bo‘lsa-da, lekin bunday shifrlash usuli uning nomi bilan yuritiladi.

Murakkab almashtirishlar shifri sifatida yunonlar shifri – “Polibiy kvadrati” sanaladi. Alifbo kvadrat jadval ko‘rinishida tasvirlanadi. Shifrlashda ochiq matn harfi jadvaldagi ikkita songa almashtirilgan, ya’ni jadval bo‘yicha kerakli harfning joylashgan ustun va qator raqamlariga. Alifboni jadvalda ixtiyoriy tarzda joylashtirish va u orqali qisqa xabarni shifrlash zamonaviy qarashlar nuqtai nazari bo‘yicha ham mustahkam shifrlash hisoblanadi. Bu g‘oya birinchi jahon urushida maxfiy ma’lumotlarni shifrlashda amalda qo‘llanilgan.

Germaniyalik Iogann Tritemiy (1462–1516 yy) kriptografiya bo‘yicha birinchi darsliklardan birini yozgan. “Ave Maria” deb nomlangan ko‘p qiymatli almashtirishli original shifrlashni taklif etgan. Ochiq matnning har bir harfi shifrlovchining tanlovi bo‘yicha bir emas, balki bir nechta harflarga almashtirilishi mumkin bo‘lgan. Bunda harflar harf yoki so‘zlar bilan shunday almashtirilganki, natijada psevdomatn hosil bo‘lgan. Ko‘p qiymatli almashtirish usulidan hozirgi kunda ham foydalaniladi (masalan, ARJ arxivatorida).

XVI asrga kelib almashtirish shifrlari matematik Djovanni Batista Port va diplomat Bleza de Vijiner ishlarida o‘z rivojini topdi. Vijiner tizimi u yoki bu ko‘rinishda hozirgi paytda ham qo‘llanilmoqda.

Lord Frensis Bekon (1562-1626 y) birinchi bo‘lib harflarni 5 qiymatli ikkilik kod bilan belgilagan: A= 00001, V =00010,... va hokazo. Bekon bu kodlarga qayta ishlov bermagan, shuning uchun bunday yashirish usuli mustahkam bo‘lmagan. Uch asrdan so‘ng, bu kodlash tamoyili elektr va elektron aloqada asos qilib olindi. Bunda Morze va Bodo kodlarini, 2-sonli xalqaro telegraf kodini, ASCII kodini, eslash ham o‘rinli, chunki ular ham oddiy almashtirish asosida yaratilgan.

Bugungi kunda axborot tizimlarida xavfsizlikni ta’minlash borasida yuqori kriptomustahkamlikka ega bo‘lgan kriptotizimlar qo‘llanilmoqda. Ma’lumotlarni kriptografik o‘zgartirishning yangi usullari intensiv

ravishda takomillashib bormoqda va ularning qo‘llanish doirasi tobora kengaymoqda.

Zamonaviy shifrlash usullari quyidagi talablarga javob berishi lozim:

– shifrning mustahkamligi kriptotahlilga shunday qarshi tura olishi kerakki, bunda shifrdan ochish faqatgina kalitlarni to‘liq topish orqali amalga oshirilishi mumkin bo‘lsin;

– kriptomustahkamlik shifrlash algoritmining maxfiyligi bilan emas, balki, kalitning maxfiyligi bilan ta’minlanishi lozim.

– shifrmatn hajm jihatidan dastlabki axborotdan sezilarli darajada yuqori bo‘lib ketmasligi kerak;

– shifrlash jarayonida yuzaga keladigan xatolar axborot buzilishi va yo‘qotilishiga olib kelmasligi kerak;

– shifrlash vaqti katta bo‘lmasligi kerak;

– shifrlash narxi shifrlanayotgan axborot qiymati bilan mos kelishi kerak.

***Ochiq va yopiq kalitlar bilan shifrlash tizimi.*** Kalitdan foydalanib shifrlash algoritmining ikki xil ko‘rinishi mavjud: *simmetrik* va *asimmetrik (ochiq kalitli)*.

Ma’lumotlarni shifrlash uchun foydalanilgan kalit shifrni ochish kalitidan olingan yoki aksincha bo‘lsa, bunday kriptografik algoritmlar simmetrik deb nomlanadi. Ko‘pgina simmetrik algoritmlarda yagona kalitdan foydalaniladi. Bunday algoritmlar *bir kalitli* yoki maxfiy kalitli algoritmlar deb ataladi hamda xabarni yuboruvchi va uni qabul qiluvchi qanday kalitdan foydalanishni kelishib olishlarini talab etadi. Bir kalitli algoritmlarning ishonchliligi kalitni tanlash bilan aniqlanadi. Agar g‘araz-go‘y kimsaga kalit ma’lum bo‘lsa, u hech qanday qiyinchiliklarsiz barcha tutib olingan ma’lumotlarni shifrdan ochish imkonigi ega bo‘ladi. Demak, bunday shifrlash usulida tanlangan kalitni begonalardan sir saqlash muhim ahamiyatga ega.

Shifrlashning simmetrik algoritmlari ikki turda bo‘ladi. Ulardan biri ochiq matnga bitlar bo‘yicha ishlov beradi. Ular *potokli algoritmlar* yoki *potokli shifrlar* deb nomlanadi. Ikkinchisida esa, ochiq matn bir necha bitdan iborat bo‘lgan bloklarga bo‘linadi. Bunday algoritmlar *blokli algo-ritmlar* yoki *blokli shifrlar* deb nomlanadi. Blokli shifrlashning zamonaviy algoritmlarida, odatda, blok uzunligi 64 bitni tashkil etadi.

Simmetriyali tizimlarda kuyidagi ikkita muammo mavjud:

1) Axborot almashishda ishtirok etuvchilar qanday yo‘l bilan maxfiy kalitni bir-birlariga uzatishlari;

2) Jo‘natilgan xabarning haqiqiyligini aniqlash.

*Elektron raqamli imzo va ochiq kalitlar strukturasi.* Elektron raqamli imzoni qo‘llashdan maqsad, avvalo, elektron hujjatdagi axborot asl nusxa ekanligini tasdiqlash, shuningdek uchinchi tarafga (arbitrga, sudga va boshqalarga) hujjatning muallifi ushbu shaxs ekanligini isbotlash. Ushbu maqsadga erishish uchun muallif o‘zining maxfiy individual raqami (individual kalit, parol) bilan hujjatga o‘rnatilgan tartibda «elektron imzo qo‘yish» jarayonini bajarishi lozim. Bunday imzo qo‘yishda, har gal individual kalit elektron hujjatdagi ma’lumotlar bilan ma’lum qoidaga muvofiq aralashib ketadi. Bunday biriktirilish natijasida hosil bo‘lgan raqam (ma’lum razrad uzunligidagi raqamlar ketma-ketligi) ushbu hujjatga muallif tomonidan qo‘yilgan elektron raqamli imzo hisoblanadi. Shunday qilib, elektron raqamli imzo qo‘yish va uni tekshirish protsedurasining har birida ishlatiladigan ikkita kalitdan bittasi foydalaniladi. Lekin bunda imzo qo‘yish kalitini tekshirish kaliti yordamida aniqlash imkoniyati umuman mumkin emasligi kafolatlangan bo‘lishi kerak. Hozirda taklif etilgan usullarda, amalda imzo qo‘yish kalitini (yopiq kalit), tekshiruv kaliti yordamida (ochiq kalit) qayta tiklash uchun uzoq davom etadigan murakkab hisoblash ishlarini bajarish lozimligi nazarda tutiladi.

Elektron imzo g‘oyasi birinchi marta Diffi va Xellman asarida hujjatning asl nusxa ekanligini va muallif tomonidan imzolanganligini aniqlash uchun taklif etilgan.

Hozirgi vaqtda axborot tizimlarida elektron raqamli imzo keng qo‘llanilmoqda (uzatiladigan yoki saqlanadigan shifrlangan matnga biriktirilgan raqam, ushbu axborotning butunligini va muallifning haqiqiyligini tekshirish imkoniyatini kafolatlaydi).

## 3.3. Shifrlovchi dasturlar va ularning imkoniyatlari

Bugungi kunda ma’lumotlarni shifrlovchi ko‘plab dasturlar ishlab chiqilgan. Ular orasida **TrueCrypt** dasturi o‘z afzalliklari va yuqori imkoniyati tufayli keng ommalashgan.

Mazkur dasturning o‘ziga xos jihati mavjud bo‘lib, uning vositasida kompyuterning doimiy xotirasida ma’lum bir soha ajratib olinadi va shifrlangan ma’lumotlar ana shu sohada saqlanadi. Ushbu sohani hosil qilish jarayoni bir necha bosqichlardan iborat bo‘ladi.

Shifrlovchi dasturlarning yana bir vakili **AxCrypt** dasturi foydalanish uchun qulay bo‘lib, unda ortiqcha sozlash ishlarini amalga oshirish talab etilmaydi. Dastur kompyuterga o‘rnatilganda, u *Provodnikning* kontekstli menusiga, ya’ni sichqonchaning o‘ng tugmasi bosilganda hosil bo‘luvchi menuga joylashadi. Ushbu dastur yordamida shifrlanayotgan yoki shifrdan chiqarilayotgan fayl yoki papka belgilanadi va kontekstli menudagi **AxCrypt** dasturida kerakli amal tanlanadi.

**AxCrypt** dasturi quyidagi imkoniyatlarga ega:

– **AES-128** va **SHA-1** shifrlash algoritmidan foydalanib, ma’lumotning asl nusxasi o‘rniga yoki alohida yangi shifrlangan faylni hosil qilish;

– dastur orqali hosil qilingan kalitli fayl yordamida himoya qilish;

– o‘zi ochiluvchi (**.exe** kengaytmali) shifrlangan faylni yaratish. Bunday holatda shifrlangan ma’lumotni ochish uchun **AxCrypt** dasturi zarur bo‘lmaydi. Foydalanuvchi parolni bilishi, agar zaruriyat bo‘lsa, kalitli faylga ega bo‘lishi kerak;

– shifrlangan faylni shifrdan chiqarmasdan, parol (kalitli fayl) orqali ishga tushirish. Bu holda faylning asl nusxasi axborot tashuvchida hosil bo‘lmaydi;

– papkalar ichidagilarni paketli shifrlash;

– o‘chirilgan ma’lumotlarni tiklashdan himoyalash. O‘chirilgan fayllar egallagan joyga tasodifiy sonlar yoziladi.

Ma’lumki, har qanday yozma hujjatni tayyorlashda muallif uning haqiqatan ham asl nusxa ekanligini isbotlovchi shaxsiy imzosini qo‘yadi. Bu holat bugungi kunda elektron hujjatlarni tayyorlash va ularni almashishda ham o‘z aksini topmoqda. Elektron hujjat bilan ish yuritishda ma’lumotni qabul qiluvchi o‘ziga avval berilgan imzoni olingan ma’lumotdagi imzoga solishtirib, uning haqiqiyligini tekshirib olishi mumkin. Shuningdek, imzo ma’lumot hujjatiga yuridik jihatdan mualliflikni kafolatlaydi. Bunday kafolat esa barcha sohalarda, jumladan, bank va savdoda alohida ahamiyatga ega.

**Elektron hujjat.** Elektron hujjatga O‘zbekiston Respublikasining «Elektron hujjat aylanishi to‘g‘risida» 2004-yil 29-apreldagi 611-II-son qonunida[1] quyidagicha ta’rif berilgan: «Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo‘lgan axborot elektron hujjatdir».

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

Elektron hujjat texnika vositalaridan va axborot tizimlari xizmatlaridan hamda axborot texnologiyalaridan foydalanilgan holda yaratiladi, ishlov beriladi va saqlanadi.

Elektron hujjatning majburiy rekvizitlari quyidagilardan iborat:

– elektron raqamli imzo;

– elektron hujjatni jo‘natuvchi yuridik shaxsning nomi yoki elektron hujjatni jo‘natuvchi jismoniy shaxsning familiyasi, ismi, otasining ismi;

– elektron hujjatni jo‘natuvchining pochta va elektron manzili;

– hujjat yaratilgan sana.

Qonun hujjatlarida yoki elektron hujjat aylanishi ishtirokchilarining kelishuvi bilan elektron hujjatning boshqa rekvizitlari ham belgilanishi mumkin.

Elektron hujjat qog‘oz hujjatga tenglashtiriladi va u bilan teng yuridik kuchga ega bo‘ladi.

**Elektron hujjat almashish.** Bunda hujjat elektron ko‘rinishda kompyuter, telekommunikatsiya va Internet tarmog‘i orqali uzatiladi. Elektron hujjatlarni almashish jarayonida maxsus ixtisoslashtirilgan tizimlardan (masalan, E-hujjat) yoki elektron pochta xizmatidan foydalaniladi.

Elektron hujjat almashish tizimlari – elektron hujjatlarni axborot tizimlari orqali jo‘natish va qabul qilish jarayonlari yig‘indisidir. Elektron hujjat aylanishidan bitimlar (shu jumladan, shartnomalar) tuzish, hisob-kitoblarni, rasmiy va norasmiy yozishmalarni amalga oshirish hamda boshqa axborotlarni almashishda foydalanish mumkin.

**Elektron raqamli imzo.** Elektron raqamli imzo (ERI) O‘zbekiston Respublikasining «Elektron raqamli imzo to‘g‘risida» 2003-yil 11-dekabrdagi 562-II-son qonuniga[1] binoan quyidagicha ta’riflanadi: «Elektron raqamli imzo — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo».

Qonunda talab etilgan shartlarga rioya etilgan taqdirda, elektron raqamli imzo qog‘oz hujjatga shaxsan qo‘yilgan imzo bilan bir xil ahamiyat, kuchga egadir. ERI manba va ma’lumotlar butligini tekshirish

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

hamda soxtalashtirishdan muhofazalash imkonini beradi. ERI kalitlari sertifikatlari ro‘yxatga olish markazlari tomonidan beriladi.

**Elektron kalitlar va sertifikatlar.** O‘zbekiston Respublikasining «Elektron raqamli imzo to‘g‘risida»gi qonunida quyidagi asosiy tushunchalarning ta’riflari keltirilgan:

«elektron raqamli imzoning yopiq kaliti – elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, faqat imzo qo‘yuvchi shaxsning o‘ziga ma’lum bo‘lgan va elektron hujjatda elektron raqamli imzoni yaratish uchun mo‘ljallangan belgilar ketma-ketligi;

elektron raqamli imzoning ochiq kaliti – elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzoning yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzoning haqiqiyligini tasdiqlash uchun mo‘ljallangan belgilar ketma-ketligi;

elektron raqamli imzoning haqiqiyligini tasdiqlash — elektron raqamli imzoning elektron raqamli imzo yopiq kalitining egasiga tegishliligi va elektron hujjatdagi axborotda xatolik yo‘qligi tekshirilgandagi ijobiy natija».

ERI kalitining sertifikati ERIning ochiq kaliti uning yopiq kalitiga mosligini tasdiqlaydigan va yopiq kalitning egasiga ro‘yxatga olish markazi tomonidan berilgan hujjatdan iborat bo‘ladi. Bu sertifikat elektron hujjat va qog‘oz hujjat shakllarida tayyorlanishi mumkin.

ERI kalitlari sertifikati, uning ochiq va yopiq kalitlari bilan ishlash, fayl va papkalarga ERI qo‘yish yoki ularni shifrlash, ERIni tekshirish, shifrlangan ma’lumotlarni ochish kabi amallarni bajarishda ko‘pgina maxsus dasturlar, jumladan, «**KriptoARM**» va «**PGP**» dasturlaridan foydalanish mumkin.

**KriptoARM** dasturi ixtiyoriy ko‘rinishdagi elektron hujjat aylanishida axborotni himoya qilish vazifalarini hal etish uchun mo‘ljallangan. Ushbu dastur foydalanuvchi uchun qulay grafik interfeysga ega bo‘lib, kriptografik amallarni bajarish, ma’lumotlarni shifrlash va shifrdan ochish, ma’lumotlarni imzolash va ERIning to‘g‘riligini tekshirish imkonini beradi. Dastur yordamida oddiy sertifikatlar bilan ishlashga oid masalalarni ham bajarish mumkin.

**PGP** (Pretty Good Privacy) dasturi F. Simmerman tomonidan yaratilgan bo‘lib, u ma’lumotlarni shifrlash va ularga ERI qo‘yishga mo‘ljallangan. Ushbu dastur yordamida elektron hujjatlarni ishonchli himoya qilish mumkin. Dastur ochiq kalit orqali shifrlashni amalga oshiradi. Har bir

foydalanuvchining ikkita: ochiq va yopiq kalitlari bo‘ladi. Ochiq kalit barchaga e’lon qilinadi. Yopiq kalit esa faqat sertifikat egasida bo‘lib, uni maxfiy saqlash kerak.

Misol uchun, **X** foydalanuvchi **Y** foydalanuvchiga xabarni shifrlab yubormoqchi bo‘lsa, u **Y** foydalanuvchining ochiq kalitidan foydalanib, xabarni shifrlaydi. **Y** foydalanuvchi esa, o‘zining yopiq kaliti bilan xabarni shifrdan chiqaradi.

***Nazorat uchun savollar***

- Kriptografiya nima?
- Kriptografiya rivojlanishining qanday bosqichlari mavjud?
- Zamonaviy kriptografiya qanaqa muammolarni hal etuvchi bilim sohasi hisoblanadi?
- Axborotlarni sodda shifrlashni qanday usullari bor?
- Sezarning shifrlash usuli qanday amalga oshiriladi?
- Kalit deganda nima tushuniladi?
- Simmetrik shifrlash qanday amalga oshiriladi?
- Simmetrik va asimmetrik kalit yordamida shifrlash qanday amalga oshiriladi?
- Raqamli sertifikatlar nima?
- Shifrlashga qanaqa talablar qo‘yiladi?
- Qaysi shifrlash algoritmlari keng tarqalgan?
- Elektron raqamli imzo nima maqsadda ishlatiladi?

# IV. AXBOROT XAVFSIZLIGINI TA’MINLASHNING APPARAT-DASTURIY VOSITALARI

## 4.1. Axborotni muhofaza qilishning asosiy va yordamchi apparat-dasturiy vositalari

Axborotni muhofaza qilishning apparat-dasturiy vositalari – bu axborotni muhofaza qilish funksiyalari (foydalanuvchilarni identifikatsiya va autentifikatsiya qilish, resurslardan foydalanishni cheklash, voqealarni qayd qilish, axborotni kriptografik berkitish va boshqalar)ni mustaqil yoki boshqa vositalar bilan birgalikda bajaradigan turli elektron qurilmalar va maxsus dasturlardir.

Axborotni muhofaza qilishning *apparat vositasi* – bu maxsus himoya qurilmasi yoki axborotni qayta ishlash texnik vositasining tarkibiga kiruvchi moslama.

Axborotlarni muhofaza qilishning asosiy apparat vositalariga quyidagilarni kiritish mumkin:

– foydalanuvchini identifikatsiyalovchi ma’lumotlarni kiritish qurilmalari (magnit va plastik kartalar, barmoq izlari va boshqalar);

– ma’lumotlarni shifrlovchi qurilmalar;

– ish stansiyalari va serverlarga noqonuniy ulanib olishga halaqit beruvchi qurilmalar (elektron qulflar va blokiratorlar).

Ma’lumotlarni muhofaza qilishning yordamchi apparat vositalariga quyidagilar misol bo‘la oladi:

– magnitli tashuvchilardagi ma’lumotlarni yo‘q qiluvchi qurilmalar;

– kompyuter vositalaridan foydalanuvchilarining noqonuniy harakatlari bo‘yicha xabardor qiluvchi (signalizatsiya beruvchi) qurilmalar va boshqalar.

Axborotlarni muhofaza qilishning *dasturiy vositalari* – bu axborot xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlardir.

Axborotlarni muhofaza qilishning dasturiy vositalari axborotlar xavfsizligini ta’minlashga mo‘ljallangan va kompyuter vositalarining dasturiy ta’minoti tarkibiga kiritilgan maxsus dasturlardan iborat.

Axborotlarni muhofaza qilishning asosiy dasturiy vositalariga quyidagilarni kiritish mumkin:

– kompyuter tizimlarida foydalanuvchilarni identifikatsiyalovchi va autentifikatsiyalovchi dasturlar;

– kompyuter tizimlari resurslaridan foydalanuvchilarning huquqlarini cheklovchi dasturlar;

– axborotlarni shifrlovchi dasturlar;

– axborot resurslarini (tizimli va amaliy dasturiy ta’minotni, ma’lumotlar bazalarini, ta’limning kompyuter tizimlarini va h.k.) noqonuniy o‘zgartirishlardan, foydalanishlardan va ko‘paytirishlardan himoyalovchi dasturlar.

Kompyuter viruslaridan va boshqa zararlovchi dasturlar ta’siridan himoyalanish kompyuter tizimlarida axborotlarni qayta ishlash jarayonini himoyalashning mustaqil yo‘nalishlaridan biri hisoblanadi. Ushbu xavfga yetarlicha baho bermaslik axborot tizimlarida foydalanuvchilarning axborotlari uchun jiddiy salbiy oqibatlarni keltirib chiqarishi mumkin.

Yuqorida ta’kidlanganidek, axborot himoya tizimi – bu chora-tadbirlar kompleksi bo‘lib, ular mos ravishda vositalar va usullar majmuini tashkil etadi. Axborot xavfsizligi tizimining apparat - dasturiy tashkil etuvchisi (komponeti) turli axborot tizimlarining kompyuter va lokal tarmoq serverlarida saqlanuvchi va qayta ishlanuvchi ma’lumotlarni himoya qilish uchun mo‘ljallangan. Odatda u quyidagi jarayonlar bilan uzviy bog‘liqlikda amalga oshiriladi:

– ruxsat etishni hamda ruxsat etish siyosatini boshqarish;

– foydalanuvchilarni identifikatsiya va autentifikatsiya qilish;

– hodisalarni ro‘yxatga olishi va audit qilish;

– kriptografik himoya;

– tarmoq himoyasi;

– virusga qarshi himoya;

– dasturiy vositalar orqali hujumlarni aniqlash.

Ruxsat etishni boshqarish vositalari foydalanuvchilar tomonidan axborot ustida amalga oshiriladigan harakatlarni chegaralash va nazorat qilish imkonini beradi. Bularga tizimga kirish uchun ruxsatni chegaralash, mualliflangan foydalanuvchi ruxsatini chegaralash kabilarni kiritish mumkin. Ushbu jarayonda ruxsat etishni boshqarish dasturiy vositalar orqali amalga oshiriladi. Ruxsat etish huquqlarini nazorat qilish dastur muhitining turli tashkil etuvchilari – tarmoq operatsion tizimining yadrosi, ma’lumotlar bazasini boshqarish tizimi, qo‘shimcha dasturiy ta’minot va boshqalar tomonidan amalga oshiriladi.

Identifikatsiya foydalanuvchining o‘z nomini xabar yuborish orqali o‘zini identifikatsiya qilishiga imkon yaratish uchun mo‘ljallangan. Autentifikatsiya yordamida esa ikkinchi tomon tizimga kirishga harakat qilayotgan foydalanuvchining haqiqatan ham o‘zi ekanligiga ishonch hosil qiladi.

Hodisalarni ro‘yxatga olish (protokollashtirish, jurnallashtirish) – bu tizimda ro‘y berayotgan hodisalar haqida axborotlarni yig‘ish va jamlash jarayonidir. Hodisalarni ikki guruhga bo‘lish mumkin:

1. Tashqi hodisalar: mualliflangan va mualliflanmagan foydalanuvchilar harakatlari orqali yuzaga keluvchi;

2. Ichki hodisalar: foydalanuvchilar va adminstratorlar harakatlari orqali yuzaga keluvchi.

Audit – bu hodisalarni jurnallashtirish natijasida jamlangan axborotlarni tahlil qilish jarayonidir. Bunday tahlil real vaqtda yoki davriy tarzda tezkor amalga oshirilishi mumkin.

Tarmoq himoyasi odatda, tarmoq chegaralariga ekran deb nomlanuvchi qurilmalarni o‘rnatish orqali amalga oshiriladi. Ekran bir tarmoqdagi foydalanuvchilarga boshqa tarmoqqa tegishli resurslardan foydalanish uchun ruxsatni chegaralash vositasi hisoblanadi. Ikki tizim orasidagi barcha axborot oqimini nazorat qilish ekranning vazifasiga kiradi. Bunga misol tariqasida tarmoq ekranini keltirish mumkin. U biror tashkilotga tegishli, internetga chiqish imkoniga ega bo‘lgan lokal tarmoqni himoya qilish uchun o‘rnatiladi.

Bugungi kunda axborot xavfsizligini ta’minlovchi apparat-dasturiy vositalarni ishlab chiqaruvchilarning deyarli barchasi virusga qarshi himoyani hamda zararlantiruvchi dasturiy vositalar hujumini aniqlovchi va ulardan himoyalovchi tizimlarni inobatga oladi. Bunga misol tariqasida D-Link tarmoqlararo ekran qurilmasini keltirish mumkin (17-rasm). U zararlovchi dasturlarni va trafikni tekshirish imkonini beradi.

**17-rasm.** *SOH tarmoqlari uchun DFL-260E – tarmoqlararo ekrani.*

Umuman olganda axborot xavfsizligi tizimining apparat-dasturiy vositalari haqida fikr yuritganda, lokal tarmoqdagi obyektlarni ochiq tarmoqlar (internet) ta’siridan yuqori samarali himoya qilish usuli – bu ular

orasida oqib yuruvchi tarmoq paketlarini nazorat qiluvchi va filtrlovchi qurilmani belgilangan qoidalarga mos ravishda o‘rnatishga alohida e’tibor beriladi. Bunday qurilma – **tarmoqlararo ekran** deb nomlanib, u yana **fayrvoll** (inglizcha firewall) yoki **brandmauer** (nemis tilida brandmauer) deb ham ataladi.

**Ekran** yoki **tarmoqlararo ekran** – apparat va dasturiy vositalar majmui bo‘lib, o‘zidan o‘tkazuvchi tarmoq paketlarini belgilangan qoidalar asosida turli protokollar bo‘yicha nazorat qiladi va filtrlaydi.

**Tarmoqlararo ekranning** asosiy vazifasi kompyuter tarmoqlarini noqonuniy ruxsat etishlardan himoya qilishdir. Ba’zida ularni **filtrlar** deb ham atashadi. Chunki ular belgilangan tuzilishga (konfiguratsiyaga) va mezonlarga mos kelmaydigan paketlarni o‘tkazmaslik (filtrlash) vazifasini bajaradi.

Yaqin vaqtlarga qadar ko‘plab kompyuter foydalanuvchilari Internetda ishlaganda yoki boshqa tarmoqlardan foydalanganda o‘z kompyuterlari viruslar bilan «kasallanishi» mumkinligi haqida tushunchalarga ega bo‘lmaganlar. Bugungi kunda esa deyarli barcha internetdan foydalanuvchilar o‘z kompyuterlariga ta’sir etishi mumkin bo‘lgan xavflarni biladilar hamda har qanday virus va hujumlardan himoyalanish zarurligini tushunadilar.

Zamonaviy IT-bozori xavfsizlikni ta’minlovchi qurilmalarning turli variantlarini taklif qilmoqda. Umuman olganda, alohida holda kompyuterlar antivirus dasturlari va tarmoqlararo ekranlar (brandmauerlar, fayrvollar) yordamida muvaffaqiyatli himoya qilinadi. Kompyuter tarmoqlarini himoya qilish esa murakkabroq bo‘lib, bunda alohida dastur ta’minoti bilan himoyani ta’minlab bo‘lmaydi. Kompyuter tarmoqlarida axborot xavfsizligini ta’minlash uchun tarmoq chegaralariga tarmoqlararo ekranlarni o‘rnatish talab etiladi.

Tarmoqlararo ekranlarning asosiy vazifasiga tashqi tarmoqlar orqali g‘arazgo‘y kimsalarning axborotni o‘zgartirish, tarqatish yoki o‘chirish maqsadida kompterga hujum qilishidan himoya qilish kiradi. Kerakli konfiguratsiyaga ega bo‘lgan tarmoqlararo ekranni tashqi tarmoq chegarasiga o‘rnatish orqali o‘z kompyuteringiz tashqaridan “ko‘rinmas” holga o‘tishiga ishonch hosil qilish mumkin. Zamonaviy tarmoqlararo ekranlar “ruxsat etilmagan barcha amallar taqiqlanadi” tamoyili asosida ishlaydi, ya’ni foydalanuvchi qaysi protokollarga yoki dasturlarga ichki tarmoqqa ruxsat berishni o‘zi hal qiladi. Tarmoqlararo ekranlar himoya vazifasidan tashqari tarmoq ilovalarining me’yorda ishlashini ham ta’minlaydi.

Albatta, tarmoqlararo ekran kompyuter olamida barcha ofatlardan saqlashni kafolatlay olmaydi. Bunda shuningdek, har doim “inson mezo-

ni”ni e’tiborga olish lozim. Chunki aynan u bilmagan holda (ba’zan esa maqsadli ravishda) xavfsizlik siyosatini buzuvchi harakatlarni qilish orqali axborot tizimiga zarar keltirishi mumkin. Bunday harakatlarga tashqi axborot tashuvchilarni ulash orqali axborotni chiqib ketishi, himoyalanmagan qo‘shimcha internet-ulanishlarni o‘rnatish, qonuniy foydalanuvchi tomonidan axborotni maqsadli ravishda o‘zgartirish kabilarni kiritish mumkin.

## 4.2. Kompyuter tizimlaridan foydalanish huquqini cheklash

Axborot xavfsizligini ta’minlashning asosiy tamoyillarini axborot tizimlaridagi turli aloqa va xavfsizlikni ta’minlovchi nimtizimlar, umumiy texnik vositalar, aloqa kanallari, dasturiy ta’minot va ma’lumotlar bazalariga ega yagona tizim integratsiyasiga asoslangan kompleks yondashuv tashkil etadi.

**Axborot tizimi** keng ma’noda olib qaralganda, tizimdan foydalanuvchilarni kerakli axborot bilan ta’minlash uchun zarur bo‘lgan texnik, dasturiy va tashkiliy ta’minot hamda xizmat ko‘rsatish xodimlarining yig‘indisi hisoblanadi.

**Axborot xavfsizligi** – saqlanuvchi axborotning salbiy ta’sirlardan himoyalanganlik holatidir.

**Tarmoq xavfsizligi** – tashkilot yoki korxonaning kompyuter tarmog‘i infratuzilmasiga hamda undan foydalanishda tarmoq resurslarini ruxsatsiz foydalanishdan himoyalash bo‘yicha qo‘yiluvchi talablar majmuidir.

**Tarmoq xavfsizligi** deganda obyektning axborot infrastrukturasini (autentifikatsiyalash, mualliflash, tarmoqlararo ekran, ruxsatsiz kirishga harakatlarni aniqlash tizimlari IDS/IPS (Intrusion Detection/Prevention System – yorib kirishlarning aniqlash/oldini olish tizimlari) va boshqa usullar yordamida), tashqaridan g‘arazgo‘y kimsalarning kirishidan hamda tasodifiy xatolardan (DLP texnologiyasi vositasida), shuningdek ruxsatga ega bo‘lgan xizmat ko‘rsatuvchi xodimlarning maqsadli harakatlaridan himoya qilish tushuniladi. DLP (Data Leak Prevention) texnologiyasi – bu axborot tizimidagi konfedensial axborotlarni ruxsatsiz chiqib ketishidan dasturiy yoki dasturiy-qurilmaviy vositalarni qo‘llash orqali himoya qilishning zamonaviy texnologiyasidir. Bunda chiqib ketish kanallari tarmoqli (masalan, elektron pochta) yoki lokal (tashqi axborot yig‘uvchilardan foydalanib) bo‘lishi mumkin.

**Autentifikatsiya –** foydalanuvchining axborot tizimiga kirishi uchun ruxsat berilishida, uning identifikatsiya ma’lumotlarini tekshirish jarayoni.

**Mualliflash (Avtorizatsiya)** – biror foydalanuvchiga ma’lum bir harakatlarni bajarish uchun huquq berish. Mualliflash autentifikatsiyadan keyin amalga oshiriladi va foydalanuvchining qaysi resurslarga ruxsati borligini aniqlashda identifikatordan foydalaniladi. Axborot texnologiyalarida mualliflash yordamida axborot resurslari va qayta ishlash tizimlaridan foydalanishga ruxsat huquqi aniqlanadi va amalga oshiriladi.

Axborotni uzatish va qayta ishlashda **autentlik** – bu axborotning butunligi bo‘lib, u ma’lumotlar haqiqatan ham qonuniy foydalanuvchilar tomonidan hosil qilinganligini hamda mualliflikdan bosh tortish imkoniyati yo‘qligini tasdiqlaydi.

Axborotni himoya qilish – bu himoyalangan axborotni chiqib ketishi, unga noqonuniy va tasodifiy ta’sir ko‘rsatishning oldini olishga yo‘naltirilgan faoliyatdir.

Kompleks xavfsizlik – vujudga kelishi mumkin bo‘lgan barcha turdagi tahdidlar (noqonuniy foydalanish, ma’lumotlarni tutib olish, terrorizm, yong‘in, tabiiy ofatlar va h.k.)ni majburiy hisobga olib, zamon va makon (faoliyatning barcha texnologik sikllari) bo‘yicha xavfsizlikni ta’minlashning majburiy bo‘lgan uzluksiz jarayonini nazarda tutadi.

Kompleks yondashuv qanday shaklda qo‘llanilishidan qat’iy nazar, u murakkab va turli yo‘nalishdagi xususiy masalalarni, ularning o‘zaro chambarchas bog‘liqlikdagi yechimi bilan hal etiladi. Bunday masalalarning eng dolzarblari bo‘lib, axborotlardan foydalanishni cheklash, axborotlarni texnik va kriptografik himoyalash, texnik vositalarning yondosh nurlanishlari darajasini kamaytirish, obyektlarning texnik mustahkamlanganligi, ularning qo‘riqlash va tahlikadan xabardor qilish (signalizatsiya) qurilmalari bilan jihozlanganligi hisoblanadi.

Foydalanuvchilar, operatorlar, administratorlarga qurilmadan foydalanishga ruxsat berishni tashkil etishda quyidagi harakatlar amalga oshiriladi:

- ruxsat olayotgan subyektni identifikatsiyalash va autentifikasiyalash;
- qurilmani blokirovkadan chiqarish;
- ruxsat berilgan subyektning harakatlarini hisobga olish jurnalini yuritish.

Ruxsat etilgan subyektni identifikatsiyalash uchun kompyuter tizimlarida ko‘p hollarda atributivli identifikatorlardan foydalaniladi. Biometrik identifikatsiyalashning oson yo‘li – klaviaturada ishlash ritmi orqali aniqlashdir. Atributivli indentifikatorlar ichidan, odatda, quyidagilaridan foydalaniladi:

- parollar;

- yechib olinadigan axborot tashuvchilar;
- elektron jetonlar;
- plastik kartochkalar;
- mexanik kalitlar.

Konfidensial ma’lumotlar bilan ishlaydigan deyarli barcha kompyuterlarda foydalanuvchilarni autentifikatsiyalash parollar yordamida amalga oshiriladi.

Parol – bu simvollar (harflar, raqamlar, maxsus belgilar) kombinatsiyasi bo‘lib, uni faqat parol egasi bilishi kerak. Ayrim hollarda xavfsizlik tizimi ma’muriga ham ma’lum bo‘ladi.

Kompyuterning zamonaviy operatsion tizimlarida paroldan foydalanish o‘rnatilgan. Parol avtonom tok manbaiga ega bo‘lgan maxsus xotirada saqlanadi. Parollarni taqqoslash operatsion tizim (OT) yuklangunga qadar amalga oshiriladi. Agar buzg‘unchi parol saqlanayotgan xotiraning avtonom tok manbaini o‘chirib qo‘ya olmaganida, ushbu turdagi himoya juda samarali hisoblanar edi. Lekin, kompyuterning OT yuklanishini amalga oshirish uchun kiritiladigan foydalanuvchi parolidan tashqari, Internetda ro‘yxati keltirilgan ayrim “texnologik” parollardan ham foydalanish mumkin.

Ko‘pgina kompyuter tizimlarida identifikator sifatida, foydalanishga ruxsat etilgan subyektni identifikatsiyalovchi kod yozilgan *yechib olinuvchi axborot tashuvchilardan* foydalaniladi.

Foydalanuvchilarni identifikatsiyalashda, tasodifiy identifikasiyalash kodlarini hosil qiluvchi – elektron jetonlardan keng foydalaniladi. Jeton – bu, harflar va raqamlarning tasodifiy ketma-ketligini (so‘zni) yaratuvchi qurilma. Bu so‘z kompyuter tizimidagi xuddi shunday so‘z bilan taxminan minutiga bir marta sinxron tarzda o‘zgartirib turiladi. Natijada, faqatgina ma’lum vaqt oralig‘ida va tizimga faqatgina bir marta kirish uchun foydalanishga yaraydigan, bir martalik parol ishlab chiqariladi. Boshqa bir turdagi jeton tashqi ko‘rinishiga ko‘ra kalkulyatorga o‘xshab ketadi. Autentifikatsiyalash jarayonida kompyuter tizimi foydalanuvchi monitoriga raqamli ketma-ketlikdan iborat so‘rov chiqaradi, foydalanuvchi ushbu so‘rovni jeton tugmalari orqali kiritadi. Bunda jeton o‘z indikatorida akslanadigan javob ketma-ketligini ishlab chiqadi va foydalanuvchi ushbu ketma-ketlikni kompyuter tizimiga kiritadi. Natijada, yana bir bor bir martalik qaytarilmaydigan parol olinadi. Jetonsiz tizimga kirishning im-

koni bo‘lmaydi. Jetondan foylanishdan avval unga foydalanuvchi o‘zining shaxsiy parolini kiritishi lozim.

Autentifikatsiyalash jarayoni kompyuter tizimlari bilan ruxsat etilgan subyekt orasida amalga oshiriladigan muloqotni ham o‘z ichiga olishi mumkin. Ruxsat etilgan subyektga bir qator savollar beriladi, olingan javoblar tahlil qilinadi va ruxsat etilgan subyektning aslligi bo‘yicha yakuniy xulosa qilinadi.

Kompyuter tizimlari qurilmalaridan foydalanishga ruxsatni masofadan turib boshqarish mumkin. Masalan, lokal tarmoqlarda ishchi stansiyaning tarmoqqa ulanishini administrator ish joyidan turib blokirovka qilishi mumkin. Qurilmalardan foydalanishga ruxsat etishni tok manbaini uzib qo‘yish orqali ham samarali boshqarish mumkin. Bunda ishdan boshqa vaqtlarda, tok manbai qo‘riqlash xizmati tomonidan nazorat qilinadigan kommutatsiyali qurilmalar yordamida uzib qo‘yiladi.

Xizmat ko‘rsatuvchi xodimning qurilmadan foydalanishiga ruxsat etishni tashkil etish foydalanuvchiga berilgan ruxsatdan farqlanadi. Eng avvalo, qurilma konfidensial ma’lumotlardan tozalanadi hamda axborot almashinish imkonini beruvchi aloqalar uziladi. Qurilmaga texnik xizmat ko‘rsatish va uning ish qobiliyatini tiklash mansabdor shaxs nazorati ostida amalga oshiriladi. Bunda ichki montaj va bloklarni almashtirishga bog‘liq ishlarni amalga oshirilishiga jiddiy e’tibor beriladi.

## 4.3. Zararlantiruvchi dasturiy ta’minot

Zararlantiruvchi dasturiy ta’minot, avvalo kompyuter viruslari axborot tizimiga jiddiy xavfni yuzaga keltiradi. Bu xavfni mensimaslik foydalanuvchi axboroti uchun jiddiy oqibatlarni keltirib chiqarishi mumkin. O‘z vaqtida kompyuter viruslari tahdidlariga o‘ta yuqori e’tibor qaratish ham axborot tarmog‘ining imkoniyatlaridan to‘liq foydalanishga salbiy ta’sir ko‘rsatadi. Zararlantiruvchi dasturiy ta’minot ta’siri mexanizmlari hamda ularga qarshi kurashish usul va vositalarini bilish, ularning kompyuter va axborotlarga zarar yetkazishiga qarshi kurashni samarali tashkil etishga imkon yaratadi.

Axborot tizimida zararlantiruvchi dastur ta’minoti mavjudligini foydalanuvchi quyidagi belgilar orqali bilib olishi mumkin:

– ekranda zararlanganlik yoki zararlanish ehtimoli mavjudligi haqida antivirus vositalarining xabarlari paydo bo‘lishi, antivirus vositalarining o‘z-o‘zidan ishlamay qolishi;

– monitor yoki printerga uzatiluvchi xabarlar, tovush effektlari, dasturlarning tasodifan ishga tushib ketishi, fayllarning o‘chirib yuborilishi kabi tizimda virus mavjudligini bildiruvchi belgilar;

– kompyuter tizimining qurilma va dasturiy ta’minotidagi ishdan chiqishlar, u yoki bu ma’lumotni qayta ishlash vaqtining cho‘zilib ketishi, disklardagi bo‘sh joylarning asossiz kamayib ketishi, skaner-dasturlar tomonidan virusni skaner qilishni rad etilishi, tizimning “osilib qolish”i va boshqalar;

– foydalanuvchi tomonidan elektron pochta orqali yuborilmagan xabarlarning tarqatilishi.

**Zararlantiruvchi dastur** (Malware, malicious software – g‘arazmaqsadli dasturiy ta’minot) – bu axborot tizimi resurslariga, mavjud qoidalarni chetlab o‘tish orqali, ruxsatsiz kirishni amalga oshirish yoki ta’sir ko‘rsatish uchun mo‘ljallangan har qanday dasturiy ta’minotdir.

Dasturiy ta’minotning zararliligi yoki foydaliligini ko‘p jihatdan foydalanuvchi tomonidan yoki uni qo‘llash usuli bilan belgilanadi. Zararlantiruvchi dasturlarning umume’tirof etilgan klassifikatsiyasi (toifalanishi) hozirgacha mavjud emas. Bu borada birinchi urinishlar o‘tgan asrning 90-yillarida CARO (Computer AntiVirus Researcher's Organization) antivirus mutaxassislari alyansi tomonidan amalga oshirilgan.

Biroq, vaqt o‘tishi bilan zararlantiruvchi dasturlarning shiddat bilan rivojlanib ketishi, yangi platformalarning yaratilishi hamda antivirus kompaniyalari sonining ortib borishi natijasida CARO tizimi ishlamay qo‘ydi. Uning ishlamay qolishiga yanada ko‘proq ta’sir qilgan sabab, bu turli antivirus kompaniyalarining detektorlash tizimi texnologiyalari turlicha bo‘lib, buning natijasida turli antivirus dasturlarining tekshirish natijalarini yaqqol taqqoslashning imkoni bo‘lmay qoldi. Shunday bo‘lsada, ba’zan antivirus dasturlari tomonidan detektorlanuvchi obyektlarni yangi umumiy klassifikatsiyasini ishlab chiqishga harakatlar qilinmoqda. Bu borada so‘nggi e’tiborli loyiha CME (Common Malware Enumeration) standartining tuzilishi bo‘lib, uning mohiyati bir xil toifadagi detektorlanuvchi obyektlarga yagona identifikator berishdan iborat.

“Kasperskiy laboratoriyasi” kompaniyasi tomonidan taklif etilgan klassifikatsiyaga ko‘ra, undagi mutaxassislar zararlantiruvchi dasturiy ta’minotni zararlantiruvchi dasturlar (Malware) va eng keraksiz dasturlarga (PUPs, Potentially Unwanted Programs) ajratishni taklif etadilar. O‘z navbatida zararlantiruvchi dasturlarga quyidagilar kiradi: kompyuter

virusi va qurtlar, troyan dasturlari, shubhali tahlovchilar (upakovkalovchilar) va zararlantiruvchi utilitlar.

***Kompyuter viruslari va qurtlar.*** “Kompyuter virusi” degan ibora bugungi kunda hech kimni ajablantirmaydi. Bu tushuncha o‘tgan asrning 80-yillarida paydo bo‘lib, zararlantiruvchi dasturlar biologik viruslarga xos bo‘lgan belgilarga ega bo‘lganligi sababli shunday nomlangan. Ular kompyuter tizimiga tezkor va sezdirmay kirib borib, tez tarqalish, ko‘payish, zararlash hamda tizim faoliyatiga salbiy ta’sir ko‘rsatish xususiyatiga ega. Axborot tizimlari bilan ishlashda “virus” atamasi bilan birga “zararlanish”, “tarqalish muhiti”, “profilaktika” kabi tushunchalardan ham foydalaniladi.

**Kompyuter virusi** – bu kompyuter yoki kompyuter tizimida foydalanuvchiga bo‘ysunmagan holda tarqalish va o‘z-o‘zidan ko‘payish xususiyatiga ega bo‘lgan kichik o‘lchamli bajariluvchi yoki interpretatsiyalanuvchi dasturlardir. Ulardan olingan nusxalar ham shunday xususiyatlarga ega bo‘ladi. Viruslar axborot saqlanuvchi obyektda yoki kompyuter tarmog‘i qurilmalarida saqlanuvchi ma’lumotlarni o‘zgartirish yoki yo‘q qilib yuborishga mo‘ljallanishi mumkin. Viruslar tarqalish jarayonida o‘zini modifikatsiya qilishi mumkin.

**Qurtlar** viruslarga xos xususiyatlarga ega bo‘lib, ular boshqa fayllarga zarar yetkazmagan holda o‘z-o‘zidan ko‘payishi mumkin. U bir kompyuterga kirib olgach, boshqa kompyuterlarga tarqalish yo‘llarini qidiradi. Qurt – bu alohida fayl, virus esa mavjud fayllarga kiritiluvchi kod.

Kompyuter virusi va qurtlar toifasiga quyidagilar kiradi:

**Virus** (virus) – kompyuterning lokal resurslari bo‘yicha foydalanuvchi ixtiyoridan tashqari noqonuniy ravishda o‘z-o‘zidan ko‘payish xususiyatiga ega bo‘lgan zararlantiruvchi dastur. Qurtlardan farqli ravishda viruslar boshqa kompyuterlarga tarqalish va kirishi uchun tarmoq servislaridan foydalanmaydilar. Virus nusxasi boshqa kompyuterga faqatgina zararlangan obyektning o‘sha kompyuterda faollashtirilishi tufayli o‘tishi mumkin. Masalan:

- virus tarmoq resursida joylashgan faylga kirib olganda;
- virus axborot tashuvchiga o‘z nusxasini ko‘chirib, undagi fayllarni zararlaganda;
- foydalanuvchi virus bilan zararlangan ilovani elektron pochta orqali yuborganda.

**Worm** (qurt) – kompyuter tarmoqlarida, uning resurslari orqali foydalanuvchi ixtiyoridan tashqari noqonuniy ravishda o‘z-o‘zidan ko‘payish xususiyatiga ega bo‘lgan zararlovchi dastur. Qurtni faollash-

tirish uchun foydalanuvchi uni ishga tushirishi kerak. Bunday toifadagi qurtlar tarmoqda o‘qish va yozish uchun ruxsati bo‘lgan tarmoq katalogiga ega kompyuterlarni qidirib, ularga o‘zining nusxasini ko‘chiradi.

**Net-Worm** (tarmoq qurti) – kompyuter tarmoqlarida foydalanuvchi ixtiyoridan tashqari noqonuniy ravishda o‘z-o‘zidan ko‘payish xususiyatiga ega bo‘lgan zararlovchi dastur.

**Troyan dasturlari.** Bunday zararlovchi dasturlar tashqaridan qaraganda qonuniy dasturiy mahsulot ko‘rinishida bo‘lib, ishga tushirilganda ma’lumotlarni yo‘q qilishga, blokirovka qilishga, modifikatsiya yoki axborotdan nusxa olishga, kompyuter yoki kompyuter tarmog‘i faoliyatini ishdan chiqarishga yo‘naltirilgan noqonuniy harakatlarni amalga oshiradi. Virus va qurtlardan farqli ravishda, bunday toifadagi zararlovchi dasturlar o‘zlarining nusxasini yaratish imkoniga ega emas.

**Backdoor** (bekdor) – zararlangan kompyuterni g‘arazgo‘y kimsa tomonidan yashirin tarzda boshqarish uchun mo‘ljallangan zararlovchi dastur. Bunday zararlovchi dasturlar kompyuterda muallif tomonidan qo‘yilgan barcha vazifalarni: fayllarni qabul qilish va yuborish, ularni ishga tushirish va yo‘q qilish, xabarlarni chiqarish, ma’lumotlarni o‘chirish, kompyuterni qayta ishga tushirish kabilarni bajarish imkonini beradi.

**Exploit** (eksployt) – oldindan g‘arazli maqsadni ko‘zlovchi, lokal yoki tarmoqqa ulangan kompyuterdagi dasturiy ta’minotning zaif joylaridan foydalanish imkonini beruvchi, ma’lumotlar yoki bajariluvchi kodlarga ega bo‘lgan dasturlar. Odatda, eksploytlar g‘arazgo‘y kimsalar tomonidan kompyuterga kirish va keyinchalik unga zararlovchi kodlarni yuborish maqsadida foydalaniladi (masalan, sindirilgan Web-saytga kiruvchi barcha foydalanuvchilarni zararlash).

**Rootkit –** tizimdagi alohida obyektlarni ochish yoki faollashtirish uchun mo‘ljallangan dastur. Odatda, ular yordamida reyestr kalitlari, fayllar yoki zararlangan kompyuter xotirasidagi jarayonlar ochilishi mumkin. Rootkit o‘z-o‘zidan hech qachon zarar keltirmaydi, biroq bu turdagi dasturlar aksariyat hollarda zararlantiruvchi dasturlar tomonidan o‘zining xususiy yashash vaqtini uzaytirish uchun foydalaniladi.

**Trojan –** noqonuniy harakatlarni amalga oshirish orqali ma’lumotlarni yo‘q qilishga, blokirovka qilishga, modifikatsiya yoki axborotdan nusxa olishga, shuningdek, kompyuter yoki kompyuter tarmog‘i faoliyatini ishdan chiqarishga mo‘ljallangan zararlovchi dastur. U o‘z toifasidagi boshqa dasturlarning birortasiga o‘xshamaydi.

Troyanlarga shuningdek, “ko‘pmaqsadli” troyan dasturlari ham kiradi. Ular bir vaqtning o‘zida bir nechta ruxsat etilmagan noqonuniy harakatlarni sodir etishga qodir bo‘lib, ularning birortasiga alohida yondashib bo‘lmaydi. Bir biridan farq qiluvchi harakatlarni amalga oshiradigan hamda “jabrlanuvchi”ga har xil ta’sir ko‘rsatuvchi troyan dasturlarning ko‘plab turlari mavjud. Ularga quyidagilarni kiritish mumkin:

*Trojan-Banker* – foydalanuvchining bank tizimlariga, elektron mablag‘larga va plastik kartalariga taalluqli axborotlarni o‘g‘rilashga mo‘ljallangan.

*Trojan-Dropper* – foydalanuvchining kompyuteriga noqonuniy tarzda zararlovchi dasturlarni yashirin ravishda installyatsiya qilishga mo‘ljallangan.

*Trojan-Proxy* – noqonuniy tarzda foydalanuvchining kompyuteri orqali anonim ravishda turli internet resurslariga ruxsat berishni amalga oshirish uchun mo‘ljallangan.

*Trojan-Clicker* – noqonuniy foydalanuvchi tomonidan Internet-resurslariga murojaatni amalga oshirish uchun mo‘ljallangan (odatda Web-sahifalarga).

*Trojan-PSW* (Password-Stealing-Ware) – zararlangan kompyuterdan foydalanuvchining akkauntlari (login va parol)ni o‘g‘rilash uchun mo‘ljallangan.

*Trojan-DDoS* – noqonuniy foydalanuvchi tomonidan zararlangan kompyuter orqali oldindan aniqlangan manzilga DoS-hujum uyushtirish uchun mo‘ljallangan.

*Trojan-Downloader* – noqonuniy foydalanuvchi tomonidan zararlangan kompyuterga zararlovchi dasturlarning yangi versiyalarini o‘rnatish va ishga tushirish uchun mo‘ljallangan. Internetdan yuklangan dasturlar yoki ishga tushiriladi yoki operatsion tizim imkoniyatlariga mos ravishda avtomat tarzda yuklash uchun troyan dasturi tomonidan ro‘yxatga olinadi.

*Trojan-Spy* – foydalanuvchi ortidan elektron ayg‘oqchilik qilish uchun mo‘ljallangan. Olingan ma’lumotlar (klaviatura orqali kiritiluvchi ma’lumotlar, ekrandagi tasvirlar, faol ilovalar ro‘yxati va boshq.). g‘arazgo‘y kimsaga uzatib turiladi.

**Shubhali taxlovchilar**. Bunday turdagi zararlovchi dasturlar maxsus usul bilan taxlashni amalga oshirib, shifrlangan fayllarni keyinchalik qayta tiklashda evristik usullardan foydalanishni murakkablashtiradi.

**Zararlovchi utilitlar** – boshqa turdagi viruslarni, troyan yoki qurtlarni yaratishni avtomatlashtirish, serverga DoS-hujumlarni uyushti-

rish, kompyuterni ishdan chiqarish kabilarni amalga oshirish uchun ishlab chiqilgan zararlovchi dasturlardir. Virus, troyan yoki qurtlardan farqli ravishda bunday toifadagi dasturlar o‘zlari ish yurituvchi kompyuterlarga to‘g‘ridan-to‘g‘ri xavf tug‘dirmaydi. Ularni ajratib turuvchi asosiy jihati – bu ular tomonidan amalga oshiriladigan harakatlardir.

Bunday toifadagi dasturlarga quyidagilarni misol keltirish mumkin:

*Constructor* – yangi kompyuter viruslari, qurtlari va troyan dasturlarini tayyorlash uchun mo‘ljallangan dasturlar.

*HackTool* – noqonuniy foydalanuvchi tomonidan lokal kompyuter yoki tarmoqdagi kompyuterga hujumlar uyushtirish uchun foydalaniladigan dasturlar.

*Spoofer*– jo‘natuvchining qalbaki manzili orqali xabarlar va tarmoq so‘rovlarini yuborish imkonini beruvchi dasturlar.

*DoS* – kompyuterlarga DoS-hujumlarni uyushtirish uchun mo‘ljallangan dasturlar.

***Nazorat uchun savollar***

- Axborotlarni muhofaza qilishning asosiy va yordamchi apparat vositalariga nimalar kiradi?
- Axborotlarni muhofaza qilishning dasturiy vositalari qanday dasturlardan iborat?
- Axborotlarni muhofaza qilishning dasturiy vositalarining afzalliklari va kamchiliklari nimalardan iborat?
- Kompyuter tizimlaridan foydalanish huquqini cheklashning qanday usul va vositalari mavjud?
- Kompleks xavfsizlik nimalardan iborat?
- Qanday atributivli indentifikatorlarni bilasiz va ular qanday tartibda ishlaydi?
- Autentifikatsiyalash qanday amalga oshiriladi?
- Zararlantiruvchi dastur deb nimaga aytiladi?
- Axborot tizimida zararlantiruvchi dastur mavjudligi qanday aniqlanadi?
- Kompyuter viruslari nima?
- Kompyuter qurtlari nima?
- Troyan dasturlari qanday vazifalarni bajaradi?
- Troyan dasturlarning qanday turlarini bilasiz?
- Zararlovchi utilitlardan nima maqsadda foydalaniladi?

# V. O‘ZBEKISTON RESPUBLIKASIDA AXBOROTNI MUHOFAZA QILISHNING DAVLAT TIZIMI

## 5.1. Axborotni muhofaza qilishning davlat tizimi

Ma’lumki, yurtimizda axborot xavfsizligi sohasidagi munosabatlarni tartibga solish borasida 1992-yil 8-dekabrda qabul qilingan O‘zbekiston Respublikasi Konstitutsiyasi asosiy qonun hisoblanadi. Konstitutsiyamizning 29-moddasiga binoan: “Har kim fikrlash, so‘z va e’tiqod erkinligi huquqiga ega. Har kim o‘zi istagan axborotni izlash, olish va uni tarqatish huquqiga ega, amaldagi konstitutsiyaviy tuzumga qarshi qaratilgan axborot va qonun bilan belgilangan boshqa cheklashlar bundan mustasnodir.”

Axborot xavfsizligi tizimi har qanday davlatning axborot sohasidagi siyosatini milliy xavfsizlikni ta’minlash borasidagi davlat siyosati bilan chambarchas bog‘laydi. Bunda axborot xavfsizligi tizimi davlat siyosatining asosiy tashkil etuvchilarini yaxlit bir butunlikka birlashtiradi. Bu esa axborot xavfsizligining roli va uning mamlakat milliy xavfsizligi tizimidagi mavqeini belgilaydi. Axborot sohasidagi O‘zbekistonning milliy manfaatlarini, ularga erishishining strategik yo‘nalishlarini va ularni amalga oshirish tizimlarini o‘zida aks ettiruvchi maqsadlar yaxlitligi davlat axborot siyosatini anglatadi.

Axborot xavfsizligi sohasida davlat siyosatini amalga oshirishga imkon beruvchi sharoitlarni yaratish, mamlakatni iqtisodiy va ilmiy-texnik taraqqiyotiga ko‘maklashish, axborotni muhofaza qilishning usul va vositalarini yaratish bugungi kunning dolzarb masalalaridan biridir.

Axborotni muhofaza qilishning davlat tizimi axborotni himoyalovchi texnikani qo‘llaydigan idoralar va ijro etuvchilar hamda himoya obyektlari majmuini ifodalaydi. Bu tizim axborotni muhofaza qilish sohasidagi huquqiy, tashkiliy-boshqaruv va normativ hujjatlarga muvofiq tashkil etiladi va faoliyat yuritadi. Shu bilan birga mamlakat milliy xavfsizligini ta’minlash tizimining tarkibiy qismi hisoblanadi va davlat xavfsizligini axborot sohasidagi ichki va tashqi tahdidlardan himoyalashga yo‘naltirilgan.

***Axborotni muhofaza qilishning davlat tizimi*** axborotni muhofaza qilish sohasida tashkilotlar faoliyatini litsenziyalash nimtizimini, axborotni muhofaza qilish vositalarini sertifikatsiyasini va axborot xavfsizligi talablari bo‘yicha axborotlashtirish obyektlarini attestatsiyasini o‘z ichiga oluvchi murakkab tizimdir.

Axborotni muhofaza qilishning davlat tizimi faoliyati quyidagi qonunlar va normativ-huquqiy hujjatlar asosida amalga oshiriladi:

- O‘zbekiston Respublikasining Konstitutsiyasi;
- «Davlat sirlarini saqlash to‘g‘risida»gi qonun;
- «Axborotlashtirish to‘g‘risida»gi qonun;
- «Mahsulotlar va xizmatlarni sertifikatlashtirish to‘g‘risida»gi qonun;
- «Faoliyatning ayrim turlarini litsenziyalash to‘g‘risida»gi qonun;
- «Standartlashtirish to‘g‘risida»gi qonun;
- «Aloqa to‘g‘risida»gi qonun;
- «Telekommunikatsiyalar to‘g‘risida»gi qonun;
- «Axborot olish kafolatlari va erkinligi to‘g‘risida»gi qonun;
- «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»gi qonun;
- «Elektron hujjat aylanishi to‘g‘risida»gi qonun;
- «Elektron raqamli imzo to‘g‘risida»gi qonun;
- «Elektron tijorat to‘g‘risida»gi qonun;
- “Elektron hukumat to‘g‘risida”gi qonun;
- O‘zbekiston Respublikasi Prezidentining farmonlari va qarorlari;
- O‘zbekiston Respublikasi Vazirlar mahkamasining qarorlari;
- Axborotni muhofaza qilish sohasidagi vazirlik, muassasa, agentlik va xo‘jaliklarning boshqa huquqiy aktlari.

Davlat xavfsizligi sohasida davlat siyosatini amalga oshirishga imkon beruvchi sharoitlarni yaratish, mamlakatni iqtisodiy va ilmiy-texnik taraq-qiyotiga ko‘maklashish, axborotni muhofaza qilish usul va vositalarini qo‘llab, O‘zbekiston milliy xavfsizligiga bo‘lgan ziyonni jiddiy kamay-tirish – bularning barchasi axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsad bo‘lib, ularni amalga oshirish uchun quyidagi vazifalarni bajarish kerak:

– yagona texnik siyosatni o‘tkazish, harbiy, iqtisodiy, ilmiy-texnik va boshqa sohalar faoliyatlarida axborotni muhofaza qilish bo‘yicha ishlarni muvofiqlash va tashkil etish;

– razvedkaning texnik vositalar yordamida axborotni qo‘lga kiritishni jiddiy qiyinlashtirish yoki yo‘l qo‘ymaslik;

– axborotni muhofaza qilish sohasida munosabatlarni tartibga soluvchi huquqiy hujjatlarni qabul qilish;

– axborotni muhofaza qilish vositalarini yaratish va ularning samaradorligini nazorat qilish kuchlarini tashkil etish;

– davlat organlari va tashkilotlarida axborotni muhofaza qilish holatini nazorat qilish;

– axborotni muhofaza qilish sohasidagi davlat tizimi holatini tahlil qilish, asosiy muammolarni aniqlash;

– axborotni muhofaza qilishni davlat tizimining muhim yo‘nalishlarini aniqlash;

– axborotni muhofaza qilish bo‘yicha ishlarni normativ-metodik va axboriy ta’minlash.

O‘zbekiston Respublikasining Fuqarolik kodeksida bank, tijorat va sug‘urta sirlari tushunchalari hamda ularni himoya qilishning zaruriy choralari belgilab qo‘yilgan.

Axborot xavfsizligi borasida O‘zbekiston Respublikasining Jinoyat kodeksi muhim o‘rin egallaydi. Ushbu kodeksning “Axborot texnologiyalari sohasidagi jinoyatlar” deb nomlanuvchi XX[1] bobida axborot texnologiyalari sohasida sodir etiluvchi jinoyatlarga jazo belgilab qo‘yilgan.

Axborotlarni kriptografik himoyalash borasidagi masalalarni tartibga solish 2007-yil 3-apreldagi O‘zbekiston Respublikasi Prezidentining “O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-614 sonli qarorida[1] o‘z aksini topgangan bo‘lib, unga ko‘ra ushbu sohada O‘zbekiston Respublikasining Milliy xavfsizlik xizmati mas’ul organ hisoblanadi. Shuningdek, mazkur qaror bilan O‘zbekiston Respublikasida axborotni kriptografik himoyalash bo‘yicha Nizom hamda O‘zbekiston Respublikasida axborotni kriptografik himoyalash vositalarini sertifikatsiyalash Nizomlari tasdiqlangan.

O‘zbekiston Respublikasi Prezidentining 2013-yil 27-iyundagi “O‘zbekiston Respublikasi Milliy axborot-kommunikatsiya tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi qarorining qabul qilinishi mamlakatimizda axborot xavfsizligi masalalarini yechish borasida muhim tashkiliy qadam bo‘ldi.

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

O‘zbekiston Respublikasi Vazirlar Mahkamasining 2013-yil 16-sentyabrdagi 250-sonli qarori[1] bilan, O‘zbekistonda elektron hukumat tizimini yanada rivojlantirish maqsadida, maxsus markazlar – «Elektron hukumat tizimini rivojlantirish markazi» hamda «Axborot xavfsizligini ta’minlash markazi»ni tashkil etish belgilangan. Ushbu qaror bilan, «Elektron hukumat tizimini rivojlantirish» hamda «Axborot xavfsizligini ta’minlash markazi»ning tuzilmasi va faoliyati tartibini belgilovchi Nizom qabul qilingan. «Axborot xavfsizligini ta’minlash markazi»ning asosiy vazifalari biri etib qonun buzuvchilarni tahlil qilish, identifikatsiyalashda, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilishda huquqni muhofaza qilish organlari bilan hamkorlik qilish belgilangan.

O‘zbekiston Respublikasi Prezidentining 2015-yil 4-fevraldagi farmoniga asosan «O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi» tashkil etildi. Mazkur farmon bilan yurtimizda axborot xavfsizligini ta’minlash va kommunikatsiya tarmoqlari, dasturiy mahsulotlar, axborot tizimlari va resurslarini himoya qilishning zamonaviy texnologiyalarini tatbiq etish chora-tadbirlarini amalga oshirish, axborot resurslarini himoya qilish bo‘yicha texnik infratuzilmani yanada rivojlantirish kabi masalalar ushbu vazirlikning asosiy vazifalari hamda faoliyat yo‘nalishlari sifatida belgilab qo‘yildi.

Bugungi kunda mamlakatimizda axborot xavfsizligi sohasida yagona konseptual hujjatni yaratish zamon talabidir. Bunday hujjat axborot xavfsizligi sohasida normativ-huquqiy bazani takomillashtirish bo‘yicha ishlarni, ushbu sohada yagona standartni ishlab chiqish va joriy etish faoliyatini yo‘naltirishga, shuningdek, mazkur sohada kadrlar siyosatini rivojlantirishning zaruriy choralarini aniqlashga imkon yaratadi.

## 5.2. Axborot muhofaza qilish sohasida litsenziyalash va sertifikatsiyalash

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

O‘zbekiston Respublikasining 2000-yil 25-maydagi «Faoliyatning ayrim turlarini litsenziyalash to‘g‘risida»gi 71-II-sonli qonuni[1] turli faoliyat sohasida litsenziyalashni amalga oshirish bo‘yicha asosiy hujjat hisoblanadi.

Ushbu qonunning 3-moddasida quyidagi asosiy tushunchalar keltirilgan:

*litsenziya* – litsenziyalovchi organ tomonidan yuridik yoki jismoniy shaxsga berilgan, litsenziya talablari va shartlariga so‘zsiz rioya etilgani holda faoliyatning litsenziyalanayotgan turini amalga oshirish uchun ruxsatnoma (huquq);

*faoliyatning litsenziyalanayotgan turi* – O‘zbekiston Respublikasi hududida amalga oshirilishi uchun litsenziya olish talab qilinadigan faoliyat turi;

*litsenziyalash* – litsenziya berish to‘g‘risidagi arizani topshirish va ko‘rib chiqish, litsenziyaning amal qilishini to‘xtatib turish yoki tugatish, shuningdek uni bekor qilish va qayta rasmiylashtirish jarayoni bilan bog‘liq tadbirlar kompleksi;

*litsenziya talablari va shartlari* – faoliyatning litsenziyalanayotgan turini amalga oshirayotganda litsenziat tomonidan bajarilishi majburiy bo‘lgan, qonun hujjatlarida belgilangan talablar va shartlarning majmui;

*litsenziyalovchi organlar* – qonun hujjatlariga muvofiq litsenziyalashni amalga oshiruvchi maxsus vakolatli organlar;

*litsenziat* – faoliyatning litsenziyalanadigan turini amalga oshirish litsenziyasi bo‘lgan yuridik yoki jismoniy shaxs;

*litsenziyalar reyestri* – berilgan, to‘xtatib turilgan, qayta tiklangan, qayta rasmiylashtirilgan, bekor qilingan litsenziyalar, shuningdek amal qilishi tugatilgan litsenziyalar to‘g‘risidagi ma’lumotlarni o‘z ichiga olgan litsenziyalovchi organlarning ma’lumotlar bazalari majmui.

Litsenziyalash sohasini davlat tomonidan tartibga solishni ushbu qonunning 4-moddasiga ko‘ra O‘zbekiston Respublikasi Vazirlar Mahkamasi hamda litsenziyalovchi organlar amalga oshiradi.

---

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

*O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilish (AKMQ) sohasida faoliyatni litsenziyalash tizimi.*

*Litsenziyalash talablari va shartlari* O‘zbekiston Respublikasi Vazirlar Mahkamasining 2007-yil 21-noyabrdagi 242-sonli qarori[1] bilan tasdiqlangan «Axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta’mirlash va ulardan foydalanish faoliyatini litsenziyalash to‘g‘risidagi Nizom»ning II bo‘limida keltirilgan.

*Axborotni muhofaza qilish sohasida faoliyatning litsenziyalanayotgan turlariga* axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta’mirlash va qo‘llash kiradi.

*Axborotni muhofaza qilishsh sohasidagi faoliyatni litsenziyalash tizimining normativ-xuquqiy bazasini* quyidagilar tashkil qiladi:

- O‘zbekiston Respublikasining 2007-yil 17-iyuldagi 102-sonli qonuni[2] «O‘zbekiston Respublikasi Oliy Majlisining 2001-yil 12-mayda qabul qilingan «Amalga oshirilishi uchun litsenziyalar talab qilinadigan faoliyat turlarining ro‘yxati to‘g‘risida»gi 222-II-sonli qarorining 1-ilovasiga o‘zgartish va qo‘shimchalar kiritish haqida»;

- O‘zbekiston Respublikasi Prezidentining 2007-yil 3-apreldagi «O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora-tadbirlari to‘g‘risida»gi 614-sonli qarori[3] bilan tasdiqlangan O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilish to‘g‘risidagi Nizom;

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2007-yil 21-noyabrdagi 242-sonli qarori[4] bilan tasdiqlangan «Axborotning kriptografik himoya vositalarini loyihalashtirish, tayyorlash, ishlab chiqarish, realizatsiya qilish, ta’mirlash va ulardan foydalanish faoliyatini litsenziyalash to‘g‘risidagi Nizom».

---

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

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

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

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

- O‘zbekiston Respublikasi Vazirlar Mahkamasining 2005-yil 25-noyabr kunidagi «Axborotlashtirish sohasida normativ-huquqiy bazani takomillashtirish to‘g‘risida»gi 256-sonli qarori[1] bilan tasdiqlangan «Davlat organlarining axborot tizimini yaratish tartibi to‘g‘risidagi Nizom»ning IV bo‘limi “Davlat organlari axborot tizimlarining axborot xavfsizligini ta’minlash” deb nomlanib, uning 24-bandiga muvofiq davlat idoralarining axborot tizimida qo‘llaniladigan axborotni himoyalash dasturiy-texnik vositalari litsenziyalangan va sertifikatlashtirilgan bo‘lishi kerak. Mazkur bo‘limning 28[1]-bandida davlat organlarining davlat sirlariga yoki maxfiy axborotlarga mansub axborot bilan ishlash uchun mo‘ljallangan axborot tizimlari qonun hujjatlarida belgilangan tartibda axborot xavfsizligi talablariga muvofiq majburiy attestatsiyadan o‘tkazilishi kerakligi belgilangan.

Maxsulotni sertifikatlashtirish O‘zbekiston Respublikasining mahsulotni (xizmatlarni) sertifikatsiyalashning Milliy tizimi (SMT) asosida amalga oshiriladi.

SMT faoliyatini reglamentatsiya qiluvchi asosiy normativ-xuquqiy akt bo‘lib O‘zbekiston Respublikasining 1993-yil 28-dekabr kunidagi «Mahsulotlar va xizmatlarni sertifikatlashtirish to‘g‘risida»gi 1006-XII-sonli qonuni[2] hisoblanadi.

Ushbu qonunning 1-moddasida quyidagi asosiy tushunchalar keltirilgan:

*sertifikatlashtirish milliy tizimi* — davlat miqyosida amal qiladigan, sertifikatlashtirish o‘tkazishda o‘z tartib va boshqaruv qoidalariga ega bo‘lgan tizim;

*mahsulotlarni sertifikatlashtirish* (matnda bundan keyin *sertifikatlashtirish* deb yuritiladi) — mahsulotlarning belgilangan talablarga muvofiqligini tasdiqlashga oid faoliyat;

*muvofiqlik sertifikati* — sertifikatlangan mahsulotning belgilangan talablarga muvofiqligini tasdiqlash uchun sertifikatlashtirish tizimi qoidalariga binoan berilgan hujjat;

---

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

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

*muvofiqlik belgisi* — muayyan mahsulot yoxud xizmat aniq standartga yoki boshqa normativ hujjatga mos ekanligini ko‘rsatish uchun mahsulotga yoxud ko‘rsatilgan xizmatga doir hujjatga qo‘yiladigan, belgilangan tartibda ro‘yxatga olingan belgi.

Sertifikatlashtirish (2-modda):

- odamlarning hayoti, sog‘lig‘i, yuridik va jismoniy shaxslarning mol-mulki hamda atrof-muhit uchun xavfli bo‘lgan mahsulotlar realizatsiya qilinishini nazorat etib borish;
- mahsulotlarning jahon bozorida raqobat qila olishini ta’minlash;
- mamlakat korxonalari, qo‘shma korxonalar va tadbirkorlar xalqaro miqyosdagi iqtisodiy, ilmiy-texnikaviy hamkorlikda va xalqaro savdo-sotiqda ishtirok etishlari uchun sharoit yaratish;
- iste’molchini tayyorlovchining (sotuvchining, ijrochining) vijdonsizligidan himoya qilish;
- mahsulot tayyorlovchisi (sotuvchisi, ijrochisi) ta’kidlagan sifat ko‘rsatkichlarini tasdiqlash maqsadlarida amalga oshiriladi.

Sertifikatlashtirish majburiy va ixtiyoriy tusda bo‘ladi.

O‘zbekiston Respublikasining sertifikatlashtirish organlari (5-modda):

- O‘zbekiston standartlashtirish, metrologiya va sertifikatlashtirish agentligi;
- Bir turdagi mahsulotlarni sertifikatlashtirishga akkreditatsiya qilingan organlar;
- Sinov laboratoriyalari (markazlari).

O‘zbekiston standartlashtirish, metrologiya va sertifikatlashtirish agentligi («O‘zstandart») O‘zbekiston Respublikasining milliy sertifikatlashtirish organidir.

Mahsulotlar (shu jumladan dasturiy va boshqa ilmiy-texnikaviy mahsulotlar), xizmatlar, shuningdek sifat tizimlari sertifikatlashtirish obyektlari hisoblanadi (6-modda).

Sertifikatlashtirish subyektlari — yuridik shaxslar SMT doirasida sertifikatlashtirish tizimlari tuzishlari mumkin. Yuridik shaxslarning sertifikatlashtirish tizimlari «O‘zstandart» agentligi belgilagan tartibda davlat ro‘yxatidan o‘tkazilishi shart.

O‘zbekiston Respublikasi hududida majburiy sertifikatlashtirilishi lozim bo‘lgan mahsulotlar nomlari (jumladan, axborotni muhofaza qilishning texnik va kriptografik vositalari) «Majburiy sertifikatlashtirilishi lozim bo‘lgan mahsulot turlari ro‘yxati»da (O‘zbekiston Respublikasi

Vazirlar Mahkamasining 2008-yil 7-may 90-sonli[1] va 2011-yil 28-aprel 122-sonli[2] qarorlari) keltirilgan.

*Axborot xavfsizligi sohasida mutaxassislarni tayyorlash, malakasini oshirish va qayta tayyorlash tizimi.*

Hozirgi kunning asosiy masalalaridan biri bo‘lib kompyuter jinoyatchiligi va kiberterrorchilikka qarshi kurash hisoblanadi. Axborot texnologiyalari sohasidagi jinoyatchilik spektri nihoyatda keng, u internet-firibgarlikdan tortib to bolalar pornografiyasi va elektron-josuslik (ayg‘oqchilik) hamda terrorlik aktlarga tayyorgarlik kabi potensial xavfli harakatlarni o‘z ichiga oladi. To‘g‘ri tanlangan milliy kadrlarni tayyorlash siyosati orqali axborot texnologiyalari sohasidagi jinoyatlarning o‘sishiga jiddiy to‘sqinlik yaratish mumkin.

Mutaxassislarni tayyorlash masalasi, ayniqsa juda dolzarb hisoblanadi. Chunki hozirgi kunda kompyuter tarmoqlarini buzishni va boshqa kiberjinoyatlarni amalga oshirishni o‘rganish bo‘yicha axborotga ega bo‘lish juda oson. Kompyuter jinoyatchiligini sodir etish texnologiyasi keltirilgan bosma va elektron nashrlar erkin tarqatiladi (misol sifatida «Xaker» va «Spetsxaker» jurnallarini keltirish mumkin). Hozirgi kunda ixtiyoriy o‘spirin axborot tizimlariga hujum qilishning elementar usullarini o‘rgatuvchi kitobni sotib olishi yoki biror saytdan ko‘chirib olishi mumkin. Kitobda bayon etilgan usullarni o‘zlashtirgan bunday o‘spirin kompyuter tizimlari xavfsizligiga tahdid soluvchiga aylanishi mumkin. Internetda kompyuter buzg‘unchiligini o‘rgatuvchi ko‘plab saytlar mavjud. Internet tarmog‘ida kompyuter jinoyatchiligini sodir etish bo‘yicha malaka almashishga imkon beruvchi forumlar, virtual konferensiyalar o‘tkaziladi. Shunday qilib, kompyuter jinoyatchilari o‘z malakasini oshirish ustida faol ish olib borishadi, o‘z qatoriga o‘sayotgan avlodlarni jalb qilib, ularni o‘qitishadi. Bularning barchasi deyarli legal ravishda amalga oshirilmoqda. Bu holatlar dolzarb va muhim bo‘lgan yana bir masalani yechishni – jinoyat olamiga yoshlarning kirishiga qarshi kurashish va yoshlar orasida tarbiyaviy ishlarni olib borishning samarali usullarini yaratish zarurligini yana bir bor tasdiqlaydi.

---

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

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

Kompyuter jinoyatchiligini sodir etishga qarshi immunitetni hosil qiluvchi yuqori odob-axloqni shakllantirish bilan uyg‘unlashgan zamonaviy axborot texnologiyalarini o‘rgatuvchi ta’lim-tarbiyaning usullarini yaratish ta’limning eng muhim masalalaridan biri hisoblanadi.

Hozirgi zamon talablarini inobatga olgan holda axborot xavfsizligi sohasida kadrlar tayyorlashning asosiy prinsiplarini quyidagicha ifodalash mumkin: nazariy bilimlar darajasi xalqaro darajaga yaqinlashishi kerak; mahalliy sharoitlarda ish yuritishning amaliy ko‘nikmalarini olishga yo‘naltirish kerak; asosiy e’tibor xavfsizlikni ta’minlash masalalariga qaratilishi kerak.

Axborot xavfsizligi sohasida kadrlarni tayyorlash tizimini rivojlantirish eng dolzarb muammolardan biri bo‘lib qolmoqda. Bunda kadrlar tayyorlashning barcha sathlarini qamrab olish (“vertikal” bo‘yicha) hamda gumanitar sohada va tabiiy–ilmiy, texnik va gumanitar yo‘nalishlar tutashgan joylarda axborot xavfsizligi muammosi hal etish (“gorizontal” bo‘yicha) zarur. Birinchi navbatda xuquqni muhofaza qiluvchi organlarda va sudlarda kompyuter sohasidagi jinoyatchilikka qarshi kurashish bo‘yicha mutaxassislarni tayyorlash lozim.

O‘zbekiston Respublikasi Vazirlar Maxkamasining 2002-yil 7-noyabrdagi “Toshkent axborot texnologiyalari universiteti faoliyatini tashkil etish to‘g‘risida”gi 385–sonli qaroriga[1] muvofiq bu universitet respublikaning aloqa va axborot texnologiyalari sohasida kadrlar tayyorlash, qayta tayyorlash va mutaxassislar malakasini oshirish bo‘yicha bazaviy oliy ta’lim muassasasi hisoblanadi.

O‘zbekiston Respublikasi Prezidentining 2014-yil 24-martdagi “Toshkent shahrida Inxa universitetini tashkil etish to‘g‘risida”gi PQ-2155-sonli qaroriga[2] asosan xalqaro standartlar darajasidagi axborot-kommunikatsiya texnologiyalari sohasida yuqori malakali mutaxassislarni tayyorlashni yanada takomillashtirish, shuningdek ilg‘or xorijiy oliy ta’lim muassasalari bilan hamkorlikni kengaytirish maqsadida Toshkent shahrida Inxa Universiteti tashkil etildi. Mazkur universitetining asosiy faoliyat yo‘nalishi etib:

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

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

– axborot-kommunikatsiya texnologiyalari sohasida xalqaro standartlarga mos yuqori malakali mutaxassislarni, birinchi navbatda dasturiy ta'minotni ishlab chiqish, axborot tizimi va kompyuter tarmoqlarini boshqarish bo‘yicha mutaxassislarni tayyorlashni ta'minlash;

– respublikaning oliy ta'lim tizimiga o‘quv jarayonini zamonaviy ta'lim texnologiyalari asosida tashkil etish bo‘yicha ilg‘or xorijiy tajribani joriy etish, ochiq axborot-ta'lim muhitining rivojlanishiga ko‘maklashish;

– respublikada axborot-kommunikatsiya texnologiyalari sohasida uzluksiz ta'lim va malaka oshirish tizimini shakllantirishga ko‘maklashish, ilmiy tadqiqot va ta'lim muassasalari, dasturiy mahsulot ishlab chiquvchilar, ishlab chiqarish korxonalari, sanoat va infratuzilma tarmoqlari hamda boshqa zamonaviy axborot-kommunikatsiya texnologiyalari iste'molchilari o‘rtasida o‘zaro mustahkam hamkorlikni o‘rnatish;

– iqtisodiyot real sektori tarmoqlarining aniq ehtiyojlarini hisobga olgan holda axborot-kommunikatsiya texnologiyalari sohasida yuqori malakali kadrlar tayyorlashni nazarda tutuvchi xalqaro standartlarga mos maqsadli ta'lim dasturlarini tashkil etish uchun sharoit yaratish belgilangan.

Qarorda Toshkent shahridagi Inxa Universitetida mutaxassislarini o‘qitish va tayyorlashning asosiy yo‘nalishlari etib kompyuter injiniringi, dasturiy injiniring va kompyuter tarmoqlari injiniringi belgilangan.

## 5.3. Xorijiy mamlakatlarda axborotni muhofaza qilish tizimi

Mamlakatning tahdidlarga mos aks ta'sir ko‘rsatish layoqatiga ega bo‘lgan axborot xavfsizlik tizimini yaratish uchun, rivojlangan chet el mamlakatlarida axborot urushining zamonaviy konsepsiyalari, o‘ziga xos xususiyatlari, axborot qurolining turlari va qo‘llash samaradorligi, shuningdek, chet el mamlakatlarida axborot xavfsizligini ta'minlash masalalari qay tarzda yechilishi haqida aniq bir tasavvurga ega bo‘lish kerak.

*Axborot quroli* deb nomlanuvchi vositalar:

- axborot massivlarini yo‘q qilish, buzish yoki o‘g‘irlash;
- himoya tizimlarini yengish;
- qonuniy foydalanuvchilar huquqlarini cheklash;
- kompyuter tizimlarini, texnik vositalarni ishini izdan chiqarish;
- shular kabi boshqa amallarni bajaradi.

Hozirda hujumkor axborot quroliga quyidagilarni keltirish mumkin:

- ko‘payish, dasturlarga kirish, aloqa liniyalari, ma’lumot uzatish tarmog‘i orqali uzatish, boshqaruv tizimini ishdan chiqarish va shu kabi boshqa qobiliyatlarga ega bo‘lgan kompyuter viruslari;

- mantiqiy bomba – dasturiy o‘rnatma qurilmalari, signal bo‘yicha yoki aniq vaqtda harakatga keltirish uchun harbiy yoki fuqarolik infratuzilma axborot-boshqaruv markazlariga oldindan kirgiziladi;

- telekommunikatsiya tarmoqlarida axborot almashishini susaytiruvchi, davlat yoki harbiy boshqarish kanallarida axborotni soxtalashtiruvchi vositalar;

- tekshiruvchi dasturlarni neytrallash vositalari;

- obyektning dasturiy ta’minotiga raqib tomonidan ongli ravishda turli xatoliklarni kiritish.

Axborot qurolini qo‘llash oqibatini kamaytirish yoki oldini olish uchun quyidagi chora - tadbirlarni ko‘rish kerak:

- axborot resurslarini fizik asosini tashkil etuvchi material-texnik obyektlarni himoyalash;

- ma’lumotlar bazasi va bankini normal va uzluksiz ishlashini ta’minlash;

- ruxsat etilmagan kirishlardan, buzish yoki yo‘q qilishdan axborotlarni himoyalash;

- axborot sifatini (vaqtidaligini, aniqligini, to‘laligini va foydalana olishlikni) saqlab qolish.

Axborot qurolidan himoyalovchi dasturiy tasnifdagi amaliy tadbirlarga quyidagilar kiradi:

1. Xalqaro tarmoq orqali turli xil axborot almashinuvida iqtisodiy va boshqa tuzilmalarning extiyojini bashoratlash va monitoringini tashkil qilish. Buning uchun transchegara, shu qatorda Internet orqali ham, almashinuvni nazorat qilish uchun maxsus tuzilmalarni yaratish; ochiq tarmoqlarda axborot xavfsizligi tahdidlarini bartaraf etish bo‘yicha davlat va nodavlat idoralarning chora-tadbirlarini koordinatsiya qilish; xalqaro hamkorlikni tashkil etish mumkin.

2. Axborot resurslarining xavfsizligi talablariga rioya qilgan xolda milliy va korporativ tarmoqlarni jahon ochiq tarmoqlariga ulanishini ta’minlovchi axborot texnologiyalarni takomillashtirish.

3. Jahon axborot tarmoqlarida ishlash uchun ommaviy foydalanuvchilarni va axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash va malakasini oshirish kompleks tizimining faoliyatini takomillashtirish.

4. Internet foydalanuvchilarining mas’uliyatlari va majburiyatlari, reglament huquqi va axborot resurslari bilan foydalanish qoidalarining milliy qonunchilik qismini takomillashtirishni davom ettirish. Jahon ochiq tarmoqlari ishlashining normativ-huquqiy ta’minotini va xalqaro qonunchiligini ishlab chiqishda faol ishtirok etish.

*AQSHning milliy xavfsizligini ta’minlash tizimi*. Milliy xavfsizlik agentligi (MXA-NBA) – radioelektron tutib qolish sohasida jahonda peshqadam xisoblanadi. Agentlikning maqsadi – texnik vositalar yordamida AQSHning milliy xavfsizligini ta’minlash.

AQSHning tashqi xavfsizligini ta’minlashda Markaziy razvedka boshqarmasi (MRB-SRU)ga asosiy o‘rinlardan biri ajratilgan. U yerda boshqa davlatlar tomonidan milliy axborot infratuzilmaga qilinadigan tahdidlar haqidagi axborotlarni qidirish va qayta ishlash bo‘yicha razvedkaning imkoniyatlarini kengaytirishga yo‘naltirilgan reja ishlab chiqilgan va tatbiq qilingan. Agentura ishiga oid an’anaviy usullardan tashqari, MRB texnik yo‘l orqali yopiq ma’lumotlar bazasiga kirishni va ochiq manbalarning tahliliga katta e’tibor qaratadi. Keyingi vaqtlarda MRB axborot va kompyuter texnologiyalari bo‘yicha mutaxassislarni, jumladan xakerlar orasidan tanlashni amalga oshirmoqda.

Federal tekshirishlar byurosi (FTB-FBR) ham, eng avvalo AQSH infratuzilmasini himoyalash nuqtai nazaridan axborot urushi doktrinasini tatbiq qilishda ishtirok etadi. AQSHda kompyuter jinoyatchiligiga qarshi kurashish maqsadida 1996-yil «Kompyuterlarni qo‘llash orqali firibgarlik va suiiste’mol qilishlar to‘g‘risida»gi federal qonun qabul qilingan va ushbu turdagi jinoyatchilik bilan kurashish bo‘yicha FTB tarkibida bo‘linma tashkil etish ko‘zda tutilgan. FTB telekommunikatsiya tarmog‘i orqali amalga oshiriladigan ayg‘oqchilik, maxfiy ma’lumotlarni oshkor qilish, davlat instansiyalarni aldash, terrorizm, xiyla ishlatish va firibgarlik kabi noxush holatlarni tekshirish bilan shug‘ullanadi. Uning tarkibiga kompyuter jinoyatchiligi bilan shug‘ullanuvchi yettita bo‘linma kiradi, ularning shtati 300 kishini tashkil qiladi.

AQSHning Mudofaa vazirligi (MV) xalqaro Internet tarmog‘ining ajdodi hisoblanib, birinchi bo‘lib mamlakatning xavfsizligiga yangi tahdidning va axborot qurolining kuchini anglab yetdi va hozirgi vaqtda harbiy sohada axborot urushi doktrinasini tatbiq qilishda yetakchi o‘rinni egallaydi. MV ilmiy kengashining ekspertlar komissiyasi axborot urushi hodisasiga qarshi harbiy telekommunikatsiya va kompyuter tarmoqlari xavfsizligini ta’minlovchi shoshilinch choralarni qabul qilish lozimligi haqida

doklad tayyorladi. Pentagon harbiy avtomatlashtirilgan axborot tizimlarini «qizil buyruqlar» deb ataluvchi zaiflikka tekshirish uchun harbiy kompyuter tarmoqlarini himoyasini ta'minlash bilan shug'ullanish maqsadida xakerlarni ishga qabul qiladi.

Hozirgi kunda AQSH idoralari faoliyatidagi umumiy tendensiya axborot urushi olib borishning asosiy tashkiliy va konseptual prinsiplarini ishlab chiqish, axborot texnologiyalarni qo'llab yangi ish usullarini qidirish hisoblanadi.

*Buyuk Britaniyadagi axborotni himoyalash tizimi.* Buyuk Britaniyada axborot xavfsizligini ta'minlash davlat tizimini yaratishda axborot urushi dushmanning axborot tizimiga ta'sir etuvchi va bir vaqtda mamlakatning shaxsiy tizimlarini himoyalovchi harakatlar deb qaraladi.

Buyuk Britaniyaning Razvedka va xavfsizlik bo'yicha parlement komiteti Britaniya maxsus xizmatlari ustidan nazorat organi sifatida 1994-yilda tashkil etilgan. Bu komitet «Razvedka xizmatlari to'g'risida»gi qonunga muvofiq uchta maxsus xizmat: SIS (Secret Intelligence Service) razvedkasi, Maxfiy xizmat (MI5 - Military Intelligence-5) va Hukumat aloqa markazi tomonidan budjet mablag'larining sarflanishini, bu xizmatlarning boshqarilishini va ularning olib borayotgan siyosatini nazorat qilish uchun tuzilgan.

SIS/MI6 - Buyuk Britaniyaning asosiy razvedka xizmati. SIS Tashqi ishlar vazirligi (TIV) tizimiga kiritilgan bo'lib xorijda 87 ta qarorgohga va Londonda shtab-kvartiraga ega. SISni Bosh direktor boshqaradi va u bir vaqtning o'zida Tashqi ishlar vazirining o'rinbosari ham hisoblanadi. Shunday qilib, formal ravishda SIS Buyuk Britaniyaning TIV nazorati ostida hisoblanadi, biroq, shu bilan birga u to'g'ridan-to'g'ri premyer-ministrga chiqishi mumkin.

Kontrrazvedka xizmati - MI-5 1909-yilda ichki xavfsizlikni ta'minlash bilan shug'ullanuvchi maxfiy xizmatlar Byurosining ichki departamenti sifatida tuzilgan.

Hukumat aloqa markazi Buyuk Britaniyaning maxsus xizmatlar tizimida radioayg'oqchilik uchun javob beradi. Markaz TIV tarkibiga kiritilgan bo'lib, xodimlarining soni va axborotni topish hajmi bo'yicha mamlakatning yirik idoralaridan biri hisoblanadi.

*Germaniyaning axborotni himoyalash tizimi.* Axborot oqimlarining xavfsizligini ta'minlashga mas'ul koordinatsiyalovchi hukumat organi bo'lib 1991-yilda tashkil etilgan Federal xavfsizlik xizmati (BSI) hisobla-

nadi. Bu xizmat axborot texnikasi sohasidagi xavfsizlikni ta’minlaydi. Hozirgi vaqtda BSI faoliyatining umumiy konsepsiyasi NATO va YES bilan yaqin hamkorlikda quyidagi funksiyalarni bajarilishini ko‘zda tutadi:

- axborot texnologiyalarni joriy etishdagi ehtimoliy xavfni baholash;
- milliy kommutatsiya tizimlarining himoyalash darajasini baholash uchun kriteriyalar, usullar va sinov vositalarini ishlab chiqish;
- axborot tizimlarining himoyalanish darajasini tekshirish va muvofiqlik sertifikatlarini berish;
- muhim davlat obyektlariga axborot tizimlarini joriy etish uchun ruxsatnoma berish;
- davlat organlari, politsiya va boshqa idoralarda axborot almashinishda maxsus xavfsizlik choralarini amalga oshirish;
- sanoat vakillariga maslahatlar berish.

Xavfsizlikni ta’minlovchi boshqa davlat organlari:

- Germaniyaning federal razvedka xizmati (Bundesnachrichten-dienst -BND). BND federal kansler boshqarmasiga bo‘ysunadigan bo‘linma hisoblanadi. BNDning shtat tarkibi 7000 kishidan ziyodni tashkil etadi, ulardan 2000ga yaqini bevosita xorijda razvedka ma’lumotlarini yig‘ish bilan band. Xodimlar orasida taxminan 70 ta turli soha vakillari: harbiy xizmatchilar, huquqshunoslar, tarixchilar, muhandislar va texnik mutaxassislar mavjud.
- Konstitutsiyani himoyalash federal byurosi (Verfassungsschutz - BfV). Ushbu byuro BND va BSI bilan bir qatorda mamlakatning uchta maxsus xizmatlaridan biri hisoblanadi va u Germaniyaning ichki ishlar vazirligiga bo‘ysinadi. Barcha federal yerlarda mahalliy ichki ishlar vazirligiga bo‘ysinadigan o‘zining mos xizmatlari mavjud. Har yili to‘plangan axborotlar asosida Konstitutsiyaga rioya etilganligi doirasidagi ish holati haqida hukumatga hisobot taqdim etiladi, unda xulosalar va tavsiyalar qilinadi. Hukumat, o‘z navbatida, aniq choralarni amalga oshirish kerakligi haqida qaror qabul qiladi. Axborotning yarmidan ko‘pini maxsus xizmat ochiq manbalardan: ommaviy axborot vositalarida chop etilgan nashrlar, Internet, majlis va mitinglarda ishtirok etish orqali yig‘adi. Axborotning bir qismi ayrim kishilardan va boshqa idoralardan kelib tushadi.

*Fransiyada axborotni himoyalash tizimi.* Fransiya kibermaydonda o‘zining fuqarolarini nazorat qilish bo‘yicha tuzilma tashkil etgan. Fransuzlar «Eshelon» nomli Amerika tizimiga o‘xshash o‘z tizimini

yaratdilar. U deyarli barcha xususiy global kommunikatsiyalarni tutib qolishga yo‘naltirilgan.

Milliy xavfsizlikni ta’minlash bo‘yicha siyosatning strategik yo‘nalishlarini ishlab chiqish bilan CLUSIF (Club de la securite informatique francaise) birlashmasi shug‘ullanadi. U o‘zining statusi bo‘yicha informatika sohasida ishlovchi yuridik va fizik shaxslarning ochiq assotsiatsiyasi hisoblanadi. CLUSIF davlat tomonidan to‘liq qo‘llab quvvatlanadi va maxsus xizmatlar bilan yaqin aloqaga ega.

Fransiyaning maxsus xizmati strukturasi. Fransiya razvedka uyushmasining umumiy shtati, uchta har xil vazirlikka bo‘ysinuvchi xizmatlarda ishlaydigan 13 mingga yaqin xodimlardan iborat. Uchta xizmat Tashqi xavfsizlikning Bosh direksiyasi (DGSE); Harbiy razvedka boshqarmasi (DRM) va Harbiy kontrrazvedka boshqarmasi (DPSD) Mudofaa vazirligi himoyasida faoliyat olib boradi. Maxsus xizmatlarga jandarmeriyani (Gendarmerie) ham kiritish mumkin. Uning vazifalaridan biri bo‘lib razvedka faoliyatini yuritish hisoblanadi – jandarmeriyaning xar bir qismida razvedka bo‘limi mavjud. Ikkita maxsus xizmat: kontrrazvedka (DST) va Bosh razvedka xizmati (RG) Ichki ishlar vazirligiga bo‘ysungan.

*Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat organlari strukturasi.* Axborot xavfsizligining davlat siyosatini ishlab chiqish, qonunlar, normativ-normativ hujjatlar tayyorlash, axborotni muhofaza qilishni ta’minlash bo‘yicha o‘rnatilgan me’yorlarni bajarilishi ustidan nazoratni davlat organlari amalga oshiradilar.

RF Prezidenti axborot xavfsizligini ta’minlovchi davlat organlariga boshchilik qiladi. U Xavfsizlik kengashini boshqaradi va davlatda axborot xavfsizligini ta’minlashga doir farmonlarni tasdiqlaydi.

Mamlakatning davlat xavfsizligiga oid boshqa masalalar bilan bir qatorda axborot xavfsizligi tizimining umumiy boshqaruvini RF Prezidenti va Hukumati amalga oshiradi.

RF Prezidenti huzuridagi Xavfsizlik Kengashi davlat xavfsizligi masalalari bilan bevosita shug‘ullanuvchi hokimiyat organi hisoblanadi. Xavfsizlik Kengashi tarkibiga Axborot xavfsizligi bo‘yicha idoralararo komissiya kiradi. Komissiya davlatning axborot xavfsizligi sohasida Prezident farmonlarini tayyorlaydi, qonun chiqarish tashabbusi bilan chiqadi, vazirlik va idoralar rahbarlarining faoliyatini muvofiqlashtiradi.

Axborot xavfsizligi bo‘yicha idoralararo komissiyaning ishchi organi bo‘lib RF Prezidenti huzuridagi Davlat texnik komissiyasi hisoblanadi. Bu

komissiya qonun loyihalarini tayyorlashni amalga oshiradi, normativ hujjatlarni ishlab chiqadi, axborotni muhofaza qilish vositalarini (kriptografik vositalardan tashqari) sertifikatlashtirishni tashkil etadi, himoya vositalarini ishlab chiqish sohasidagi faoliyatni litsenziyalashtiradi va axborotni muhofaza qilish bo‘yicha mutaxassislarni o‘qitadi. Axborotni muhofaza qilish sohasida izlanishlar olib boruvchi davlat ilmiy-tadqiqot tashkilotlari faoliyatini muvofiqlashtiradi. Bu komissiya Davlat sirini himoyalash bo‘yicha idoralararo komissiya ishini ham ta’minlaydi.

Davlat sirini himoyalash bo‘yicha idoralararo komissiyasiga davlat sirini tashkil etadigan ma’lumotlardan foydalanish, axborotni muhofaza qilish vositalarini yaratish hamda davlat sirini himoyalash bo‘yicha xizmat ko‘rsatish bilan bog‘liq korxona, muassasa va tashkilotlarni litsenziyalashni boshqarish vazifasi yuklatilgan.

***Nazorat uchun savollar***

- Axborotni muhofaza qilishning davlat tizimi nima?
- Axborotni muhofaza qilishning davlat tizimi ish yuritishi qanday qonun, normativ-normativ hujjatlar asosida amalga oshiriladi?
- Axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsad nima?
- Axborotni muhofaza qilishning davlat tizimida ko‘zlangan maqsadni amalga oshirishda qanday vazifalarni bajarish kerak?
- «Litsenziya» va «Litsenziyalash» tushunchalari nimani anglatadi va ularning ta’rifi qaysi qonunda berilgan?
- Axborotni kriptografik muhofaza qilish sohasidagi faoliyat qanday litsenziyalanadi?
- Axborotni muhofaza qilishsh sohasidagi faoliyatni litsenziyalash tizimining normativ-huquqiy bazasi nimalardan iborat?
- Sertifikatsiyalashning milliy tizimi nima?
- Sertifikatsiyalash nima maqsadda amalga oshiriladi?
- Axborot xavfsizligi sohasida mutaxassislarni tayyorlash bo‘yicha qanday ishlar olib borilmoqda?
- Axborot quroli qanday amallarni bajarishga yo‘naltirilgan?
- Axborot qurolidan himoyalovchi amaliy tadbirlarga nimalar kiradi?
- AQSH va Buyuk Britaniyadagi axborotni himoyalash tizimi haqida nimalarni bilasiz?

 Germaniya, Fransiya va Rossiyada axborotni himoyalash tizimi qanday tashkil qilingan?

# FOYDALANILGAN ADABIYOTLAR

Ўзбекистон Республикасининг Конституцияси. – Т., 2014.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ўзбекистон Республикаси Президентининг ПҚ-2155-сонли «Тошкент шаҳрида Инха университетини ташкил этиш тўғрисида»ги 2014 йил 24 март қарори // Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси – www.lex.uz

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Internet saytlar va davriy nashrlar:**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# MUNDARIJA

**KARIMOV Israil Mirzayevich,**
fizika-matematika fanlari nomzodi, katta ilmiy xodim;

**TURGUNOV Nozimjon Abdumannopovich,**
fizika-matematika fanlari nomzodi, dotsent

# AXBOROT XAVFSIZLIGI ASOSLARI

*Darslik*

*Muharrir* **S.S.Qosimov**
*Texnik muharrir* **D. R. Djalilov**

Bosishga ruxsat etildi 16. 12. 2016. Nashriyot hisob tabag‘i 6,0.
Adadi 100 nusxa. Buyurtma № . Bahosi shartnoma asosida.

O‘zbekiston Respublikasi IIV Akademiyasi,
100197, Toshkent shahri, Intizor ko‘chasi, 68.